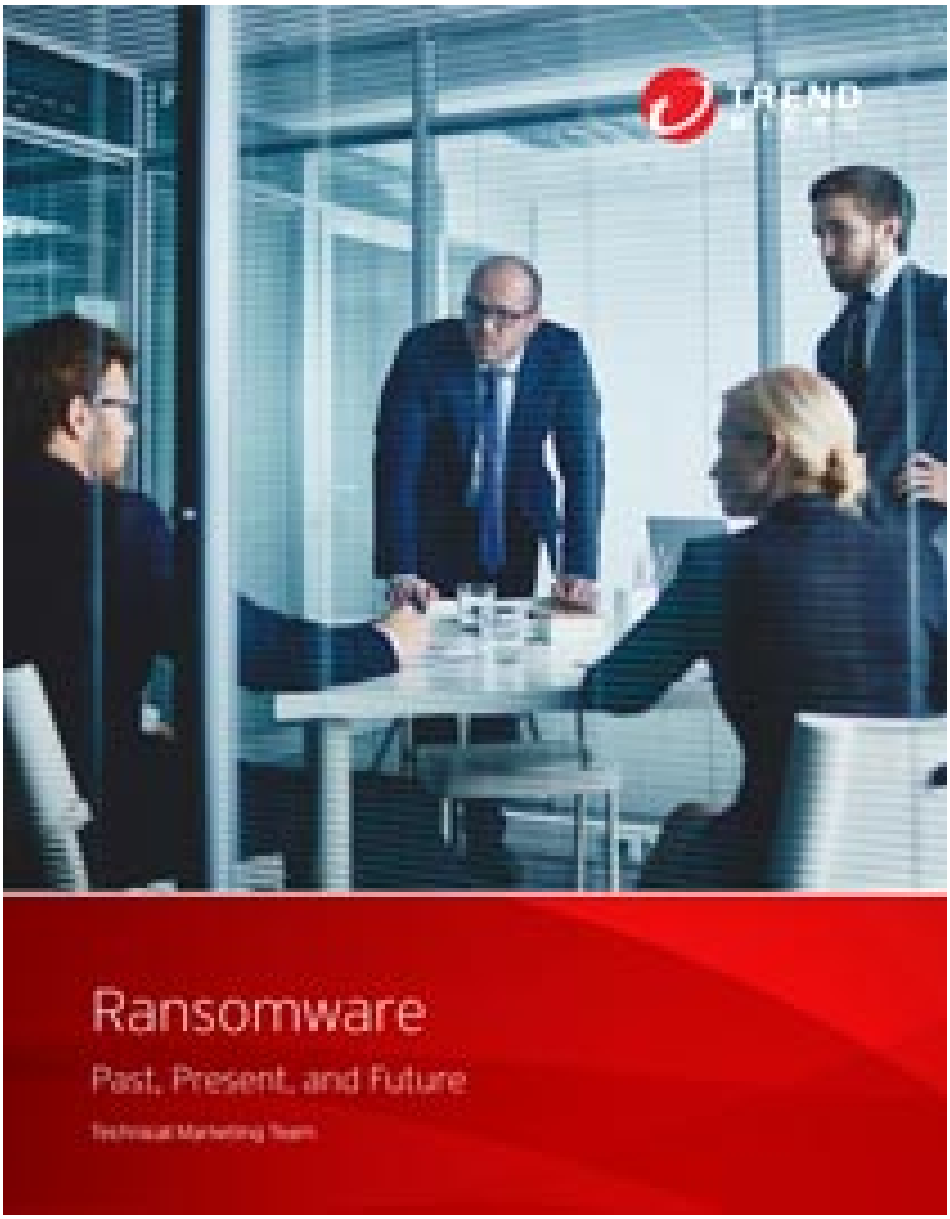
Ransomware



View Ransomware Past, Present, and Future

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively

unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

Ransom Prices and Payment

Ransom prices vary depending on the ransomware variant and the price or exchange rates of digital currencies. Thanks to the perceived anonymity offered b cryptocurrencies, ransomware operators commonly specify ransom payments in bitcoins. Recent ransomware variants have also listed alternative payment option such as iTunes and Amazon gift cards. It should be noted, however, that paying th ransom does not guarantee that users will get the decryption key or unlock tool required to regain access to the infected system or hostaged files.

Ransomware Infection and Behavior

Users may encounter this threat through a variety of means. Ransomware can be downloaded onto systems when unwitting users visit malicious or compromised websites. It can also arrive as a payload either dropped or downloaded by other malware. Some ransomware are known to be delivered as attachments from spammed email, downloaded from malicious pages through malvertisements, or dropped by exploit kits onto vulnerable systems.

Once executed in the system, ransomware can either lock the computer screen, or, in the case of crypto-ransomware, encrypt predetermined files. In the first scenario, a full-screen image or notification is displayed on the infected system's screen, which prevents victims from using their system. This also shows the instructions on how users can pay for the ransom. The second type of ransomware prevents access to files to potentially critical or valuable files like documents and spreadsheets.

Ransomware is considered "scareware" as it forces users to pay a fee (or ransom) by scaring or intimidating them. In this sense, it is similar to FAKEAV malware, but instead of capturing the infected system or encrypting files, FAKEAV shows fake antimalware scanning results to coax users into purchasing bogus antimalware software.

Latest Ransomware News

- Ransomware Recap: Business as Usual after WannaCry Surge
- Ransomware Recap: The Week of WannaCry
- WannaCry/Wcry Ransomware: What Your IT/Sysadmins Need to Do
- WannaCry/Wcry Ransomware: How to Defend against It
- Ransomware Recap: Ransomware as a Service Surge, SLocker Resurfaces

The History and Evolution of Ransomware

Early Years

Cases of ransomware infection were first seen in Russia between 2005 – 2006. Trend Micro published a report on a case in 2006 that involved a ransomware variant (detected as TROJ_CRYZIP.A) that zipped certain file types before overwriting the original files, leaving only the password-protected zip files in the user's system. It also created a text file that acted as the ransom note informing users that the files can be retrieved in exchange for $300.

In its earlier years, ransomware typically encrypted particular file types such as DOC, .XLS, .JPG, .ZIP, .PDF, and other commonly used file extensions.

In 2011, Trend Micro published a report on an SMS ransomware threat that asked users of infected systems to dial a premium SMS number. Detected as TROJ_RANSOM.QOWA, this variant repeatedly displayed a ransomware page to users until they paid the ransom by dialing a certain premium number.

Another notable report involved a ransomware type that infects the Master Boot Record (MBR) of a vulnerable system, preventing the operating system from loading. To do this, the malware copies the original MBR and overwrites it with malicious code. It then forces the system to restart so the infection takes effect and displays the notification (in Russian) once the system restarts.

View infographic: Ransomware 101 - What, How, & Why

Ransomware Spreads Outside Russia

Ransomware infections were initially limited to Russia, but its popularity and profitable business model soon found its way to other countries across Europe. By March 2012, Trend Micro observed a continuous spread of ransomware infection across Europe and North America. Similar to TROJ_RANSOM.BOV, this new wave c ransomware displayed a notification page supposedly from the victim's local polic agency instead of the typical ransom note (see Reveton, Police Ransomware below).

During this period, different tactics were being used to spread ransomware. A cas in 2012 involved a popularFrench confectionaryshop's website that was compromised to serve TROJ_RANSOM.BOV. This watering hole tactic resulted in widespread infections in France and Japan, where the shop also had a significant

fan-base. Instead of the usual ransom note, TROJ_RANSOM.BOV displayed a fake notice from the French police agency *Gendarmerie Nationale*.

The Rise of Reveton and Police Ransomware

Reveton is a ransomware type that impersonates law enforcement agencies. Known as Police Ransomware or Police Trojans, these malware are notable for showing a notification page purportedly from the victim's local law enforcement agency, informing them that they were caught doing an illegal or malicious activity online.

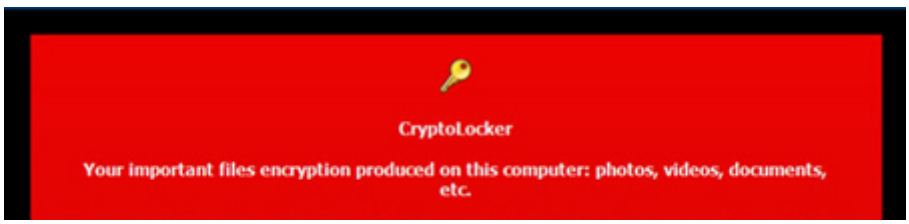
To know which local enforcement agency is applicable to users, Reveton variants track the geographical location of their victims. Thus, affected users living in the U receive a notification from the FBI while those located in France are shown a notice from the *Gendarmerie Nationale*.

Reveton variants also employ a different payment method compared to early ransomware attacks. Once a system is infected with a Reveton variant, users are prompted to pay through *UKash*, *PaySafeCard*, or *MoneyPak*. These payment methods afford ransomware perpetrators anonymity, as both Ukash and PaySafeCard have a faint money trail.

In 2012, different types of Reveton variants were seen exhibiting new techniques. During the latter part of that year, Trend Micro reported on variants that played an audio recording using the victim's native language, and another one bearing a fake digital certificate.

The Evolution to CryptoLocker and Crypto-ransomware

In late 2013, a new type of ransomware emerged that encrypted files, aside from locking the system. The encrypted files ensured that victims are forced to still pay the ransom even if the malware itself was deleted. Due to its new behavior, it was dubbed as "CryptoLocker". Like previous ransomware types, crypto-ransomware demands payment from affected users, this time for a decrypt key to unlock the encrypted files.



Although the ransom note in CryptoLocker only specifies “RSA-2048” as the encryption method used, analysis shows that the malware uses AES + RSA encryption.

RSA is asymmetric key cryptography, which means it uses two keys. One key is used to encrypt the data and another is used to decrypt the data (one key, called the public key, is made available to any outside party; the other is kept by the use and is called the private key.) AES uses symmetric keys, which uses the same key to encrypt and decrypt information.

The malware uses an AES key to encrypt files. The AES key for decryption is writte in the files encrypted by the malware. However, this key is encrypted with an RSA public key embedded in the malware, which means that a private key is needed t decrypt it.

decrypt it.

Further research revealed that a spam campaign was behind the CryptoLocker infections. The spammed messages contained malicious attachments belonging t TROJ_UPATRE, a malware family characterized by its small file size and simple downloading function. It downloads a ZBOT variant, which then downloads the CryptoLocker malware.

Near the end of 2013, a new variant of CryptoLocker emerged —with propagation routines. This variant, detected as WORM_CRILOCK.A, can spread via removable drives, a routine unheard of in other CRILOCK variants. This means that the malware can easily spread compared to other variants. The new variant doesn't rely on downloader malware like CRILOCK to infect systems; rather, it pretends to be an activator for software used on peer-to-peer (P2P) file sharing sites. Technica differences have led some researchers to believe this malware was produced by a copycat.

Another file-encrypting ransomware type soon came into the picture. The crypto-ransomware known as CryptoDefense or Cryptorbit (detected as TROJ_CRYPTRBIT.H) encrypts database, web, Office, video, images, scripts, text, and other non-binary files, deletes backup files to prevent restoration of encrypte files, and demands payment for a decrypt key for the locked files.

The Foray into Cryptocurrency Theft

Ransomware soon began to incorporate yet another element: cryptocurrency (e.g Bitcoin) theft. In 2014, Trend Micro saw two variants of a new malware called BitCrypt. The first variant, TROJ_CRIBIT.A, appends ".bitcrypt" to any encrypted files and displays a ransom note in English. The second variant, TROJ_CRIBIT.B, appends the filename with ".bitcrypt 2" and uses a multilingual ransom note in 10 languages. CRIBIT variants use the encryption algorithms RSA(426)-AES and RSA(1024)-AES to encrypt the files, and specifies tha the payment for unlocking files be made in Bitcoins.

It was discovered that a variant of the FAREIT information stealing malware, TSPY_FAREIT.BB, downloads TROJ_CRIBIT.B. This FAREIT variant can steal information from various cryptocurrency wallets, including *wallet.dat* (Bitcoin), *electrum.dat* (Electrum), and *.wallet* (MultiBit). These files contain important information such as transaction records, user preferences and accounts.

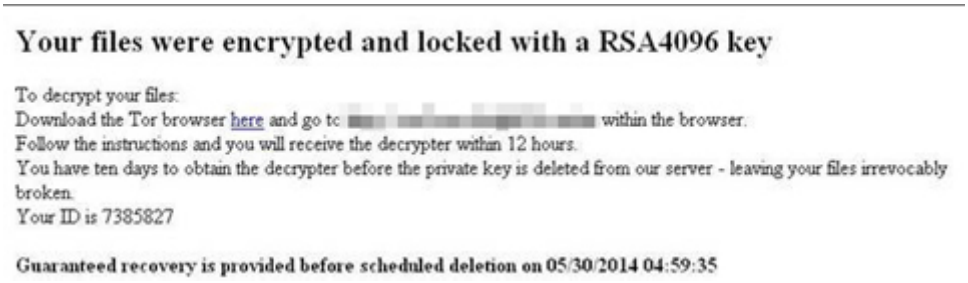
The Angler Exploit Kit

In 2015, the Angler exploit kit was one of the more popular exploit kits used to spread ransomware, and was notably used in a series of malvertisment attacks through popular media such as news websites and localized sites. Angler was constantly updated to include a number of Flash exploits, and was known for being used in notable campaigns such as the Hacking Team leak and Pawn Storm Because of its easy integration, Angler remains a prevalent choice as a means to spread ransomware.

POSHCODER: PowerShell Abuse

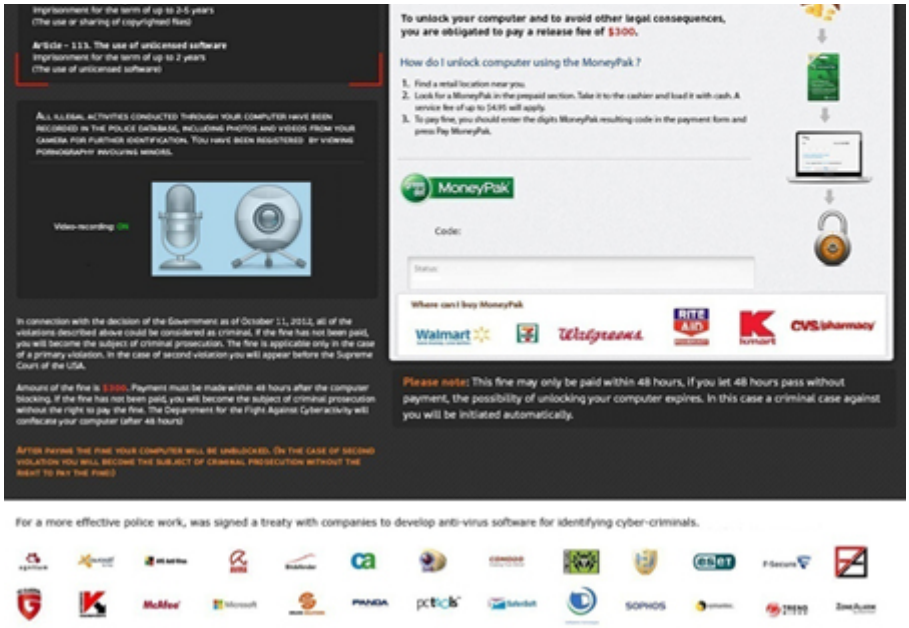
A new variant of Ransomware and Cryptolocker threats surfaced that leverages the Windows PowerShell feature to encrypt files. Trend Micro detects this as TROJ_POSHCODER.A. Windows PowerShell is a built-in feature in Windows 7 and higher. Cybercriminals often abuse this feature to make threats undetectable on the system and/or network.

POSHCODER uses AES encryption and an RSA 4096 public key to encrypt the said AES key. Once all files on the infected system are encrypted, it displays the following image:



Ransomware Infects Critical Files

While crypto-ransomware may have become popular with cybercriminals, this doesn't mean that other types of ransomware disappeared from the landscape. Police ransomware was still observed locking screens of infected computers with this screen:



What makes this particular ransomware different from other police ransomware that it rides on patched malware to infect systems. Patched malware is any legitimate file that has been modified (via addition or injection) with malicious code. Modifying a legitimate file can be advantageous to cybercriminals as the rat of execution of malicious code will depend on the infected file's frequency of use.

This ransomware is also notable for infecting *user32.DLL*, a known critical file. Infecting a critical file can be considered an evasion technique as it can help prevent detection by behavioral monitoring tools due to whitelisting. Additionally, cleaning critical files such as user32.DLL requires extra care as one misstep can crash a system, which could be seen as a possible obstacle for cleaning tools.

The infected *user32.DLL* performs a chain of routines that ends with the ransomware being loaded. It also locks the infected computer's screen and projects a "ransom" image, similar to previous police ransomware messages.

Within a couple of years, ransomware has evolved from a threat that targeted Russian users to an attack that spread to several European and North American countries. With a profitable business model and a payment scheme that affords anonymity for its operators, ransomware development is expected to accelerate over the coming years. Thus, it is crucial for users to know how ransomware work and how to best protect themselves from this threat.

Files to Encrypt

Earlier crypto-ransomware types targeted .DOC, .XLS, .JPG, .ZIP, .PDF, and other commonly-used files to encrypt. Cybercriminals have since included a number of

other file types critical to businesses, like database files, website files, SQL files, ta related files, CAD files, and Virtual desktop files.

Ransomware Evolved: Modern Ransomware

After the shift to crypto-ransomware, the extortion malware has continued to evolve, adding features such as countdown timers, ransom amounts that increase over time, and infection routines that enable them to spread across networks and servers. The latest developments show how threat actors are experimenting with new features, such as offering alternative payment platforms to make ransom payments easier, routines that threaten to cause potentially crippling damage to non-paying victims, or new distribution methods.

Some of the most notable crypto-ransomware families seen in 2016:

Show full timeline

LOCKY (RANSOM_LOCKY.A) – Discovered in February 2016, Locky was notable for its distribution methods, first seen arriving as a macro in a Word document, and then spotted being spread via Adobe Flash and Windows Kernel Exploits. One of the most actively-updated ransomware families, Locky ransomware is known for

deleting shadow copies of files to make local backups useless, and is notorious fo being used in multiple high-profile attacks on healthcare facilities.

PETYA (RANSOM_PETYA.D) – First seen in March 2016, PETYA overwrites the affected system's master boot record (MBR), and is known to be delivered through legitimate cloud storage services such as Dropbox.

CERBER (RANSOM_CERBER.A) – When it was first seen in early March 2016, CERBER was notable for having a 'voice' feature that reads out the ransom message. CERBER was also found to have a customizable configuration file that allows distributors to modify its components—a feature common for malware that's being sold in underground markets. CERBER is also notorious for being usec in an attack that potentially exposed millions of Microsoft Office 365 users to the infection.

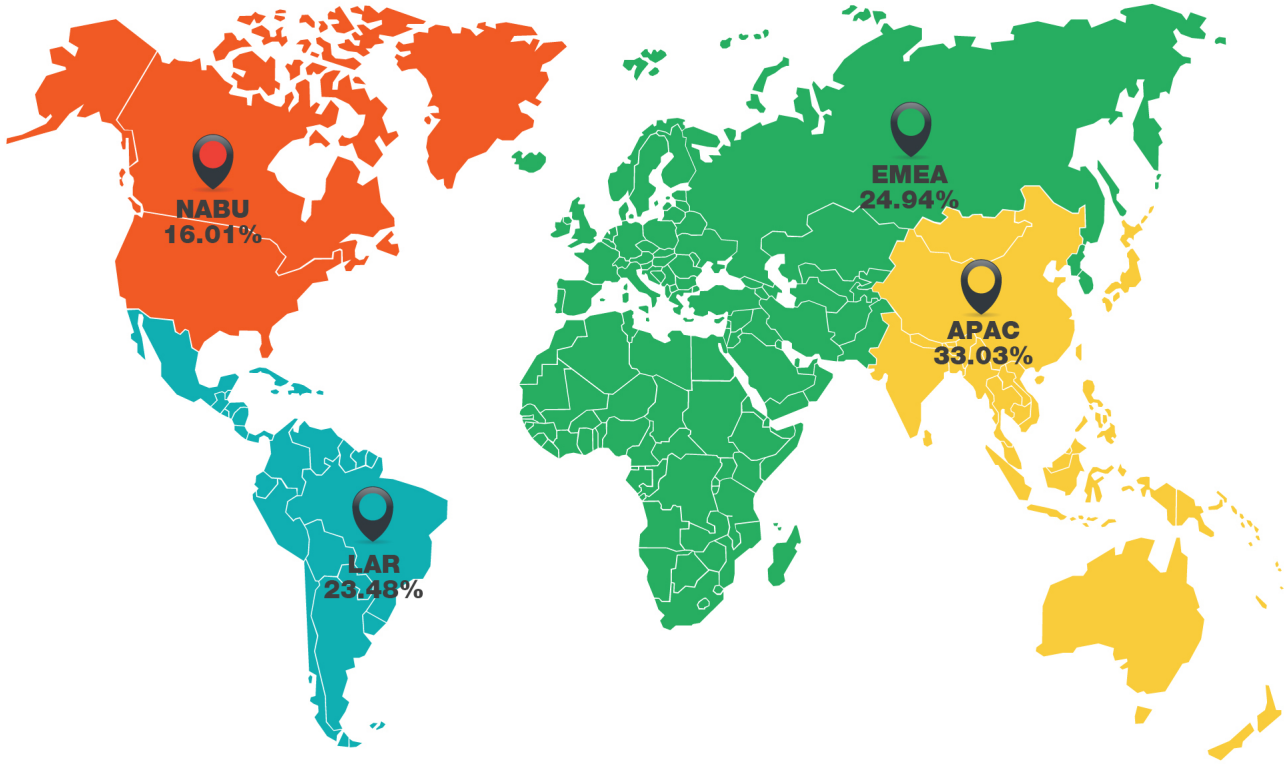
SAMSAM (RANSOM_CRYPSAM.B) – Discovered in March 2016, SAMSAM is installed after the attackers exploit vulnerabilities on unpatched servers—instead of the usual malicious URLs and spam emails—and uses these to compromise other machines.

JIGSAW (RANSOM_JIGSAW.I) – The first JIGSAW variant seen in April 2016 mixed effective scare tactics with an innovative routine. Featuring imagery from the *Saw* movie franchise, Jigsaw's ransom note features a countdown timer to pressure its victims into paying—with a promise to increase the ransom amount while deletin portions of the encrypted files every time the timer runs out. Recent Jigsaw variants also featured a chat support feature that allows victims to contact the cybercriminal.

The Biggest Attack to Date

Though ransomware routines are not altogether new, they still work and so are still used by operators. Case in point: ransomware variant WannaCry/WCRY, which originally spread via malicious Dropbox URLs embedded in spam, took an unexpected turn this May. It began exploiting a recently patched vulnerability in the SMB Server, thus resulting in the biggest ransomware attack to date.

Even before WannaCry reared its ugly head, companies and individuals worldwide have already been suffering the threat's dire consequences—all documented in our report, Ransomware: Past, Present, and Future. After just one year, we saw a staggering 752% increase in the number of ransomware families.



Regional distribution of ransomware threats from January 2016 to March 2017

The Future of Ransomware

It will not be surprising if ransomware change in a few years. In terms of potentia they can evolve into malware that disable entire infrastructure (critical not only to a business's operation but also a city's or even a nation's) until the ransom is paid Cybercriminals may soon look into approaches like hitting industrial control systems (ICS) and other critical infrastructure to paralyze not just networks but ecosystems. A key area that could become a bigger target for cybercriminals are payment systems, as seen with the Bay Area Transit attack in 2016 where the service provider's payment kiosks were targeted with ransomware.

We have seen ransomware operators hit hospitals and transportation service providers. What would stop attackers from hitting even bigger targets like the industrial robots that are widely used in the manufacturing sector or the infrastructure that connect and run today's smart cities? Online extortion is boun to make its way from taking computers and servers hostage to any type of insufficiently protected connected device, including smart devices, or critical infrastructure. The return on investment (ROI) and ease with which cybercriminal can create, launch, and profit from this threat will ensure it continues in the futur

The Bitcoin Connection

With the exception of some ransomware families that demand high amounts, ransomware variants typically ask for 0.5–5 Bitcoins (as of 2016) in exchange for a decrypt key. This is important for two reasons—some variants increase the ransom as more time elapses with nonpayment, and the Bitcoin exchange rate is on the rise. In January 2016, 1 BTC was worth US$431. Bitcoin's value has risen dramatically since then, topping out at US$1,082.55 at the end of March, 2017.

Ransomware Defense, Prevention, and Removal

Ransomware Defense

There is no silver bullet when it comes to stopping ransomware, but a multi-layered approach that prevents it from reaching networks and systems is the best way to minimize the risk.

For Enterprises: Email and web gateway solutions such as Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security prevent ransomware from reaching end users. At the endpoint level, Trend Micro Smart Protection Suites features behavior monitoring and application control, as well as vulnerability shielding to minimize the risk of getting infected by ransomware threats. Trend Micro Deep Discovery Inspector detects and blocks ransomware on

networks, while Trend Micro Deep Security™ stops ransomware from reaching enterprise servers—whether physical, virtual or in the cloud.

For small and medium-sized businesses, Trend Micro Worry-Free Services Advanced offers cloud-based email gateway security through Hosted Email Security. Its endpoint protection also delivers several capabilities such as behavio monitoring and a real-time web reputation service that detects and blocks ransomware.

For home users, Trend Micro Security 10 provides robust protection against ransomware by blocking malicious websites, emails, and files associated with this threat.

Ransomware Prevention:

- Avoid opening unverified emails or clicking links embedded in them.
- Back up important files using the 3-2-1 rule—create 3 backup copies on 2 different media with 1 backup in a separate location.
- Regularly update software, programs, and applications to protect against the latest vulnerabilities.

Anti-Ransomware Tools and Solutions

Trend Micro offers free tools such as the Trend Micro Lock Screen Ransomware Tool, which is designed to detect and remove screen-locker ransomware. The Trend Micro Crypto-Ransomware File Decryptor Tool can decrypt files locked by certain variants of crypto-ransomware without paying the ransom or the use of the decryption key.

Latest Notable Ransomware

The latest notable ransomware analyzed by Trend Micro:

Trend Micro Detection	Notable Features	Month-Year discovered
RANSOM_MILICRY.A	• Uses Imgur photo upload service for its C&C routine	09 2016

RANSOM_POGOTEAR.A	• Uses Pokemon Go as social engineering	08 2016
RANSOM_CRYPBEE.A	• Also known as R980 ransomware • Resembles RANSOM_MADLOCKER	08 2016
RANSOM_JSRAA.D	• Written in Jscript • Arrives via .LNK file • Opens a fake Russian error message	07 2016
RANSOM_CRYPMIC.A	• Distributed by Neutrino exploit kit • Shares similarities with WALTRIX/CRYPTXXX	07 2016
RANSOM_STAMPADO.A	• Has similarities with JIGSAW • Threatens to delete encrypted files after certain hours of non-payment • Sold in the underground	07 2016
RANSOM_MIRCOP.A	• Arrives as fake Thai customs form • Asks for 40 bitcoins, one of the highest ransom demands, as payment	06 2016
RANSOM_JOKOZY.A	• Employs RSA 2048 asymmetric encryption	06 2016
RANSOM_JSRAA.A	• Uses Jscript for relatively easy execution in Internet	06 2016

	Explorer	
RANSOM_ZCRYPT.A	• Capable of spreading via USB • Runs on Windows 64-bit operating systems • Increases ransom when not paid during a certain time period	05 2016

Visit the Threat Encyclopedia for the latest notable ransomware

List of Known Ransomware Families

Security News

- Securing Smart Cities
- Ransomware Recap: Business as Usual after WannaCry Surge
- The State of SCADA HMI Vulnerabilities
- EternalRocks Emerges, Exploits Additional ShadowBroker Vulnerabilities
- Ransomware Recap: The Week of WannaCry

Security Intelligence Blog

- Red on Red: The Attack Landscape of the Dark Web
- Yara Used to RickRoll Security Researchers
- A Rising Trend: How Attackers are Using LNK Files to Download Malware
- Victims Lost US$1B to Ransomware
- Android Security Bulletin Tackles Additional Critical Mediaserver Issues

Privacy

Support