of oficie for atem

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

Jul 23 Jul 24 Jul 25 Jul 26 Jul 27 Jul 28 Jul 29 Jul 30 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

Norton Small & Medium Business Enter1 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 Jan Feb Mar Apr May Jun Jul Aug Sep

Norton Small & Medium Business Enterprise

Downloader.Tenirem Backdoor.Cobrike Jul Aug Sep

Partners SymantecE-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 D

Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep

Threats | View all

isclosure 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

04/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014

*For continued protection, make sure that your Symantec subscription and virus definitions are up to date.

Trojan.Cryptowall

is a Trojan horse that encrypts files on the compromised computer and 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 on malicious or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it

Norton Pequenas e Médias Empresas da empresa
Parceiros 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 AZ 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

[illegible]
Norton Small & Medium Business Enterprise
[illegible]
Partners Symantec | United States Enterprise
[illegible]
Change CountryUnited States Shopping Products &
[illegible]
Solutions 2015 Internet Security Threat Report, Vol 20
[illegible]
Support & Communities Security Response Take a
[illegible]
Bold Look into the Face of Cybercrime Try & Buy Get
[illegible]
up to 33% off MSRP / Add Security Response Our
[illegible]
security research centers around the world provide
[illegible]
unparalleled analysis of and protection from IT
[illegible]
security threats that include malware, security risks,
[illegible]
vulnerabiliti Norton Small & Medium Business
[illegible]
Enterprise Partners Symantec | United States
[illegible]
Enterprise Change CountryUnited States Shopping
[illegible]
Products & Solutions 2015 Internet Security Threat
[illegible]
Report, Vol 20 Support & Communities Security
[illegible]
Response Take a Bold Look into the Face of
[illegible]
Cybercrime Try & Buy Get up to 33% off MSRP / Add
[illegible]
Security Response Our security research centers
[illegible]
around the world provide unparalleled analysis of and
[illegible]
protection from IT security threats that include
[illegible]
malware, security risks, vulnerabilities, and spam.
[illegible]
Overview Threats Risks Vulnerabilities Spam A-Z
[illegible]
2015 Internet Security Threat Report, Volume 20 2015
[illegible]
Internet Security Threat Report, Volume 20 The

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Papers Symantec TV Podcast Channel Information Security
Response THREATCON Level 2: Elevated Level 2:
Elevated [illegible] Risk Landscape Intelligence
Subscribe to 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 Security Response
Blogs on Symantec Connect [illegible] Locked [illegible] the
Eye 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
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

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 yourself from malware. Want to [illegible] your 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 [illegible] especially created by Symantec to increase your protection. Information available here. A White Paper Spotlight: Mistakes in the cloud could put your data at risk Security researchers and cybercriminals alike pay close 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 storing in the cloud. You can read the full details of our [illegible] 90-Day Global Threats, Risks, [illegible] Symantec Security Response whitepaper. [illegible] 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 Infected Files System 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 Notify Security Response about Threats 24/7 [illegible] Threats & Risks [illegible] powered by [illegible] Intelligence Products [illegible] STAR [illegible] Internet Security Threat Report Symantec Intelligence Report Security White Papers Symantec Podcast Channel for Security Response [illegible] Level 2:

emerging trends in today's dynamic threat landscape. [illegible] Risk Threat Vulnerability Jul [illegible] 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-[illegible] Local Privilege Escalation Vulnerability Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability [illegible] Trojan.[illegible] W32.Liberpy [illegible] Exp.CVE-2015-2425 [illegible] Exp.CVE-2015-2426 [illegible]

[illegible] Intelligence

[illegible] Twitter feed

[illegible]

[illegible] healthcare

[illegible] Team

[illegible]

[illegible]

[illegible]

[illegible] into the

[illegible] Report,

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] Security

[illegible]

[illegible] of

[illegible] / Add

[illegible] date.

[illegible]

[illegible] include

[illegible]

Overview Threats Risks Vulnerabilities Special 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 Threat, Risk, and Vulnerability Timeline Risk Threat Vulnerability 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 Best Practices Security CVE-2015-1233 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

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 manual means. 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 keys. 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 write-up. Best Practices 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 information from malware. Want to go further and really beef up protection on your company 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 how to use it especially created by Symantec to increase your protection. Information available in the White Paper Spotlight: Mistakes in the [illegible] 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 infrastructure on demand. During our research, we found many issues in how the security of cloud 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 cloud environments in our whitepaper. View the full list of Symantec Security

Vulnerability in Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2367 Local Information Disclosure Vulnerability Adware.[illegible] Android.Crisis Adware.Arcade[illegible] Trojan.[illegible] Trojan.[illegible] Packed.Dromedan [illegible] Trojan.[illegible] W32.Liberpy Android.Beyonce Trojan.Dionis Exp.CVE-2015-2425 PUA.FCPrivacyLock Exp.CVE-2015-2426 Backdoor.Darkmoon.B Trackware.SafeBrowse Android.Cupi Adware.Simpl[illegible] Trojan.Mamba Trojan.Rspam Backdoor.Speedup W97M.APMP W97M.Solitary!s1 Downloader.Tendrit Backdoor.[illegible] Trojan.Cryptolocker.N 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 [illegible] Discovered Trojan.FakeAV.Cgen 121 Trojan 06/21/2016 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 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 on malicious or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a registry entry to store the path of the encrypted files

Contact Security Response

Submit Virus Samples

Report a Suspected Erroneous Detection (False Positive)

Software White Listing

Report a Symantec Product Vulnerability

Report Norton Seal Abuse

A-Z Listing of Threats & Risks

Vulnerabilities

Symantec Threat Monitor, powered by DeepSight

DeepSight Security Intelligence

Glossary

Publications

Internet Security Threat Report

Symantec Intelligence Report

Security White Papers

Symantec TV Podcasts Channel for Security Response

THREATCON Level 2: Elevated

Level 2: Elevated

Threat Intelligence

Subscribe

Best Practices

cyberespionage group targeted aerospace, health since 2012 5:50 AM 2015-07-28 Leaked Hacking Team Windows vulnerability could facilitate more 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 Cyber Crime 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

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 list of best practices for today's threat landscape. Use these recommendations to know what you 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 About Symantec| Careers| Events| News| Site Map| Legal| Privacy| Cookies| Contact| RSS Norton Small & Medium

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

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

Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 *For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today’s threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the

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 About Symantec| Careers| Events| News| Site Map| Legal| Privacy|

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

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

Adware.InstallerSetup Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Most Active New Threats View all Threats | View all Risks Subscribe Name Type Protected* Discovered Trojan.FakeAV!gen121 Trojan 04/21/2014 04/21/2014 JS.Bondat Worm 02/19/2015 02/18/2015 Trojan.Shylock!gen12 Trojan 04/17/2014 04/17/2014 Trojan.Pandex!gen4 Trojan 04/16/2014 04/16/2014 Trojan.Zbot!gen74 Trojan 04/15/2014 04/15/2014 Trojan.Shylock!gen10 Trojan 04/14/2014 04/13/2014 Trojan.Shylock!gen11 Trojan 04/14/2014 04/13/2014 Downloader.Ponik!gm Trojan 05/22/2014 Packed.Generic.460 Trojan 04/12/2014 04/11/2014 *For continued protection, make sure that your Symantec subscription and/or license are up to date. Threat Spotlight: Trojan.Cryptowall Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted. The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware. Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key. This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom. More information on Trojan.Cryptowall is available in the threat family writeup. Best Practices IT Security ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it’s harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it’s harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today’s threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 About Symantec|

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

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

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

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

Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it’s harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today’s threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device

Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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

ThreatsWith the rapid rise in the number of malware attacks it's harder than ever to prevent machines from getting infected. But have you done everything you can do? Have you done the things you must do to stay protected? Following some simple best practices can make a tremendous difference in improving your protection. Symantec has assembled a set of best practices for today's threat landscape. Use these recommendations to know what you must, should and can do to protect your endpoints from malware. Want to go further and really beef up protection on your endpoint machines? Symantec Endpoint Protection has a feature called Application and Device Control that gives you additional tools to protect your endpoints. Find out about Application and Device Control and download rulesets especially created by Symantec to increase your protection. Information available here. White Paper Spotlight: Mistakes in the 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 About Symantec| Careers| Events| News| Site Map| Legal| Privacy| Cookies| Contact| RSS