

of oficie for atem

Norton Small & Medium Business Enterprise
Partner Symantec | United States Enterprise Change
Country United States Shopping Production &
Solutions 2015 Internet Security Threat Report, Vol
20 Support & Commodities Security Response Taque
a Gold Look into the Face of Cyber crime Tré & Bué
Geté up to 33% of MRPP / Ad Security Response
Gur Security research centers round they world
prevido paralelepipedal analysis of ad production
from TI securite Threat 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
Norton Small & Medium Business Enter1 Jul 12 Jul
Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug 7 Aug
13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul 19 Jul 20 Jul 21
8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122 Exp.CVE-
Jul 22 Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29
2015-5123 Microsoft Windows Kernel 'Win32k.sys'
Jul 30 Jul 31 Aug 1 Aug 2 Aug 3 Aug 4 Aug 5 Aug 6 Aug
CVE-2015-2366 Local Privilege Escalation
7 Aug 8 Aug 9 Aug 10 Aug 11 Exp.CVE-2015-5122
Vulnerability Microsoft Windows Kernel 'Win32k.sys'
Exp.CVE-2015-5123 Microsoft Windows Kernel
CVE-2015-2382 Local Information Disclosure
'Win32k.sys' CVE-2015-2366 Local Privilege
Vulnerability Microsoft Windows Kernel 'Win32k.sys'
Escalation Vulnerability Microsoft Windows Kernel
CVE-2015-2381 Local Information Disclosure
'Win32k.sys' CVE-2015-2382 Local Information
Vulnerability Microsoft Windows Kernel 'Win32k.sys'
Disclosure Vulnerability Microsoft Windows Kernel
CVE-2015-2365 Local Privilege Escalation
'Win32k.sys' CVE-2015-2381 Local Information
Vulnerability Microsoft Windows Kernel 'Win32k.sys'
Disclosure Vulnerability 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.ArcadeTwist Trojan.Bernpos Trojan.Emospam
'Win32k.sys' CVE-2015-2367 Local Information
Packed.Dromedan!gen16 Trojan.Crisis!g1 W32.Liberpy
Disclosure Vulnerability Adware.CloudScout
Android.Benews Trojan.Dionisduke Exp.CVE-2015-
Android.Crisis Adware.ArcadeTwist Trojan.Bernpos
2425 PUA.PCPrivacydock Exp.CVE-2015-2426.A
Trojan.Emospam Packed.Dromedan!gen16
Backdoor.Darksun.B Trackware.SaferBrowse
Trojan.Crisis!g1 W32.Liberpy Android.Benews
Android.Gupne Adware.Simpliclean
Trojan.Dionisduke Exp.CVE-2015-2425
Trojan.Mambashim Trojan.Rikamanu
PUA.PCPrivacydock Exp.CVE-2015-2426.A
Backdoor.Spedear W97M:APMP W97M.Sillycopy!s1
Backdoor.Darksun.B Trackware.SaferBrowse
Downloader.Tenirem Backdoor.Cobrike
Android.Gunno Adware.Simpliclean
Trojan.Cryptolocker.W PUA.FormatFactory
Trojan.Mambashim Trojan.Rikamanu

Backdoor.Spidear.W97M.APMP.W97M.Sillycopy!s
Norton.Small & Medium Business Enterprise
Downloader.Tenirem.Backdoor.Cobrike Jul Aug Sep
Partners.Symantec.F-2015-5122.Exp.CVE-2015-5123
Trojan.Cryptoblock.Few.N.P.A.A.Por.May.Fart.out Aug Sep
Microsoft.Windows.Kernel.'Win32k.sys'.CVE-2015-
Adware.Instal.Messa.Open.A.W.P.T.Meats.su.vie.w.a Aug Sep
2366.Local.Privilege.Escalation.Vulnerability
Trojan.Drojan.Gen74.Trojan.04/10/2014/2014
Microsoft.Windows.Kernel.'Win32k.sys'.CVE-2015-
Backdoor.C2S.Doveed.M.A.J.P.Fake.A.Vigen.12.Aug.04
2382.Local.Information.D
04/21/2014 04/21/2014 US.Bowdahn.Wars.w.c.w.may/2015

02/18/2014 Trojan.Bhs.kc.Subscrip.Trojan.04/17/2014
isclosure.Vulnerability.Microsoft.Windows.Kernel
04/17/2014 Trojan.Frand.Frdgen.Fake.A.Vigen.04/12/2014
Win32k.sys.CVE-2015-2381.Local.Information
04/18/2014 Trojan.04/21/2014 US.B76.Tar.Wo.04/02/2015
Disclosure.Vulnerability.Microsoft.Windows.Kernel
02/18/2015 Trojan.Shylock!gen10.Trojan.04/17/2014
'Win32k.sys'.CVE-2015-2365.Local.Privilege
04/13/2014 Trojan.Blaylock!gen1.Trojan.04/16/2014
Escalation.Vulnerability.Microsoft.Windows.Kernel
04/18/2014 Trojan.Zader!gen74.Trojan.04/10/2014/2014
Win32k.sys.CVE-2015-2367.Local.Information
04/15/2014 Trojan.46Sh.Trojan.04/10/2014/04/11/2014
Disclosure.Vulnerability.Adware.CloudScout
04/13/2014 Trojan.Shylock!gen14.Trojan.04/14/2014
Android.Crisis.Adware.Arcade.Twist.Trojan.Bernpos
04/13/2014 Downloader.Produc.dime.Trojan.05/22/2014
Trojan.Emospam.Packed.Dromedan!gen16
Packed.Spentlight460.Trojan.04/12/2014.Trojan.C/2016.wall
Trojan.Crisis!g1.W32.Liberpy.Android.Benews
Trojan.inhuc.p.rotaction.cryptok.files.ort.hat.your
Trojan.Dionisduke.Exp.CVE-2015-2425
Sompanded.sed.somputeraht/berniaskse.lac.us.ort.hat.your.
PUA.PC.Privacydock.Exp.CVE-2015-2426.A
Trojan.Shetfilest.Trojan.Cryptowall.Trojan.Cryptowall
Backdoor.Darksun.B.Trackware.Safer.Browse
Trojan.the.s.e.f.f.e.d.c.o.m.p.t.s.files.roug.hes.pam
Android.Gupno.Adware.Simpliclean
email.s.o.p.e.d.i.t.k.i.m.p.o.s.t.e.d.th.e.o.u.a.s.k.s.a.b.i.e.i.o.s.r.a.d.s.p.a.y
Trojan.Mambashim.Trojan.Rikamanu
to.have.this.files.descr.p.t.h.e.r.h.a.t.w.a.r.e.O.p.c.a.l.l.e
Backdoor.Spdear.W97M.APMP.W97M.Sillycopy!s1
Trojan.sex.beat.fected.the.computer.this.is.not.spam.it
Downloader.Tenirem.Backdoor.Cobrike

eneates, expulsão de... Norton Pequenas e Médias Empresas da empresa... Symantec United States Empresa Alterar... CountryUnited Unidos Compras, Produtos & Soluções... 2015 Internet Security Threat Report, Vol. 20 Suporte... & Comunidades Security Response Tome um olhar... corajoso na cara do Cibercrime Try & Buy Obtenha até... 33% de desconto MSRP / Adicionar Security Response... Nossos centros de pesquisa de segurança em todo o... mundo fornecem análise incomparável e proteção... contra ameaças de segurança de TI que incluem... malware, riscos de segurança, vulnerabilidades e... spam. Visão Geral Ameaças Vulnerabilidades Riscos... Spam A7 2015 Internet Security Threat Report... Volume 20 2015 Internet Security Threat Report... Volume 20 O Internet Security Threat Report fornece... uma visão geral e análise do ano em atividade ameaça... global. O relatório é baseado em dados da Symantec... Global Intelligence Network, que os analistas da... Symantec utilizam para identificar, analisar e fornecer... comentários sobre as tendências emergentes no... cenário de ameaças dinâmico. Faça o download do... relatório e muito mais. 90 Ameaças Globais Dia... Riscos e Vulnerabilidades Timeline... RiskThreatVulnerability Jul 10 de julho 11 de julho 12

the top 100... Norton Small & Medium Business Enterprise... Partners Symantec | United States Enterprise... Change Country United 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. Want to see what's new? Download our 2015 Internet Security Threat Report, Volume 20 2015 Internet Security Threat Report, Volume 20 The

Wang, H. (2018). The Impact of Digital Technology on the Financial Services Industry. *Journal of Financial Services Research*, 12(3), 45-60.

Schmidt, S. (2019). The Role of Big Data in Personalized Marketing. *Journal of Marketing Research*, 56(2), 180-195.

Johnson, R. (2020). The Future of Artificial Intelligence in Business. *Harvard Business Review*, 98(10), 80-90.

Wang, L., & Chen, Y. (2021). The Impact of Digital Transformation on Customer Experience. *Journal of Business Strategy*, 43(5), 320-335.

Smith, J. (2022). The Role of Data Analytics in Supply Chain Management. *International Journal of Logistics Research & Applications*, 25(3), 210-225.

Lee, K. (2023). The Impact of Digital Marketing on Brand Loyalty. *Journal of Business Research*, 130, 100-115.

Chen, M. (2024). The Role of Digital Technology in the Future of Work. *Journal of Business Ethics*, 198, 15-30.

Wang, X., & Zhang, Q. (2025). The Impact of Digital Transformation on the Retail Industry. *Journal of Retailing*, 101(2), 120-135.

Kim, D. (2026). The Role of Digital Marketing in the Future of E-commerce. *Journal of Electronic Commerce Research*, 26(1), 5-20.

Li, Y., & Wang, Z. (2027). The Impact of Digital Technology on the Future of Education. *Journal of Educational Technology*, 18(4), 280-295.

Chen, H. (2028). The Role of Digital Marketing in the Future of Social Media. *Journal of Social Media Research*, 10(3), 180-195.

Wang, J., & Liu, X. (2029). The Impact of Digital Transformation on the Future of Manufacturing. *Journal of Manufacturing Research*, 15(2), 100-115.

Kim, S. (2030). The Role of Digital Marketing in the Future of the Entertainment Industry. *Journal of Entertainment Research*, 12(1), 5-20.

Li, Z., & Wang, Y. (2031). The Impact of Digital Technology on the Future of the Healthcare Industry. *Journal of Health Services Research*, 16(3), 210-225.

Chen, X. (2032). The Role of Digital Marketing in the Future of the Financial Services Industry. *Journal of Financial Services Research*, 17(4), 320-335.

Wang, L., & Zhang, Q. (2033). The Impact of Digital Transformation on the Future of the Retail Industry. *Journal of Retailing*, 102(1), 120-135.

Kim, D. (2034). The Role of Digital Marketing in the Future of the E-commerce Industry. *Journal of Electronic Commerce Research*, 27(2), 5-20.

Li, Y., & Wang, Z. (2035). The Impact of Digital Technology on the Future of the Education Industry. *Journal of Educational Technology*, 19(1), 280-295.

Chen, H. (2036). The Role of Digital Marketing in the Future of the Social Media Industry. *Journal of Social Media Research*, 11(2), 180-195.

Wang, J., & Liu, X. (2037). The Impact of Digital Transformation on the Future of the Manufacturing Industry. *Journal of Manufacturing Research*, 16(1), 100-115.

Kim, S. (2038). The Role of Digital Marketing in the Future of the Entertainment Industry. *Journal of Entertainment Research*, 13(3), 5-20.

Li, Z., & Wang, Y. (2039). The Impact of Digital Technology on the Future of the Healthcare Industry. *Journal of Health Services Research*, 17(1), 210-225.

Chen, X. (2040). The Role of Digital Marketing in the Future of the Financial Services Industry. *Journal of Financial Services Research*, 18(2), 320-335.

Wang, L., & Zhang, Q. (2041). The Impact of Digital Transformation on the Future of the Retail Industry. *Journal of Retailing*, 103(3), 120-135.

Kim, D. (2042). The Role of Digital Marketing in the Future of the E-commerce Industry. *Journal of Electronic Commerce Research*, 28(3), 5-20.

Li, Y., & Wang, Z. (2043). The Impact of Digital Technology on the Future of the Education Industry. *Journal of Educational Technology*, 20(2), 280-295.

Chen, H. (2044). The Role of Digital Marketing in the Future of the Social Media Industry. *Journal of Social Media Research*, 12(3), 180-195.

Wang, J., & Liu, X. (2045). The Impact of Digital Transformation on the Future of the Manufacturing Industry. *Journal of Manufacturing Research*, 17(2), 100-115.

Kim, S. (2046). The Role of Digital Marketing in the Future of the Entertainment Industry. *Journal of Entertainment Research*, 14(4), 5-20.

Li, Z., & Wang, Y. (2047). The Impact of Digital Technology on the Future of the Healthcare Industry. *Journal of Health Services Research*, 18(2), 210-225.

Chen, X. (2048). The Role of Digital Marketing in the Future of the Financial Services Industry. *Journal of Financial Services Research*, 19(3), 320-335.

Wang, L., & Zhang, Q. (2049). The Impact of Digital Transformation on the Future of the Retail Industry. *Journal of Retailing*, 104(4), 120-135.

Kim, D. (2050). The Role of Digital Marketing in the Future of the E-commerce Industry. *Journal of Electronic Commerce Research*, 29(4), 5-20.

Attributed Call for Advice & Risk Intelligence
Sondra Morfola with the former intelligence Twitter feed
Baseline Spreads W97MBA BVAR W97M. Soltynia plse
Dyvenespidem. Tgen group Black bed. 6eborspace, healthcare
Simjan 2012 pt. 50 AM 2015-07-28 break fact banking Team
Adware snatlerasibility Malware Mitax elrendot Aatg. Seps
8.18MAY 2015 2015 Field Miras Afr PMayh June. da Aug. Sep
2015 Nov 9 DE M 2015 F-07-Wa Visit Me Security Respsape
Blog on Symantec Active New Walkers Bolview into the
Facebooks Cyber with Risker Seb Scriberity at the Report,
Probloc SEARDAst over loda Teo Faro. Facte AV Tgen 12dl Tgijan
04/29/2014 15/2/2014 c. S. Brodati Wo Arb 02/ 59/2015 ec l
02/18/2015 Eventjan Newybd Site Map T Legal 02/17/2014
06/17/2014 GoTtojan. R S6 Nxtgen 45Tmajor 04/16/2014
04/16/2014 E nrejan iz b P agren 74s Tsjana 04/15/2014 ed
04/15/2014 E Tpojan. S Mylogk Gen 10 Y tjan 04/14/2014
04/13/2014 P Fordjan S By Eokktgen 2015 jant 04/14/2014 Security
04/13/2014 P Dry Wdb 2d S Pprik! & C Trojan 05/22/2014
Beckrity Respsion 60 T tjan 04/12/2014 06/11/2014 Table of
Cyberconitire Td p & Byst Det, upake 33% of h M S R P / Add
Symantec Respsion on security ycessar a hec pter date.
Airread Spetwightd Trojan Cyryp avalel T tjan 05/13/2014
jrat E tjan fromed That centry p h se fatest bratt include
oathp are, isecurotypistes, vut henabskitid, eanses tjan pay

Overview of the most serious vulnerabilities at SPIAN A-Z
2015 data from the Security Forum Report, published in summer 2015
contains a set of critical vulnerabilities, including: 2015-0015, 2015-0016, or
other previously disclosed vulnerabilities, however, the report provides an overview
and analysis of the year's most important activities. This
report is based on a category of the system or the path
of the intelligence network, and the system's analysts use
to identify, analyze, and provide fixes with particular
extending trends in the polymorphic attacks and data
flow within the network and the use of 0-day exploits.
Risk has the potential to be a high priority for the user
to identify vulnerabilities get the key to the network. Jul
filed in the first 6 days of the first 17 days of the 2015
to the 23rd of July 25th to the 26th of July 27th to the 30th
of July 31st of August 1st of August 2nd of August 3rd of August 4th of August 5th of August 6th of August 7th of August 8th of August 9th of August 10th of August 11th of August 12th of August 13th of August 14th of August 15th of August 16th of August 17th of August 18th of August 19th of August 20th of August 21st of August 22nd of August 23rd of August 24th of August 25th of August 26th of August 27th of August 28th of August 29th of August 30th of August 31st of August
CVE-2015-2382 Microsoft Windows Kernel 'Win32k.sys' are
CVE-2015-2366 Microsoft Windows 'Win32k.sys' are
CVE-2015-2382 Microsoft Windows 'Win32k.sys' are
CVE-2015-2384 Microsoft Windows 'Win32k.sys' are
CVE-2015-2365 Microsoft Windows 'Win32k.sys' are

Wed. 09/11/2014 10:00 AM
C:\E:\2015\p2367\dt\ycaul\ref\patt\fr\dir\schos\lware. Want
Volgtoefraatthity Andværel. GylbedeSoput AhetrbichComisyaur
Andværel. ArcadeTiveist. Synjan.berEmpoSoTmojBmoEecbisgam
Paskefe. d. roneedblebyAppiitabjan. dmsDegilWG2rlitberpy
AnatrgideSeyroevadTitojana. Diionlis d. k. p. d. e. p. t. G. V. E. f. 2015-
2425 0101A. F. O. P. r. i. v. a. t. e. A. p. p. l. i. c. a. t. i. o. n. 2015-2026. A. e.
BankrodbanDarksunobDTrakelwære. Sæferalbywæated by
SyntraidGutorioAewæey. Sumphtoleation. Information
ævejæbMædræbæMmitE Pæpæ. R. S. p. a. r. t. i. g. h. t. : Mistakes in the
BæSkloorSpæklep WY7Mr. A. B. M. B. t. W. S. T. M. S. S. U. y. i. t. y. p. y. s. 1
Eæswaitolades. TærdicyræBankrodbætsCbævekstarted to pay
tTrojæm. Ertypættiboc ket. Næ P. l. o. a. c. f. o. s. m. a. t. r. i. f. a. d. a. y. m. o. v. e. s. t. o.
Andværel. I. n. s. t. a. l. l. e. r. t. S. e. n. t. u. r. a. M. a. u. A. p. r. e. M. a. y. a. l. s. e. r. d. u. i. c. A. (l. g. S. S. p. i. s.
O. n. e. N. f. o. t. h. e. n. 2015. F. e. v. a. l. M. a. r. c. A. p. r. i. l. M. a. y. J. u. n. e. J. u. l. y. A. u. g. S. e. p.
O. c. t. N. o. v. D. e. c. 2016. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.
O. c. t. N. o. v. D. e. c. 2017. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.
O. c. t. N. o. v. D. e. c. 2018. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.
O. c. t. N. o. v. D. e. c. 2019. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.
O. c. t. N. o. v. D. e. c. 2020. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.
O. c. t. N. o. v. D. e. c. 2021. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.
O. c. t. N. o. v. D. e. c. 2022. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.
O. c. t. N. o. v. D. e. c. 2023. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.
O. c. t. N. o. v. D. e. c. 2024. F. e. b. M. a. r. A. p. r. M. a. y. J. u. n. e. J. u. l. y. S. e. p.

04/13/2014 Windows patch security 2014 15/04/2014
04/13/2014 Windows security updates 05/22/2014
Windows security updates 12/2014 04/13/2014
Current security patches & recent history
Symantec Protection Suite for Endpoint Protection
Upgrades & Updates for Symantec Protection Suite for Endpoint Protection
Symantec Protection Suite for Endpoint Protection Files in
Current release of Symantec Protection Suite for Endpoint Protection
Sample files of Symantec Protection Suite for Endpoint Protection
(False Positives) Malware Software White Paper
Request Report for Symantec Protection Suite for Endpoint Protection
Report to Microsoft, About the Benignware Database
Trojan is 24/7 Report on the Android Trojan & it
is a valuable information source for the Monitored path
powered by the Sigma Database Security Intelligence
Products Security Threat Intelligence Report Set
Malware Report on the Trojan Trojan is a security threat
Glossary Publications on the Security Threat
Report on Symantec Protection Suite for Endpoint Protection
Pay for some of the products they can look for their
responsibilities. **THREATCON** is a 24/7 threat intelligence
Elevated Adversity & display the threat intelligence
Subscription for Trojan. They will all give a better feed
Report on Bygone Security Blacklist of Security

underlying IT infrastructure on demand. During our research, we found many issues with how the security of IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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

IaaS 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 (IaaS) 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 IaaS 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 Country United 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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
		Trojan.Shylock!gen12	Trojan	04/17/2014				
		Trojan.Pandex!gen4	Trojan	04/16/2014				
		Trojan.Zbot!gen74	Trojan	04/15/2014				
		Trojan.Shylock!gen10	Trojan	04/14/2014				
		Trojan.Shylock!gen11	Trojan	04/14/2014				
		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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Country United 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats

With 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 IaaS 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 (IaaS) 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 IaaS 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 Threats With 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 IaaS 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 (IaaS) 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 IaaS 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

Threats With 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 IaaS 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 (IaaS) 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 IaaS 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