

Norton Small & Médium Business Enterprise Partner Symantec | United States Enterprise Change Country United States Shopping Production & Solutions 2015 Internet Security Thread Report, Dol 20 Support & Commodities Security Response Taque a Gold Look into te Face ofá Cyber crime Tré & Bué Geté upe to 33% ofá MRPP / Adê Security Response Gur Security research centers round they world prevido paralelepipedal analysis ofá ad production from TI securite Thread that include malpare, Security risos, vulnerabilizas, ande spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22

Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Norton Small & Medium Business Enter 1, Jul 12 Jul 31 Aug 7 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 33 Jul 9 4 Jul 16 Jul 16 Exp. 2 VEL 28 5-512 VEL 20 VEL 21 14122-14123 Jul 24 Jul 25 Jul 26 Jul 27 Jul 38 Jul 29 CVE-2015-2366 Pocal Privilege Escatation 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp. CVE-2015-5122 Vulnerability Microsoft Windows Kernet Win32k.sys Exp. CVE 2015-5123 Microsoft Windows Kernel CVE-2015-2382 Local Information Disclosure Win32k,sys' CYE-2015-2366 Local Privilege Vulnerability Microsoft Windows Kernel Win32k.sys' Escalation Vulnerability Microsoft Windows Kernel Win32k,sys' CVE-2015-2382 Local Information Vulnerability Microsoft Windows Kernel Win32k.sys' Disclosure Vulnerability Microsoft Windows Kernel 'Win32k, sys' CVE-2015-2381 Local Information Vulnerability Microsoft Windows Kernel Win32k.sys' Disclosure Yulnerability Microsoft Windows Kernel CVE-2015-2367 Local Information Disclosure 'Win32k,sys' CVE-2015-2365 Local Privilege Vulnerability Adware. CloudScout Android: Crisis Escalation Vulnerability Microsoft Windows Kernel Adware. Arcade Twist Trojan: Bernpos Trojan. Emospam 'Win32k sys' CVE-2015-2367 Local Information Packed Dromedan gen 16 Trojan Crisis g 1 W32 Liberpy Disclosure Vulnerability Adware Clouds 604t-2015-Android Crisis Adward Arcade Twist Ingjan Bernpos Trojan Emospam Packed Dromedan gen 16 Backdoor Darksun Brackware Safer Browse Trojan Crisis!g1W32 Liberpy Android.Benews Android.Gupne Adware.Simpliclean Trojan Dionisduke Exp. CVE-2015-2425 Trojan Mambashim Trojan Rikamanu BUA BCP siyagydock FXM: GYF 79 W 97 M. Sillycopy!s1 Backdoor Darksun B Trackware Safer Browse Bownloader. Tenirem Backdoor. Cobrike Android Gupno Adware Simpliclean Factory Trojan.Mambashim Trojan.Rikamanu

Belowlanded in Spælder Schloff M. Arpand P. May 7 Mu. Sill Lulca proj. Sép Down boader Len Brail & Medium Business Enterprise Dog art pers Symanter F-2015-5122 Exp. CVF 2015-5123 Adward Discarders A april 1 Win 32k sys CVE-2015-Obtebos Dece 20 at Pas Was use crimbay Name ulypung Sep B collaboration of the property of the collaboration of the collaboratio 04/2N/20D404M25/2014iVS1Bewolan Noorsh T2/169/12017 Tiewiah Bhoke Subsoft 20 Er Niam 94/17/2014 isclosure Vulnerability Microsoft Windows Kernel P4617/2014 Disjanverenderdigen Fakre Avhoem 12/2014an Win32k.svs CVE-2015-2381 Local Information 04/28/2014 T46/24/2016t USeB 74 Tarb Morton 02/29/2015 Disclosure Vulnerability Microsoft Windows Kernel 02/18/2015 Trojan Shylock gen 10 Trojan 04/17/2014 Win 32k sys CVE-2015-2365 Local Privil 04/13/2014 Trojan Bayloek! Internal Trojan 04/4/6/2/02014
Escalation Vulnerability Microsoft Windows Kernel
04/18/2014 Drojan Zandy Georgia Government Office CVE-2015-2367 Local Information P4/dl542004nTerrora469hTxtorakl04/12/12014104/4/11/2/121044 Disclosure Vulnerability Adware CloudScout OF613/2014 Tediamos by took gentle Turbent 84/164/12014 Android Crisis Adware Arcade Twist Trojan Bern S4/113/12014s Dbs: cripater. Produkt dine Frse are 5/22620 atte Trojan. Emospam Packed. Dromedan! gen 16
Packatd Spent eight 4400 Taojan Wat/12/2014 of 6/10/2014 owall Trojan. Crisis! gl W32. Liberpy Android. Benews řs-er-Toganinhiouros prototato těnoch v pak filosorént hat your Trojan. Dionis duke Exp. CVE-2015-2425 Symphoenised sonimula eraltd/herlieskselaeusert bodese. PUA.PCPrivacydock Exp.CVE-2015-2426.A To have \$ betfillest de cojant extyphewale artificial wat owall Backdoor. Darks un. B Trackware. Safer Browse æraiversjam thæra efebbede og nyptus eritels rom og hæspam Android. Gupno Adware. Simpliclean e oma piso newi peodito kaitus bitosut eta tihe orugustkus tahine ino susurat disposity Trojan Mambashim Trojan Rikamanu to manure this éidesites composible it ment hranat typice all he Backdoor. Spedear W97M. APMP W97M. Sillycopy!s1 Trojæsisætbeutfedotædkæromberothisædotospanter, it Downloader: Tenirem Backdobr.Cobrike

e neatles, expulioritijkeirisõingestiedibtykeentlõjle Bid AliEinonoesabbeepodrohy Narton Pequenas e Médias Empresas da empresa Sep Parceiros Symantes Linited States Empresa Alterare Country United Unidos Compras Produtos & Soluções exercistros de la confedera de la confederación de la co 2015 Internet Security Threat Report. Vol. 20 Suporte dites evelocity subolites security Threat Report. & Comunidades Security Response Tome um olhar pe corajoso na cara do Cibercrime Try & Buy Obtenha até ex **la viencia es** i**bracción recipier dia de la compania** a té 33% de des són to MSR En Malicion de Security Response Nossos centros de pesquisa de segurança em todo en 4 mundo fornecem apálise jncomparável e proteção 2014 contra ameacas de segurança de Tloque incluem /2014 malware riscos de segurança vulnerabilidades e 2014 nam, Visão Geral Ameacas Vulnerabilidades Riscos 14 pany AZ 2015 Intérnet Security Threat Report by 2014 Yolume 20 2015 Internet Security Threat Report want 4 Volume 20 0 Internet Security Threat Report fornece at ayours feet leaded leading of the supplementation of the su global O relatório é baseado em dados da Symanitecall Global Intelligence Network que os analistas da tides etacendo de la companya de Symantec utilizam para identificar analisar e fornecer cecompike na seu remopused ille range ska u pie sa egylodaray comentários sobre as tendências emergentes no paoteotion provecto y de la comentación de la comentació cenário de ameacas dinâmico. Faca o download do por ajot residente social de la composició Riscos e Vulnerabilidades Timeline Dan eo competicanis en spinario de la competicación RiskThreatVulnerability Jul 10 de julho 11 de julho 12

tle apoblisce ti Scetez in all the id laboral titip cell trap in the production of t Norton Small & Medium Business Enterprise de la chienath Rartners Symantec LUnited States Enterprise illudizae Change Country United States Shopping Products & lar Sólutions 2015 Internét Sécurity Threat Report Vol 20 Support & Communities Security Response Take a justine with the contract of th Bold Look into the Face of Cybercrime Try & Buy Get LOS TO BENEFIT DE LA CONTROL D security research centers around the world provide a unparalleled analysis of and protection from IT security threats that include malware security risks, a manual constitution of the con vulnerabiliti Norton Small & Medium Business Vinterality in grant grant in the composition of the compositio Enterprise Éartners Symantec United States de la viate Enterprise Change Country United States Shopping nes enterprise Shopping nes Products & Solutions 2015 Internet Security Threat Change Change Country United States Shopping nes Products & Solutions 2015 Internet Security Threat Change Chang Report Vol. 20 Support & Communities Security 100 Persons of the East of the E Cybercrime Try & Buy Get up to 33% off MSRP. / Add Security Response Our security research centers in est around the world provide unparalleled analysis of and supported by the company of protection from IT security threats that include intermediate the control of the malware security risks vulnerabilities and spamwant Ryerview Threats Risks Vulnerabilities Spam AZZyour 2015 Internet Security Threat Report, Volume 20 2015 Eleten a particular de la companya del companya del companya de la compan Internet Security Threat Report, Volume 20 The

Mytechnicate state & Existing & Total Lagrangian and the content of the content o **Sydalitan assakinatib kajulaa Pyata najan bilikinaa Akuban bilahin anertii sialisid etsiyie** u r **Record patriculation of the Sandwall of Section 1999** (1999) The Sandwall of **Support Maria Republica de la constant de la const Escribbanh Pricing United National Process of Grand Association (National Process of Contract Contrac O lestado a ligitar o Transilla de California de Californ INTentenside Anglot Astelle Polanik Phylopeas Prilonis chain the Photol Astella in the Estain al apros tAs**op a y Ried Jest Pathwald Gasto Chynel o collectiva all all alla vision allonda successive succ Monstretretallation to the colors of the col **PALISS & BETT HOUR AND FOR PORT IN CONSTITUTION OF THE PARENT HOUR AND THE PARENT HOU** Red Carrie 1885 Canada de de la company de l **Produción (Septembra de la compacta del compacta de la compacta de la compacta del compacta de la compacta del la compacta del la compacta de la compacta del la compacta de la compacta** RELITERATE AND TO RESERVE AND THE RESERVE AND RKH wall Carry Rand all true trail Charles in the carry state of the c Readpreson Salbight Hogal Nobies restricted to Mariant to 1820 the Marian Conference of the 1820 Salve (1824 to 1820 to 1820 the 1820 to 1820 RV Se allo de a la company de SN/TESPEZ/PROTREATESTAD VAAN/ALTAID OF ENDING TEACHER AND VERNAMENT AND THE TEACHER LANGUE TEACHER AND VALUE OF THE TEACH **Profili cicintalibri il profili elibri il cicintali di il cic BYOLE ARPS DE CONTROL DE PROPERTATION DE CONTROL DE CO** 

**Balcardary and Sanghote district it all recole in tuto tisse de it and la principa de la company de** Palatrichi (Caldana de la Calda la Calda de la Calda la C **XOCIONALE PREPARADA INTERNAL SANDANANA INTERNAL PROPARADA INTERNAL PR EXTENDAD dato 2550 non la pointación de contractor de con** Banadad (not place and in the substantial and Kondrous 100 marks the Riscon Sembodie the bits native left hot eglesting **Read Parameter 2005 to Escape incompute copation opinis each leave eductor also Escape read tie it l** Banneten Banneten Breten Broth Broth Banneten Breten Broth B **Dout Reluse after after for the religion of a history de religion of the reli** Brosinvels is kniphtentricinal 1842 Ptiles Example and Early and Etal in it or. **Soluti e selezitat e per selezitat e pesico a capadole de Saintet in 1824 contra de California de como e** Starto Previotabilen Revission Schedulen i Friedrich (Stebender Amporten Managierin Laberto Ambrechen Designation (1974) Dictably of the provided by the providence of th **Seth Akide Allesets Mond-Packtatis et a Resta United Alles Siede Aucai Peet du dé** a t **Contraggeous te Skinet vas verste de Bluerk (skieting de procede) i 18 le statement de la statement de la skinet de la sk** Sect territore Birlanda de Control de la con Bád Pátriscola do Parte Ithia Barando **6 Boltar/12 Celvaria en paripalit : Salery desteta y la ferri de Bot la social de la Tradello des** noce **Bará luas (2001) é a Front i a try. Planté de inslateur é valler la jui pa soja é Tob a plané i**l li e e d On A Foreign Variet transities and resident and the state of the state 17 day 15 50/12 13 50/14 to 15 tracing earcy Editological or tempertural alternation in increasing interests 2 18 of the content of the conte Chéti é nCada2020142 Térritoj CayA 3 Sithi 34 Cait 5 la Caige par de 1 La Vérat tajand pola 26 de 1 Vérit i 29 Tré a m ONNAMIONA S/a Oldinicta de Tabilite et la Richida de la Significa de la Signif Prace Nateral Action and the Nation of the N

<del>dender tradestig also de la folicie de la final de la</del> (Expendición de condition de la condition de l The sequentary of the later of esenae Vrodojan esta a Adroceltrica de vrosa per se fielden escele de prédet Cartemptic exalibité de l'Espanse de la light de la li Buistance and the process of the control of the con Set is a content of the set of the content of the c septification and the action of the properties are the properties and the properties and the properties and the properties are 8 fila neutrel 9. Libeur Ing. ei irrotte der til opset literatif i iss porto, dokum britantide statis i plovide 200 fila og file October 19 i i se porto. Dokum britantide statis i plovide 200 fila og fila october 19 i se porto fila octob 2011/5ne554233ch\$13166rob4ffoltste\$1491670b/orand pek@exantichtiots\/4671@62bkbsv4se Oeur Ché is pessibilité de la company de la compa **SALATE PAROUTHA LE 2008 ARTIECUNIONAL El montro Utione de l'objet de l'objet** 18 pyrt VELDAN bei 1944 po 1911 i i deen osabryt bhah benoutvoet dee / théasan Geryek b 1949 i i chéadail de speek s 6a/v6a 20a/otoreanan bersteet Bratalent Ast Zona Gir Seventare transit Series or o te/ Yd seksi. e Nearbristiethy i Ar Osigo goinge tsyd Ytu Mahir Er e Leadan ea Clánsoir harbitae i Mehiceniù Sa le cealyear t 🗸 60/45-1220011-paga-660 hepakozeth Modypita-erta 6-5 daneta totteen Met d 6-e osi rity Voteficati <del>den sadajih alinge ky latior dojee no koli dy je taahowaadd leh keetien vae labahddi ewa 20 ky Issiges 'o f</del> **(1) at leasily (statern aligh door chitocertate**th to**rest extera cel**utrización utilibre se**d torres** concecut crist et mars e cl White the sept add the tradfavour point the attack to proper but the state of the september At Nacika mit de a habitisto de la mana de l Praviotal legicated inches inches reconstructed in the control of the control of

t so a eatre and a comparate a 2 to a large de la Bakirokoitaataris Baktirokataeratni alastilisis ekifikeisista disaataa di Etopomeertaaloj hytyetele l Antiquent tilhossig för ja 23 betykkeste år stock og ker til bled år för blude år som led ligest ut 18 To esciptuita Netha desila 200 hidan ficazi di harte 6 222 data al salcabre describit de Sel ul 26 Beconstate the second and the second DanyAphdettable icht excesseniberendtjolophucesetschibre?achtve?achtve?ide Woosjanfold typetresoldaesawky Poblest. Grow hontaetheant born Venjayo Euxp. CV Additionated nontraliber for Cleps Man taken Eld dry white Proto Seconi Seco **Date the feeable resolute Salous Existe in a stain on Many Dielet milicité desoude Salous** Enche Ngioxee Boeye not Catalogi libiado de Make callus et no dipany Sulvenon tultude de Gereri ty Elepatel Andrewat IP er Food Material Andrewat Marcan Linda et al. and a second enter a large et al. And a l Po briet into the and the contract of the cont Systemative 8th office care respect to not an attack block to entitle to the state of the care of the Beind 20 Valor College 20 All May College de Construction de la Toyloettra M Organia de Calo College de Construction de la College de College de Construction de la College de C December 1985 2014 4 September 1985 2014 4 Complete Compl Beed to 3/25 bees to ordon versus development les Taran a not Cat / 1 & de 2 co 1 rd by Bledsie 220 teachino annazithos topos ole svirojane Celeptus Vaio Vera a o Chévis E/c2001 don tron eineuto a Ettliff pubs do kolons in 1920 to Scotters de 1940/10 é A/21 Bata de 1980 8 4.25 CH 200 eAntastantieleadente la bord de Teoriant Byorté 6216 les **37 áulthás**lít**2051 s**í taddríviondiseth idearcarla itióix ire n'h othebha pare 65 1/2426/126 164 **L'ésteur foint de material en caleiron is crosel sécus intére a libitalitat de con i** ty 6 fy Ira a 6 terc v 3 rtotore ante invitision in teason de l'armétique de l'agreco e l'Opte de préciai inst.

Blacereza i sapata Fluing lotu: t To colober Carry option act la tradición in participa de la color de The art Tarking week of ear Size of threat recease Tryest earlieftes stripment and our Sot are Tarking to the A e tomethein a to be color to a color that even bent Tree to a stables build to be end stable of even a color to a color t Restantation de la le editation de la éche e de la companyation de la **Parteritare és conseint de la constant de la const** Brecon learnessed Wolf til elect Bet prest sel 52/94/12/10/15/fre Tr Valenco intreass in a lea e r a Berdinpittor Reserved Sees Just to the Country and Cou A treprendice Tescherooper dynámy Salve Richard posta drei pesad Rochadelivo de la Completivo de la Completi Substations Superior Continued and the Continued of the C Efinitaheorietate Februares State de en televas Scientetim, legistrativo televas frances en que o Charge peudieiro & edigiera re Stoat trae Polent, piet s Tvine este invoiet la presentail du slavir de Societa and a contraction of the Ellanskain the ign. Etpreutdete Mice do wints yordets potentaine. Et et e rehet avgiputeis n Scerymott losis Of Berjasan 2013 a 155 0 37 / 224 it lette in loss to the Particular en lette in la scalar en la (15 bb) sp2 Britishi ety. Erit Manadety B 25 afet W britek Adult be ela issate in qui met iy Rlesso eta ta Respo estrara de transcription de la reconstitución de la Rospenio s dividente antiscelas Albines e ser et diverte successor de la company de la This ocean et 22/2017 For et and it in the interest of the int Priedkest Mewhaileg Prindtleer à 650er 319 Pre 2011 hours, in 17/5 certoet comit y To by recontent Worth District School Stututa de li Sacta carrat el lo Teni telo Ten Colassamyd Publiavet yonus dorter theet their as it you I hreat do to Rtegyanta Seasti by Whites

Pamperra Keyan terretre ce Tild Pusaddiafet r Elmaen irre I rfoor r Seinuaritou r Rrestreatisen. TSVR FEAT @ONAs. enveslezn Electat set Lefvelezt EtevateesAturViodse's & Reisk ta Tidseap to the sleigherese Seutoson riteen Eatlons the Kirtoway hattely big ences (T, without deepend Rærs plontsepBobget Svolus cerinde bil hetekt nyd me mFælvmælide bMænt to lover fish tilo ena que di recalli y arrecelt end acerotisco a be allo bicare eimotreo 2011 2n 5a:510 i AAS 28 V 5n 8 i 1 28 Eerakpeedin H archoitreac filie a m Más dofest vurbnead bid i Appolicatifanci bin at Deviroe Coattracks 8h 28 AMe 20/box - Oxford in Mindrosouts People by Teats day - July 2015 6i:50sPMn20015+050-014tVAspip tibet Some anithy Drewis peonse Bloods of radianted actional estells be per Bially Lorde tied by he Sacrea of the original enterior of the sacre avaai28bseAnera.nwimiatewPampePropectiontTextils.naokeesieis the 12/2013 6 US various treatment in a KAS excut r Stymantec Commenced to the control of the cont Clossicient to the contract to RSS esquadras pragned a service of the contract to the contract This earns i Pois knee Yitul hrefradsitlinue subreams -A-Ze2016el (HearS) es See consist in a home at Riceproante in Vocal Lora de 20 n 20 1 La imagement de la Sedual tow/Ishardent i Riespoart o Woltronner 20t Eh,ed nove sincert Seder Ltyin Tohline aith fir asptoret cip uovei desdæmnavred: v Dewriamodo u r aersate process of the force of imaging local uters exait a chioxity. The have curity of parties and in the parties of the brank in Issaltisgenasein Neutronectly we birding Syedan teess area hysissions t baid ention, each analyzen ea hod accrossisses economitriven traffyr on at ion

etoeædimattre rode ud. tYroeu obarra ne iaxxxx thre af u la detacitas ef our Desse autobadit tree them set a nid vno 6 rea 50 eDair of orbeat the reatus. Wisikepaper Vilewerth beilfulds set me Symmantec Security Resto Tomissee twhite ear a bidirty 128456 J St alvi Skeet uir 2 J Vitus Jul Definitionsuario Securityu Upolatuksi Sylmla 20 etu 620 whity22 Auw 232 de 624 Puto 625 moi 18 y 26 a hoit e 27 Llo e 28 e l Rie 29 e viu al 30 Oveln3 & rASverc 1 valuage Beasture Baasture es ARverc 5 valuage on Alexent 7 Aug Exadoppina Pordice Attign 1 Secourie W Ee 20 in Signs 1 Noon Ecorp. CVE-20o1cfr-acides & Reene out a New Indeposis Tree at en d'Unine 22 le es ys ' 6 VSE e210 \$5 V220 6 Value of the IPP pixale Topeo Eschedition at e Files in Quarrement bin let Continuents Setc Writing or ves programme S'Uno im 32 ki sus' 63/16-p2l@35R233627 LecSalls pfootherds Eloro Diesclas subtrection WallserPloisitive)iMraksefa Skiftokowe Weritne-L'Ne/tim32k.sys' RVELU2015-2001 tLancymarter Striodulis Vlusierability Reprentablicitty M Scrads Att Usen Bewist Grennedla Wan 82k.sys' CMEe20032423453dpooralnPgrAviZebesEngabatilorThreats & Riuske nablihiev and i bitosso Bynniandoevo sTK eerante Movinta 2k.sys' powered at 50-92 1000 Jep 6 is gent of the president solic authors, where the ligence Purbodencal bi Beyc And twya Fe. Otho a blogsy oant dAin despirid n Siei SI & A R Modular ear eA Paradle Etvio sit Tierohamo. Bogireso Se duro itan Reasposipsaen Blackscark. DPourble datiboges Not Errojeath Secisis isty T W 22 tLiberpy Reployids Symmetric Thotach Ligitarie of Rukyeo Etx 6 & CV LE it 20 White 242056 PSUSA, PhG PtreveTcVy dPoodloc Esoto CCN455-1261150-12526. LArity Beskdose Dat Resiat Bondalckwebize. Safera Beroduseel 2:

A hedratied GAU In Noir Audious & Bienkest Te heraenat Intelligence Sodia or Mozen Foldso twinth Er Tohane at it is trained a rouge note Twitter feed Beskdose Soledesa Sund 97 Michael WWA 78 M. Sold projection Dydwendespidem. Toen in earn p Btaark of beat. 6 e borske ce, healthcare \$\frac{1}{2}\text{pt:500} \text{ENA+201B+0A-28-logate} \text{Departies to the application of the control of the Addressores sneated beressetting of a holding intent el wend of exact seeps 8.318 MADY DOE'C 5207 52 Fell Midrans After Physics hulling established 20ct 5 No. 5 9Die M220 65-617 - Web Visit it Messekurrityl Response Bto of son December and a steel december and a stee Fance autis Clybinewaraith & Inkersone b Serribeity a Thee Entere port, Porb 20c5 & ATRDAsat overley da Teo Paro, teach early Toearth 1201 dones an @4/2952020105452/1/12001&cJS. Obroprodratt No/to Arb 00.2/S9/f2101105ec C2/fee/f20 15ventialn/Setylad SiteeM 22 | Theigan | DR/f17420 | 14 046/61k7/6201740Thtajath.RS6dNabten4STrajar&0M/4di/22014 B4/si6/esss & Trejamize of Earen & 4sTSay pana 104/d \$/26 it/ed 84415\$2014eFporiisme.Shydnogks.Qenn10rVcbnistre0145/124/22014 84/6103/27061 42 Food just \$58 y 500d ku tojoenn \$120775 jent eprin ê4/524264 rity U4/163/12R640 OrdyWdb 266 Choproikt! Com Corojanu 66/22/2014 Beackreidy Greensprion \$ 60T Taken am BDAI/d 2/220K1 4nd 6/th/e/2421c/e of \*\*CF bre room trineuTerd/p&roBersyt Coent, unpartice 3331/6eoff h 241 SyRuPr / Add SymumityeRespossion and worth in censeral heaven the relate. Throughout Spettightd Trojaide Cryptoralaell Edicinal Cryptoradl per at Ecolon from ad Theat counciry phosefaltes to batt free lude combunation pister, but he natisk tiets, eaunstern pay

Overavie while if iteest stercies host evolution be eath in the set of Spoint and LA-Z 2015 de a term ni ble Saéteuctie of Elomepatut Reept burto Worth carponer 20 2015 emberitsete Se coit ikit 5 hrested & poot of to ha etiec 200 5 lads or brotherpretn Seed is the 3 horeaut Responsal paramed ean an object in the contract of the cont a not am asystem cof there one at hencolor branch hissed a china tut. eThick cepates sabrased en odateofistmy tenet System ten teor@ltdbabath brittellei cerccept et viidek and lichn Seve en tercie three lysts use too indepatiery, raansalayztes, ath encorpyide fibers revertht aprayr birdular extensiron srends encthrepdy hemaired breates additapreal Dless reviotand i the merctoot a root impowet 80 library nGtlbb ade thy retaiten. Resyk 5 has on the letter ambilities the lime convince the user Risplat/Immenter/ulm coralleritity det 110elke/11 oluh 12ckut hierul flikesult 1 Eislest 26/2 drile 1.7 ofudit Bedenht 1 Peduhn 20 west 221 okolle 22 thate 23 dut 22 fe Julie 25 stert 126 ptant 127 e Juan 23 ptal 129 ptal 30 ibuflood fin Action of Action of Phaeura CaryActor of a Aluins 5a Action to the up the up 8hArevart 9raAmrid 1/1 0v Aitueru 101. Bxept CPV rEa-2101 6s 51 1128 dEcupr. iCW E-2015-at \$20 it Mithesoft Not misle wat Kerneth Weim 32 kn alvevare EME E28115-2366 deceth anniewiet des los explexition achines thom expetting interiors of B Windows solved one by Em 32 kinsgs' CONTECTION 1500 238 The Operation of the Content of Ytaky probekity di? i Eodsoutti Maji a dovess kne pihe lb'eyt no izako siyosis Califeral like-2384 rhe palo lust odiffrent in palo lis otrops consing your blood the crtaibility Mhiam be of the absence by Ced messelve of Balestys' 6 Nation 120 et 5 - 1202 et 5 dans alt Privat e que descapt et il de la these

Wedomenrateinhidativoircs asolftn Www.dows voermels Wish 22klasasid CallE el20115 p2:36@dt.oxcoalrl e frompro etterf nD rachos luvere. Want Vou groefreat thisty Andolvered Cyl be d5 a put nA testration Comission ur Addressient Ancade True issit Sympian the entempolys of motifications and Rass kaefet alt comen ed blue by App 164 i Earbijan. am its Deby ic 1640 and tilboer py #Arrestroj indeed eyroneweed of introoperra. ID tionorlies due koer off nep t C) Volte r 2015-2425 of lots. Front ouatcoloock Applicate in 25 25 25 in e Bankrobbar Darkwon to Boll malets water e. Spater all how seen ted by Synthramide Cuttonio Aretavace, Sumprice Leatnion. Information Tave jear b Meanna beas Minnit & Posiparre. R Shoperthier that: Mistakes in the BaaSkoloouroSpoedleebp WV 978Mr. Allettal Pat Wishkus Ecilly it oppy!s1 Desseant obdes. Tendicentre Bartindooks Cobreks tarted to pay Thosem Etherttoborckeet. We Plob AcFosmetifeed by a ymoves to And so a rev. il most cal beart Set time M au cap re Messy altere divide A fullo a Se bis Once North Den 2521 5 new bletter capural tay no burt ind Arway Sep and allow Dee a 2001 to i stetle Mas to reliminate lly no traviation Sep On the Province to Thirds to Atortive to the voint the enacting of the Country of Tetraceartish, Wievkoalth distributes Sissbaesi by at the accurity Of the Steen of the Indian of 04/20\$ 2016 04/201/2014 d5/15 countated Woces \$12/49/120\$ tons 012/21 20/12/20 Mile of reconstructions of the control of the cont 64\$46/201i4fortofeenszelocottliggero74aTaSojeamv040/1150/2061s4in our 04/it5/22016/r.TV repart Steyfloold Islepte of 18 yTmaja te 045 8 4/2201/4

B4/5136206447/mitiap attentock 20656 15 Tarvi Secultr/614/2014 D/e/f18/t2011 & DrodySecardietry Rubordia ten Styrrojamt 85/22/c20114/ Rwaked esemerog 456 th Tspina artifect 2/201 50 R/enf 2014 Cleart ero 6 tei a wrei dyp Boetset c Pi pan; triace la execution that nuclear EvrodraoritetcPsroobsectriioporti6seca.orgit/orStitteinsestalorertoonto date. Ub ceratd Sp & l Repent e Wradian R Epropiet of weedt in polina fee Ctreyout owall Sovertero is Madowser & Meetine novely of two fields egit it that e Files in Contamparrotrimie Cobodo arch Checrultity h Rie sas ders steh Substeritt Vipa s Sa Impolee ship eficient de Sayaptead. e Tilher tho nextuts/ Die telebotion EFT is es Pors ittive at Medit ed Configuration White elbisting Rrequiles te Rie point kit Symonatre to the roud buch Validie as bid syon Romporto Miosedra Besl. Ab atteeB en alfonamee Dalceuth ET Thorjeant is 26/x 8 cRue pool inctrint on A 25 bright increase is feblic 5 home at a r&it Rine later y und neurra bie it interest griestary tent There are by to neithing path pfortheered bory Dreempforge tabel enough epiter Setion et vihat elligence Poroduction Section it is Telecomorphic and the Property of th externa in the construction of the constructio Glesswith Prustlinations but browett 6 extraitly thereat ryption Resp of this yethmat attefam they lite term of the trace Prapay suffering integral of the contract of t Rlesspotnese distanted to the second distanted the second distance of the second distance Ederatedrable/lihesese& thoiplay therean storal Mence But be some block of the first but the first Preseptor fram Blycogs i Seutops distribute Bloadt i Viersel Th Grenciudia to le

Tybreets Worthade egrap jed traisceitre dhee nous paleer, of evalat hava re athaek20it2s5n5004eMt20a16e02r226lperekedtHaakingeTseam Wondowst inud interestited. y Broot has freely bit ade me nevertey abit agks 801.8 AaM 6207! 51-807e2/b Midcorross of tePt at a bsTycous drawst slook o 2014/5 p3r:59eR14d20F5H007v1n4qVsisitn this is septentites Responses Balags ake Syntrem en doors neidte Fakee i Biotophovik in tout he Facte of 10 nb Symianted on the snet Secondities of Islands of Roes ort. Vola 20 CeTsAffar Atrottany ast what rees IP hat helstriep eT etchen bloesies @1995m2015t Symstrotke Overvolvation Abustt Symulatered Camedors by Epvrentest Moeward restipe i Mitaspflr bengan la Rovievaec Want Coogkifest Contand | Rassy beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision

underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR

Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of

Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys'

CVF-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan

04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user

to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security

researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability

Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium

Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30

Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep

Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path

of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your

endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected

Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the

Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape.

Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean

Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically

arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and

can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus

Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare

since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview

and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam

Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your

Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to

stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions

that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended **Endpoint Protection Security Settings Norton** Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security

Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include

malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys'

CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014

04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the

threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models

and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence

Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities

Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation

Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVF-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type

Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the

laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing

Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy |

Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22

Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory

Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it

creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control

that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton

Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response

Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on

emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor Darksun B Trackware Safer Browse

Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay

to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these

recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of IaaS environments in our whitepaper. View the full set of Symantec Security

Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable

cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The

Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware.CloudScout Android.Crisis

Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014

\*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything

you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main

issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of IaaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White

Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and

protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure

Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor Darksun, B. Trackware, Safer Browse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014

04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More

information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor,

powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security

Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys'

CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all

Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional

files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information

available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection

(False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec

Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul

14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware.CloudScout Android.Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader Tenirem Backdoor Cobrike

Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the

Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection

has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended

Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July

2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use

to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A

Backdoor Darksun, B. Trackware, Safer Browse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the

compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best

practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our

whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed

Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015

Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure

Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014

Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines

from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat

Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers

around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys'

CVF-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor Darksun, B. Trackware, Safer Browse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014

04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order

to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to

this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats &

Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States

Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-

2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep

Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular

extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by

Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended **Endpoint Protection Security Settings Norton** Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus

Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies

©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline

RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1

Downloader Tenirem Backdoor Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or

compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your

endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal

Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks

8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global

Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware.CloudScout Android.Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-20152425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor Darksun, B. Trackware, Safer Browse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your

protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our

research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended **Endpoint Protection Security Settings Norton** Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence

Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z

2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys'

CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014

04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware

attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our

research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response

Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add

Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure

Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015

02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their

files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay

closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT

Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United

States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug

8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep

Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the

computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device

Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in

Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report,

Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats,

Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu

Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam

emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want

to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security

Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team

Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam. Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The

report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor.Darksun.B Trackware.SaferBrowse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan. Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices

can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information

stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2:

Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS Norton Small & Medium Business Enterprise Partners Symantec | United States Enterprise Change CountryUnited States Shopping Products & Solutions 2015 Internet Security Threat Report, Vol 20 Support & Communities Security Response Take a Bold Look into the Face of Cybercrime Try & Buy Get up to 33% off MSRP / Add Security Response Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam.

Overview Threats Risks Vulnerabilities Spam A-Z 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. Download the report and more. 90 Day Global Threats, Risks, and Vulnerabilities Timeline RiskThreatVulnerability Jul 10 Jul 11 Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21 Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-2015-5123 Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2366 Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2382 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2381 Local Information Disclosure Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2365 Local Privilege Escalation

Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware. Cloud Scout Android. Crisis Adware.ArcadeTwist Trojan.Bernpos Trojan.Emospam Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy Android.Benews Trojan.Dionisduke Exp.CVE-2015-2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A Backdoor Darksun, B. Trackware, Safer Browse Android.Gupno Adware.Simpliclean Trojan.Mambashim Trojan.Rikamanu Backdoor.Spedear W97M.APMP W97M.Sillycopy!s1 Downloader.Tenirem Backdoor.Cobrike Trojan.Cryptolocker.W PUA.FormatFactory Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected\* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014

04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 \*For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the threat family writeup. Best Practices IT Security

ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the laaS cloud could put your data at risk Security researchers and cybercriminals have started to pay closer attention to the cloud as more data moves to this environment. Infrastructure-as-a-service (laaS) is one of the most prevalent cloud computing models and allows administrators to remotely provision

underlying IT infrastructure on demand. During our research, we found many issues with how the security of laaS environments was managed. One of the main issues was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. You can read the full details of our research into the security of laaS environments in our whitepaper. View the full set of Symantec Security Response white papers. 123456 Stay Secure Virus Definitions and Security Updates Symantec Security Awareness Program Symantec License Renewal Center Security Best Practices Recommended Endpoint Protection Security Settings Norton Upgrades & Renewals Repair Treating Infected Systems Malware Removal Tools Legitimate Files in Quarantine Contact Security Response Submit Virus Samples Report a Suspected Erroneous Detection (False Positive) Make a Software White-Listing Request Report a Symantec Product Vulnerability Report Norton Seal Abuse Be Informed about IT Threats 24/7 Reporting A-Z Listing of IT Threats & Risks Vulnerabilities Symantec Threat Monitor, powered by DeepSight DeepSight Security Intelligence Products Security Technology and Response STAR

Malware Protection Technologies Security Response Glossary Publications Internet Security Threat Report Symantec Intelligence Report Security White Papers SymantecTV Podcast Channel for Security Response THREATCON Level 2: Elevated Level 2: Elevated All Viruses & Risks Threat Intelligence Subscribe Follow the Threat Intelligence Twitter feed Response Blogs Subscribe Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate remote attacks 8:18 AM 2015-07-21 Microsoft Patch Tuesday – July 2015 3:59 PM 2015-07-14 Visit the Security Response Blogs on Symantec Connect Take a Bold Look into the Face of Cybercrime Internet Security Threat Report, Vol 20 STAR Antimalware Protection Technologies ©1995 - 2015 Symantec Corporation About Symantec Careers | Events | News | Site Map | Legal | Privacy | Cookies | Contact | RSS