KnowBe4
Human error. Conquered.

WHITEPAPER

Your Money or Your Life Files

KnowBe4

whitepaper

Your Money or Your Life Files

A Short History Of Ransomware

> *"The year 2014 may well go down in the history books as the year that extortion attacks went mainstream." -Brian Krebs, security journalist*

"Fueled largely by the emergence of the anonymous online currency Bitcoin, these shakedowns are blurring the lines between online and offline fraud, and giving novice computer users a crash course in modern-day cybercrime," said Krebs. Symantec reported in their August 2014 Intelligence report that crypto-style ransomware has seen a 700 percent-plus increase. These file-encrypting versions of ransomware began the year comprising 1.2 percent of all ransomware detections, but made up 31 percent at the end of August.

One of the key methods cybercriminals are using is ransomware, most famously the Cryptolocker malware, and its numerous variants, which encrypts the files on a user's computer and demands the user pay a ransom, usually in Bitcoins, in order to receive the key to decrypt the files. But Cryptolocker is just one approach that criminals are taking to demand ransom, and the techniques are evolving on a daily basis. To guard against ransomware, it is not enough to know the malware that is making the rounds that day. It is vital to have a broader understanding of the topic, so one can take effective countermeasures against this evolving threat.

Hacking Generations

Let's begin by taking a look at how cyberattacks have changed over the years. What we are facing nowadays is a far cry from when people like Kevin Mitnick were breaking into phone company networks to see what they could get away with. It is now a multi-billion global activity being run by organized cybercrime hiring experienced, professional coders and running e-commerce sites and cloud computing services for criminal activities. For the purposes of this article, however, we will ignore nation-state sponsored targeted actions such as the Stuxnet attack on Iran's uranium enrichment facilities or the cyberespionage specialists of People's Liberation Army Unit 61398 operating out of a 12-story building near Shanghai.

Generation One - Those were the teenagers in dark, damp cellars writing viruses to gain notoriety, and to show the world they were able to do it – relatively harmless, no more than a pain in the neck to a large extent. We call them sneaker-net viruses as it usually took a person to walk over from one PC to another with a floppy disk to transfer the virus.

Generation Two - These early day 'sneaker-net' viruses were followed by a much more malicious type of super-fast spreading worms (we are talking 10 minutes around the globe) like Sasser and NetSky that started to cause multi-million dollar losses. These were still more or less created to get notoriety, with students showing off their "elite skills".

Generation Three - Here the motive shifted from recognition to remuneration. These guys were in it for easy money. This is where botnets came in: thousands of infected PCs owned and controlled by the cybercriminal that used the botnet to send spam, attack websites, identity theft and other nefarious activities. The malware used was more advanced than the code of the 'pioneers' but was still easy to find and easy to disinfect.

Generation Four - Here is where cybercrime turned professional. The malware began to hide itself, and those behind it became better organized. They were mostly in Eastern European countries, and utilized more mature coders which resulted in much higher quality malware. This is when the first rootkit flavors showed up. They were going for larger targets where more money could be stolen. This was also the time where traditional mafias got wise to the potential and muscled into the game. Rackets like extortion of online bookmakers started to show their ugly face in Generation Four.

Generation Five - The main event that created the fifth and current generation was the formation of an active underground economy, where stolen goods and illegal services are bought and sold in a 'professional' manner, if there is such a thing as honor among thieves. Note that because of this, cybercrime has recently been developing at a much faster rate. All the tools of the trade are now for sale. This has opened the 'industry' to relatively inexperienced criminals who can learn the trade and get to work quickly. Some examples of this specialization are:

- Cybercrime has its own social networks with escrow services
- Malware can be licensed and receive tech support
- You can rent botnets by the hour, for your own crime spree
- Pay-for-play malware infection services have appeared that quickly create botnets
- A lively market for zero-day exploits (unknown software vulnerabilities) has been established

> *"Cybercrime now specializes in different markets (you can call them criminal segments), that taken all together form the full criminal supply-chain."*

The problem with this is that it provides unfortunate economies of scale. The advent of Generation Five increases malware quality, speeds up the criminal 'supply chain' and effectively spreads risk among these thieves, meaning it becomes much harder to apprehend the culprits, not to mention jurisdiction problems. Due to these factors, it is clear that we are in this for the long haul. We need to step up our game, just like the miscreants have done over the last 10 years.

The History Of Ransomware

Now that we've sketched out the various hacking generations let's zero in on ransomware and how it has evolved over time.

1989: Ransomware can be simply defined as a type of malware that restricts access to a computer system until a ransom is paid. First to hit the market was the AIDS Trojan, also known as the PC Cyborg, released way back in 1989. It was written by Harvard-trained evolutionary biologist Joseph L. Popp who sent 20,000 infected diskettes labeled "AIDS Information – Introductory Diskettes" to attendees of the World Health Organization's international AIDS conference. He included a leaflet with the diskettes warning that the software would "adversely affect other program applications," and that "you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally." The AIDS Trojan would count the number of times the computer was booted and once the count reached 90 would hide the directories and encrypt the names of the files on the C: drive. To regain access, the user would have to send $189 to PC Cyborg Corp. at a post office box in Panama.

The AIDS Trojan was Generation One malware and relatively easy to overcome. The Trojan used simple symmetric cryptography and tools were soon available to decrypt the filenames. But the AIDS Trojan set the scene for what was to come – though it took a little while to move into high gear.

2006: When the professionals entered the picture, they combined ransomware with RSA encryption. In 2006, the Archiveus Trojan encrypted everything in the MyDocuments directory and required victims to purchase items from an online pharmacy to receive the 30-digit password. In June 2006, the GPcode, an encryption Trojan which initially spread via an email attachment purporting to be a job application, used a 660-bit RSA public key. Two years later, a variant (GPcode.AK) used a 1024-bit RSA key.

In the meantime, other types of ransomware circulated that did not involve encryption, but simply locked out users. WinLock displayed pornographic images until the users sent a $10 premium-rate SMS to receive the unlocking code. Another ransomware worm imitated the Windows Product Activation notice and gave the person an international number to call to input a six-digit code. The call would be rerouted through a country with high international phone rates, and the person would be kept on hold while the fees racked up.

An alternative approach seen in recent years is scareware. Instead of encrypting files or locking people out, you do something to spook them into making payments. Such scareware, for example, can consist of a notice, appearing to be a Windows alert, which would pop up on the infected machine telling the person that spyware was detected on their computer and which would then entice the person to purchase software to remove the spyware. Others report that child pornography or illegally downloaded movies were found on the computer with a demand that the person pay a fee to avoid prosecution. In January 2013, Mark Russinovich, developer of the sysinternals Windows management tools noted that since he first wrote about scareware in 2006, many of the attacks had now moved over into full-blown ransomware.

Source: McAfee Labs, 2014.

"The examples in my 2006 blog post merely nagged you that your system was infected, but otherwise let you continue to use the computer," says Russinovich. "Today's scareware prevents you from running security and diagnostic software at the minimum, and often prevents you from executing any software at all."

Techniques include blocking the execution of other programs by simply watching for the appearance of new windows and forcibly terminating the owning process, hiding any windows not belonging to the malware, creating a new desktop, creating a full-screen window and constantly raising the window to the top of the window order. Other than the first which actually kills the processes, these techniques allow the user's processes to continue running, but mask them so they are inaccessible.

> *"Without advanced malware cleaning skills, a system infected with ransomware is usable only to give in to the blackmailer's demands to pay."*

2012: The first large scale ransomware outbreak

By mid-2011, ransomware had moved into the big time. According to McAfee's Quarterly Threats Report, there were about 30,000 new ransomware samples detected in each of the first two quarters of 2011. Then during the third quarter, the number doubled, and it surpassed 100,000 in the first quarter of 2012. Amazingly, it doubled again by the third quarter to more than 200,000 samples, or more than 2,000 per

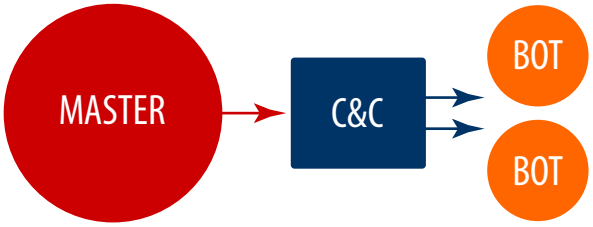
day. According to McAfee, part of this was that anonymous payment services made it much easier to collect money than the credit card payment systems that were used with the earlier wave of fake AV software scams.

But more importantly, the cybercrime ecosystem had come of age. Key to this was Citadel, a toolkit for distributing malware and managing botnets that first surfaced in January 2012. As the McAfee report stated:

"An underground ecosystem is already in place to help with services such as pay-per-install on computers that are infected by other malware, such as Citadel, and easy-to-use crime packs are available in the underground market. Criminals can buy kits like Lyposit—whose malware pretends to come from a local law enforcement agency (based on the computer's regional settings) and instructs victims to use payment services in a specific country—for just a share of the profit instead of for a fixed amount."

Citadel and Lyposit led to the Reveton worm, an attempt to extort money in the form of a fraudulent criminal fine. The exact "crime" and "law enforcement agency" are tailored to the user's locality. The crimes might be pirated software or child pornography, for example. The user would be locked out of the infected computer and the screen be taken over by a notice informing the user of their crime and instructing them that to unlock their computer they must pay the appropriate fine using a service such as Ukash, Paysafe or MoneyPak. Some versions also would take over the computer's webcam and show it on the screen to give the appearance that the person is being recorded by the police.

Reveton first showed up in Europe countries in early 2012. In the UK, the screen appeared to be coming from organizations such as the music copyright organization PRS for Music, London's Metropolitan Police Service or the Police Central e-Crime Unit. In Germany, it was the Bundespolizei; in Norway, the Norsk Politi Institutt for Cybercrime; and so on. Trend Micro researchers located templates for U.S. and Canadian versions in May 2012, and by late summer one of them was making the rounds. It appeared to be from the FBI, demanding a $200 dollar payment via a MoneyPak card. In November, another version came out pretending to be from the FBI's Internet Crime Complaint Center (IC3).



Like most malware, Reveton continues to evolve. In July 2013, the IC3 announced a version for OSX that ran in Safari and demanded a $300 fine. This time it didn't lock the computer or encrypt the files, but just opened a large number of iframes (browser windows) that the user would have to close. In July 2013, a version purporting to be from the Department of Homeland Security locked computers and demanded a $300 fine. In August 2013, Christopher Boyd, Senior Threat Researcher for ThreatTrack Security found a version masquerading as fake security software known as Live Security Professional.

It is important to note that just because a person pays to unlock the computer, it doesn't mean that the malware is gone. Once the ransom is paid, the Citadel software continues to operate and the computer can still be used to commit bank or credit card fraud. Reveton, for instance, included the Papras family of malware, which includes password stealers and which can also disable security software. In August 2014, Avast Software reported that Reveton had added a new, more powerful password stealer called Pony

BitCoin 101 And Why Criminals Want To Be Paid In Bitcoin

Money is simply anything that people consider valuable and are willing to exchange for goods and services. Ultimately you could say that money is an "idea backed by confidence". Over the years, this has meant shells, beads, precious metals, pieces of paper and electronic numbers stored in a bank's data center. Most money, these days, only exists in electronic form, with the number of zeros and ones regulated by governments to limit the supply and maintain its scarcity and its value. BitCoin operates in a similar fashion, but is a private, not a governmental agency.

Stealer. According to Avast: "This addition affects more than 110 applications and turns your computer to a botnet client. Reveton also steals passwords from 5 crypto currency wallets. The banking module targets 17 German banks and depends on geolocation. . . . The stealer includes 17 main modules like OS credentials, FTP clients, browsers, email clients, instant messaging clients, online poker clients, etc. and over 140 submodules."

Reveton is a good example of the criminal ecosystem that now exists; malware writers license other malware writer's apps and integrate them for more profit. Pony is very advanced and can pluck and decrypt encrypted passwords for FTP, VPN and email clients, web browsers and instant messaging programs.

September 2013: CryptoLocker burst onto the scene

Lockscreens and scareware are bad enough, but cryptographic malware is far worse. At least with a lockscreen, someone eventually develops a tool to remove it so one can regain access to their data. With encryption, however, the code must be cracked before the files can be decrypted. And, though there are persistent rumors that the NSA can crack 2048-bit encryption, which it of course denies, it is impossible for anyone without a $10 billion budget.

Cryptographic malware burst onto the scene in September 2013 with the arrival of CryptoLocker, essentially a ransomware Trojan. CryptoLocker spread through email attachments and drive-by downloads from infected websites. It generated a 2048-bit RSA key pair, uploaded it to a command-and-control server, and used it to encrypt files with certain file extensions, and delete the originals. It would then threaten to delete the private key if payment was not received within three days. Payments initially could be received in the form of Bitcoins or pre-paid cash vouchers. With some versions of CryptoLocker, if the payment wasn't received within three days, the user was given a second opportunity to pay a much higher ransom to get their files back. While prices vary over time and with the particular version being used, in mid-November 2013 when the going ransom was 2 Bitcoins or about $460, if they missed the original ransom deadline they could pay 10 Bitcoins ($2300) to use a service that connected to the command and control servers. After paying for that service, the first 1024 bytes of an encrypted file would be uploaded to the server and the server would then search for the associated private key.

According to Dell SecureWorks, "The earliest CryptoLocker samples appear to have been released on the Internet on September 5, 2013. Details about this initial distribution phase are unclear, but it appears the samples were downloaded from a compromised website located in the United States." Versions were also distributed to business professionals in the form of email attachments that were made to look like customer complaints. Payments could be made by CashU, Ukash, Paysafecard, MoneyPak or Bitcoin. Prices were initially set at $100, €100, £100, two Bitcoins or other figures for various currencies. But over the next few months the cash price was raised to $300 while, with the rapid price inflation of Bitcoins, it was lowered to 0.3 Bitcoins.

December 2013: 250,000 machines infected

In December 2013, Dell SecureWorks reported that about 250,000 machines had been infected. ZDNet researched four Bitcoin accounts associated with CryptoLocker and found that 41,928 Bitcoins had been moved through those four accounts between October 15 and December 18. Given the then current price of $661, that would represent more than $27 million in payments received, not counting all the other payment methods.

CryptoLocker was spread and controlled through the Gameover ZeuS botnet which had been capturing online banking information since 2011. June, 2014, a multi-national team composed of government agencies (U.S., Australia, Netherlands, Germany, France, Italy, Japan, Luxembourg, New Zealand, Canada,

BitCoins are created on a fixed schedule, currently 12.5 BitCoins about every ten minutes, with about 13,000,000 currently in circulation. The ownership of all the BitCoins is held in a publicly accessible ledger, called the block chain, which is updated several times an hour. People maintain a digital wallet and make payments by transferring BitCoins from one wallet to another. Payments can be made in fractions of BitCoins.

Although all the BitCoin transactions are publicly noted, who holds the wallets is kept anonymous. This makes them ideal for criminals. They don't have to use the highly-regulated banking systems, they don't pay credit card transaction processing fees, and BitCoins aren't subject to limitations on sending currency internationally. Therefore, there is no need to hire mules to transport cash across borders.

BitCoins, like other electronic activities, are not completely secure. For example, the Tokyo-based Mt. Gox BitCoin exchange, which had been handling about 70% of all transactions, suspended trading in February 2014 and announced that 850,000 BitCoins were missing, probably stolen. And when the U.S. FBI shut down the Silk Road online black market, it seized 144,000 BitCoins. But, at least for now, cybercriminals consider the level of security good enough to make it a superior way of doing business than working with government-issued currencies.

Ukraine and UK) and private companies, primarily Dell SecureWorks and CloudStrike, managed to disable the Gameover ZeuS Botnet. The U.S. Department of Justice also issued an indictment against Evgeniy Bogachev who operated the botnet from his base on the Black Sea. However, you will notice that Russia is not listed as one of the participating governments, and given the current geopolitical situation it is unlikely that he will ever show up in court.

August 2014, security firms FireEye of Milpitas, California and Fox-IT of Delft, The Netherlands announced that they had jointly developed a program that may be able to decrypt files that were encrypted by the original CryptoLocker botnet. The program, DecryptCryptoLocker (https://www.decryptcryptolocker.com/) is free to anyone who still has those encrypted files, but it is unlikely to work on any machines infected after the original network was brought down in late May since later infections are likely to use different encryption keys.

CryptoLocker Copycats

It is a myth that Arpanet, the predecessor to the internet, was designed to survive a nuclear attack. But it is true that the internet is highly resilient and will reroute packets whenever any particular node goes down. The same applies to criminal networks.

As Tyler Moffit of Webroot put it: "While seizing the majority of the GameOver Zeus Botnets from the suspected "mastermind" Evgeniy Bogachev was a big impact to the number of computers infected with GameOver Zeus – about a 31 percent decrease, it's a very bold claim to state that Cryptolocker has been 'neutralized'. . . . Most malware authors spread their samples through botnets that they either accumulated themselves (Bogachev), or just rent time on a botnet from someone like Bogachev (most common). So now that Bogachev's servers are seized, malware authors are just going to rent from some of the many other botnets out there that are still for lease."

The original Gameover ZeuS/CryptoLocker network was taken down late May 2014, but resurfaced by July 2014. In fact, you didn't even have to wait for that network to be rebuilt since copycats had already hit the Net. While they generally have a similar overall operating pattern of encryption and extortion, they come from different sets of hackers and each has their own unique characteristics.

"All of these work in almost exactly the same way as the infamous traditional cryptolocker we've all seen, but they have some improvements," says Moffit. "First is that there is no GUI and instead just background changes and texts instructions in every directory that was encrypted. Second is that you no longer pay using a MoneyPak key in the GUI, but instead you have to install Tor or another layered encryption browser to pay them securely and directly. This allows malware authors to skip money mules and increase the percent of profits."

Here are some of the variations we have seen so far:
Locker – This was apparently the first copycat software, initially noted in early December 2013. It cost users $150 to get the key, with money being sent to a Perfect Money or QIWI Visa Virtual Card number. But apparently the code was poorly designed: security firm IntelCrawler said it found a way to decrypt the files without paying ransom.

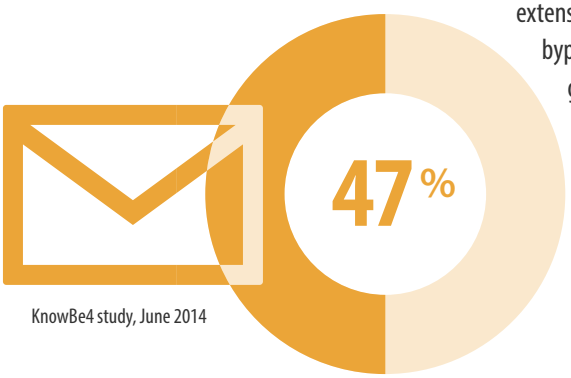
CryptoLocker 2.0 – This version was also on the market by mid-December. Despite the name similarity, CryptoLocker 2.0 was written using C# while the original was in C++ so it was likely done by a different programming team. Among other differences, 2.0 would only accept Bitcoins, and it would encrypt image, music and video files which the original skipped. And, while it claimed to use RSA-4096, it actually used

RSA-1024. However, the infection methods were the same and the screen image very close to the original CryptoDefense arrived in February 2014. It used Tor and Bitcoin for anonymity and 2048-bit encryption. However, because it used Windows' built-in encryption APIs, the private key was stored in plain text on the infected computer. Despite this flaw, the hackers still managed to earn at least $34,000 in the first month, according to Symantec.

SynoLocker appeared in August 2014. Unlike the others which targeted end-user devices, this one was designed for Synology network attached storage devices. And unlike most encryption ransomware, SynoLocker encrypts the files one by one. Payment was 0.6 Bitcoins and the user has to go to an address on the Tor network to unlock the files.

CTB-Locker (Curve-Tor-Bitcoin Locker) - Also known as Critoni.A. This was discovered midsummer 2014 and Fedor Sinitisyn, a security researcher for Kapersky. Early versions only had an English language GUI, but then Russian was added. The first infections were mainly in Russia, so the developers were likely from an eastern European country, not Russia, because the Russian security services immediately arrest and shut down any Russians hacking others in their own country.

CryptorBit surfaced in December 2013. Unlike CrytoLocker and CryptoDefense which only target specific file extensions, CryptorBit corrupts the first 212 or 1024 bytes of any data file it finds. It also seems to be able to bypass Group Policy settings put in place to defend against this type of ransomware infection. The cyber gang uses social engineering to get the end-user to install the ransomware using such devices as a fake flash update or a rogue antivirus product. Then, once the files are encrypted, the user is asked to install the Tor Browser, enter their address and follow the instructions to make the ransom payment – up to $500 in Bitcoin. The software also installs cryptocoin mining software that uses the victim's computer to mine digital coins such as Bitcoin and deposit them in the malware developer's digital wallet.



KnowBe4 study, June 2014

47% feel email attachments pose the largest threat

CryptoWall – April 2014, the cyber criminals behind CryptoDefense release an improved version called CryptoWall. While largely similar to the earlier edition, CryptoWall doesn't store the encryption key where the user can get to it. In addition, while CryptoDefense required the user to open an infected attachment, CryptoWall uses a Java vulnerability. Malicious advertisements on domains belonging to Disney, Facebook, The Guardian newspaper and many others led people to sites that were CryptoWall infected and encrypted their drives. According to an August 27 report from Dell SecureWorks Counter Threat Unit (CTU): "CTU researchers consider CryptoWall to be the largest and most destructive ransomware threat on the Internet as of this publication, and they expect this threat to continue growing." More than 600,000 systems were infected between mid-March and August 24, with 5.25 billion files being encrypted. 1,683 victims (0.27%) paid a total $1,101,900 in ransom. Nearly 2/3 paid $500, but the amounts ranged from $200 to $10,000.

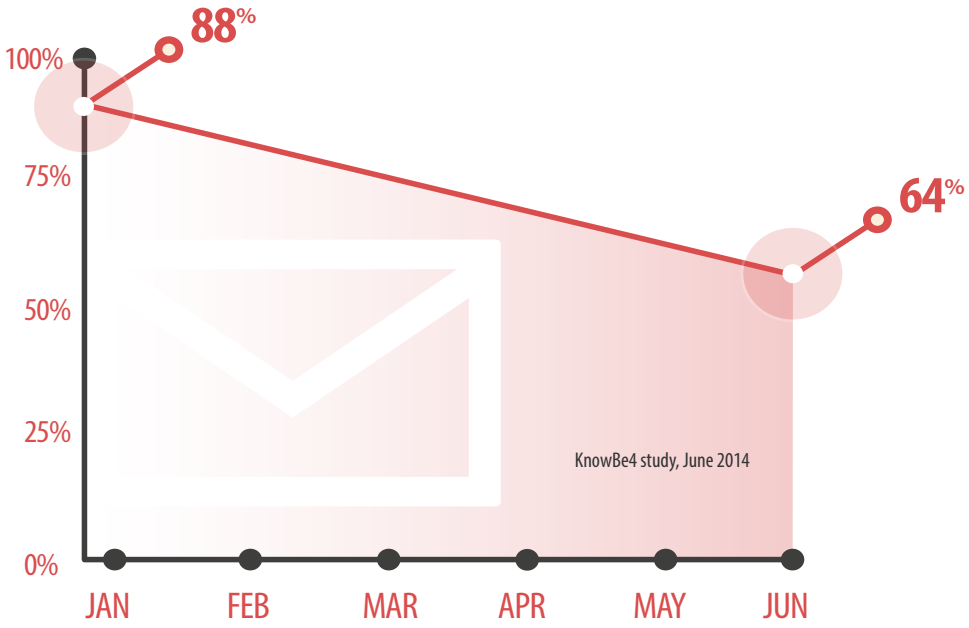
TorrentLocker – According to iSight Partners, TorrentLocker "is a new strain of ransomware that uses components of CryptoLocker and CryptoWall but with completely different code from these other two ransomware families." It spreads through spam and uses the Rijndael algorithm for file encryption rather than RSA-2048. Ransom is paid by purchasing Bitcoins from specific Australian Bitcoin websites.
Cryptoblocker – July 2014 Trend Micro reported a new ransomware that doesn't encrypt files that are larger than 100MB and will skip anything in the C:\Windows, C:\Program Files and C:\Program Files (x86) folders. It uses AES rather than RSA encryption.

Different Ransomware Families

Ransomware breaks down into several different malware families.

WinLock/Police Ransomware–Police Ransomware is software, like Reveton, that displays a message that the user is being pursued by the police because they broke the law by viewing pornography, or downloaded or shared intellectual property. The malware takes over the computer, locking out the user and displaying a screen giving the message from the "police." This software started out in Eastern Europe, perhaps preying on citizens' understandable distrust and fear of the police forces after half a century of dealing with Communist secret police organizations. Starting in 2012, however, these infections began spreading worldwide.

One factor that is unique about this type of software is that it must be tailored to the local area. While other types of malware can butcher the grammar, non-idiomatic language in a police ransomware attack will signal that it is not from the agency it purports to be from. Enigma Software lists three common Police Ransomware families.



Email and spam filtering effectiveness dropped from 88% to 64%

The Gimemo family appeared in 2010 and infected computer systems in Russia. The earliest variants demanded payment through text messaging before switching to PaySafeCard and Ukash. The Gimemo family frequently sends messages from copyright enforcement agencies such as the United Kingdom's PRS or France's SACEM. A US variant, FBI MoneyPak claims the person viewed child pornography and demand a $100 fine be sent via MoneyPak.

- The Reveton family of malware is covered earlier in this paper also includes the variants Matsnu and Rannoh.

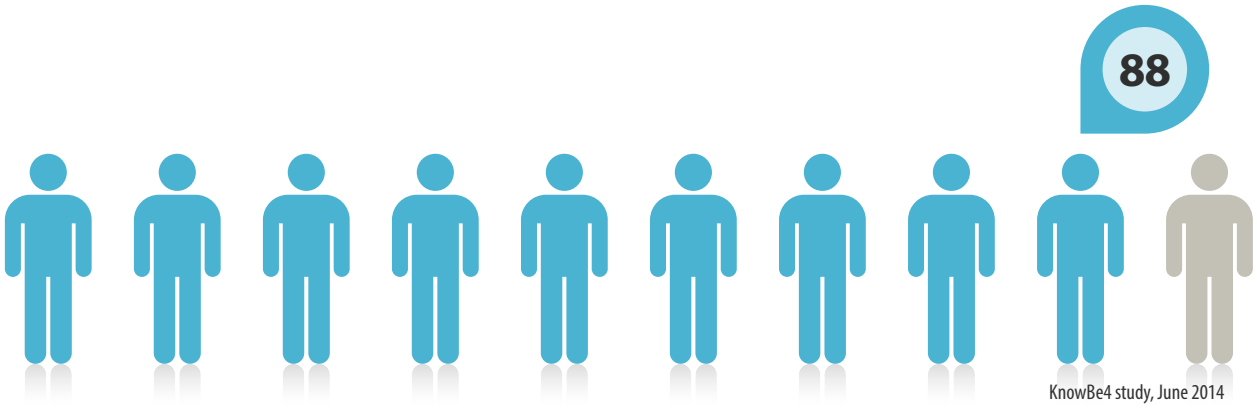
- Urausy Police Ransomware Trojans are some of the most recent entries in these attacks and are responsible for Police Ransomware scams that have spread throughout North and South America since April of 2012.

SMS Ransomware: This a variation on the usual type of type of lockout ransomware in terms of the payment method. The screen will display a code with instructions to send that code via text message to premium-rate SMS number. The user then receives an SMS message giving the unlock code.
File Encryptors: These are ransomware which encrypt all or some of the files on the disk, while leaving the applications in place. The screen will show display a ransom note with payment instructions and may or may not lock the screen. The most prominent example is CryptoLocker and its variants, discussed above. Once payment in is made, the code is sent to decrypt the files.

MBR Ransomware: The Master Boot Record (MBR) is the partition of the hard drive that contains the data that allows the system to boot up. MBR ransomware changes the computer's MBR so that, when the computer is turned on, the ransom message is displayed and the computer will not boot. The message may say that the files have been encrypted although they are not. Since the computer won't load the operating system, the user can't run tools to remove the infection and repair the system.

Mobile Ransomware: Most ransomware targets desktop/laptops, but there are also hacks designed for mobile devices. These include:

- **Koler.a:** Launched in April, this police ransom Trojan infected around 200,000 Android users, ¾ in the US, who were searching for porn and wound up downloading the software. Since Android requires permission to install any software, it is unknown how many people actually installed it after download. Users were required to pay $100 - $300 to remove it. On July 23, Kapersky reported that Koler had been taken down, but didn't say by whom.



KnowBe4 study, June 2014

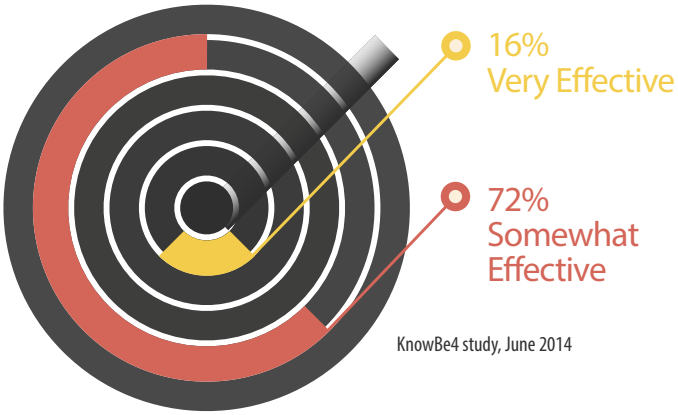
88% expect ransomware to increase the rest of the year

- **Svpeng:** This mobile Trojan targets Android devices. It was discovered by Kapersky in July 2013 and originally designed to steal payment card information from Russian bank customers. In early 2014, it had evolved into ransomware, locking the phones displaying a message accusing the user of accessing child pornography. By the summer of 2014, a new version was out targeting U.S. users and using a fake FBI message and requiring a $200 payment with variants being used in the UK, Switzerland, India and Russia. According to Jeremy Linden, a senior security product manager for Lookout, a San Francisco-based mobile security firm, 900,000 phones were infected in the first 30 days. The software also scans for mobile banking apps but was not yet stealing the credentials. Unless phones already have security software, the option to boot into safe mode and then erase all the data on the phone, leaving the data on the SIM and SD cards intact.

• **Find My Phone –** In May 2014, iDevice users in Australia and the U.S. started finding a lock screen on their iPhones and iPads saying that it had been locked by "Oleg Pliss" and requiring payment of $50 to $100 to unlock. It is unknown how many people were affected, but in June the Russian police arrested two people responsible and reported how they operated. This didn't involve installing any malware, but was simply a straight up con using people's naiveté and features built into iOS. First people were scammed into signing up for a fake video service that required entering their Apple ID. Once they had the Apple ID, the hackers would create iCloud accounts using those ID's and use the Find My Phone feature, which includes the ability to lock a stolen phone, to lock the owners out of their own devices.

The Future Of Ransomware

Starting September 2013, ransomware has become much more vicious and has inspired several copycats. At the time of this writing, summer 2014, the very first strains of second-generation ransomware have been identified.



KnowBe4 study, June 2014

Only 16% feel their current solutions are very effective, while 72% feel they are somewhat effective

The reasons that these strains being called second generation are as follows:

1) They use the TOR network for their Command & Control (C&C) servers which makes them much harder to shut down.

2) Traffic between the malware that lives on the infected machine and its C&C servers is much harder to intercept.

3) Second-gen ransomware uses super strong cryptography which makes decrypting it yourself impossible.

4) They compress files before encrypting them.

5) Second-gen ransomware is built as commercial crimeware, so it can be sold globally to other cybercriminals. It uses Bitcoin ransom amounts that the "customer" can specify and a choice of which files types will be encrypted, so that the criminal can compete and differentiate themselves.

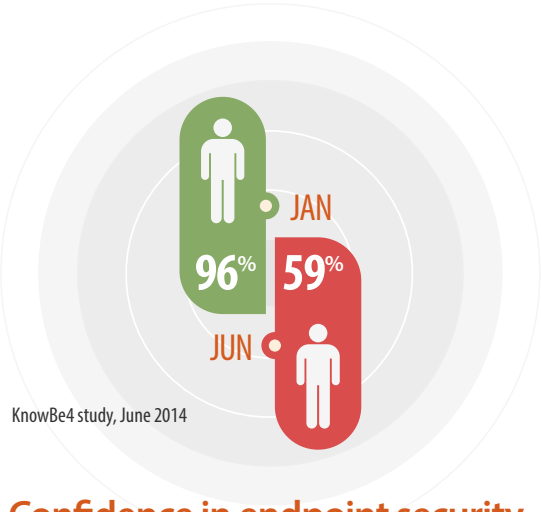
What does the appearance of second generation ransomware mean? And what can be expected in the future? Here are several likely areas of malware evolution that are likely to appear:

1) Second-gen ransomware will proliferate. Several large (and competing) Eastern European cyber mafias will become big players in this field, followed by dozens of smaller operations spread all over the planet that buy "pay-and-play" commercial ransomware.

2) Ransomware will expand beyond the Windows platform onto Apple's devices. Being hit with a ransom demand to unlock your iMac, iPhone or iPad, although it has already taken place, will be likely to occur with greater frequency. Similarly, this will also be the case for the Android OS, which runs on both phones and tablets. The first waves of Android infections have occurred in 2014.

3) Criminal RaaS (Ransomware-as-a-Service) subscriptions will become more widely available, where would-be cyber criminals can buy all the required elements needed for an attack. These RaaS subscriptions comprise a range of elements including potential victim email lists, phishing templates that use successful social engineering ploys, bulletproof email servers (or botnets) to send the attacks, the malware that includes encryption / decryption features, and last but not least, the financial infrastructure that allows victims to pay.

The vast majority of these attacks will be launched from countries that do not have legislation (or insufficient enforcement) to stop this kind of attack vector, with the result that U.S. law enforcement will continue to be severely challenged to do something effective about it and will be forced to continue the whack-a-mole game i.e., like the popular arcade game, the targets keep ducking out of the way before detection only to pop up almost immediately somewhere else.



KnowBe4 study, June 2014

Confidence in endpoint security dropped from 96% in January to 59%

4) Infection vectors will continue to be more creative and hard to defend against. At the moment, links to cloud storage are being used as a social engineering trick so people are tempted to open up zip files. But it is likely that drive-by ransomware infections will be the norm. Visiting a legit website that has been compromised and clicking on a link will be enough to encrypt the files on the workstation and/or the file server.

5) Attacks will technically become far more sophisticated and will be able to evade normal detection methods like antivirus and sandboxing technologies. "With target audiences so large, financing mechanisms so convenient, and cyber-talent so accessible, robust innovation in criminal technology and tactics will continue its surge forward in 2014," said Vincent Weafer, senior vice president of McAfee Labs in the company's 2014 Predictions Report. "The emergence and evolution of advanced evasion techniques represents a new enterprise security battlefront, where the hacker's deep knowledge of architectures and common security tactics enable attacks that are very hard to uncover."

IT Managers Lack An Effective Approach To Ransomware

In January 2014, IT Security company Webroot used Spiceworks to survey 300 IT professionals on the threat of ransomware. At that time, 48% said that they were either very or extremely concerned about ransomware, and only 2% were not at all concerned. One-third stated that their organization had already experienced a ransomware attack and two-thirds expected the number of attacks to increase in the next year. (How right they were!) And, while 82% were using some means of protection against ransomware, less than half (44%) considered their current solution to be even somewhat effective. Given that they couldn't protect effectively against a ransomware attack, the top strategy for dealing with it was to wipe the device (82%) or restore the device from backup files (19%) rather than having a security service provider try to remove the encryption (22%) or doing it manually (9%).

Given the rapid rise in ransomware, KnowBe4 decided to conduct a similar survey in June of more than 300 Spiceworks users to see how much attitudes had changed. This time, we found that 88% expected ransomware to increase by the end of the year, and while 72% felt their current solutions were somewhat effective, only 16% thought it was very effective. Nearly half (47%) considered email attachments to be the largest threat, while confidence in the effectiveness of email and spam filtering had dropped from 88% to 64% and confidence in endpoint security had fallen from 96% to 59%. Given this lack of confidence, it is

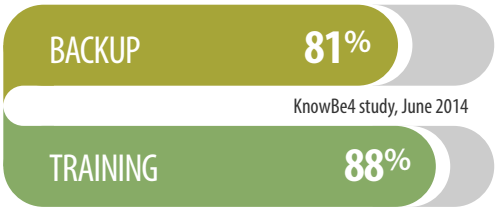
not surprising that they cited Security Awareness Training (88%) as the most effective protection against ransomware, followed by backup at 81%.

Russian Cyber Mob Has Picked A Highly Profitable Business Model

The study asked what they would do when confronted with a scenario where backups have failed and weeks of work might be lost, an astounding 57% would begin with paying the $500 ransom and hope for the best. Based on these findings, it appears the Russian cyber mob has picked a highly profitable business model. While the overwhelming majority of IT pros think the criminals behind ransomware should be prosecuted and sent to jail for a long time, U.S. law enforcement has no jurisdiction in Eastern Europe where these criminals are largely free to commit their crimes. The chances of them being brought to justice at this time are remote. The Russian government seems to use these cybercriminals as a resource they can bring to bear against countries they are in conflict with.

Surprisingly, while Security Awareness Training was considered the most effective defense against ransomware, an April 2014 report from Enterprise Management Associates (EMA), Security Awareness Training: It's Not Just for Compliance found that 56% of employees, excluding security and IT staff, had not received any Security Awareness Training from their organizations. The quality of such training also left a lot to be desired. The EMA report found that out of those who have had some training, it was not done frequently enough to have the desired results. "Employees predominantly received training annually, even though a higher frequency of training has been found to be more effective," said the EMA report.

David Monahan, EMA Research Director, Security and Risk Management, believes that training is one of the most important elements in any ransomware defense strategy.



88% consider Security Awareness Training the most effective protection from ransomware over 81% for backup

"Security awareness training is critical for a solid security program," said David Monahan, EMA Research Director, Security and Risk Management. "The organizations that fail to train their people are doing their business, their personnel and the Internet as a whole a disservice because the training they provide at work affects how their employees make security decisions while they are on the Internet at home as well."

Given that IT expects that ransomware will increase, that they know Security Awareness Training is the best defense, and they also know that most employees receive no or ineffective Security Awareness Training, it is no surprise why such a high percentage are concerned about ransomware and feel their systems are ineffective.

Guarding Against Ransomware

Given the rapid spread and potentially high cost of ransomware, it is important to take effective steps to guard against this menace. It would be great if one could rely on law enforcement to do the job, but that is not a realistic expectation. True, there are occasional high profile successes, like the one against the Gameover ZeuS botnet, but that only happened after years of operation and hundreds of millions in losses. And Evgeniy Bogachev, his collaborators and his many competitors are still out causing mischief as they were before.

If one is hit and can't recover the data, it may be best to pay the ransom. But that just gives the criminals more money for future attacks so it is far better to take steps ahead of time to ensure that one doesn't become a victim in the first place. This requires a complete, defense-in-depth strategy.
A simple step to start with is making sure that every piece of software is kept up to date. The hackers are looking for vulnerabilities they can exploit to take over systems. Vendors generally do a good job of patching any flaws once they are found, but if the patches are never applied you have left the door wide open for attacks.

One should also ensure that every device that connects to the company's network is secured. This includes employees' smartphones, tablets, laptops and home computers. Protection should comprise anti-malware and/or whitelisting software as well as establishing secure policies such as not allowing programs to auto-install, blocking ports, web filtering, share access restrictions, and encryption of data at rest and in flight. The two biggest steps, however, are those that came up in the survey: backup and user training. Real-time or near-time backup can be an effective countermeasure to minimize the damage caused by ransomware if an infection ever occurs. The infected device can be thoroughly wiped and all applications and data can be reloaded. Yes, it will probably take several hours to restore the device to full working order, but at least one is not spending money that criminals can use to finance further attacks.

But this, or course, assumes that the backup is complete, is current and is able to be restored. It would be nice if those three conditions were the norm for backups, but unfortunately that is far from the case. The fact is that backups consistently fail.

In surveys, most IT managers said they rely on backup to get them out of a tight spot. However, 57% of them agree that if their backup fails, they would be forced to pay the ransom. Sadly, too many backups fail for this to be a wise approach. According to a 2013 report by Symantec, Avoiding the Hidden Costs of the Cloud, 47% of enterprises lost data in the cloud and had to restore their information from backups, 37% of SMBs have lost data in the cloud and had to restore their information from backups and a startling 66% of those organizations saw recovery operations fail.

"Storage media fails regardless of type; it is just a matter of when," said Jeff Pederson, manager of data recovery operations for Kroll Ontrack. "To avoid such a failure, one should regularly defrag their computer, check its storage capacity, and run antivirus software as well as hard drive monitoring software. Beyond good health practices, businesses and home users should have working redundancies, such as a backup device or service in place, and a continuity plan that is current and accessible in the event of a loss."

Backup Is Not Enough

So, by all means have backup processes in place, apply the 3-2-1 strategy (three copies of the data, on two different types of media, with one offsite) and test the restore function on a regular basis. But a better approach is to make sure you never get infected in the first place. This requires Security Awareness Training. Regardless of how well the defense perimeter is designed the bad guys will always find a way in. Why? Employees are the weakest link in any type of IT system. Data recovery firm Kroll Ontrack reports that with traditional IT systems, human error accounts for 26% of data loss incidents, more than hardware failures or power outages. For virtualized systems, the human error rate rises to 65%. Similarly, human error is also the weakest point when it comes to blocking ransomware.

Let's review some of the methods that are used to spread ransomware:

- Scareware works by tricking unsuspecting people into thinking that their computer is infected. (It is, but by the scareware itself.)
- CryptoLocker sent emails with infected attachments masked as resumes to companies that had posted job listings on sites like Craigslist. The moment anyone opens these documents, the ransomware kicks in and downtime is the result. Part of the problem is that the people involved with hiring are very often those with the most access; the owner, CEO, HR or department heads. If they are duped by the bad guys, the consequences for the entire organization can be dire.
- The iPhone lockout worked by getting people to disclose their Apple IDs.
- The Android hack got people to download the software thinking they would be seeing some porn.
- Many forms of malware use ads on legitimate websites such as Yahoo or YouTube. Click on the ad and download the software.

It isn't enough to include the security information covered in the employee handbook or conduct an annual training session, perhaps during lunch break. To be effective, employees must be reminded throughout the year of security best practices and must be tested on the job, not in the classroom, to see if they are applying what they have learned.

How Effective Is Security Awareness Training In Combatting Ransomware?

Well, we are willing to bet our own money that our methods of training will work. KnowBe4's Kevin Mitnick Security Awareness Training comes with a crypto-ransom guarantee. If an employee who has taken our training and received at least one phishing security test per month clicks on a link and infects their workstation, KnowBe4 pays your crypto-ransom. Find out how affordable this is for your organization now, visit our website **www.knowbe4.com**.

Drew Robb is a freelance writer living In Florida specializing in IT and engineering. Originally from Scotland, he is the author of the book Server Disk Management in Windows Environments (CRC Press) as well as hundreds of articles in magazines such as Computerworld, information week and writers digest.

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created by two of the best known names in cybersecurity, Kevin Mitnick (the World's Most Famous Hacker) and Inc. 500 alum serial security entrepreneur Stu Sjouwerman, to help organizations manage the problem of social engineering tactics through new school security awareness training.

More than 1,700 organizations use KnowBe4's platform to keep employees on their toes with security top of mind. KnowBe4 is used across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance.

- KnowBe4 wrote the book on cyber security (8 books and counting between Mitnick and Sjouwerman).
- KnowBe4 is the only set-it-and-forget-it security awareness training platform "by admins for admins" with minimum time spent by IT to get and keep it up and running.
- The platform includes a large library of known-to-work phishing templates.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com