A new wave of the Petya (also known as “Mischa” or “GoldenEye”) ransomware has been affecting a significant number of organizations across a wide range of target industries since Tuesday, 27 June. Many victims have already been named in open source, including multiple global entities. This is reminiscent of the May 2017 WannaCry outbreak, which also had worldwide reach, compromising a similarly broad range of organizations at speed. As with the WannaCry ransomware campaign, Petya includes exploits that allow it to propagate in an automated fashion with no user interaction (wormable), drastically increasing the scope of a potential compromise from one asset to the entire environment.

This ransomware is slightly different and is more sophisticated than previous variants, such as WannaCry, and is impacting organizations with varying levels of hygiene. The impacts can also be more severe as users will not only be limited from accessing their files, but accessing their operating systems as well. It also uses several different methods to ensure that it affects as many machines as possible.

pwc

Ransomware is a name given to malware that prevents or limits users access to computer systems or files, typically demanding a ransom payment in exchange for a key to acquire access to impacted assets. Modern ransomware behavior typically involves the encryption of end user files using strong encryption algorithms, which make them inaccessible to victims. A decryption key is often provided to victims in exchange for some type of currency, often cryptocurrency such as Bitcoin. Multiple ransomware variants have been observed across the globe over the past several years. The variants are often distributed and behave in different ways. Due to those differences, it is key to understand each variants behavior to plan for, respond to, and recover from a ransomware attack.

For example, some variants of ransomware have implemented poorly designed encryption mechanisms, allowing security researchers to develop decryption tools which are often freely shared with victims.

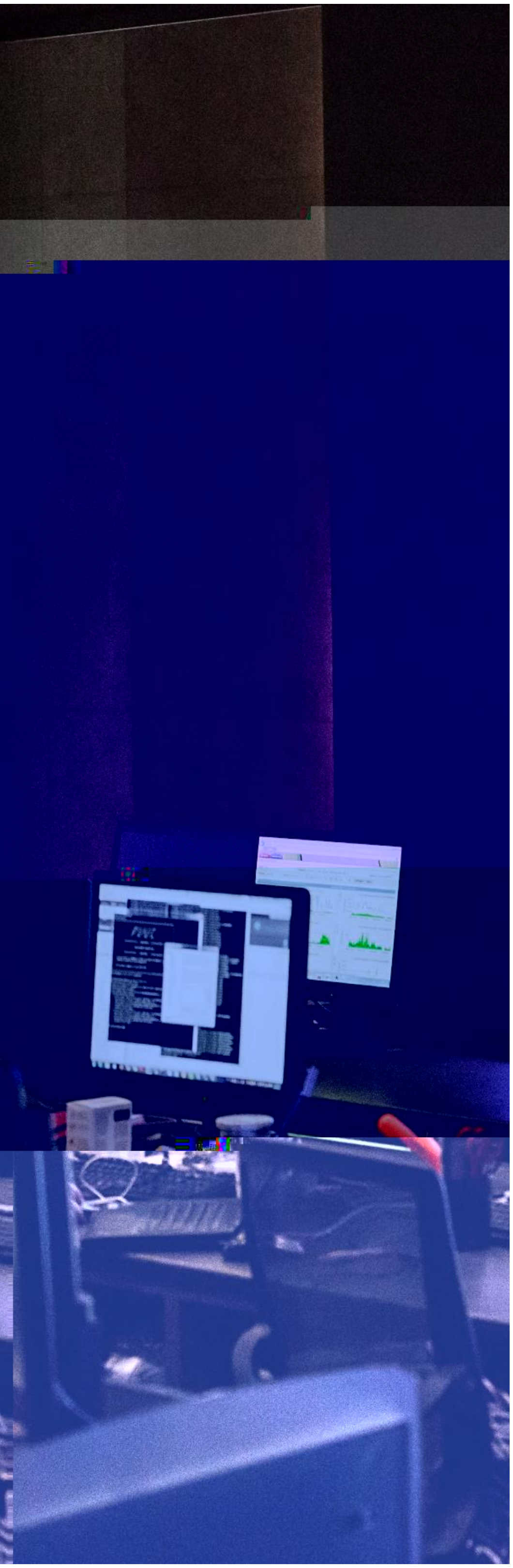
Ransomware is an increasingly prevalent threat, with a rising number of variants designed to target corporate networks. In spite of this scourge, there are many pragmatic steps which organizations can take to reduce the likelihood of incidents, limit their impact when one does occur, and to recover swiftly and effectively. These span several aspects of IT operations and security and primarily relate to:

Robust business continuity planning and exercising - ensuring that individual user systems and key servers can be restored rapidly from backups, and that the frequency of backups aligns to the timeframe of data your organization is prepared to lose in the event of any system being rendered unusable;

Crisis and incident response planning and exercising - ensuring that there are formal procedures in which employees and those responsible for the management of high priority incidents are well versed to streamline the organization's reaction to ransomware events and its ability to restore service to employees and customers;

Strong security hygiene policies and user awareness - preventing ransomware entering your IT environment through the most common delivery vector, phishing, by enforcing strong controls at your email gateways and network perimeters, and developing vigilant employees through robust awareness campaigns; and,

Rigorous patch and vulnerability management - the vulnerabilities exploited in this attack have already been addressed via Microsoft 'critical' patches released in March, as well as this week, and a robust vulnerability management program will help reduce the likelihood of exploitation.



The initial infection vector of this latest wave of ransomware is not currently known. The malware is actually a combination of Petya and Mischa. If the malware is run as administrator, it will encrypt the Master Boot Record (MBR) but not the files on disk.

The effect of encrypting the MBR means that the user will be unable to restart the system in its normal fashion, and instead will be displayed with a ransomware message.

However, if the malware is run as a normal user, files with specific extensions (as provided in Appendix A) will be encrypted. This is also known as the 'Goldeneye' combination.

The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) is designed to assist organizations in structuring their cybersecurity program in five functions: Identify, Protect, Detect, Respond, and Recover.

Identify

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Action:

I. Executives should make an effort to identify assets within their organization which are vulnerable to this variant of ransomware, specifically those vulnerable to the EternalBlue and DoublePulsar SMB exploit. This includes all Microsoft Windows systems which require but have yet to install Microsoft patch MS17-101.

II. Know, understand, and enhance your enterprise and disaster recovery procedures. Ensure your mission and business critical data is backed up in a secure and timely manner.

Protect

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Action:

I. Executives should also understand that IT operations teams, on the recommendation of their security team, may need to cause temporary disruption to some services within their environment as additional controls are implemented and vulnerable services disabled;

II. Ensure your IT teams have taken action to, or develop plans to:

   A. Disable all external SMB access (blocking ports 137, 139 and 445 to/from the internet);

   B. Disable the use of the SMBv1 network file sharing protocol across the entirety of your environment;

   C. Disable the ability to execute unsigned macros in Office documents, using group policy settings (and sign legitimate macros from your own organization);

   D. Ensure two factor authentication is in place for all necessary external access to systems (e.g. VPN and RDP);

   E. Identify and prevent all systems without the MS17-010 security update from connecting to core corporate networks, and segment guest networks from all ability to access core corporate networks;

   F. Force an enterprise wide update of antivirus signatures;

   G. Rapidly isolate any infected systems from your corporate network to limit the spread to other systems.

Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Action:

I. Organizations should leverage all available intelligence sources to build a comprehensive library of indicators to enhance detection capabilities. In support of this phase, the following Indicators of Compromise (IOC's) have been observed related to this campaign. These IOC's are provided with medium confidence, may not be comprehensive for all variants of this ransomware, and should be assessed for appropriate actions by the recipient. Please see the Appendix.

Respond

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Action:

I. If a Petya ransomware event is detected, your organization should be prepared to activate its Incident Response plan. Due to the ransomware's ability to rapidly spread through a susceptible environment, containment actions should be taken with some urgency. Additionally, while PwC does not recommend paying a ransomware ransom, any victim organization should be prepared to understand and quantify the impact of an infection and take appropriate action to limit the impact of the incident in the most effective manner.

II. For organizations working in regulated industries like healthcare and financial services where PHI or PII is impacted by ransomware, be familiar with the Department of Health and Human Services, Office of Civil Rights Fact Sheet on Ransomware and the Healthcare sector.

III. Conduct an impact analysis to quantify disruptions to business, and leverage that analysis to make the appropriate risk-based decisions.

Recover

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Action:

Leverage current disaster recovery programs and processes within your organization to enable "back to business" operations.

Identify whether your organization is required to notify regulators, partners, or customers of a compromise or business disruption and take appropriate action.

Conduct post incident analysis to ensure lessons are incorporated into your cybersecurity program.

PwC’s global team of 3,300+ practitioners include specialized consultants, former law enforcement agents, cyber-forensic investigators, intelligence analysts, technologists, attorneys and industry leaders in cybersecurity and privacy. Our team has deep experience helping global businesses across industries strategically assess, design, deploy and improve cybersecurity programs. Learn more at pwc.com/cybersecurityandprivacy

Diverse Network of Resources

PwC has deep experience helping organizations strategically assess, design, deploy and improve cybersecurity programs. We also have a long history of building professional relationships with business leaders at all levels.

Experience

Our tactical knowledge gleaned from decades of projects across industries, geographies and technologies informs our services.

Global analytics and cybersecurity impact centers

Our Impact Centers give companies and organizations from around the world access to experts and experience from across the PwC global network to help with the challenges of keeping pace in this era of digital disruption and to successfully transform for the future.

Certified Incident Response Capabilities

The National Security Agency (NSA) awarded PwC its Certified Incident Response Assistance (CIRA) accreditation and the first professional services firm in the UK to receive accreditation by Cyber Incident Response (IR) scheme run by CESG – the information assurance arm of GCHQ - and the Centre for the Protection of National Infrastructure (CPNI).

CyberArk named PwC its 2016 Systems Integrator of the Year

SailPoint named PwC its 2016 Global Advisory Firm of the Year

Palo Alto Networks named PwC its 2016 Partner of the Year

For any enquiries on how to best prevent or address ransomware or other cyber-attacks, please email: us_pwc_cyber_ir@pwc.com or contact one of our practice leaders.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

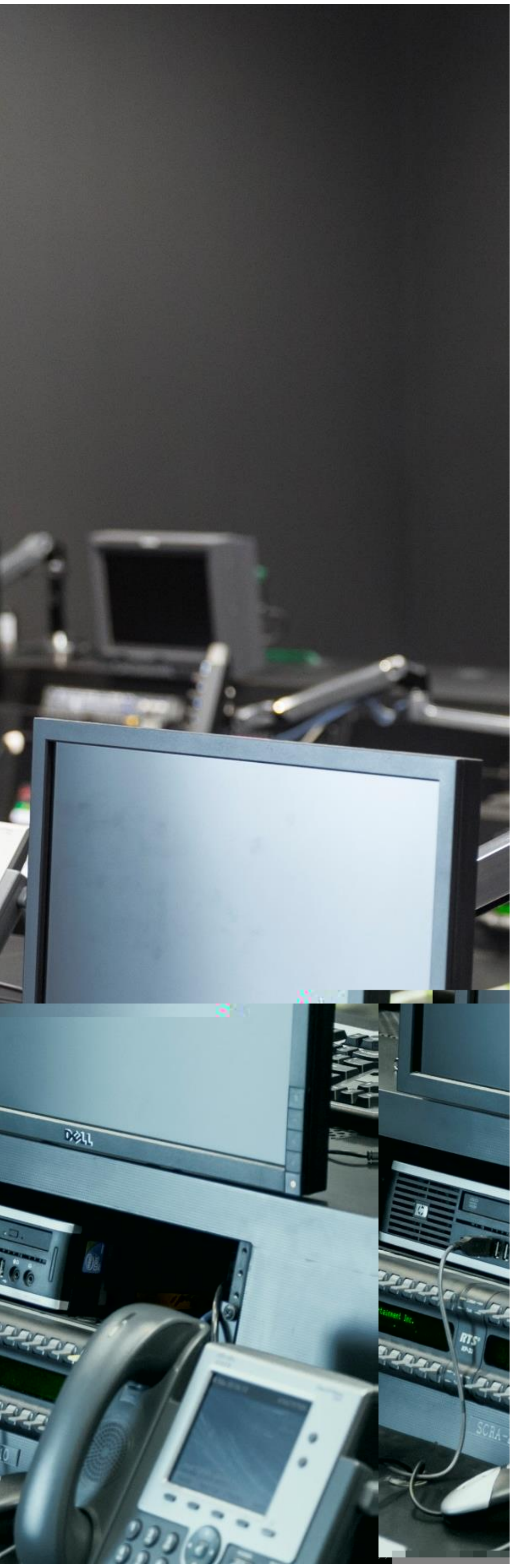
At PwC, our purpose is to build trust in society and solve important problems. a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC has exercised reasonable professional care and diligence in the collection, processing, and reporting of this information. However, the data used is from third party sources and PwC has not independently verified, validated, or audited the data. PwC makes no representations or warranties with respect to the accuracy of the information, nor whether it is suitable for the purposes to which it is put by users.

PwC shall not be liable to any user of this report or to any other person or entity for any inaccuracy of this information or any errors or omissions in its content, regardless of the cause of such inaccuracy, error or omission. Furthermore, in no event shall PwC be liable for consequential, incidental or punitive damages to any person or entity for any matter relating to this information.

.

en1 .92 TEO05.754(/1TC0.00000912 0 612 792 reW/F4 6 5 rg00234.632 . 0.137 0.122 0.12 l40.TE 4559559.25 BT1 .92 TE01589.754(/1TC0.00000912 0 612 792 reW/F4 6.4C12(/12b10e10 1 10s12e10 civ ad



PwC Quick Response Tipper

See attachment

Indicators of Compromise (Assessed with Medium Confidence)

:

- dllhost.dat

Behavior

- schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d

:

- 71b6a493388e7d0b40c83ce903bc6b04
- a1d5895f85751dfe67d19cccb51b051a
- 7e37ab34ecdcc3e77e24522ddfd4852d
- e285b6ce047015943e685e6638bd837e
- fe2c47fbb22139f790287272e9a9e365
- E595c02185d8e12be347915865270cca

:

- wowsmith123456@posteo[.]net

:

- http://mischapuk6hyrn72.onion/
  http://petya3jxfp2f7g3i.onion/
  http://petya3sen7dyko2n.onion/
  http://mischa5xyix2mrhd.onion/MZ2MMJ
  http://mischapuk6hyrn72.onion/MZ2MMJ
  http://petya3jxfp2f7g3i.onion/MZ2MMJ
  http://petya3sen7dyko2n.onion/MZ2MMJ

Indicators of Compromise (Assessed with Medium Confidence)

- alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - OPTIONS /"; flow:established,from_client; urilen:1; content:"OPTIONS"; http_method; content:"DavClnt"; http_user_agent; content:"translate: f|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000199; rev:2017062701;)
- alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - OPTIONS /admin$"; flow:established,from_client; urilen:7; content:"/admin$"; http_uri; content:"OPTIONS"; http_method; content:"Microsoft-WebDAV-MiniRedir"; http_user_agent; content:"translate: f|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000200; rev:2017062701;)
- alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - PROPFIND /admin$"; flow:established,from_client; urilen:7; content:"/admin$"; http_uri; content:"PROPFIND"; http_method; content:"Microsoft-WebDAV-MiniRedir"; http_user_agent; content:"translate: f|0d 0a|"; http_header; content:"Depth: 0|0d 0a|"; http_header; content:"Content-Length: 0|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000201; rev:2017062701;) Petya - the latest wave

Indicators of Compromise (Assessed with Medium Confidence)

- Ooops, your important files are encrypted. If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service. We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key. Please follow the instructions: 1. Send $300 worth of Bitcoin to following address: 2. Send your Bitcoin wallet ID and personal installation key to email wowsmith123456@posteo[.]net. Your personal installation key: If you already purchased your key, please enter it below.