

CERT-MU eSecurity Newsletter

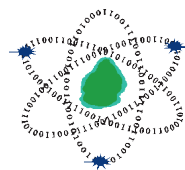


Featured

Understanding, Preventing &
Responding to Ransomware Attacks

CERT-MU Is Now ISO 27001: 2013
Certified

Volume 7 | Issue 1 | July 2017



CERT-MU **Computer Emergency Response Team** **of Mauritius** **(CERT-MU)**

Your Partner in Cyber Security
www.cert-mu.org.mu

CERT-MU SERVICES

Reactive Services:

- ⇒ Incident Handling
- ⇒ Vulnerability Scanning and Penetration Testing

Proactive Services:

- ⇒ Dissemination of Information Security News, including virus alerts, advisories, vulnerability notes and warnings on latest cyber-attacks
- ⇒ Awareness campaigns on different Information Security themes for corporates, youngsters and the public in general
- ⇒ Organisation of international events such as Safer Internet Day and Computer Security Day
- ⇒ Organization of professional trainings on Information Security areas
- ⇒ Provision of educational materials through publications (includes guidelines, e-security newsletters, brochures, booklets, flyers) and a dedicated cyber security portal

Security Quality Management Services:

- ⇒ Assistance to organisations for the implementation of Information Security Management System (ISMS) based on ISO 27001
- ⇒ To conduct third party information security audits
- ⇒ To carry out technical security assessment of ICT infrastructure of organisations

Cyber Security Portal

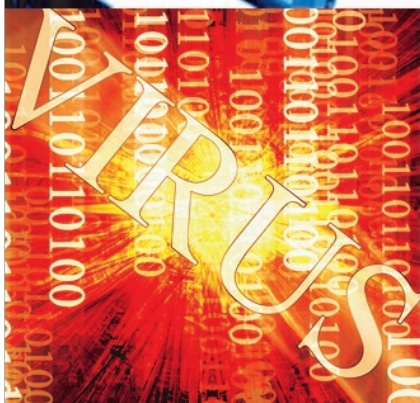
The Cyber Security Portal is an initiative of CERT-MU to sensitise and raise awareness of the general public on technological and social issues facing Internet users .

The Portal consists of Internet best practices for:

- ⇒ Organisations
- ⇒ Parents
- ⇒ Kids
- ⇒ Home users

More information is available on:

www.cybersecurity.ncb.mu



IN THIS ISSUE

Featured



Understanding, Preventing & Responding to Ransomware Attacks



CERT-MU Is Now ISO 27001:2013 Certified



Cyber Security in Healthcare

News Section



The Petya Cyber Attack



SamSam Ransomware

Technology Watch



Parental Control Software : K9 Web Protection

Security Tips



Our Top 10 Security Tips





Dear Readers,

Greetings from CERT-MU and welcome to the first issue of CERT-MU eSecurity Newsletter for the year 2017.

We are pleased to inform you that CERT-MU is now ISO 27001: 2013 Certified. This certification will allow CERT-MU to have greater confidence in their information security management and will be able to use the certificate to help assure trading partners with whom they share information.

This e-Security Newsletter is aimed at providing our key readers an overview of the key developments on the information security arena.

This edition covers in depth information about the burning topic - "Ransomware", which is one of the main cyber security challenge that organisations and users across the world is facing. To address this issue, our main article is based on understanding, preventing and responding to ransomware attacks. In this article, emphasis has been laid on the rise and different types of crypto ransomware, new attack techniques of ransomware and the various infection vectors. At the same time, the article also reflects the most affected platforms and advanced attack techniques that are employed by cybercriminals to carry out ransomware attacks. Finally, the preventive measures are discussed.

Our second article covers cyber security the healthcare sector. Healthcare organisations are becoming the primary targets of cybercriminals due to the large amount of sensitive data that are processed. Thus, the importance of cyber security is highlighted in this article and recommendations that these organisations can take to improve cybersecurity in the sector are discussed.

Other issues highlighted in this e-security newsletter include latest information security news, technology updates, best practices and tips.

We hope that you will find the articles interesting and enjoy reading!

Sign up to our
Newsletter

subscribe@cert.ncb.mu



CERT-MU Is Now ISO 27001:2013 Certified

The Computer Emergency Response Team of Mauritius (CERT-MU) is now ISO 27001: 2013 Certified. The objective of an Information Security Management System based on ISO 27001 is to provide organisations with a common basis for maintaining information security and to allow the secure sharing of information between organisations.

Certification of an organisation's Information Security Management System is a means of providing assurance that the certified organisation has implemented a system for the management of information security in line with the standard ISO 27001. This should serve as a foundation for the interests of international trade.

ISMS certification ensures that the certified organisation has undertaken a risk assessment and has identified and implemented controls appropriate to the information security needs of the business.

Organisations that successfully complete the certification process can have greater confidence in their information security management and will be able to use the certificate to help assure trading partners with whom they share information. The certificate makes a public statement of capability whilst permitting the organisation to keep details of its information security measures confidential.

The certification to the ISO 27001:2013 Standard will provide the following benefits to CERT-MU:

- ⇒ It makes a public statement of capability whilst permitting CERT-MU to maintain the confidentiality and integrity of its information and systems, including the online incident reporting system, thus given assurance to incident reporters in terms of privacy.
- ⇒ This certification will allow CERT-MU to gain credibility, trust and confidence of its constituents and also provides a competitive advantage. Thus, it will lay the foundation for CERT-MU to target its constituents on a larger scale for the implementation of the ISMS service which it provides to parastatal and private organisations since 2010.
- ⇒ It will also provide an effective way of reducing the risk of suffering a data breach.



Understanding, Preventing & Responding to Ransomware Attacks



priority. While a multilayered approach to security minimises the chance of infection, it's also vital to educate end users about ransomware and encourage them to adopt best practices. As ransomware gangs continue to refine their tactics, organisations cannot become complacent. Businesses should continue to review and improve their security and have an effective incident response plan in the face of this rapidly evolving threat.

Ransomware Variants

Ransomware is a growing criminal activity involving numerous variants. Since 2012 when police locker

Ransomware has quickly emerged as one of the most dangerous cyber threats facing both organisations and consumers, with global losses now likely running to hundreds of millions of dollars. The latest global ransomware cyber-attack WannaCry has created havoc in the world with more than 150 countries affected and hundreds thousands computers infected. The past 2 years have seen an increase in ransomware attacks, which have reached a new level of maturity and menace. The distribution of malware in such type of attacks is widely spread and is targeting millions of computers. Users who are victim to ransomware attacks find their valuable data locked with strong, often unbreakable encryption. The lucrative ransomware business model has created a gold-rush mentality amongst cyber criminals, as growing numbers seek to cash in. The rate of infection are climbing with the number of new ransomware families are being discovered. Today, the average ransom demanded by attackers has jumped to US\$679. (Source: *Special Report, Ransomware and Businesses, Symantec 2016*)

Attacks against organisations are slowly increasing. While wide-scale, indiscriminate ransomware campaigns remain the most prevalent form of threat, new and more advanced attacks are emerging. A growing number of ransomware gangs are beginning to focus on targeted attacks against large organisations. These attacks require high technical expertise to break into and traverse the target's network.

Although it is more complex and time-consuming to perform a successful targeted attack on an organisation, the attack can potentially infect thousands of computers, thus causing massive operational disruption and serious damage to revenues and reputation. Once cybercriminals see some businesses accede to these attacks and pay the ransom, more attackers will follow suit in a bid to grab their share of the potential profits.

Organisations need to be fully aware of the threat posed by ransomware and make building their defenses an ongoing

ransomware variants first emerged, ransomware variants have become more sophisticated and destructive. Some variants encrypt not just the files on the infected device, but also the contents of shared or networked drives, externally attached storage media devices, and cloud storage services that are mapped to infected computers. These variants are considered destructive because they encrypt users' and organisations' files, and render those files useless until a ransom is paid.

Recent investigations revealed that ransomware authors continue to improve ransomware code by using anonymizing services like "Tor 3" for end-to-end communication to infected systems and Bitcoin virtual currency to collect ransom payments. Currently, the top ransomware variants targeting companies and individuals are CryptoWall, CTBLocker, Petya, TeslaCrypt, MSIL/Samas/SamSam and Locky. New ransomware variants are continually emerging.

WannaCry Ransomware

The WannaCry ransomware attack was a worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments of \$300 US dollars in the Bitcoin cryptocurrency. The attack began on Friday, 12 May 2017, and within a day was reported to have infected more than 230,000 computers in over 150 countries.

Parts of Britain's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide. Shortly after the attack began, a web security researcher who blogs as "MalwareTech" discovered an effective kill switch by registering a domain name he found in the code of the ransomware. This greatly slowed the spread of the infection, effectively halting the initial outbreak on Monday, 15 May 2017, but new versions have since been detected that lack the kill switch.

WannaCry propagates using EternalBlue, an exploit of Windows' Server Message Block (SMB) protocol. Much of the attention and comment around the event was occasioned by the fact that the U.S. National Security Agency (NSA) had discovered the vulnerability in the past, but used it to create an exploit for its own offensive work, rather than report it to Microsoft. It was only when the existence of this vulnerability was revealed by The Shadow Brokers that Microsoft became aware of the issue and issued a "critical" security patch on 14 March 2017 to remove the underlying vulnerability on supported versions of Windows, though many organisations had not yet applied it.

CryptoWall

CryptoWall and its variants have been actively used to target victims since April 2014. CryptoWall was the first ransomware variant that only accepted ransom payments in Bitcoin. The ransom amounts associated with CryptoWall are typically between \$200 and \$10,000. Following the takedown of the CryptoLocker botnet, CryptoWall has become the most successful ransomware variant with victims all over the world. Between April 2014 and June 2015, IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over \$18 million. CryptoWall is



primarily spread via spam email but also infects victims through drive-by downloads and malvertising.

CTB-Locker

CTB-Locker emerged in June 2014 and is one of the first ransomware variants to use Tor for its C2 infrastructure. CTB-Locker uses Tor exclusively for its C2 servers and only connects to the C2 after encrypting victims' files. Additionally, unlike other ransomware variants that utilise the Tor network for some communication, the Tor components are embedded in the CTB-Locker malware, making it more efficient and harder to detect. CTB-Locker is spread through drive-by downloads and spam emails.

TeslaCrypt

TeslaCrypt emerged in February 2015, initially targeting the video game community by encrypting gaming files. These files were targeted in addition to the files typically targeted by ransomware (documents, images, and database files). Once the data was encrypted, TeslaCrypt attempted to delete all Shadow Volume Copies and system restore points to prevent file recovery. TeslaCrypt was distributed through the Angler, Sweet Orange, and Nuclear exploit kits.

MSIL/ Samas/ SAMSAM

MSIL/ Samas/SAMSAM) was used to compromise the networks of multiple victims, including 2016 attacks on healthcare facilities that were running outdated versions of

the JBoss content management application. SAMSAM exploits vulnerable Java-based Web servers. SAMSAM uses open-source tools to identify and compile a list of hosts reporting to the victim's active directory. The actors then use psexec.exe to distribute the malware to each host on the network and encrypt most of the files on the system.



The actors charge varying amounts in Bitcoin to provide the decryption keys to the victim.

Locky

In early 2016, a destructive ransomware variant, Locky, was observed infecting computers belonging to businesses globally, including those in the United States, New Zealand, Australia, Germany and the United Kingdom. Locky propagates through spam emails that include malicious Microsoft Office documents or compressed attachments (e.g., .rar, .zip) that were previously associated with banking Trojans such as Dridex and Pony. The malicious attachments contain macros or JavaScript files to download the Locky files. Recently, this ransomware has also been distributed using the Nuclear Exploit Kit.

Links to Other Types of Malware

Systems infected with ransomware are also often infected with other malware. In the case of CryptoLocker, a user typically was infected by opening a malicious attachment from an email. This malicious attachment contained Upatre, a downloader, which infected the user with GameOver Zeus. GameOver Zeus was a variant of the Zeus Trojan used to steal banking information and other types of data. After a system became infected with GameOver Zeus, Upatre would also download CryptoLocker. Finally, CryptoLocker encrypted files on the infected system and demanded a ransom payment. The disruption operation against the GameOver Zeus botnet also affected CryptoLocker, demonstrating the close ties between ransomware and other types of malware. In June 2014, an international law enforcement operation successfully weakened the infrastructure of both GameOverZeus and CryptoLocker.

THE RISE OF CRYPTO-RANSOMWARE

Security researchers noted a noticeable trend shifting towards crypto-ransomware. The trend continued into 2016 onwards. Ten years ago, the market was dominated with misleading applications, many of which were designed to pose as antivirus software. These risks informed users that something was wrong with their computer, such as a malware infection or software fault. The attackers then requested payment to "fix" the problem. Locker-type threats later posed as fake antivirus apps. Lockers block access to an infected device but do not encrypt or delete any files. If the malware is removed, full access to the device is usually restored. After enjoying a brief heyday in 2012 and 2013, lockers have steadily declined, with crypto-ransomware taking over.

The shift towards crypto-ransomware can be explained by the fact that it is usually the most effective form of ransomware. If implemented correctly, crypto-ransomware will use unbreakable encryption on the user's files. Removing the malware will not solve the problem; the user will still be left with inaccessible files. If the victim has no backups of these files, then paying the ransom may be the only way to recover them. The crypto-ransomware business model has been perfected over the past two years and it is hardly surprising that it is now dominating the scene.

NEW ATTACK TECHNIQUES

Ransomware attacks have evolved and became more sophisticated over the past years as attackers have added new techniques to their arena. Several new ransomware families have been coded in different programming languages such as JavaScript, PHP, Powershell or Python. These languages are used to bypass detection by security products.

A number of high-profile ransomware families have also begun to add features beyond the core functionality of locking devices or encrypting files. For example, the latest ransomware WannaCry (Ransom: Win32/WannaCrypt) which affected more than 150 countries worldwide does not require user interaction to encrypt files. It spreads itself within corporate networks, without user interaction, by exploiting a vulnerability in the Server Message Block (SMB) remote code execution vulnerability in Microsoft Windows.

Another variant of the Crypto Ransomware family, CryptXXX (Trojan.Cryptolocker.AN) have an additional feature that allows it to gather Bitcoin wallet data and send it to the attackers. Cerber (Trojan.Cryptolocker.AH) is capable of adding the infected computer to a botnet which can be used to carry out distributed denial of service (DDoS) attacks. Moreover, Chimera (Trojan.Ransomcrypt.V) makes an additional threat in its ransom message. In addition to encrypting files, the malware threatens to post the victims files, including pictures and videos, on the internet. The adoption of these new techniques demonstrates how ransomware is continuously evolving to maintain its foothold and remain profitable.

ORGANISATIONS TO BE MOSTLY INFECTED

Almost every sector has been affected by ransomware in recent years, but certain sectors were more targeted. An Analysis of infections carried out by Symantec in 2016 in known sectors indicated that between January 2015 and April 2016, the Services sector, with 38 percent of infected computers, was by far most affected by ransomware (source: Symantec, 2016). Other sectors which were affected include Manufacturing, Finance, Insurance, Real Estate, Public Administration, Transportation, Communications, Utilities, Retail Trade, Construction, Mining and Agriculture, Forestry and Fishing. Certain sectors are more affected than others due to the high dependency on different Internet services and this tends to have a higher exposure to infection risks.

THE GROWTH FACTORS OF RANSOMWARE

During the past two years, security analysts have noted an effective growth in the crypto-ransomware market. The ransomware business model has been driven by a number of key factors, which include:

Encryption

One of the main factors of growth has been the easy availability of strong encryption implementations, which has helped malicious actors to create powerful threats. Effective deployment of encryption was one of the main obstacles attackers have had to overcome, and they have made significant strides in recent years. Early variants of crypto-ransomware often had obvious design flaws. The errors included leaving the encryption key on the infected computer or using the same encryption key for all infections, which meant anyone who obtained the key could share it with other victims. While such mistakes still occur, they are now far less common. The latest ransomware families generate new unique keys for each infection. Many of the recent generations of ransomware use a combination of symmetric and asymmetric encryption. Symmetric encryption uses the same private key for encrypting and decrypting files. The advantage symmetric encryption provides is that it can quickly encrypt files. This is important for attackers since they wish to complete encryption before the infection is discovered. The downside of symmetric encryption for the attackers is that if the key is discovered during encryption, the victim can use it to decrypt all the data.

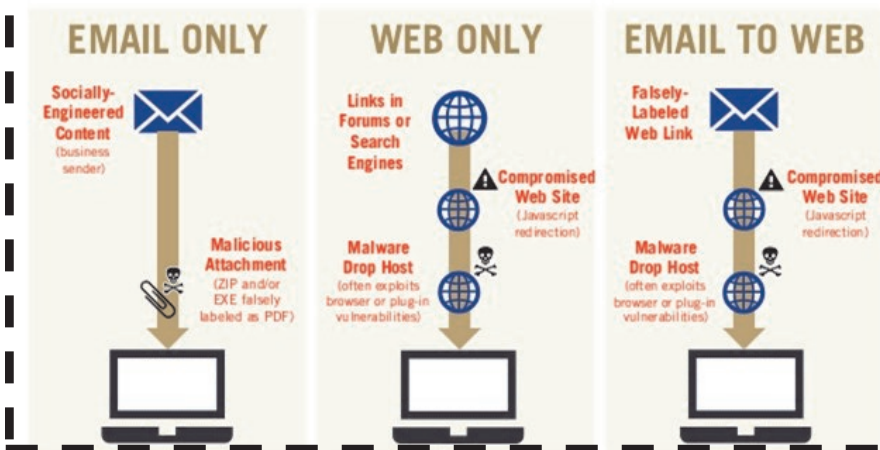
Advent of Cryptocurrencies

Ransom payment has always proved a challenge for cybercriminals, who need a method that is easily accessible to victim and easily convertible to cash but also untraceable. Previously attackers relied largely on payment vouchers. The rise of Bitcoin and other cryptocurrencies provided an



alternative that operates outside the traditional financial system. Although not entirely anonymous, Bitcoin movements can be obfuscated by moving through chains of wallets and tumbler services. Bitcoin wallets are free and disposable, meaning attackers can generate a new, unique wallet for each infection, making it more difficult for law enforcement to follow all earnings. Widespread public awareness of Bitcoin also means that victims may be less suspicious of the cryptocurrency, so are more likely to buy bitcoins and pay the ransom. Some ransomware families have experimented with voucher cards for online shops as payment, such as iTunes gift cards, but with not as much success, as they are easier to trace and harder to cash out.

MULTIPLE ATTACK VECTORS



and malware in general, is through malicious spam email. This spam is distributed using botnets - networks of compromised computers, ranging from hundreds to millions of infected computers. The botnet sends out large numbers of spam emails that use social-engineering tactics to trick recipients into compromising their computers. Infection may occur if the user performs any of the following actions:

- ⇒ Opens a malicious attachment that directly installs the ransomware
- ⇒ Opens a malicious attachment that initiates a second-stage delivery through a downloader (usually a macro), which subsequently downloads and installs the ransomware.

Effective Infection Vectors

Developing an effective form of ransomware is only half the battle for attackers. They also need to ensure that their ransomware spreads to as many users as possible. The past year has seen some ransomware groups, such as TeslaCrypt and Locky, mount major spam campaigns. This resulted in millions of users being hit on an almost daily basis. Even if only a small fraction became infected, the attackers behind these compromises would be likely to profit significantly. In addition to this, several major exploit kits have been observed distributing ransomware. For example, in recent months, the Angler exploit kit was one of the main delivery channels for CryptXXX. The Neutrino exploit kit has been spotted pushing a number of ransomware variants including Locky, Cerber, and CryptoWall (Trojan.Cryptowall).

- ⇒ Clicks a link that points to an exploit kit which will ultimately lead to the malware being installed on the computer.

The spam used to distribute ransomware often takes the form of an important email from a well-known organisation, such as the following:

- ⇒ A notification from the post office or another shipment company, informing the recipient of a delivery
- ⇒ A message from a utility provider about an overdue bill
- ⇒ An alert about the recipient's tax return
- ⇒ Invoices for goods and services
- ⇒ Fake credit card reward schemes

Advanced Attack Techniques

A number of ransomware groups have begun using advanced attack techniques to mount targeted attacks against organisations. The level of expertise employed in these attacks is similar to that seen in many cyberespionage attacks. Attackers have managed to gain a foothold on networks by exploiting vulnerabilities in public-facing web servers and then traversing the network using legitimate tools, before identifying and infecting hundreds of computers. The time and skill required to mount such attacks is far in excess of that required for standard ransomware campaigns, but the rewards are potentially much greater.

Ransomware-as-a-Service

The emergence of RaaS has made entry into the ransomware arena possible for many who would otherwise be excluded. It is now possible for someone with relatively little skill to pay for a ransomware executable and access to a user interface to track their victims. The RaaS creators then sit back and wait for their customers to distribute the malware, earning a percentage of the profits.

INFECTION METHODS

There are multiple ways ransomware can infect a computer, some of which are more prevalent than others. They are as follows:

Malicious Email

One of the most common methods to spread ransomware,

Each spam variation relies on users' inherent instinct to act on messages that appear to be urgent. Attackers employ various tactics to help them effectively spread ransomware through spam email. For example, Windows Script Files (WSF) is used to bypass email filtering. Files with the .wsf extension can be launched like an executable file. Once the email attachment a zipped folder appearing to contain a .doc file is opened, the .wsf file is executed and CryptoWall is installed on the victim's computer.

Exploit Kits

Exploit kits (EKs) are another predominant infection vector for ransomware. These toolkits exploit vulnerabilities in software in order to install malware. Exploit kit attackers compromise third-party web servers and inject iframes into the web pages hosted on them. The iframes direct browsers to the exploit kit servers. Attackers can redirect users to EKs in the following ways:

- ⇒ Malicious links in spam email or social media posts
- ⇒ Malvertisements
- ⇒ Redirected web traffic from traffic distribution services

The criminals behind these kits rely on users running outdated or unpatched software on their computers and, unfortunately, have an overabundance of potential targets. While email and exploit kits are the two main methods used to spread ransomware, the other techniques are also deployed such as malvertising, brute forcing passwords, exploiting server vulnerabilities, self-propagation, SMS messages and third part app stores.

The criminals behind these kits rely on users running outdated or unpatched software on their computers and, unfortunately, have an overabundance of potential targets. While email and exploit kits are the two main methods used to spread ransomware, the other techniques are also deployed such as malvertising, brute forcing passwords, exploiting server vulnerabilities, self-propagation, SMS messages and third party app stores.

MOST AFFECTED PLATFORMS BY RANSOMWARE

Although attacks against Windows continue to dominate the ransomware landscape, there have been a growing number of ransomware campaigns against other platforms. Some of the most affected platforms are:

Windows

Most attack groups simply attempt to infect as many com-



puters as possible to maximize their returns. As a result, the majority of ransomware variants are designed to attack Windows computers. For example the WannaCry Ransomware which appeared on the 12th May 2017 also targeted the Windows platform by exploiting a vulnerability in the Windows SMB.

Windows home users continue to be one of the biggest victim groups. In comparison to businesses, home users are less likely to use security software or keep up-to-date backups of valuable data, making their computers more vulnerable to attack. While home users may not have the means to pay large ransoms, the sheer volume of potential victims means that they can still be a highly lucrative target.

Businesses are also affected by the same ransomware attacks hitting home users. If the organisation is not protected, the consequences could be devastating. While the home user may be faced with a \$500 ransom demand for one infected computer, the ransom demand for multiple infections at an organisation could quickly rack up to tens of thousands of dollars. In addition to these wide-scale attacks, ransomware groups are now showing a growing interest in specifically targeted organisations.

Mobile Phones

Given the popularity of smartphones, it is not surprising that ransomware attackers are increasingly looking to compromise these devices. A number of Android threats have emerged in recent years, the majority of which are locker-type threats. However, crypto-ransomware for Android devices has also emerged in the form of the Russian-language Simplocker (Android.Simplocker) and its English-language variant (Android.Simplocker.B). At present, there have been no documented cases of iOS-specific ransomware, but web-based variants do affect iOS devices.

Mac OS X

Until recently, ransomware groups mostly ignored Mac OS X users. In March 2016, a threat known as KeRanger (OSX.Keranger) became the first widespread ransomware to target the Mac OS X operating system. KeRanger was briefly distributed in a compromised version of the installer for the Transmission BitTorrent client. KeRanger behaved similarly to modern Windows ransomware, searching for and encrypting approximately 300 different file types before demanding a ransom of one bitcoin (US\$678 at the time of writing). The malware was signed with a valid Mac Developer ID. This meant that KeRanger could bypass Mac OS X's Gatekeeper feature, which is designed to block software from untrusted sources. Apple quickly revoked the Developer ID that KeRanger used.



PREVENTING AND RESPONDING RANSOMWARE ATTACKS

Educate Your Personnel

Attackers often enter the organisation by tricking a user to disclose a password or click on a virus-laden email attachment. Remind employees to never click unsolicited links or open unsolicited attachments in emails.

To improve workforce awareness, the internal security team may test the training of an organisation's workforce with simulated phishing emails.

Proactive Prevention is the Best Defense

Prevention is the most effective defense against ransomware and it is critical to take precautions for protection. Infections can be devastating to an individual or organisation, and recovery may be a difficult process requiring the services of a reputable data recovery specialist. Users and administrators are recommended take the following preventive measures to protect their computer networks from falling victim to a ransomware infection:

Preventive Measures

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralised patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

Business Continuity Considerations

- Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it is working.
- Conduct an annual penetration test and vulnerability assessment.
- Secure your backups. Ensure backups are not connected permanently to the computers and networks they are backing up.

In case of Ransomware infection, the following steps are recommended:

- Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking networked or shared drives.
- Isolate or power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
- Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
- If available, collect and secure partial portions of the ransomed data that might exist.
- If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.
- Delete Registry values and files to stop the program from loading
- Contact CERT-MU for advice.

⇒ Implement your security incident response and business continuity plan

Ideally, organisations will ensure they have appropriate

backups, so their response to an attack will simply be to restore the data from a known clean backup. Having a data backup can eliminate the need to pay a ransom to recover data.

⇒ There are serious risks to consider before paying the ransom.

It is not advised paying a ransom to criminal actors. However, after systems have been compromised, whether to pay a ransom is a serious decision, requiring the evaluation of all options to protect shareholders, employees, and customers.

- Victims will want to evaluate the technical feasibility, timeliness, and cost of restarting systems from backup. Ransomware victims may also wish to consider the following factors:
- Paying a ransom does not guarantee an organisation will regain access to their data; in fact, some individuals or organisations were never provided with decryption keys after paying a ransom.
- Some victims who paid the demand were targeted again by cyber actors.
- After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

More information about Ransomware:

[CERT-MU WhitePaper on the WannaCry Ransomware Guideline on Ransomware Removal](#)



Law enforcement and IT Security companies have joined forces to disrupt cybercriminal businesses with ransomware connections. The “**No More Ransom**” website is an initiative by the National High Tech Crime Unit of the Netherlands’ police, Europol’s European Cybercrime Centre and two cyber security companies – Kaspersky Lab and Intel Security – with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

The “**No More Ransom**” platform offers 39 decryption tools, all free. Useful tools and manuals have also been uploaded to the website to help either mitigate the results of ransomware attack or to prevent those attacks.

Cyber Security in Healthcare



Cyber-attacks in the healthcare sector are increasing at an alarming rate. More than 100 million healthcare records were compromised in 2015, according to a report published by IBM. In fact, 2015 was named as the year of the healthcare breach as per IBM's 2016 Cyber Security Intelligence Index. Health records contain a wealth of information that can be used for medical identity theft and fraud. These records typically contain credit card data, email addresses, social security numbers, employment information and medical history records, much of which will remain valid for years. This information can be used to launch cyber-attacks such as spear phishing attacks, commit fraud and steal medical identities.

As per security experts, the healthcare sector is an appealing target for cybercriminals because the industry's approach to cybersecurity is behind the times. A survey conducted by Sophos in 2016 found an alarming laxity in many organisations' approach to data security. The survey indicated that the healthcare sector had the lowest rates of data encryption. Another survey carried out by Sophos on the National Service (NHS) organisations in the UK found that encryption was well established in just 10% of them; while a 2016 study of hospital cybersecurity found that patient health records are "extremely vulnerable" because of a lack of focus on cyberattacks and insufficient training. Beyond data breaches perpetrated by hackers, health data is frequently exposed through accidental loss, device theft and employee negligence.

There are certain factors due to which healthcare organisa-

tions are facing increased security threats and they are:

- ⇒ Adoption of digital patient records and the automation of clinical systems
- ⇒ The use of antiquated Electronic Medical Record (EMR) and clinical applications that are not designed to securely operate in today's networked environment and software vendors who push that problem to the provider.
- ⇒ The ease of distributing electronic Protected Health Information (ePHI) both internally (laptops, mobile devices, thumb drives) and externally (third parties, Cloud services).
- ⇒ The heterogeneous nature of networked systems and applications (i.e. network-enabled respirator pumps on the same network as registration systems that can browse the Internet).
- ⇒ The evolving threat landscape, where cyber-attacks today are more sophisticated and well-funded given the increased value of the compromised data on the black market.

The healthcare sector has become the primary targets of malicious hackers as cyberattacks are becoming increasingly sophisticated and disruptive to operations. The dramatic increase in hacking attacks in 2016, coupled with the large number of patient records compromised in those incidents, points to a pressing need for providers to take a much more proactive and comprehensive approach to protecting their information assets.

With the changing nature, depth and consequences of cyberattacks in healthcare, the nature of preventing, monitoring and managing those threats requires a new approach. Some of the recommendations that the healthcare organisations can take to improve cybersecurity in the sector are:

Increase the security and resilience of medical devices and health IT

The Healthcare Sector is charged with keeping patients safe and that includes protecting patients and their information. This includes physical and privacy related harms that may stem from vulnerability or exploit. If the exploited, a vulner-



ability may result in medical device malfunction, disruption of health care services (including treatment interventions), and inappropriate access to patient information, or compromised EHR data integrity. Such outcomes could have a profound impact on patient care and safety. Some foundational challenges that will need to be addressed in order to enhance the cybersecurity of medical devices and EHRs include legacy operating systems, secure development lifecycle, strong authentication, and strategic and architectural approaches to product deployment, management, and maintenance on hospital networks.

Employ strategic and architectural approaches to reduce the attack surface for medical devices, EHRs, and the interfaces between these products

The healthcare sector need to take a long-range approach to considering viability, effectiveness, security, and maintainability of those products when setting up the IT network and at the outset of product deployment. The desired end-state is that every product (whether new or when it is being upgraded) have a defined strategy, architectural approach, and design that supports the deployment and overall lifecycle management of that product.

Establishment of a Computer Security Incident Response Team (CSIRT)

Establish a CSIRT to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures. There is a need for a CSIRT that focuses on medical devices because of the inherent impacts to patient safety when vulnerabilities are disclosed and/or exploited. The CSIRT would have a broad range of expertise (including hardware, software, networking, biomedical engineering,

and clinical) that will enable it to understand the patient safety implications of incidents and vulnerabilities, and comprehensively coordinate responses.

Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities

Every sector faces challenges in meeting its need to recruit and retain qualified cybersecurity professionals. Due to the rise in IT adoption in the health care industry, there is a need to develop and train employees in the areas of cyber security and improve technical capabilities. These can include tailored technology workshops in cybersecurity and healthcare.

Secure legacy systems

Legacy systems include both legacy medical devices and legacy EHR applications, which may not have any ongoing support from the hardware and software vendors that provided these solutions. They may impact the entire system or system components, including firmware, drivers, operating systems, and all applications in use. Many of these legacy systems have security weaknesses, which may contribute to the compromise of provider networks and systems.



Identify best practices for governance of cybersecurity across the healthcare sector

Effective cybersecurity requires leadership at all levels of the organisation. Not every organisation is able to find, recruit, and retain cybersecurity expertise. The healthcare sector needs cybersecurity governance models that work for organisations of all sizes and provider types. Governance is an issue of responsibility and authority, not specific cybersecurity expertise. Management of these organisations must be engaged in key activities that include: identifying, valuing, protecting, and managing assets and risks; establishing governance to include appropriate controls, training, processes, and procedures; and security incident response planning, readiness, and communications to ensure timely handling of and recovery from cyber events.

Identify the cybersecurity leadership role for driving for more robust cybersecurity policies, processes, and functions with clear engagement from executives

Accountability and responsibility for cybersecurity in an organisation is often poorly defined and many healthcare organisations view cybersecurity as an IT problem. Organisations need to identify a cybersecurity leader to drive change. In many organisations, this may be the Chief Information Security Officer (CISO) role.

Increase healthcare industry readiness through improved cybersecurity awareness and education

Cybersecurity can be an enabler for the healthcare industry, supporting both its business and clinical objectives, as well as facilitating the delivery of efficient, high-quality patient care. However, this requires a holistic cybersecurity strategy. Organisations that do not adopt a holistic strategy not only put their data, organisations, and reputation at risk, but also most importantly the welfare and safety of their patients.



Cybersecurity must be governed with a collaborative approach whereby all members of the health care industry work together towards the common goal of protecting one another and the sector's most critical assets – patients. To achieve this, an educated workforce and an informed public is required who make evidence-based decisions and that are reliant on cyber-secure data.

Cyber Security Healthcare Event 2017

Cyber Security Exchange 1 Healthcare

September 13-15 | Dallas, Texas

Top Data Breaches in Healthcare

National Health Service (NHS) in England hit by the WannaCry Ransomware in May 2017

NHS services across England and Scotland have been hit by a large-scale cyber-attack that has disrupted hospital and GP appointments. Some hospitals and GPs have been unable to access patient data, after their computers were locked by a ransomware program demanding a payment worth £230.

Anthem; Second Largest Health Insurer in the United States: 80 Million Records Compromised

Anthem was the victim of the largest data breach in the healthcare industry (to date). In the cyber-attack, occurring in December 2014, Anthem found that hackers might have stolen the names, Social Security numbers, addresses, income data, and health care identification numbers of nearly 80 million customers. In addition, and perhaps equally as concerning, was the fact that Anthem believed, but could not confirm, that medical records or credit cards of customers were compromised.

Premiera Blue Cross; Medical Insurance Company: Over 11 Million Records Compromised Via Hacker Breach

Early in 2015, over 11 million customers' data records were compromised as a result of illicit access to Premiera Blue Cross' networks by an unknown hacker. While information compromised was very similar to the Anthem data breach, Premiera announced that this data breach might have also compromised customers' banking information and detailed insurance claims of customers dating as far back as 2002.

TRICARE; 4.9 Million Patient Records Stolen from Employee's Car

In perhaps one of the most unique incidents of compromised health care records, 4.9 million healthcare records were compromised when the car of a TRICARE subcontractor was broken into; electronic backup tapes containing the patient records were among several items stolen from the car.

Community Health Systems; Operates 200 United States Hospitals: 4.5 Million Patient Records Compromised

Community Health Care Systems fell victim to a cyber-attack resulting from hackers exploiting Heartbleed, a known SSL vulnerability. As a result, 4.5 million patients had their names, dates of birth, and Social Security numbers potentially stolen in a cyber-attack that may have been connected in some way to the Anthem data breach.

NEWS

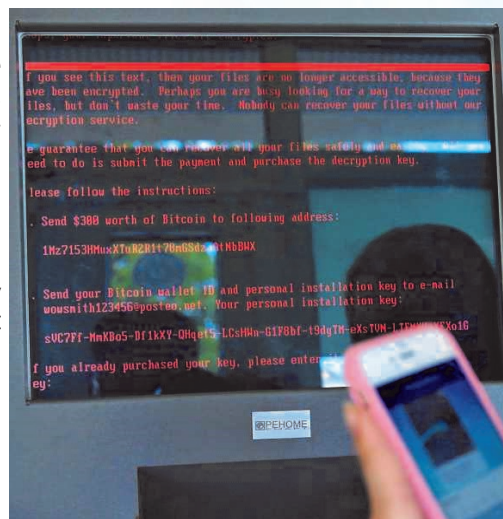


Petya Cyber Attack

The world has witnessed another major cyber-attack known as “Petya” since Tuesday 27th June 2017. The malware is a new variant of the Petya Crypto Ransomware which firstly made its apparition in March 2016. The malware is spreading rapidly with the help of same Windows SMBv1 vulnerability that the WannaCry Ransomware exploited in May 2017 and uses the same NSA EternalBlue Exploit. The exploit, known as “Eternal Blue,” was released online in April 2017 in the latest of a series of leaks by a group known as the Shadow Brokers, who claimed that it had stolen the data from the Equation cyber espionage group.

The first infections began spreading across Europe, most particularly in Ukraine, where more than 12,500 machines encountered the threat. Then infections were observed in another 64 countries, including Belgium, Brazil, Germany, Russia, India and the United States. Many critical systems, organisations, airports, banks and Government departments were affected.

Petya is a ransomware family that works by modifying the Window's system's Master Boot Record (MBR), causing the system to crash. When the user reboots their PC, the modified MBR prevents Windows from loading and instead displays an ASCII Ransom note demanding payment of US \$300 in Bitcoin from the victim to retrieve their individual decryption key.



WARNING!!!
“PETYA”
Ransomware
Cyberattack
Spreading
Worldwide

For more information about the Petya Cyber Attack:


[CERT-MU Whitepaper— The Petya Global Cyber Attack](#)

SamSam Ransomware Attack

Another ransomware attack dubbed as “SamSam” is on the rise and using a targeted approach to infect unpatched servers. The ransomware variant SamSam made its apparition in 2016 and has again resurfaced with new attack techniques. The malware is written in the C# language and once infected, the threat targets over 300 File types to encrypt. Then, a ransom up to \$33,000 is demanded from victims. In 2016, SamSam was used to compromise the networks of multiple U.S. victims, including attacks on healthcare facilities that were running outdated versions of the JBoss content management application.

SAMSAM/MAKTUB

Samas/Samsam/MSIL.B/C

**WARNING!**
Your personal files are encrypted!
11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.
Open <http://maklubuyq@qfny.anton-link>
or <http://maklubuyq@qfny.hardam.org>
or <http://maklubuyq@qfny.farweb.org>

- Exploits known vulnerabilities in unpatched servers.
- Specifically JBOSS.
- 3.2 Million Servers vulnerable.
- Once in, laterally moves to cause the most amount of destruction

Technology Watch: Parental Control Software - K9 Web Protection

The Internet is an incredible tool as it offers the possibility to become part of an enormous virtual community connected by mutual interest. The Internet can provide the younger and the older generations' users with benefits such as independent learning, improved research and communication skills, learn new technologies, access and create resources. ⇒ Logging Features

Children access the Internet for different purposes including entertainment, research, school assignments and to communicate. While doing so, they can often unknowingly place themselves in risky situations. For example by:

Children access the Internet for different purposes including entertainment, research, school assignments and to communicate. While doing so, they can often unknowingly place themselves in risky situations. For example by:

- ⇒ Giving out personal information about themselves to people or organisations they do not know
- ⇒ Posting inappropriate information on the Internet
- ⇒ Accepting to meet people they have met online, without speaking to their parent
- ⇒ Sharing passwords
- ⇒ Posting public profiles about themselves
- ⇒ Unsafe browsing or searching
- ⇒ Opening messages from people they do not know
- ⇒ Responding to unpleasant or suggestive messages
- ⇒ Accessing illegal or inappropriate material.

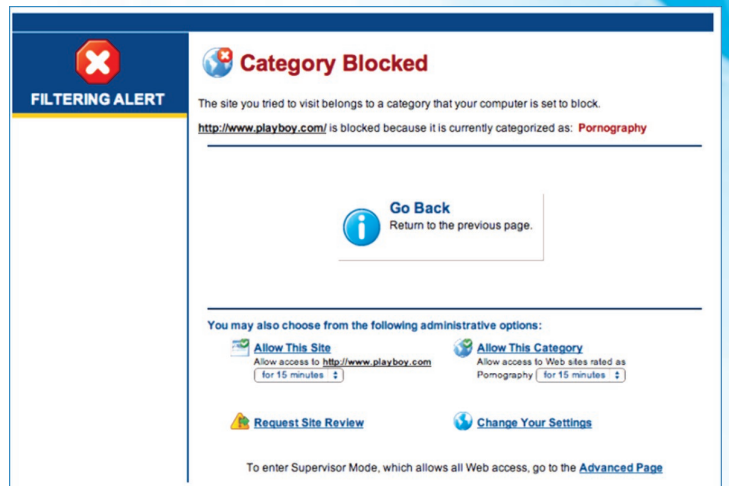
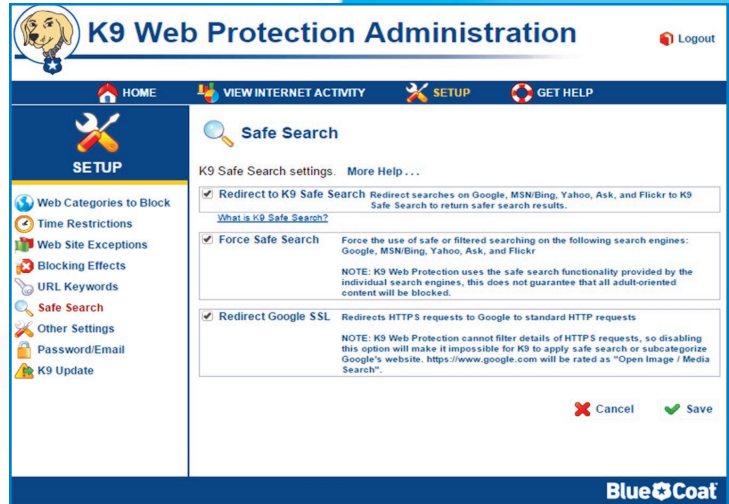
It is therefore imperative for parents to watch out what their kids are doing online. However, it may be impractical for a parent to sit and watch a child for hours while they do their homework, or parents may still be at work when their kids get home from school. Some kids are just a bit mischievous and sneak onto the computer late at night to play games or chat with their friends. In this situation, parental control software may help in monitoring the activities of children on the Internet.

One such example of a free parental control software is the K9 Web Protection. K9 is a Web filter that determines where the computer user can go inside your Web browser. You use K9 in conjunction with other antivirus, anti-spam or firewall products from vendors such as Computer Associates, McAfee, Symantec, ZoneLabs, Microsoft and others.

K9 Web Protection Features:

Some of the features of K9 are:

- ⇒ Website blocking by category (pornography, violence, racism..)
- ⇒ Safe Search enabled
- ⇒ Time restrictions
- ⇒ Custom "always allow" and "always block" lists for your personal preferences
- ⇒ Reports showing activity to categories of web sites
- ⇒ Real-time categorisation of new web sites
- ⇒ Available in Google play and App Store
- ⇒ Night Guard



The Technical details of K9 are as follows:

- ⇒ Runs on Microsoft Windows (Windows 8, Windows Vista, Windows XP) and Mac OS X
- ⇒ Requires very little disk space, memory, or processing power
- ⇒ Requires K9 Web Protection license before installation, which can be obtained by submitting an email address

The software can be downloaded on:
<http://www1.k9webprotection.com/>

Our Top 10 Security Tips



1. Realise that you are an attractive target to hackers. Do not ever say "It won't happen to me."

2. Practice good password management. Use a strong mix of characters, and don't use the same password for multiple sites. Do not share your password with others, don't write it down, and definitely don't write it on a post-it note attached to your monitor.

3. Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time, no matter how short, lock it up so no one can use it while you're gone. If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.

4. Always be careful when clicking on attachments or links in email. If it is unexpected or suspicious for any reason, don't click on it. Double check the URL of the website the link takes you to: bad actors will often take advantage of spelling mistakes to direct you to a harmful domain.

5. Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a network that you trust. Whether it is a friend's phone, a public computer, or a cafe's free WiFi - your data could be copied or stolen.

6. Back up your data regularly, and make sure your anti-virus software is always up to date.

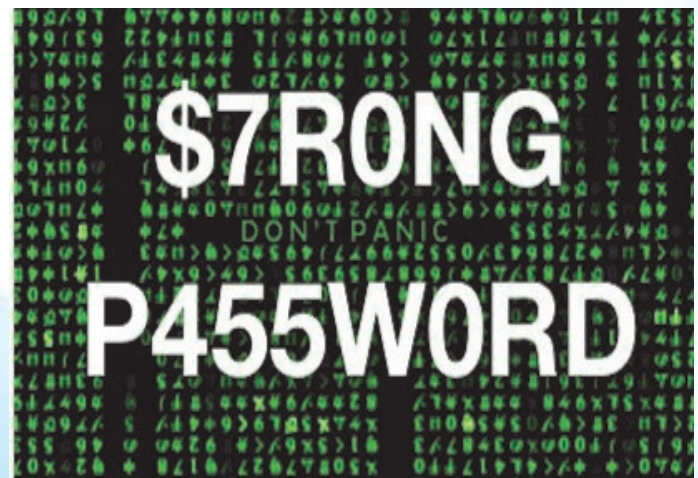
7. Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.

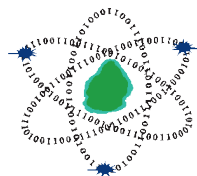
8. Watch what you are sharing on social networks. Criminals can befriend you and easily gain access to a shocking amount of information where you go to school, where you work, when you are on vacation that could help them gain access to more valuable data.

9. Offline, be wary of social engineering, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it's okay to say no. You can always call the company directly to verify credentials before giving out any information.

10. Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, it could be a sign that you've been compromised.

Think Before You Link





CERT-MU

Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudriere Street, Port Louis

Tel: 210 5520

Fax: 208 0119

Website: www.cert-mu.org.mu

Incident Reporting

Hotline: 800 2378

Email: incident@cert.ncb.mu

Vulnerability Reporting

Email: vulnerability@cert.ncb.mu

For Queries

Email: contact@cert.ncb.mu

Subscription to Mailing Lists

Email: subscribe@cert.ncb.mu