SECURITY RESPONSE

The evolution of ransomware

Kevin Savage,
Peter Coogan,
Hon Lau

Version 1.0 – August 6, 2015

> *Never before in the history of human kind have people across the world been subjected to extortion on a massive scale as they are today.*

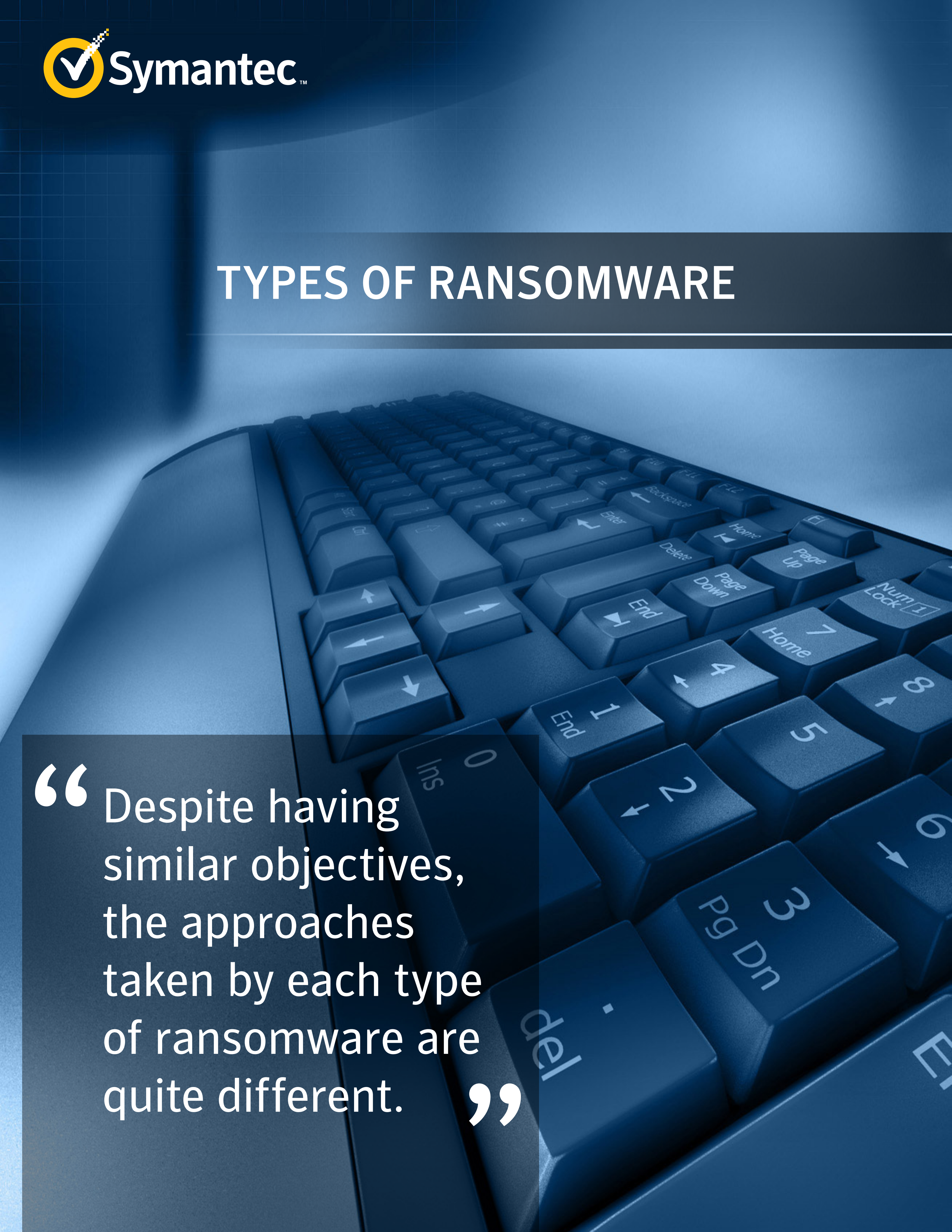
CONTENTS

OVERVIEW

Never before in the history of human kind have people across the world been subjected to extortion on a massive scale as they are today. In recent years, personal use of computers and the internet has exploded and, along with this massive growth, cybercriminals have emerged to feed off this burgeoning market, targeting innocent users with a wide range of malware. The vast majority of these threats are aimed at directly or indirectly making money from the victims. Today, ransomware has emerged as one of the most troublesome malware categories of our time.

There are two basic types of ransomware in circulation. The most common type today is crypto ransomware, which aims to encrypt personal data and files. The other, known as locker ransomware, is designed to lock the computer, preventing victims from using it. In this research, we will take a look at how the ransomware types work, not just from a technological point of view but also from a psychological viewpoint. We will also look at how these threats evolved, what factors are at play to make ransomware the major problem that it is today, and where ransomware is likely to surface next.

Symantec



TYPES OF RANSOMWARE

> “Despite having similar objectives, the approaches taken by each type of ransomware are quite different.”

Key information

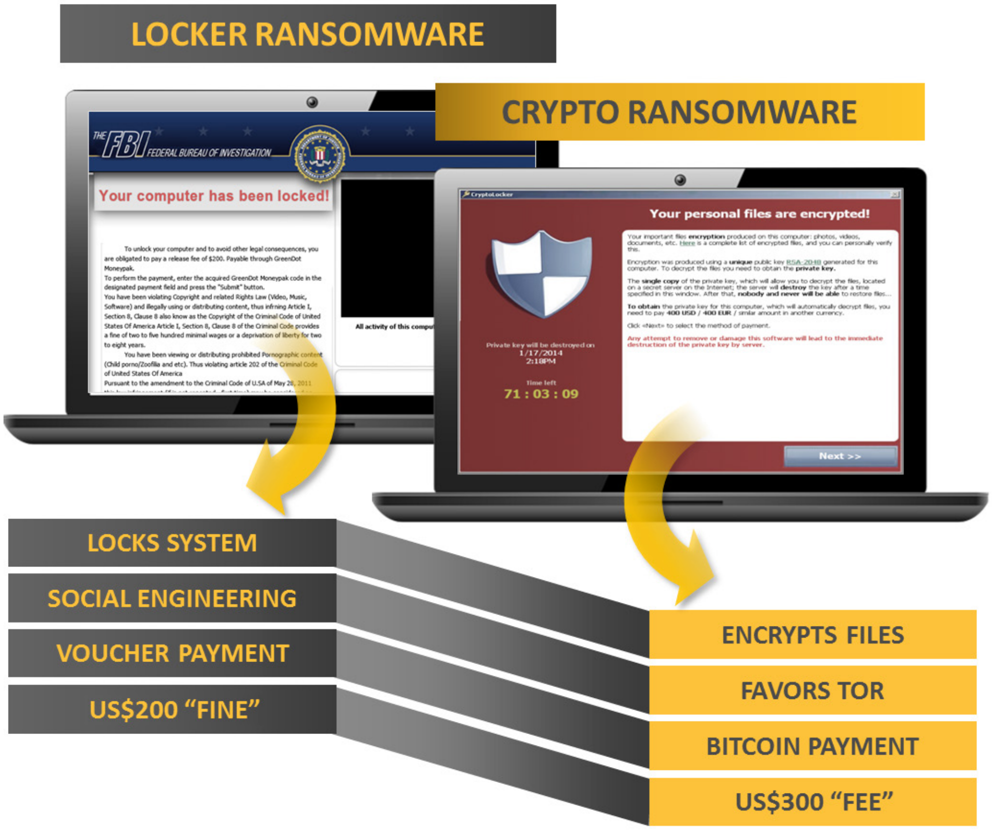
- The first wave of modern ransomware started in 2005 with Trojan.Gpcoder.
- Ransomware is designed for direct revenue generation. The four most prevalent direct revenue-generating risks include misleading apps, fake antivirus scams, locker ransomware, and crypto ransomware.
- Direct revenue-generating malware went through four major pivot points in the past decade. Each pivot point indicates a shift from one type of malware to another, ultimately leading to ransomware.
- The top six countries impacted by all types of ransomware in 2015 are the United States, Japan, United Kingdom, Italy, Germany, and Russia.
- The average ransom amount is US$300. The favored payment method for locker ransomware is payment vouchers and for crypto ransomware, it's bitcoins.
- In the past 12 months, 64 percent of binary-file-based ransomware detected have been crypto ransomware while binary-based locker ransomware made up the remaining 36 percent.
- Between 2013 and 2014, there was a 250 percent increase in new crypto ransomware families on the threat landscape.
- Cybercriminals behind ransomware are constantly innovating. With more connected devices around, we can expect to see ransomware appear in new device categories where they were never seen before.
- In our research, we have demonstrated ransomware operating on a smartwatch but so far, we have not seen any ransomware in the wild specifically designed to target smartwatches.

Types of ransomware

There are two main forms of ransomware in circulation today:

- Locker ransomware (computer locker): Denies access to the computer or device
- Crypto ransomware (data locker): Prevents access to files or data. Crypto ransomware doesn't necessarily have to use encryption to stop users from accessing their data, but the vast majority of it does.

Both types of ransomware are aimed squarely at our digital lifestyle. They are designed to deny us access to something we want or need and offer to return what is rightfully ours on payment of a ransom. Despite having similar objectives, the approaches taken by each type of ransomware are quite different.



Your computer has been locked!

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $200. Payable through GreenDot Moneypak.
To perform the payment, enter the acquired GreenDot Moneypak code in the designated payment field and press the "Submit" button.
You have been violating Copyright and related Rights Law (Video, Music, Software) and illegally using or distributing content, thus infrning Article I, Section 8, Clause 8 also know as the Copyright of the Criminal Code of United States Of America Article I, Section 8, Clause 8 of the Criminal Code provides a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States Of America
Pursuant to the amendment to the Criminal Code of U.SA of May 28, 2011

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **400 USD / 400 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
1/17/2014
2:18PM

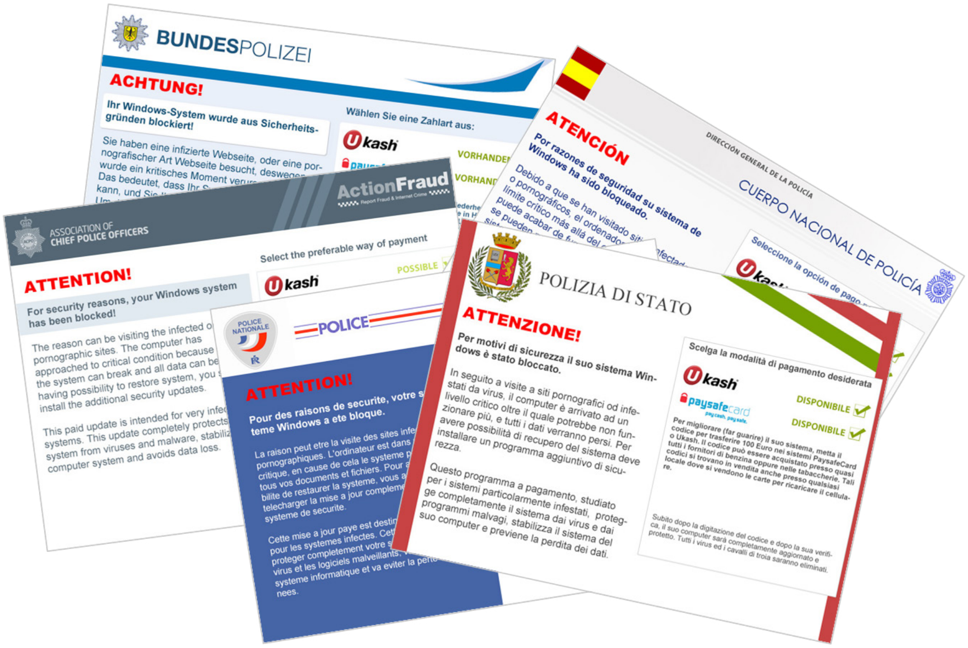
Time left
71 : 03 : 09

Figure 1. Two main types of ransomware are locker ransomware and crypto ransomware

Locker ransomware (Computer locker)

Locker ransomware is designed to deny access to computing resources. This typically takes the form of locking the computer's or device's user interface and then asking the user to pay a fee in order to restore access to it. Locked computers will often be left with limited capabilities, such as only allowing the user to interact with the ransomware and pay the ransom. This means access to the mouse might be disabled and the keyboard functionality might be limited to numeric keys, allowing the victim to only type numbers to indicate the payment code.

Locker ransomware is typically only designed to prevent access to the computer interface, largely leaving the underlying system and files untouched. This means that the malware could potentially be removed to restore a computer to something close to its original state. This makes locker ransomware less effective at extracting ransom payments compared with its more destructive relative crypto ransomware. Tech-savvy victims are often able to restore access using various tools and techniques offered by security vendors such as Symantec.



BUNDESPOLIZEI

ACHTUNG!

Ihr Windows-System wurde aus Sicherheitsgründen blockiert!

Sie haben eine infizierte Webseite, oder eine pornografischer Art Webseite besucht, deswegen wurde ein kritisches Moment verur

Das bedeutet, dass Ihr S

kann, und Sie

Wählen Sie eine Zahlart aus:

Ukash VORHANDEN

VORHANDEN

ActionFraud Report Fraud & Internet Crime

ASSOCIATION OF CHIEF POLICE OFFICERS

ATTENTION!

For security reasons, your Windows system has been blocked!

The reason can be visiting the infected o pornographic sites. The computer has approached to critical condition because the system can break and all data can be having possibility to restore system, you s install the additional security updates.

This paid update is intended for very infec systems. This update completely protects system from viruses and malware, stabiliz computer system and avoids data loss.

Select the preferable way of payment

Ukash POSSIBLE

POLICE NATIONALE

POLICE

ATTENTION!

Pour des raisons de securite, votre s teme Windows a ete bloque.

La raison peut etre la visite des sites infe pornographiques. L'ordinateur est dans critique, en cause de cela le systeme p tous vos documents et fichiers. Pour a bilite de restaurer la systeme, vous a telecharger la mise a jour compleme systeme de securite.

Cette mise a jour paye est destin pour les systemes infectes. Cett proteger completement votre s virus et les logiciels malveillants, systeme informatique et va eviter la perte nees.

DIRECCIÓN GENERAL DE LA POLICÍA

CUERPO NACIONAL DE POLICÍA

ATENCIÓN

Por razones de seguridad su sistema de Windows ha sido bloqueado.

Debido a que se han visitado siti o pornográficos, el ordenador límite crítico más allá del puede acabar de fu se pueden

Seleccione la opción de pago

Ukash

POLIZIA DI STATO

ATTENZIONE!

Per motivi di sicurezza il suo sistema Windows è stato bloccato.

In seguito a visite a siti pornografici od infestati da virus, il computer è arrivato ad un livello critico oltre il quale potrebbe non funzionare più, e tutti i dati verranno persi. Per avere possibilità di recupero del sistema deve installare un programma aggiuntivo di sicurezza.

Questo programma a pagamento, studiato per i sistemi particolarmente infestati, protegge completamente il sistema dai virus e dai programmi malvagi, stabilizza il sistema del suo computer e previene la perdita dei dati.

Scelga la modalità di pagamento desiderata

Ukash DISPONIBILE ✓

paysafecard paycash. paysafe. DISPONIBILE ✓

Per migliorare (far guarire) il suo sistema, metta il codice per trasferire 100 Euro nei sistemi PaysafeCard o Ukash. Il codice può essere acquistato presso quasi tutti i fornitori di benzina oppure nelle tabaccherie. Tali codici si trovano in vendita anche presso qualsiasi locale dove si vendono le carte per ricaricare il cellulare.

Subito dopo la digitazione del codice e dopo la sua verifica, il suo computer sarà completamente aggiornato e protetto. Tutti i virus ed i cavalli di troia saranno eliminati.

Figure 2. A selection of law enforcement-themed demand notifications seen in locker ransomware

Because locker ransomware can usually be removed cleanly, it tends to be the type of ransomware that goes to great lengths to incorporate social-engineering techniques to pressure victims into paying. This type of ransomware often masquerades as law enforcement authorities and claims to issue fines to users for alleged online indiscretions or criminal activities.

Locker ransomware can particularly be effective on devices that have limited options for users to interact with. This is a potential problem area considering the recent boom in wearable devices and the Internet of Things (IoT), where millions of connected devices could potentially be at risk from this type of ransomware.

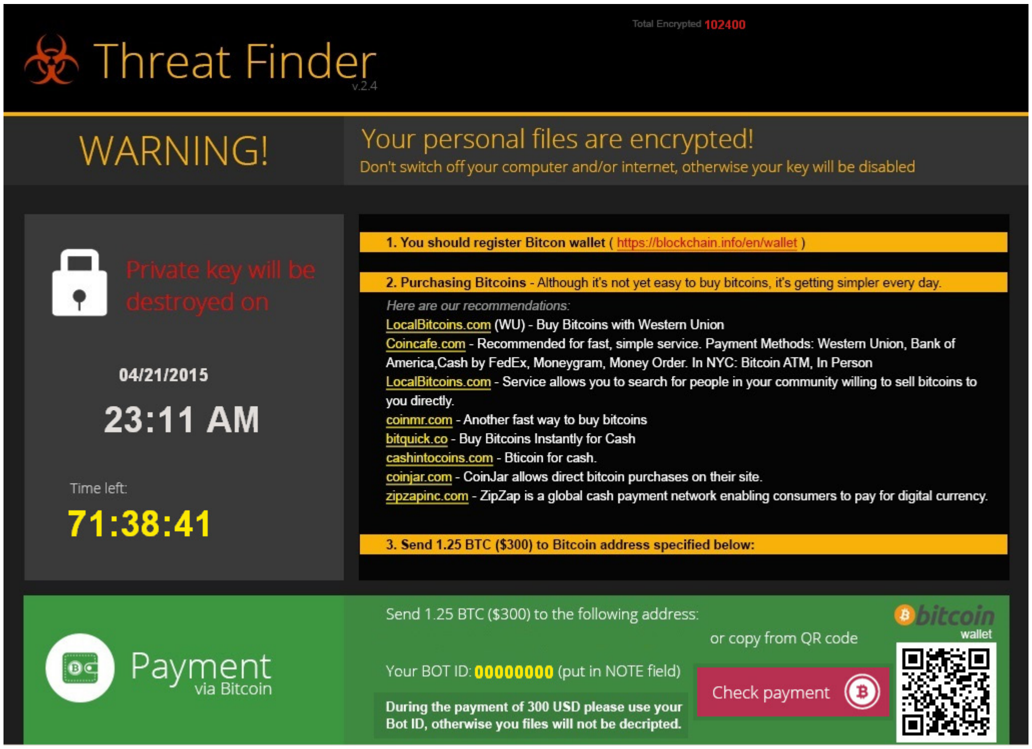
Crypto ransomware (Data locker)

This type of ransomware is designed to find and encrypt valuable data stored on the computer, making the data useless unless the user obtains the decryption key. As people's lives become increasingly digital, they are storing more important data on their personal computers and devices.

Many users are not aware of the need to create backups to guard against hard disk failures or the loss or theft of the computer, let alone a possible crypto ransomware attack. This could be because users don't have the know-how or don't realize the value of the data until it is lost. Setting up an effective backup process requires some work and discipline, so it's not an attractive proposition for the average user.

Crypto ransomware targets these weaknesses in the typical user's security posture for extortion purposes. The creators of crypto ransomware know that data stored on personal computers is likely to be important to users. For example, the data could include things like memories of loved ones, a college project due for submission, or perhaps a financial report for work. The ransomware victims may be desperate to get their data back, preferring to pay the ransom to restore access rather than simply lose it forever and suffer the consequences.

After installation, a typical crypto ransomware threat quietly searches for and encrypts files. Its goal is to stay below the radar until it can find and encrypt all of the files that could be of value to the user. By the time the victim is presented with the malware's message that informs them that their data is encrypted, the damage is already done.



Total Encrypted 102400

Threat Finder v.2.4

WARNING!

Your personal files are encrypted!

Don't switch off your computer and/or internet, otherwise your key will be disabled

Private key will be destroyed on

04/21/2015

23:11 AM

Time left:

71:38:41

1. You should register Bitcon wallet (https://blockchain.info/en/wallet)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

LocalBitcoins.com (WU) - Buy Bitcoins with Western Union

Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person

LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.

coinmr.com - Another fast way to buy bitcoins

bitquick.co - Buy Bitcoins Instantly for Cash

cashintocoins.com - Bticoin for cash.

coinjar.com - CoinJar allows direct bitcoin purchases on their site.

zipzapinc.com - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.25 BTC ($300) to Bitcoin address specified below:

Payment via Bitcoin

Send 1.25 BTC ($300) to the following address:

or copy from QR code

Your BOT ID: 00000000 (put in NOTE field)

During the payment of 300 USD please use your Bot ID, otherwise you files will not be decripted.

Figure 3. A typical crypto ransomware demand screen

With most crypto ransomware infections, the affected computer continues to work normally, as the malware does not target critical system files or deny access to the computer's functionality. This means that users can still use the computer to perform a range of activities apart from accessing the data that has been encrypted.

How ransomware has evolved

The evolution of ransomware has been greatly influenced by a range of developments in technology, economics, security, and culture since 1989.

Today's ransomware is a sophisticated threat affecting users in many regions worldwide, particularly those living in developed and high-tech economies. The ransomware world is like any real life ecosystem. Threats that can adapt and evolve to their surroundings can survive and even thrive, while those that can't or won't adapt may eventually disappear. The ransomware world is a good example of where Darwinian-style evolution is at work.

Ransomware origins

The modern-day ransomware has evolved considerably since its origins 26 years ago with the appearance of the AIDS Trojan. The AIDS Trojan was released into the unsuspecting world through snail mail using 5¼" floppy disks in 1989. Despite the public being unprepared for this new type of threat all those years ago, the AIDS Trojan was ultimately unsuccessful due to a number of factors. Back then, few people used personal computers, the World Wide Web was just an idea, and the internet was mostly used by experts in the field of science and technology. The availability and strength of encryption technology was also somewhat limited at the time. Along with this, international payments were harder to process than they are today.

While the emergence of the AIDS Trojan established the ransomware threat, this type of malware didn't get widely used in cybercrime until many years later. The threat landscape was considerably different back in the nineties and early noughties. That was an era when malware was used in pranks and vandalism to gain notoriety; nowadays, malware is mostly being deployed for financial gain.

The evolution of ransomware, particularly crypto ransomware, accelerated in recent years as more copycat criminal enterprises jumped into the arena to build on others' success.

Pivotal moments in ransomware history

As we look at the recent history of ransomware, it is useful to consider the overall picture of money payment/extortion threats over the past 10 years to get an idea of where modern-day ransomware evolved from.

The graph in Figure 4 shows how the market for extortion malware has been divided up each year since 2005. While each threat never disappeared entirely, it's easy to identify how preferences shifted from one type of extortion malware to another.

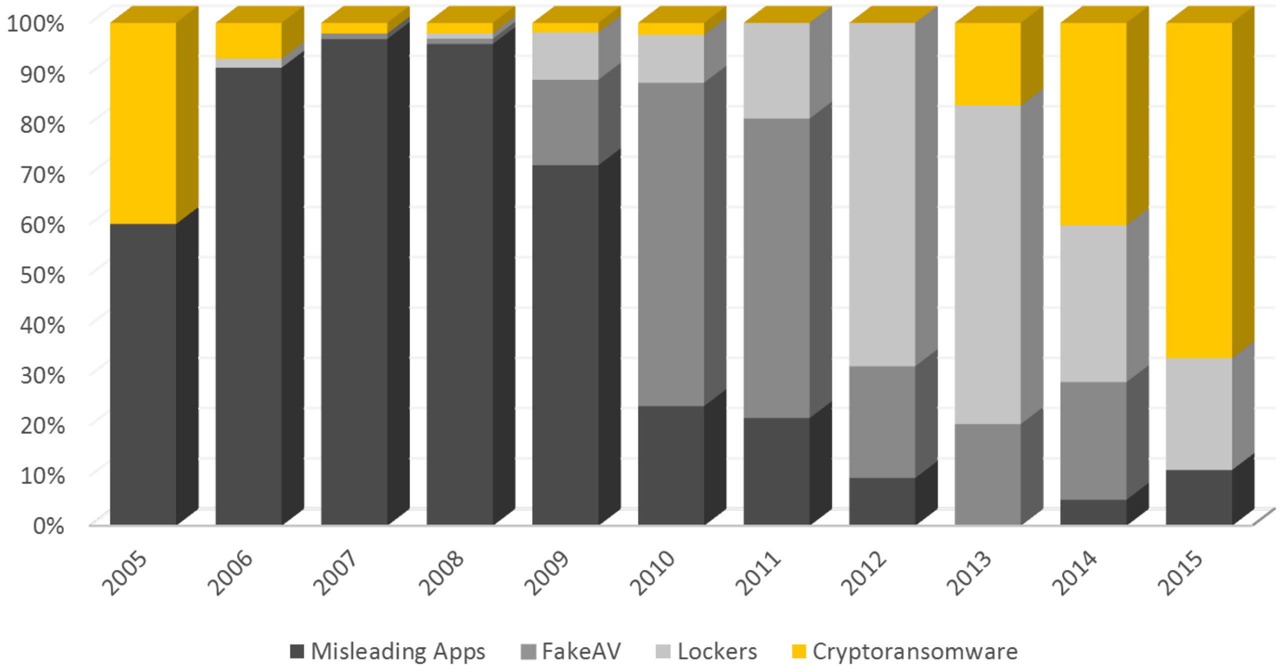


Figure 4. Percentage of new families of misleading apps, fake AV, locker ransomware and crypto ransomware identified between 2005 and 2015

Misleading applications and early ransomware

The first wave of misleading applications began to appear in 2005. The apps posed as fake spyware removal tools, such as SpySherriff, or performance enhancement tools, such as PerformanceOptimizer and RegistryCare. These fake tools mainly affected Windows computers, but also targeted Mac OS X computers. They typically exaggerated the impact of issues on the computer, such as unused registry entries and corrupt files, and said that they would resolve these issues if the user paid between US$30 and US$90 for a license. In reality, many of them did not fix anything.

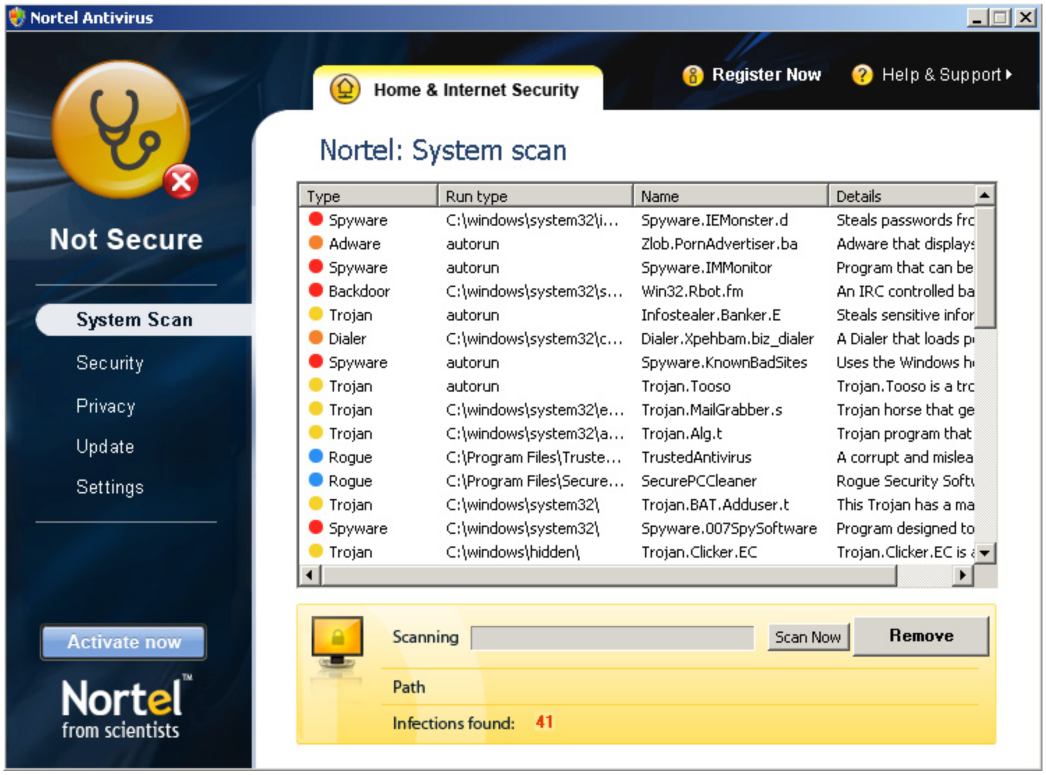
Even at this early stage, the first wave of modern crypto ransomware threats appeared. The Trojan.Gpcoder family emerged in May 2005, initially using custom-encryption techniques which were weak and easily overcome. They also used symmetric encryption algorithms, which meant the same key was used for both encryption and decryption. Despite initial failures, the malware authors did not give up and continued to create newer versions of the threat, making refinements at each step as they learned the lessons from the past failures.

By early 2006, the concept of crypto ransomware started to gain traction as attackers started to experiment with the idea. This renaissance in crypto ransomware led to the appearance of threats like Trojan.Cryzip in March 2006. Cryzip copied data files into individual password-protected archive files and then deleted the originals. However, the password was actually embedded inside the code of the Trojan itself, making it easy to recover the password.

Trojan.Archiveus also emerged in 2006. Like Cryzip, Archiveus used password-protected archive files but in a bizarre twist, the malware did not ask for cash payment. Instead, it asked the victim to buy medication over the internet using certain online pharmacy URLs. The victim then needed to submit the order ID to get the password to decrypt the archive files. In this way, the attackers could have earned commission from the purchase which was then considered as a ransom payment–though the makers of Archiveus would not have approved of this terminology.

Fake AV

The next pivot point happened between 2008 and 2009, when cybercriminals switched to using fake antivirus programs, a more aggressive subcategory of misleading applications. The tools mimicked the appearance and functionality of legitimate security software and performed mock scans, claiming to find large numbers of threats and security issues on the computer. The user was then asked to pay a fee of between US$40 and US$100 to fix the fake problems. They may also have been asked to pay for bogus multi-year support services. However, some fake AV victims chose to ignore the alerts or removed the software, resulting in a lower return on investments for the cybercriminals.



Nortel: System scan

Type	Run type	Name	Details
● Spyware	C:\windows\system32\i...	Spyware.IEMonster.d	Steals passwords frc
● Adware	autorun	Zlob.PornAdvertiser.ba	Adware that displays
● Spyware	autorun	Spyware.IMMonitor	Program that can be
● Backdoor	C:\windows\system32\s...	Win32.Rbot.fm	An IRC controlled ba
● Trojan	autorun	Infostealer.Banker.E	Steals sensitive infor
● Dialer	C:\windows\system32\c...	Dialer.Xpehbam.biz_dialer	A Dialer that loads p
● Spyware	autorun	Spyware.KnownBadSites	Uses the Windows h
● Trojan	autorun	Trojan.Tooso	Trojan.Tooso is a trc
● Trojan	C:\windows\system32\e...	Trojan.MailGrabber.s	Trojan horse that ge
● Trojan	C:\windows\system32\a...	Trojan.Alg.t	Trojan program that
● Rogue	C:\Program Files\Truste...	TrustedAntivirus	A corrupt and mislea
● Rogue	C:\Program Files\Secure...	SecurePCCleaner	Rogue Security Soft
● Trojan	C:\windows\system32\	Trojan.BAT.Adduser.t	This Trojan has a ma
● Spyware	C:\windows\system32\	Spyware.007SpySoftware	Program designed to
● Trojan	C:\windows\hidden\	Trojan.Clicker.EC	Trojan.Clicker.EC is

Scanning

Path

Infections found: 41

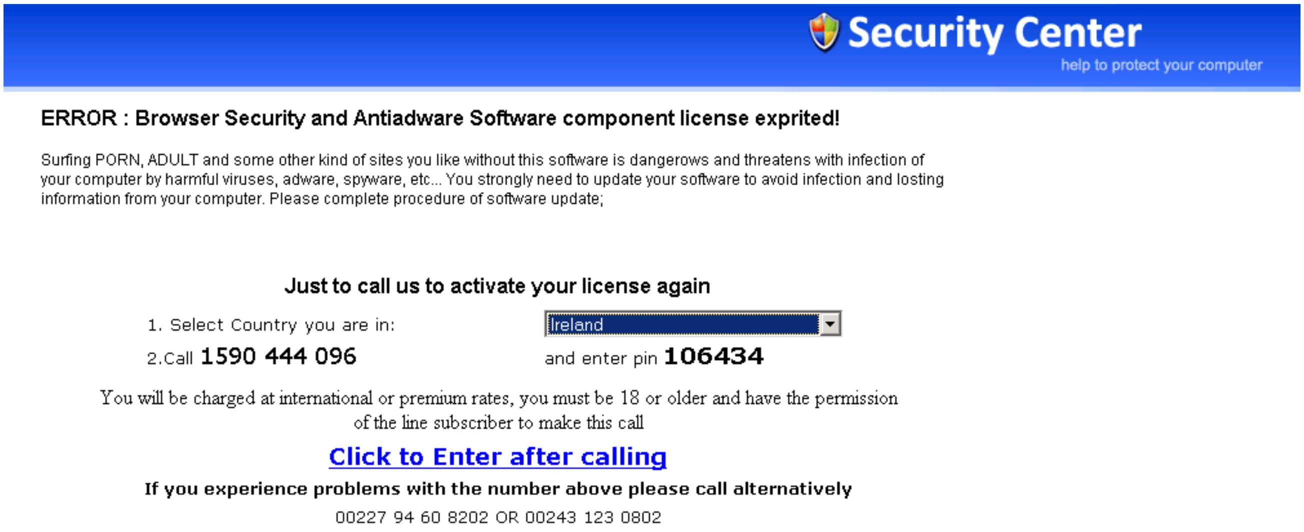
Figure 5. "Nortel Antivirus" is designed to mimic the Norton antivirus software

To address the fundamental weaknesses of fake antivirus scams, cybercriminals looked for new ways to make the call-to-action stronger.

The move to locker ransomware

From 2011 to 2012, attackers transitioned from fake antivirus tools to a more disruptive form of extortion. This time, the cybercriminals disabled access and control of the computer, effectively locking up the computer from use. In terms of ransom amounts, locker ransomware pushed up the benchmark compared with fake antivirus and misleading apps. A typical locker ransomware threat charges around US$150 to US$200 payable through electronic cash vouchers.

Locker ransomware emerged a few years before its peak between 2011 and 2012. The first of the pure computer-locking malware hit users around the start of 2008 in the shape of Trojan.Randsom.C. This pioneer spoofed a Windows Security Center message and asked the user to call a premium-rate phone number to reactivate a license for security software. The computer was locked during this time, so the user was unable to use the computer for any other purpose.



ERROR : Browser Security and Antiadware Software component license exprited!

Surfing PORN, ADULT and some other kind of sites you like without this software is dangerows and threatens with infection of your computer by harmful viruses, adware, spyware, etc... You strongly need to update your software to avoid infection and losting information from your computer. Please complete procedure of software update;

Just to call us to activate your license again

1. Select Country you are in: Ireland

2.Call **1590 444 096** and enter pin **106434**

You will be charged at international or premium rates, you must be 18 or older and have the permission of the line subscriber to make this call

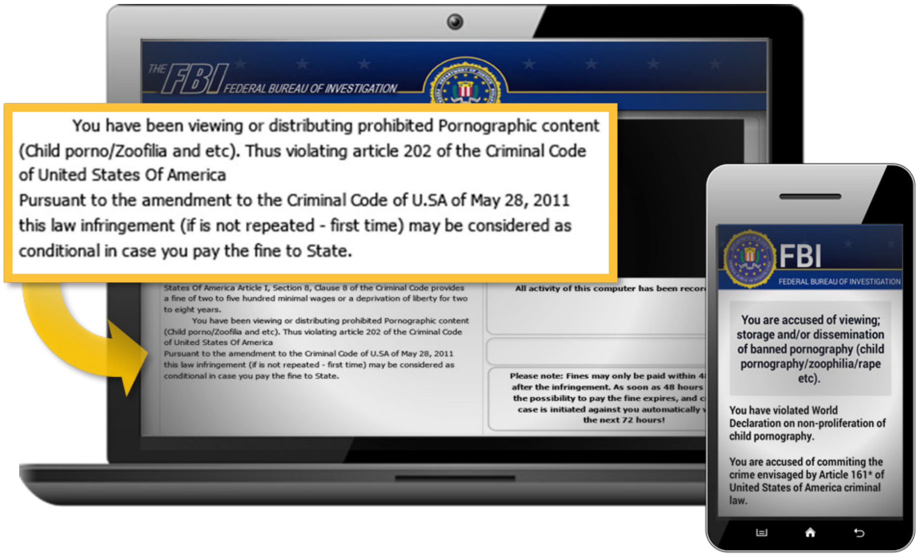
If you experience problems with the number above please call alternatively

00227 94 60 8202 OR 00243 123 0802

Figure 6. Fake Windows Security Center message demanding payment from victims for using "exprited" software (Trojan.Randsom.C)

As locker ransomware was refined, it went from just reporting non-existent errors to actually beginning to introduce errors and problems. Eventually, it dropped any pretense of being a helpful tool to just displaying a blatant request for payment to restore access to the computer. This is because in the early days, attackers tricked victims into downloading fake tools to fix computer issues. Today, ransomware can be installed without any user interaction through attacks such as drive-by downloads.

Despite this, locker ransomware creators still continued to use social-engineering techniques to convince users to pay the ransom. The threats began to pose as law enforcement notices instead of antivirus software and system performance tools. They typically claimed that the user had broken the law by downloading copyrighted materials such as pirated music, movies, or software (a common occurrence according to various industry statistics), or viewing other illegal digital materials such pornographic images depicting minors or animals.



You have been viewing or distributing prohibited Pornographic content (Child porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States Of America
Pursuant to the amendment to the Criminal Code of U.SA of May 28, 2011 this law infringement (if is not repeated - first time) may be considered as conditional in case you pay the fine to State.

States Of America Article I, Section 8, Clause 8 of the Criminal Code provides a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States Of America
Pursuant to the amendment to the Criminal Code of U.SA of May 28, 2011 this law infringement (if is not repeated - first time) may be considered as conditional in case you pay the fine to State.

All activity of this computer has been recor

Please note: Fines may only be paid within 4
after the infringement. As soon as 48 hours
the possibility to pay the fine expires, and c
case is initiated against you automatically v
the next 72 hours!

You are accused of viewing; storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc).

You have violated World Declaration on non-proliferation of child pornography.

You are accused of commiting the crime envisaged by Article 161* of United States of America criminal law.

Figure 7. A typical law enforcement-themed locker ransomware notice alleging access to illegal content

These serious allegations, along with realistic-looking (but fake) threats from law enforcement authorities, allowed the cybercriminals to evolve their ransom demands from being about a price for a service to a payment of a fine.

Judging by the number of law enforcement-themed ransomware that proliferated between 2012 and 2014, this was clearly an effective way to make victims pay. The technique can be very convincing but it can also lead to unexpected outcomes. For example, a man in Virginia handed himself over to police after seeing the charges of handling child porn appear on his screen because he believed that the faked law enforcement notice was real.

While locker ransomware was effective, it was still possible for people to remove these threats using security software from Symantec and other vendors and restore access to the computer. An increased number of reports on these scams helped to raise awareness of them, causing attackers' revenue to sink.

The move to crypto ransomware

Deficiencies in all the other extortion schemes ultimately led the cybercriminals back to the original type of ransomware. From 2013 to the present day, there has been a pivot back to crypto ransomware. Crypto ransomware tends not to use social engineering; instead it is upfront about its intentions and demands. The threats typically display an extortion message, offering to return data upon payment of hefty ransoms.

Crypto ransomware has raised the ransom amounts bar to a new level. A typical crypto ransomware threat requests payment of around US$300 for a single computer. Today's crypto ransomware threats are much more capable than its predecessors, with stronger operational and encryption procedures.

Learning the "key" lessons

The lesson that crypto ransomware makers failed to learn in the early days was that when using encryption, proper key management is crucial for success.

For example, Trojan.Gpcoder.E (July 2007) boasted of using asymmetric RSA encryption with a 4096-bit key, but in reality, it only used custom symmetric encryption. It generated a four-byte long encryption key (32-bit) which was then stored in the registry of the compromised computer, meaning that it was possible for people to find the key on the computer.

The other common method for mishandling keys is to have the keys stored within the crypto ransomware itself, which is the equivalent of hiding the house keys under the door mat. To make matters worse for the attackers, they used the same key in all of the variants, so if one victim extracted the key, it would work in all samples.

Another important lesson that some cybercriminals learned from earlier mistakes was the need to choose the right encryption algorithm. This led to attackers using industry-standard encryption algorithms, such as RSA, Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) with a suitably large key in their ransomware. Trojan.Gpcoder.F (June 2008) was one of the first threats to implement what was then industrial-strength encryption. It used RC4 to encrypt files, then encrypted the RC4 encryption key using an RSA-1024 public key, and went on to delete the original key. Even though the RC4 key remained on the infected computer, it was protected by strong public-key encryption, making it impractical to brute force at the time.

But even with improved encryption, some recent ransom schemes are still not always water tight. Poor operations and procedures dog the efforts of cybercriminals, leaving victims with room to maneuver. Even today, some still continue to make rookie mistakes such as leaving behind keys. This suggests that the current ransomware scene is highly fragmented with many new actors trying to establish themselves in a market already dominated by small groups of professional cybercriminals.

Technically capable cybercriminals have now evolved their crypto ransomware to a high level of maturity. Sophisticated crypto ransomware variants generate a new individual asymmetric key for each infection and wipe the session key from memory after usage. They use industrial-strength, public/private-key encryption combined with good operational procedures to make it virtually impossible to get around them without paying the ransom. They also use privacy-enabling services, such as Tor, and favor bitcoins for payment. This is all designed to help them avoid being identified by law enforcement agents, who are paying closer attention to this ongoing menace than ever before.

TARGETS FOR RANSOMWARE

> “The cybercriminals behind ransomware do not particularly care who their victims are, as long as they are willing to pay the ransom.”

Targets for ransomware

The cybercriminals behind ransomware do not particularly care who their victims are, as long as they are willing to pay the ransom. With this in mind, it is easy to see why the cybercriminals tend to take a scatter-gun approach to propagating the ransomware, casting a wide net across targeted regions and types of users. With the cybercriminals hitting millions of users worldwide, if even a small percentage of victims pay the ransom, then it could make the scheme worthwhile. This is why our default recommendation is not to pay the ransom.

Home users

Ransomware is perhaps the most effective against individuals who are not fluent with computers or are not familiar with ransomware and how it works. The most common group that we see impacted by ransomware is the home user, who often has the least amount of access to technical assistance. The lack of support may leave the user feeling isolated and helpless, further increasing the pressure to pay.

Home users often have sensitive information, files, and documents that are personally valuable stored on the computer, such as college projects, photos, and video game save files. Despite these things being of value to users, home users are still unlikely to have an effective back up strategy in place to successfully recover from events such as a fire or theft, let alone a crypto ransomware attack. A previous survey by Symantec/Norton showed that 25 percent of home users did not do any backups at all. Fifty-five percent backed up some files. In terms of backup frequency, only 25 percent of users backed up files once a week. The rest only made backups once a month or even less frequently than that. This means users are potentially leaving themselves exposed in the event of a ransomware attack.

Even if the home user has a backup process, some threats delete local backups on the computer and encrypt backup files on external storage devices that are connected to the computer.

Businesses

For many businesses, information and the technology to use it is their life blood, without which the act of conducting day-to-day business is impossible. Consider a retailer running a computerized point-of-sale (POS) system. If the POS system was unavailable due to a ransomware infection, the retailer would not be in a position to transact sales. Business computers are also more likely to contain sensitive data and documents of critical importance, such as customer databases, business plans, proposals, reports, source code, forms, and tax compliance documents. Modern crypto ransomware threats can enumerate all accessible drives, such as local file-share servers, and encrypt files on these as well. This means more than one system can be impacted by just a single crypto ransomware infection.

The loss of this information could have a catastrophic impact on the business. While many companies have backup and disaster recovery plans, there are still many who do not. Some organization’s disaster recovery plans may not extend to cover the individual end users. Even if the businesses had plans, it is quite possible that they have not been tested and may not work as expected when required. These factors make individual business users a viable target for traditional crypto ransomware.

Aside from ransomware impacting individual business users, there have also been cases reported where the company itself had been targeted with file-encrypting ransomware. In a case involving PHP.Ransomcrypt.A, the attackers were believed to have compromised an organization for months, quietly encrypting the database along with all of the incremental backups. At the appropriate time, the attackers made their substantial ransom demands known to the business, threatening them with the potential loss of several months’ worth of data.

Public agencies

Public agencies such as educational institutes and even law enforcement entities are not excluded from the attention of these cybercriminals and in some cases, they may be specifically targeted. There have been several reports of law enforcement agencies that had been hit with crypto ransomware in the past. In another case, a

New Jersey school district, which runs four elementary schools in the Swedesboro-Woolwich area, was hit by cybercriminals who demanded a ransom payment of 500 bitcoins (US$124,000).

The latter incident proved to be highly disruptive, as the attackers compromised computers and files used by staff and students. These cases highlight the brazenness of the attackers who are not even afraid of holding law enforcers to ransom. The cybercriminals believe that they are beyond the reach of the law by operating from another jurisdiction.

Systems impacted by ransomware

Modern ransomware can impact many different types of systems. With the increasing computerization of everyday activities, we are finding that computers are becoming ubiquitous and can be found almost everywhere. Trends such as IoT will widen the horizon further for computerization. There are already lightweight Linux-based systems in many types of small gadgets and household appliances, such as portable media players, routers, refrigerators, TVs, mobile phones, tablets, set top boxes, network-attached storage (NAS) devices, and surveillance cameras. Most of these can potentially be targeted with ransomware attacks.

However, at this time, the most frequently targeted computing environments for ransomware are personal computers, mobile devices, and servers.

Personal computers

The vast majority of ransomware threats today are designed to target personal computers running the Windows operating system. This is unsurprising, as Windows-based computers make up around 89 percent the OS market share for desktop computers, with Mac OS X and Linux making up the rest. Given that ransomware is a commercial activity for cybercriminals, it makes sense for them to maximize potential returns on their investments.

Ransomware has to be tailored specifically for a given operating system because it often has to leverage system API hooks to block or limit access to controls such as the mouse or keyboard. In addition, many crypto ransomware threats now make use of inbuilt encryption libraries or APIs supplied with the operating system to perform the encryption and decryption process itself. This saves the attackers from inventing their own secure encryption method (a very difficult task) and propagating additional files and libraries with their ransomware distribution.

The downside of using OS-specific APIs is that the ransomware is tied to a particular operating system, but given the massive market share of the Windows operating systems, this minor drawback may not be a major factor for cybercriminals

However, in recognition of the small but significant pool of non-Windows users, some enterprising cybercriminals have created the Browlock Trojan (detected by Symantec as Trojan.Ransomlock.AG). The threat is implemented in JavaScript and is designed to work on a wide range of web browsers, making it operating system agnostic. While this browser-locking technique is less effective from a technical point of view, this tactic is designed to hoover up the remaining potential victims who may not otherwise be targeted.

Mobile devices

The next most targeted types of devices are tablets and mobile phones. These devices have become ubiquitous worldwide, with studies showing that users are spending more time on mobile devices than ever before. Ever since the advent of the iPhone back in 2007 and Android in 2008, smartphone and tablet device ownership has been on a steep upward trajectory. Today, there are basically just two main players in the mobile OS market: Android and iOS. Android has a massive global footprint, with a share of over 80 percent of the mobile market, representing billions of smartphone and tablets worldwide. In terms of the malware landscape, there is a world of difference between the Android and iOS world.

iOS users who have not jail-broken their phones have been quite well protected by Apple's tightly controlled ecosystem. For a non-jail-broken iOS user, the ability to install apps outside of the official App Store is extremely limited with some exceptions such as apps developed with enterprise-provisioning certificates. A ransomware developer who wishes to explore this route would first have to obtain an enterprise developer certificate from Apple, build their app, sign it with the enterprise certificate, distribute it to potential victims, and convince them to install it. The problem for the cybercriminals in this scenario is that their room to maneuver could be highly restricted and Apple could easily shut down their operation simply by revoking the certificate. This makes ransomware development activity for iOS very risky with little prospect of payback.

Android is a much more open and permissive platform. This openness has advantages and disadvantages. Many users like the freedom and flexibility to choose to install whatever type of app they wish from any source they like. The downside is that this same flexibility can make it easier for malware creators to operate and spread their creations. This is one key reason why we see many more Android-based threats compared with threats for iOS.

To tap into this growing and potentially lucrative user base, ransomware targeting Android devices has already been created. Android.Fakedefender, discovered in June 2013, marked the crossover from the standard fake antivirus scam to locker ransomware on the Android platform. Android.Fakedefender purported to be a security scanner but when it inevitably found "critical threats," the device interface was locked down to prevent victims from launching other apps or change settings in the operating system. The malware also tried to prevent victims from uninstalling it. These tactics were all designed to coerce victims into paying for a license for the fake software, which the ransomware promised would resolve the issues reported.

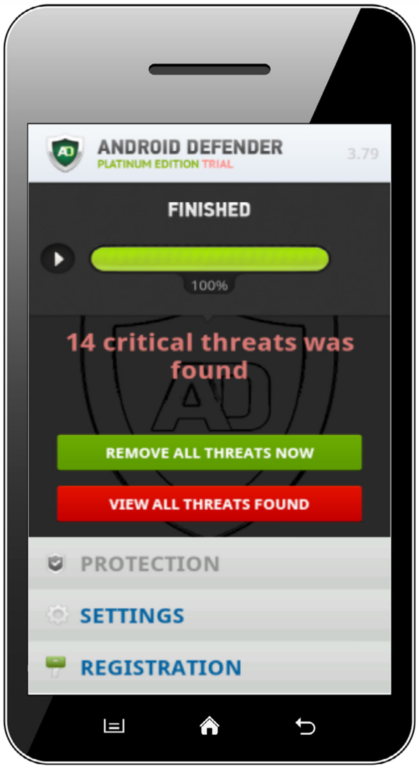
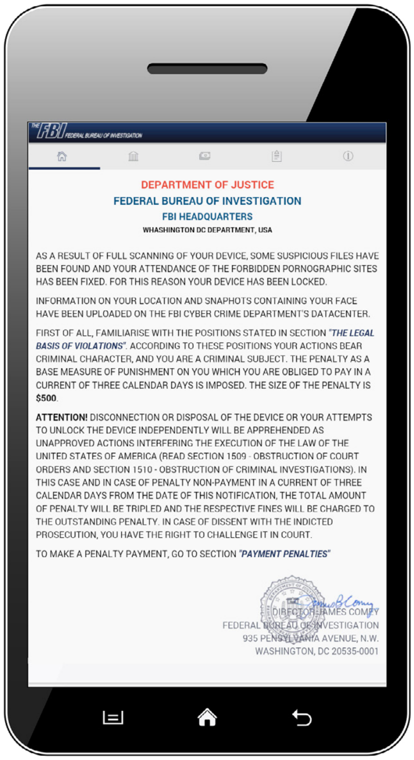


Figure 8. False threats found by Android.Fakedefender

Later entrants began to focus purely on being a locker ransomware rather than pretending to be a security tool. Android.Lockdroid.E, seen in 2014, was one of the earliest examples of this class of ransomware hitting Android devices. It borrowed heavily from the techniques and tactics used by desktop-locker ransomware, which had reached a high level of maturity by this time. Lockdroid.E was packaged up as a mobile app for a popular adult video website to entice potential victims into installing it. Once installed, the Trojan displayed a fake FBI warning that demanded payment of a US$500 fine for accessing "forbidden pornographic sites" and then locked the device while displaying the notice.

In 2014, we also saw the emergence of crypto ransomware for Android devices in the shape of Android.Simplocker. Simplocker was heavily inspired by desktop crypto ransomware at the time, but its execution of the scam was somewhat curtailed by the security model of the Android operating system. Security restriction prevents apps from accessing file and data belonging to other apps. However, in previous versions of Android, files such as images, documents, and media files stored on external SD memory cards were often not protected by this mechanism in older versions of the OS, so they could be accessed by other apps. This means Simplocker could access and encrypt files stored in the memory card. Many Android devices are designed with meagre amounts of internal storage, so an SD card is a common upgrade that users implement to boost the internal storage of the device. Some Android-



DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WHASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION *"THE LEGAL BASIS OF VIOLATIONS"*. ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED. THE SIZE OF THE PENALTY IS **$500**.

ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS NOTIFICATION, THE TOTAL AMOUNT OF PENALTY WILL BE TRIPLED AND THE RESPECTIVE FINES WILL BE CHARGED TO THE OUTSTANDING PENALTY. IN CASE OF DISSENT WITH THE INDICTED PROSECUTION, YOU HAVE THE RIGHT TO CHALLENGE IT IN COURT.

TO MAKE A PENALTY PAYMENT, GO TO SECTION *"PAYMENT PENALTIES"*

James B Comey
DIRECTOR JAMES COMEY
FEDERAL BUREAU OF INVESTIGATION
935 PENSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20535-0001

Figure 9. FBI-themed lock screen from Android.Lockdroid.E, one of the first pure locker ransomware for mobile devices

based ransomware even tried to set a device PIN code if there was none implemented, making it impossible for the user to access content on their phone.

Studies have shown that mobile devices tend to be used more for messaging and leisure-related activities such as web browsing or media consumption rather than productivity. This makes it less likely that highly valuable files will be present on the mobile device compared to a desktop computer. Based on these usage trends along with the technical limitations previously mentioned, the chances of securing payment using crypto ransomware on mobile devices are likely to be considerably smaller.

At this time, we would still consider mobile ransomware to be at the experimental stage of development, where cybercriminals are releasing their ransomware into the field and observing the results before making decisions on future iterations. We have not yet seen an explosion of ransomware for mobile devices as we had for desktop computers. This may change in the future as mobile technology and usage patterns such as mobile payments continue to evolve, blurring the line between mobile and desktop computing.

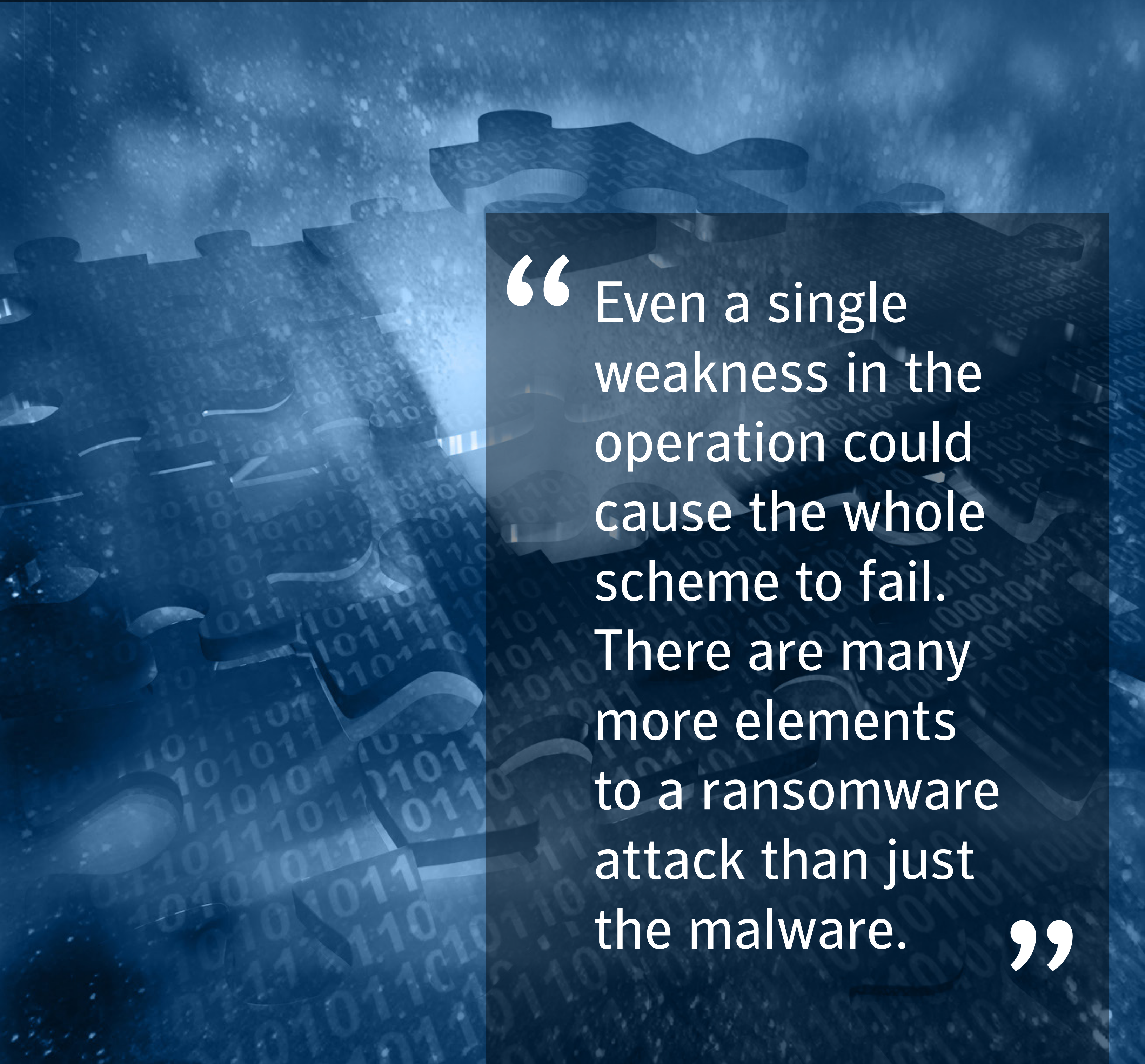
Servers

Servers represent a different type of proposition for cybercriminals aiming to extract ransom payments. Servers are much more likely to contain data that is critical to the operations or even survival of an organization. They act as central repositories for documents, source code, financial records and transactions, user databases, and trade secrets, making them high-value potential targets. Given the critical role that servers play, many organizations have disaster recovery and business continuity plans (BCP) built around maintaining operations and ensuring the backup of data. Despite this, taking out a critical server even for a short time could be incredibly disruptive and damaging. Because of these contingency plans, cybercriminals have been forced to adopt a different approach to extracting ransoms when attacking organizations and their servers.

Symantec has previously observed that attackers traditionally blackmail businesses by unleashing an unexpected distributed denial-of-service (DDoS) attack against an organization’s servers and then following up with an extortion demand. As a result of this, many organizations who are susceptible to DDoS attacks have enlisted the help of DDoS mitigation services to reduce the impact of these attacks. This in turn has encouraged cybercriminals to look for alternative ways to hold organizations to ransom by targeting one of their most critical infrastructural assets–the servers and the data held in them.

Some groups do this by infiltrating the target server and patching the software so that the stored data is in an encrypted format where only the cybercriminals have the key to decrypt the data. The premise of this attack is to silently encrypt all data held on a critical server, along with all of the backups of the data. This process may take some time, depending on the organization, so it requires patience for the cybercriminals to carry it out successfully. Once a suitable number of backups are encrypted, the cybercriminals remove the decryption key and then make their ransom demands known, which could be in the order of tens of thousands of dollars.

RANSOMWARE: HOW IT WORKS



“Even a single weakness in the operation could cause the whole scheme to fail. There are many more elements to a ransomware attack than just the malware.”

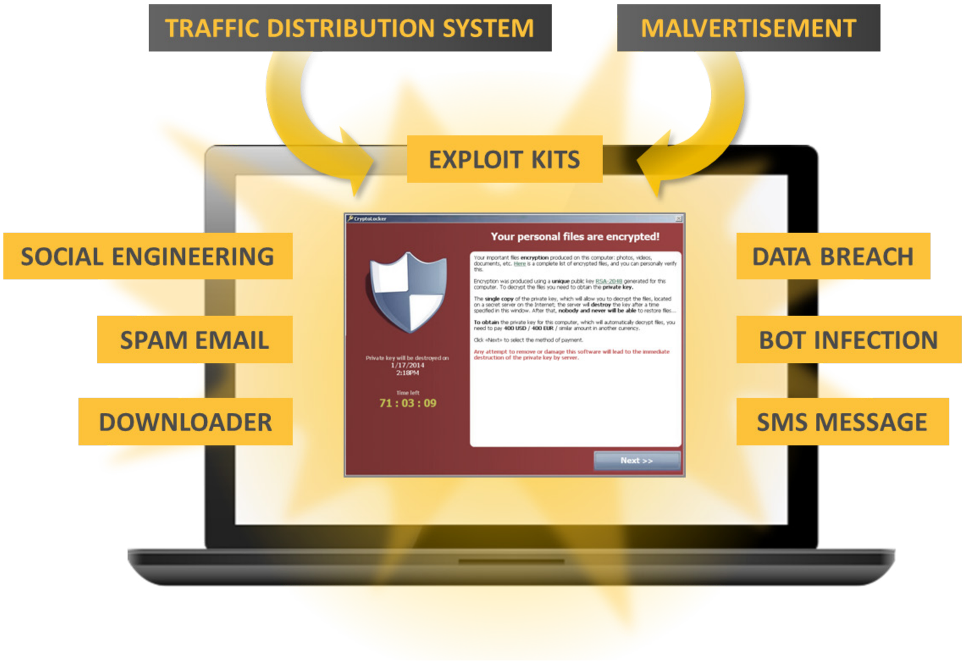
Ransomware: How it works

Carrying out digital extortion using ransomware is a carefully planned and executed process for cybercriminals. Even a single weakness in the operation could cause the whole scheme to fail. There are many more elements to a ransomware attack than just the malware.

Propagation

One of the first questions many victims ask is “how did I get infected with ransomware?” While it is not always immediately clear, the infection method for ransomware follows the same modus operandi used by cybercriminals to infect victims with any malware.

As seen in Figure 10, there are many paths that can lead to a ransomware infection. However, the skillset and resources required to overcome modern defenses for the distribution of malware is outside of the scope of many amateur cybercriminals. This has led to an underground cybercrime ecosystem where different groups specialize in distinct areas of cybercrime, such as malware distribution, for a price. In many ways, these malware distribution services are run like any other business service. In some cases, they have even adopted common software industry compensation methods for malware installs, such as the pay-per-install (PPI) model.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **400 USD / 400 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
1/17/2014
2:18PM

Time left
71 : 03 : 09

Figure 10. Routes for ransomware to arrive on a computer

Ransomware attackers have been seen to use different techniques or services to get their malware onto a victim’s computer.

Traffic distribution system (TDS)

A common method used by these distribution services is to buy redirected web traffic from a Traffic Distribution Service (TDS) vendor and point it to a site hosting an exploit kit. In a lot of cases, the redirected traffic originates from adult content-related websites. If the exploit kit is successful in exploiting a vulnerability in the visiting victims’ computer, it can lead to what is commonly referred to as the drive-by-download of malware.

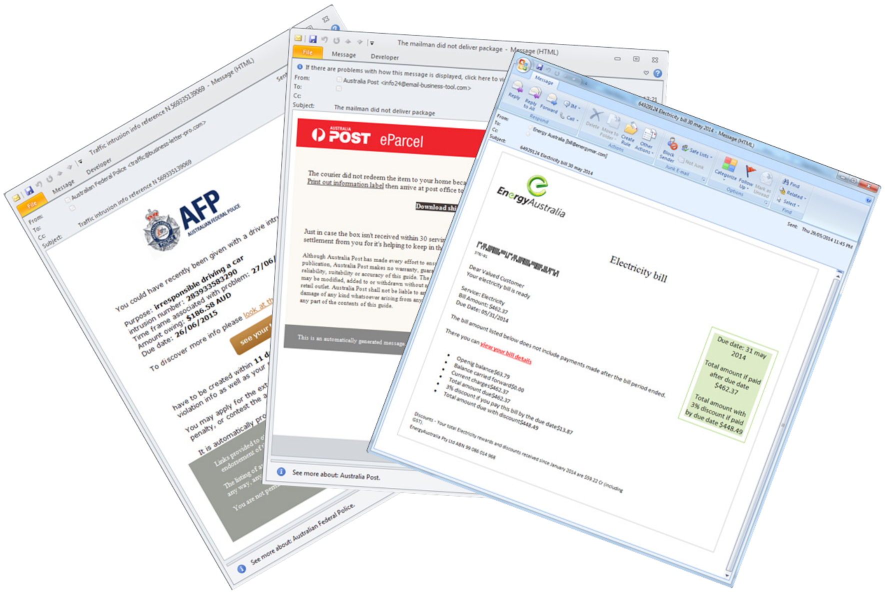
Malvertisement

Similarly, malicious advertisements known as malvertisments can get pushed onto legitimate websites in order to redirect traffic to a site hosting an exploit kit. In one case, we even observed unintentional cross contamination as a result of a click-fraud malware infection, where clicking on the malvertisment led to a ransomware infection. In both cases, cybercriminals can use real-time bidding to purchase traffic or ad space of interest that can allow them to geographically target victims and operate without borders.

Spam email

For many years, email spam using social-engineering themes has been the method of choice for distributing all types of malware including ransomware. Cybercriminals use a botnet to send the spam. These cybercriminals may also offer a spamming service to other attackers for a fee.

The spam usually comes in the form of an email containing a malicious attachment or a link in the email leading to a site hosting an exploit kit. The spam may also involve the download of malware through other social-engineering means. The spam emails embody a whole range of social-engineering and psychological levers to trick users into installing the ransomware.



Traffic intrusion info reference N 569335139069 - Message (HTML)

From: Australian Federal Police <traffic@business-letter-pro.com>
To:
Cc:
Subject: Traffic intrusion info reference N 569335139069

AFP AUSTRALIAN FEDERAL POLICE

You could have recently been given with a drive intr
Purpose: irresponsible driving a car
intrusion number: 283933583290
Time frame associated with problem: 27/06/
Amount owing: $186.58 AUD
Due date: 26/06/2015
To discover more info please look at th
see your
have to be created within 11 d
violation info as well as your
You may apply for the ext
penalty, or contest the a
It is automatically pro
Links provided to o
endorsement of
The listing of a
any way, any
You are not perm
See more about: Australian Federal Police.

The mailman did not deliver package - Message (HTML)

If there are problems with how this message is displayed, click here to vi
From: Australia Post <info24@email-business-tool.com>
To:
Cc:
Subject: The mailman did not deliver package

AUSTRALIA POST eParcel

The courier did not redeem the item to your home beca
Print out information label then arrive at post office to
Download shi
Just in case the box isn't received within 30 servi
settlement from you for it's helping to keep in th
Although Australia Post has made every effort to ens
publication, Australia Post makes no warranty, guar
reliability, suitability or accuracy of this guide. The
may be modified, added to or withdrawn without n
retail outlet. Australia Post shall not be liable to an
damage of any kind whatsoever arising from any
any part of the contents of this guide.
This is an automatically generated message
See more about: Australia Post.

64929124 Electricity bill 30 may 2014 - Message (HTML)

From: Energy Australia [bill@energymar.com]
To:
Cc:
Subject: 64929124 Electricity bill 30 may 2014
Sent: Thu 29/05/2014 11:45 PM

EnergyAustralia

Electricity bill

Dear Valued Customer
Your electricity bill is ready
Service: Electricity
Bill Amount: $462.37
Due Date: 05/31/2014
The bill amount listed below does not include payments made after the bill period ended.
There you can view your bill details

- Openig balance$63.79
- Balance carried forward$0.00
- Current charges$462.37
- Total amount due$462.37
- 3% discount if you pay this bill by the due date$13.87
- Total amount due with discount$448.49

Due date: 31 may 2014
Total amount if paid after due date $462.37
Total amount with 3% discount if paid by due date $448.49

Discounts - Your total Electricity rewards and discounts received since January 2014 are $59.22 Cr (including GST).
EnergyAustralia Pty Ltd ABN 99 086 014 968

Figure 11. Examples of crypto ransomware-distribution emails posing as the Australian police, mail service, and a local energy supplier

In recent years, the spam emails used to distribute ransomware have favored the following themes:

- Mail delivery notification
- Energy bills
- Job seeker resume
- Tax returns and invoices
- Police traffic offense notifications

Downloaders & botnets

This method is one of a number of ways to distribute malware known as downloaders. Once the downloader infects a computer, its job is to download secondary malware onto the compromised system. The cybercriminals behind downloaders offer a malware-installation service onto already compromised computers, at a price to other malware authors. Trojan botnets have also been known to download ransomware onto computers they have infected. This is usually done by cybercriminals as a final way of monetizing infected computers that they control.

Social engineering and self-propagation

Some ransomware also contain functionality to spread. For example, on Android, there are some samples that not only lock the device or encrypt files, but employ worm-like capabilities to spread to all contacts within the device's address book by sending social-engineering SMS messages.

On the Windows platform, a variant of the Ransomlock (W32.Ransomlock.AO) screen locker is known to infect other files as a way to spread. Self-propagation is potentially an effective way for the ransomware to spread itself, but it does cause problems for the cybercriminals who are hoping for a ransom to be paid. If the ransomware is continuously spreading through a network, infecting multiple computers and demanding payment each time, the cybercriminal's promise to repair the damage after the victim pays the ransom is broken. Nobody will be willing to pay if the same gang continues to demand ransom payment after payment.

Affiliate schemes

Cybercriminals who have paid attention to the growing interest in ransomware have started to provide services to those who wish to carry out these attacks, effectively providing ransomware-as-a-service (RaaS). They offer a way to buy into the growing ransomware scene without needing to have the skills to create a ransomware or to maintain and run the operations.

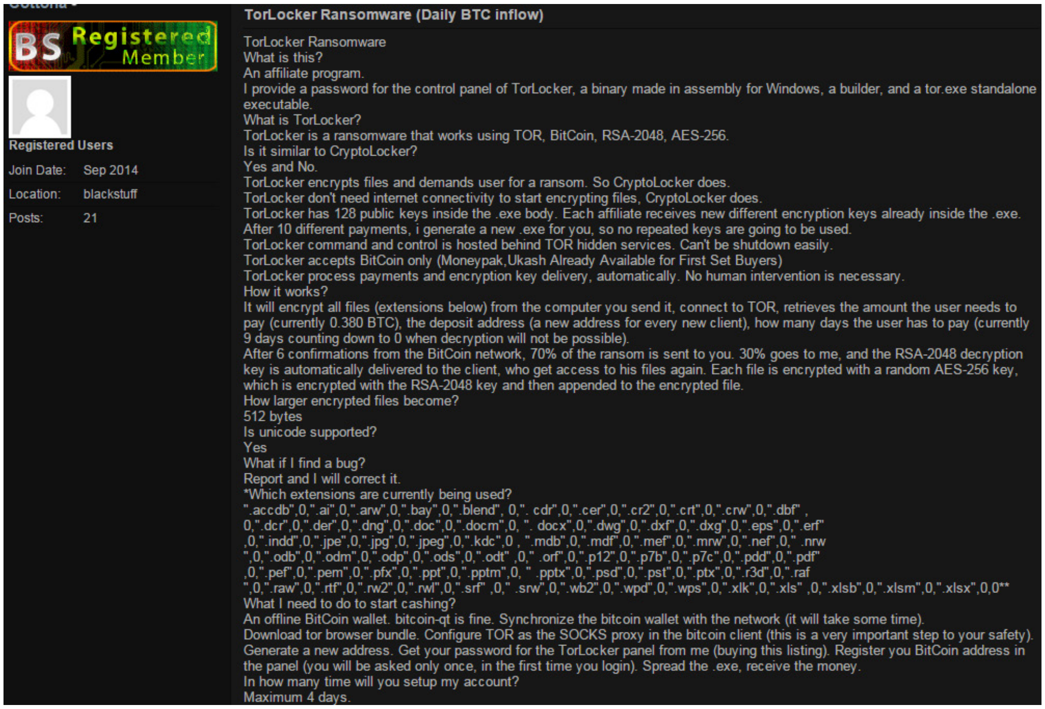
Affiliate schemes can offer members a substantial cut of the profits from each ransomware infection, making it a strong incentive. All the affiliate member has to do is to spread the ransomware as far and wide as possible to maximize the chances of extracting a ransom. This offers the RaaS vendor a better opportunity to get their ransomware to a wider group of potential victims, letting them focus on developing and enhancing the ransomware and leaving the propagation to others.

In the case of Torlocker, the malware author marketed their RaaS to other cybercriminals, offering them the opportunity to join an affiliate program. Affiliates would be provided with the crypto ransomware binary file and access to a control panel at a cost of US$300. They would then be required to spread the crypto ransomware on behalf of the malware author. For each ransom paid, the malware author would receive 30 percent while the affiliate would pocket the remaining 70 percent.

Another recent example of RaaS was created by a teenage student who apparently wrote the Tox RaaS platform and offered it to customers to allow them to carry out extortion attacks. The kit boasted of a user-friendly environment to create and manage the ransomware operation. Just like other affiliate schemes, the Tox creator simply took a cut of the earnings. Just one week after Tox was made available, its student creator had a sudden change of heart, putting the whole scheme up for sale in a PasteBin post. In it, he explained that it experienced huge growth and went out of control. His original intent was to stay below the radar, possibly to avoid the attention of law enforcement or perhaps other cybercriminals whose business he may have trespassed on. Either way, the scheme was brought to an abrupt end under mysterious circumstances.

These schemes are attractive to cybercriminals who are already in possession of their own botnets or have access to large numbers of compromised computers. Ransomware affiliate schemes can offer an alternative route to monetizing the botnet.

With these types of affiliate schemes springing up and lowering the barrier to entry into the world of ransomware, it's no wonder that this threat is such a persistent problem.



Registered Users
Join Date: Sep 2014
Location: blackstuff
Posts: 21

TorLocker Ransomware (Daily BTC inflow)

TorLocker Ransomware
What is this?
An affiliate program.
I provide a password for the control panel of TorLocker, a binary made in assembly for Windows, a builder, and a tor.exe standalone executable.
What is TorLocker?
TorLocker is a ransomware that works using TOR, BitCoin, RSA-2048, AES-256.
Is it similar to CryptoLocker?
Yes and No.
TorLocker encrypts files and demands user for a ransom. So CryptoLocker does.
TorLocker don't need internet connectivity to start encrypting files, CryptoLocker does.
TorLocker has 128 public keys inside the .exe body. Each affiliate receives new different encryption keys already inside the .exe.
After 10 different payments, i generate a new .exe for you, so no repeated keys are going to be used.
TorLocker command and control is hosted behind TOR hidden services. Can't be shutdown easily.
TorLocker accepts BitCoin only (Moneypak,Ukash Already Available for First Set Buyers)
TorLocker process payments and encryption key delivery, automatically. No human intervention is necessary.
How it works?
It will encrypt all files (extensions below) from the computer you send it, connect to TOR, retrieves the amount the user needs to pay (currently 0.380 BTC), the deposit address (a new address for every new client), how many days the user has to pay (currently 9 days counting down to 0 when decryption will not be possible).
After 6 confirmations from the BitCoin network, 70% of the ransom is sent to you. 30% goes to me, and the RSA-2048 decryption key is automatically delivered to the client, who get access to his files again. Each file is encrypted with a random AES-256 key, which is encrypted with the RSA-2048 key and then appended to the encrypted file.
How larger encrypted files become?
512 bytes
Is unicode supported?
Yes
What if I find a bug?
Report and I will correct it.
*Which extensions are currently being used?

```
".accdb",0,".ai",0,".arw",0,".bay",0,".blend", 0,". cdr",0,".cer",0,".cr2",0,".crt",0,".crw",0,".dbf" ,
0,".dcr",0,".der",0,".dng",0,".doc",0,".docm",0, ". docx",0,".dwg",0,".dxf",0,".dxg",0,".eps",0,".erf"
,0,".indd",0,".jpe",0,".jpg",0,".jpeg",0,".kdc",0 , ".mdb",0,".mdf",0,".mef",0,".mrw",0,".nef",0," .nrw
",0,".odb",0,".odm",0,".odp",0,".ods",0,".odt" ,0," .orf",0,".p12",0,".p7b",0,".p7c",0,".pdd",0,".pdf"
,0,".pef",0,".pem",0,".pfx",0,".ppt",0,".pptm",0, " .pptx",0,".psd",0,".pst",0,".ptx",0,".r3d",0,".raf
",0,".raw",0,".rtf",0,".rw2",0,".rwl",0,".srf" ,0," .srw",0,".wb2",0,".wpd",0,".wps",0,".xlk",0,".xls" ,0,".xlsb",0,".xlsm",0,".xlsx",0,0**
```

What I need to do to start cashing?
An offline BitCoin wallet. bitcoin-qt is fine. Synchronize the bitcoin wallet with the network (it will take some time).
Download tor browser bundle. Configure TOR as the SOCKS proxy in the bitcoin client (this is a very important step to your safety).
Generate a new address. Get your password for the TorLocker panel from me (buying this listing). Register you BitCoin address in the panel (you will be asked only once, in the first time you login). Spread the .exe, receive the money.
In how many time will you setup my account?
Maximum 4 days.

Figure 12. Discussion in an underground forum between a ransomware-as-a-service (RAAS) seller and a prospective buyer, offering the buyer a 70 percent cut of potential earnings

Ransomware mind tricks

Once the ransomware infects the victim's computer and blocks access to their data, it then needs to convince the user to pay the ransom to regain access. Both locker ransomware and crypto ransomware employ several behavioral-economic, psychological, and social-engineering techniques to persuade the user into paying the fee.

Locker ransomware has been known to display a fake law enforcement notice, claiming that the user needs to pay a fine for downloading or accessing illegal content. It plays up to the user's inherent trust in law enforcement, along with their need to obey it, by using the authorities' imagery and wording to back up its claims. Additionally, by claiming that the user has access illegal content, it may scare the victim into not seeking help out of embarrassment, instead paying the ransom to make it go away quickly. Ransomware has been distributed through piracy and adult websites in the past, giving a stronger sense of legitimacy to the ransom demand's claims.

Crypto ransomware messages typically include a time limit, indicating that if the user doesn't pay within a few days, then the decryption key will be deleted and their files will be lost forever. This instills a sense of anxiety in the user, who may feel further pressured into quickly paying the ransom before the deadline. A fear of regret may also influence the victim's decision-making capabilities, where they may pay the ransom as they'd rather not regret it if they didn't.

The appendix gives further details on the behavioral-economic, psychological, and social-engineering techniques that ransomware authors use in their scams.

Pricing and payment systems

Ransomware is a cybercrime business and just like real companies, the pricing and payment systems have to be honed and perfected in order to strike a balance of making it easy and feasible for victims to pay.

For the cybercriminals, one of the most important criteria for the chosen payment system is that it must provide for anonymity. In this section, we will take a closer look at some of the financial aspects of pricing and payment systems related to ransomware.

The price is right?

Can you put a price on your data? Ransomware extortionists seem to think they can and have been doing so since the first known crypto ransomware AIDS Trojan appeared in 1989. The AIDS crypto ransomware payment demand was US$189.

Surprisingly, this price has not changed too much over the intervening years. Taking inflation into account, US$189 in 1989 is now worth US$368 in 2015. Looking at the initial ransomware from various malware families from the start of 2014 to June 2015, we can see that the ransom demand has ranged from US$21 up to US$700, with the average being just over US$300. This average is close to the price that the original AIDS Trojan demanded. We cannot be sure whether the similarity in ransom prices is purely coincidental or by design but ultimately, the ransom has to be within reach of the victim's means to pay.

Cybercriminals could opt for different pricing strategies: a low-price strategy in the hope that they would get a higher volume of payments or a high-price-but-low-volume approach. This is the same dilemma that legitimate businesses face all the time: how to price goods and services to ensure maximum return but still present enough value to the customer to attract purchase.

Dynamic pricing

Nowadays, ransomware is found throughout the world. The challenge for the cybercriminals is that the populations of different countries have different purchasing powers and currencies. Based on this idea, we can see that the ability to pay US$200 is different for inhabitants of US versus the inhabitants of India who may find this amount to be out of reach. To tackle the issue of international purchasing power, we can see that the idea of dynamic geographical pricing is employed by some ransomware, such as Cryptowall (aka Trojan.Cryptodefense).

This means that users are given a different ransom demand amount depending on their location.

When a computer is compromised, Cryptowall reports back to a command-and-control (C&C) server with the IP address of the infection. The server performs a lookup of the IP address and determines the country that the infected computer is located in. Then, based on various factors, the price returned to the infected computer is adjusted to suit the location.

Different prices for home and business "customers"

Today, in knowledge-based economies, data is known to be a critically important driver of business success, meaning that it is possible to put a price on the data. Cybercriminals, who specifically target businesses or other organizations with the intention of encrypting and holding their data to ransom, have incorporated this understanding into their ransom payment demands. While public reports of these incidents and ransom demands are rare, several reported cases in Australia in 2012 show attackers hacking into businesses, encrypting their databases, and demanding ransoms of up to AU$5,000 (US$4,750). Another reported case in 2015 shows an attacker encrypting a financial website database and demanding a ransom of US$50,000.

Information security researchers, however, suggest that some cybercriminal extortionists have found US$10,000 to be the sweet spot between what organizations are willing to pay and what law enforcements are reluctant to investigate. This US$10,000 price point for business users is a steep rise from the average of US$300 for end users.

Payment systems

Having looked at pricing, another important topic of ransomware is the method of payment. Over the years, the options and preferred methods of payment have changed as different services became available. In 1989, the AIDS crypto ransomware Trojan demanded payment by way of a check sent to a post office box in Panama. Since then, other payment methods have been used by ransomware. These methods include money wire transfers and sending premium-rate text messages to the attacker's number, as seen in Trojan.Ransomlock in 2009. More recently, the use of payment voucher systems such as Paysafecard, MoneyPak, UKash, CashU, and MoneXy have and are still being used by some ransomware threats.

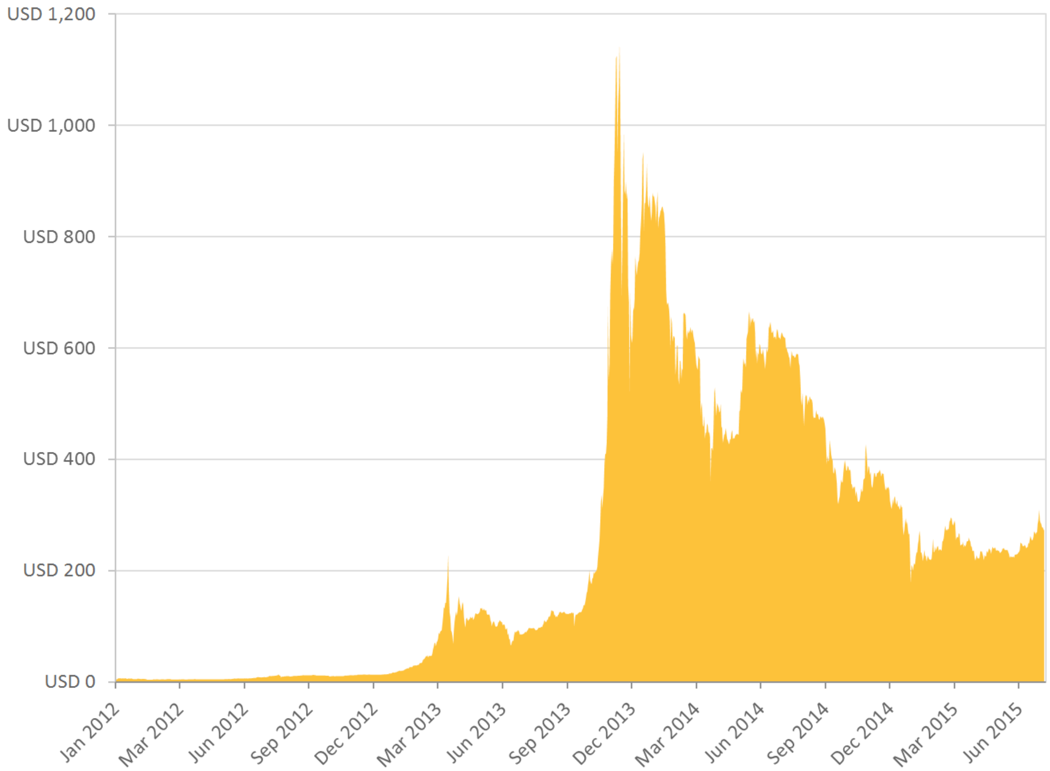


Figure 13. Bitcoin versus US dollar exchange rate from 2012 to 2015, showing the wild movement in the exchange rate (Data from the CoinDesk Bitcoin Price Index)

The arrival of cryptocurrencies

in the form of Bitcoin (BTC) in 2009 shook up the money transfer landscape. Bitcoin was the first decentralized cryptocurrency that really caught the world's imagination and gained relatively widespread acceptance. For a time, many home computing enthusiasts dreamed of making money from nothing by mining for bitcoins, but this quickly became a pipe dream as the ramp up in the difficulty factor soon brought bitcoin mining out of the capability of the hardware owned by the average home user.

The increasingly widespread acceptance of bitcoins made it easier for victims to purchase them to make ransom payments and then for the cybercriminals to convert them back into hard cash later. Today, the majority of new ransomware threats hitting the streets are opting for payments through cryptocurrencies like Bitcoin (some use Litecoin [LTC] and Dogecoin [DOGE]) due to the anonymity that they can provide, making it easier for cybercriminals to launder their ill-gotten gains. These payments are made through sites hosted on the dark web (often accessed through Tor), making it more difficult for law enforcement to track down the cybercriminals behind these attacks.

Despite its advantages for cybercriminals, Bitcoin has been dogged by controversies, as well as having a history of wild exchange rate movements which means holding it for any length of time is not for the faint-hearted. On several occasions in the past, major Bitcoin exchanges were hacked or impacted by high-volume DDoS attacks, preventing the normal functioning of the exchanges which caused panic in the market. In one of the most well-known examples of a Bitcoin breach, Mt Gox, previously a leading Bitcoin exchange, suffered a second major breach in February 2014 which proved to be a fatal blow to the company. The breach ultimately led to the closure of the exchange and the disappearance of around US$375 million worth of bitcoins, including client funds.

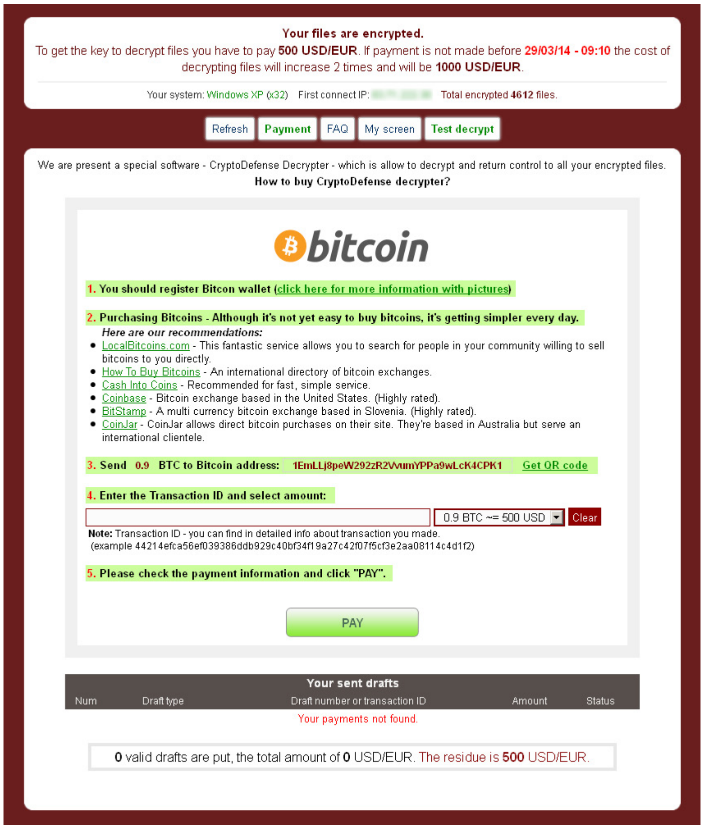
Incidents like this proved to cybercriminals that while bitcoins provide some level of anonymity for payments, they need to be quickly converted to a more stable currency.

Favored payment systems

In general, we found that crypto ransomware tend to favor cryptocurrencies as the preferred payment method whereas locker ransomware prefer to use payment voucher systems.

A possible reason for this is because of the way that the two different types of ransomware work. Locker ransomware locks the computer leaving it largely unusable. Therefore it would not be possible for victims to buy online currencies or access Bitcoin wallets using the computer to make payment. If the computer is locked, it would be easier for victims to buy payment vouchers from a local shop or outlet and then enter the payment code.

Crypto ransomware generally does not restrict any functionality of the impacted computer. This leaves the victim with the ability to use the internet to research and buy cryptocurrencies to make payment. Many crypto ransomware threats even actively encourage victims to read up on bitcoins by supplying links to articles and even videos explaining what bitcoins are and how to buy them.



Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **29/03/14 - 09:10** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted **4612** files.

We are present a special software - CryptoDefense Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoDefense decrypter?

1. **You should register Bitcon wallet (click here for more information with pictures)**

2. **Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**
   Here are our recommendations:
   - LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
   - How To Buy Bitcoins - An international directory of bitcoin exchanges.
   - Cash Into Coins - Recommended for fast, simple service.
   - Coinbase - Bitcoin exchange based in the United States. (Highly rated).
   - BitStamp - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
   - CoinJar - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.

3. **Send 0.9 BTC to Bitcoin address: 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 Get QR code**

4. **Enter the Transaction ID and select amount:**
   0.9 BTC ~= 500 USD
   Note: Transaction ID - you can find in detailed info about transaction you made.
   (example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. **Please check the payment information and click "PAY".**

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found.

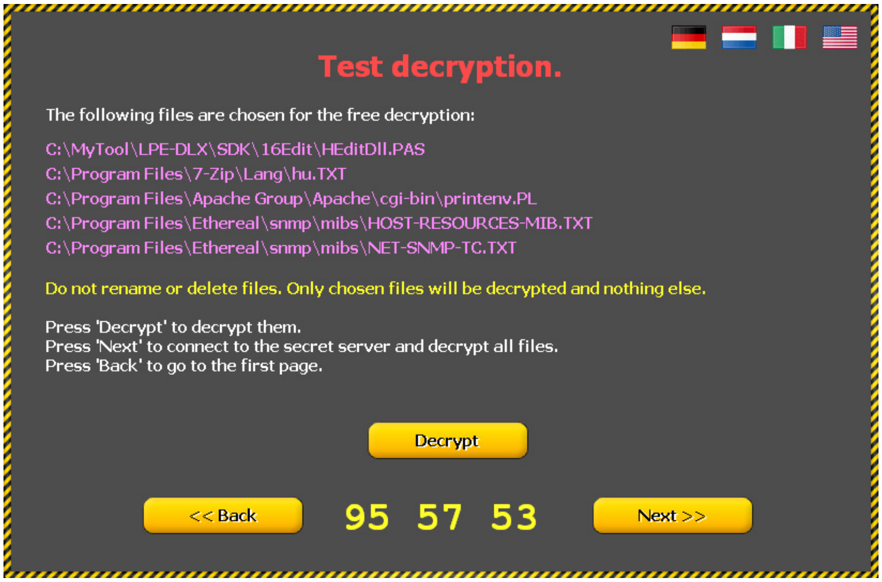
0 valid drafts are put, the total amount of **0** USD/EUR. The residue is **500** USD/EUR.

Figure 14. Ransom note demanding payment of US$500 in bitcoins for decryption of files (Trojan.Cryptodefense)

To pay or not to pay?

It is not easy for victims to decide whether or not to pay the ransom demand to get their files back. With data now being essential to many organizations, not paying the demands and losing data could have catastrophic effects, such as closing a business down. On the other hand, paying the ransom demand only encourages even more crypto ransomware campaigns. While law enforcement officials will advise victims not to pay the ransom, there are several documented cases where they themselves have paid the extortion demand to get their own files back.

Of course there is always the question of whether victims can trust the cybercriminals to actually unlock their files. That said, crypto ransomware cybercriminals seem to possess some business acumen. They realize that without their reputation of being trusted to decrypt the files after the ransom demand is paid, no new victims will pay the ransom demands, which is bad for business. However, there is still no way of being sure that when a victim pays the ransom, the attackers will decrypt their files. The cybercriminals also seem to realize that a little bit of something is better than nothing at all, as there are documented cases where security researchers have negotiated with crypto ransomware attackers to lower the ransom demand to a more affordable price.



Test decryption.

The following files are chosen for the free decryption:

C:\MyTool\LPE-DLX\SDK\16Edit\HEditDll.PAS
C:\Program Files\7-Zip\Lang\hu.TXT
C:\Program Files\Apache Group\Apache\cgi-bin\printenv.PL
C:\Program Files\Ethereal\snmp\mibs\HOST-RESOURCES-MIB.TXT
C:\Program Files\Ethereal\snmp\mibs\NET-SNMP-TC.TXT

Do not rename or delete files. Only chosen files will be decrypted and nothing else.

Press 'Decrypt' to decrypt them.
Press 'Next' to connect to the secret server and decrypt all files.
Press 'Back' to go to the first page.

Figure 15. CTBLocker offers a "try-before-you-buy" service

To build trust, some crypto ransomware schemes allow the victim to "try-before-you-buy" by decrypting some files for free. For example, CTBLocker (Trojan.Cryptolocker.G) has an option to allow users to decrypt five randomly chosen files for free. This is a trust-building exercise to show victims that the cybercriminals can and are willing to decrypt files–if the ransom is paid.

Interestingly, there are even cybercriminals that have a heart. Symantec has observed a number of cases where cybercriminals behind crypto ransomware schemes have decided to return files to their original state if the victim does not pay by the deadline. These acts of altruism are rare, so waiting for the cybercriminal to give up is not a viable tactic to regain your files.

How much are cybercriminals earning through ransomware?

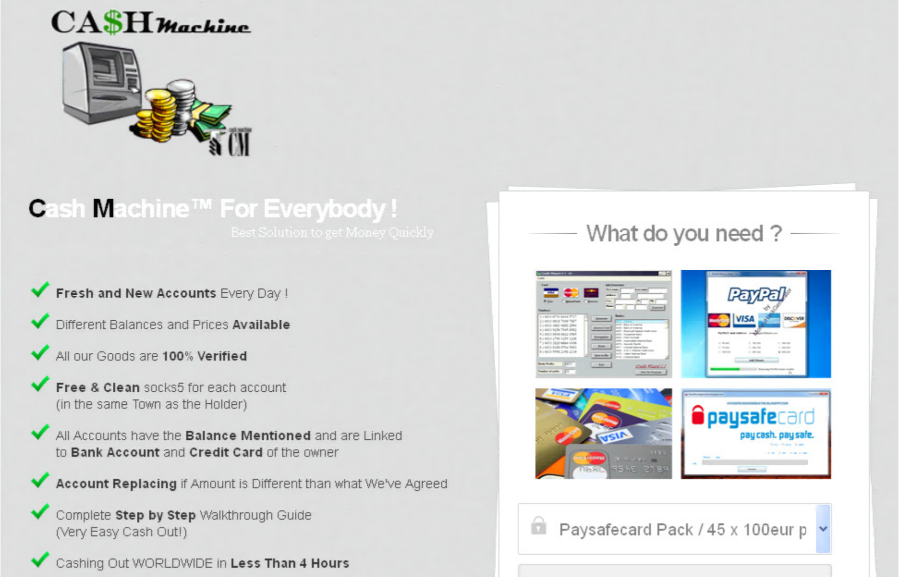
While this is not an easy question to answer, several published reports provide insights into cybercriminal ransomware earnings. In 2012, a Symantec report found that as many as 2.9 percent of victims paid the ransom demands. The report also found that one of the smaller ransomware players managed to infect 68,000 computers in just one month, which could have resulted in victims being defrauded of up to US$400,000 in total.

In March 2014, Symantec found that Trojan.Cryptowall earned at least US$34,000 in its first month of operations. A further study of Cryptowall by other information security researchers found that by August 2014, Cryptowall had earned more than US$1.1 million. In June 2015, data from the FBI's Internet Crime Complaint Center (IC3) showed that between April 2014 and June 2015, it had received 992 Cryptowall-related complaints. The victims were a mix of end users and businesses, and the resulting losses from these cases amounted to more than US$18 million.

How are cybercriminals cashing out?

The method chosen by cybercriminals for money laundering varies and can depend on how the ransom payment was made. Cybercriminals opting for ransomware payments in the form of payment vouchers generally use specialized money-laundering services. These cash-out options use services like online betting and casino sites that accept voucher codes for payment. The sites used are hosted in different geographical and legal jurisdictions, making it difficult for law enforcement to track the money.

Once laundered through these sites, the money is transferred to fraudulently obtained prepaid debit cards and the funds are withdrawn from ATMs by money mules. The cash-out service then sends on an agreed percentage of the payment vouchers' value to the ransomware cybercriminals.


CA$H Machine

Cash Machine™ For Everybody !

Best Solution to get Money Quickly

- ✓ Fresh and New Accounts Every Day !
- ✓ Different Balances and Prices Available
- ✓ All our Goods are 100% Verified
- ✓ Free & Clean socks5 for each account (in the same Town as the Holder)
- ✓ All Accounts have the Balance Mentioned and are Linked to Bank Account and Credit Card of the owner
- ✓ Account Replacing if Amount is Different than what We've Agreed
- ✓ Complete Step by Step Walkthrough Guide (Very Easy Cash Out!)
- ✓ Cashing Out WORLDWIDE in Less Than 4 Hours

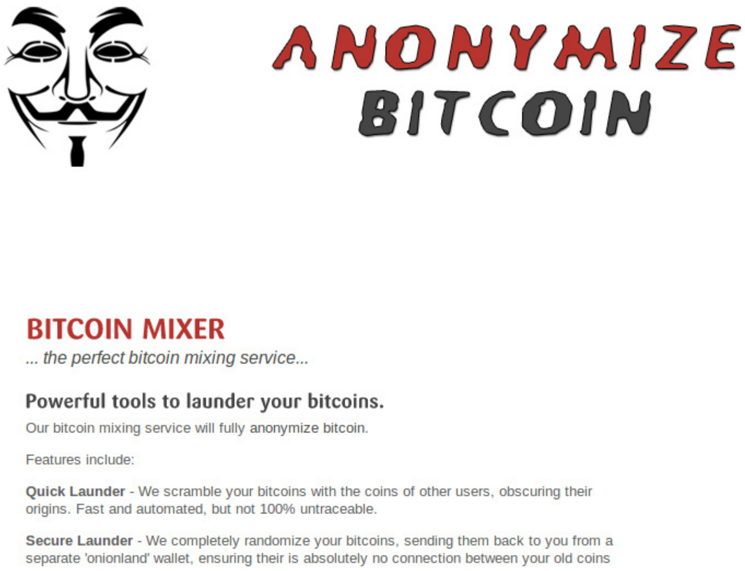
What do you need ?

Paysafecard Pack / 45 x 100eur p

Figure 16. A website accessed through Tor offers cash-out services, allowing cybercriminals to quickly convert illicit gains into hard cash

Other ransomware payment methods, such as those made through Bitcoin, often do not require the use of cash-out services due to the increased privacy afforded by the cryptocurrency. But cybercriminals are aware that law enforcement investigators are on their trail, so Bitcoin-laundering services have sprung up to meet the demands of cybercriminals who don't want to be identified. These shady businesses mix up bitcoins from legitimate sources as well those from ill-gotten gains.

Cybercriminals can launder their bitcoins themselves by transferring their bitcoins through multiple Bitcoin block transaction wallets, adding layer upon layer of obfuscation. Alternatively, they can procure the services of Bitcoin anonymizers to do the job for them. Once the Bitcoin-laundering process is complete, it becomes very difficult to differentiate between legitimate transactions and cybercrime payments in the bitcoin transaction history. By the time the bitcoins are cashed out, the cybercriminals have plausible deniability of any link back to criminal activity related to the original ransomware payment transaction.



BITCOIN MIXER

... the perfect bitcoin mixing service...

Powerful tools to launder your bitcoins.

Our bitcoin mixing service will fully anonymize bitcoin.

Features include:

Quick Launder - We scramble your bitcoins with the coins of other users, obscuring their origins. Fast and automated, but not 100% untraceable.

Secure Launder - We completely randomize your bitcoins, sending them back to you from a separate 'onionland' wallet, ensuring their is absolutely no connection between your old coins

Figure 17. A bitcoin-laundering service offers to mix bitcoins from different sources to make it harder for investigators to track the bitcoins

Perhaps the biggest risk with handling bitcoins is the potential for large price fluctuations, leaving cybercriminals who do not immediately cash out open to a substantial loss of earnings.

RANSOM TECHNIQUES

> “While all ransomware types are designed to extort money from their victims, they can be quite different both operationally and technically.”

Ransom techniques

While all ransomware types are designed to extort money from their victims, they can be quite different both operationally and technically. To understand just how different they can be, this section will look at common locker ransomware and crypto ransomware to see how they work on a technical level.

File encryption

Modern crypto ransomware typically uses both symmetric and asymmetric encryption techniques. In symmetric encryption, a single key is used to encrypt the data and the same key is used to decrypt the encrypted data. Knowing the key allows the user to decrypt data that has been encrypted with the same key. Ransomware using symmetric encryption will usually generate a key on the infected computer and send this to the attacker or request a key from the attacker before encrypting the user's files. The attacker needs to ensure that the key is not available to the user after encrypting their files, otherwise the user might be able to decrypt the files themselves without paying.

The advantage of using symmetric encryption algorithms is that they are generally much faster than asymmetric algorithms and use small keys (typically 256-bit). A typical crypto ransomware has to quickly search and encrypt a large number of files, so performance is essential to encrypt files before the victim can discover the threat's activities.

Asymmetric encryption uses two keys: the public key is used to encrypt the data and the private key is used to decrypt the encrypted data. Knowing the public key does not allow you to decrypt files encrypted with this key. Only the related private key can be used for this purpose. Crypto ransomware may use asymmetric encryption by encrypting the user's files with the public key with the attacker keeping the private key for themselves. The attacker does not need to be as protective of the public key as they would need to be with the symmetric-encryption approach, because knowing the public key does not allow the affected user to decrypt their files.

There are a number of drawbacks to using a public key to encrypt huge numbers of potentially large files. Public key cryptography is much slower than symmetric key encryption. Taking a long time to complete encryption could risk exposing the operation before the encryption process is fully completed.

More advanced crypto ransomware typically uses a combination of symmetric and asymmetric encryption techniques. The variants that use asymmetric encryption may also generate specific public-private key pairs for each infected computer. This allows the attacker to decrypt files on one infected computer without revealing the private key that could potentially also be used to decrypt files on every other computer infected using the same pubic key.

The location of the keys in either encryption approach can have a fundamental impact on the effectiveness of the scheme and ultimately the outcome for the user. For example, if a key is generated on the infected computer and then sent to the attacker, then the user's files can be encrypted even if the crypto ransomware cannot contact the attacker's server. If the encryption key is only stored on the attacker's server, then the file-encryption process cannot begin unless the ransomware can contact the server and download the encryption key. A fundamental weakness in this approach is its dependency on a remote server before the start of operation.

The following sections will look at a few crypto ransomware families to see how they choose different approaches to the encryption problem.

Downloaded public key

Cryptodefense (Trojan.Cryptodefense) uses a combination of symmetric and asymmetric encryption techniques. AES is a powerful and fast symmetric encryption algorithm which is used by Cryptodefense to encrypt the user's files. The 256-bit AES key is first generated on the user's computer and after file encryption is completed, the AES key is itself encrypted with a different RSA asymmetric public key which is downloaded from the attacker's server. The resulting encrypted AES key is then stored in the user's encrypted file. Even though the AES key is stored in each encrypted file on the user's computer, the victim has no way of using it as the attacker controls the RSA private key needed to decrypt it.

The weakness of this approach is that if the attacker's server cannot be reached to download the RSA public key, then the encryption process will not be successful. The advantage of this approach is that the attacker can use a different RSA asymmetric key pair for each infection. Exposure of a single RSA private key will not allow any other victims to unlock their files.

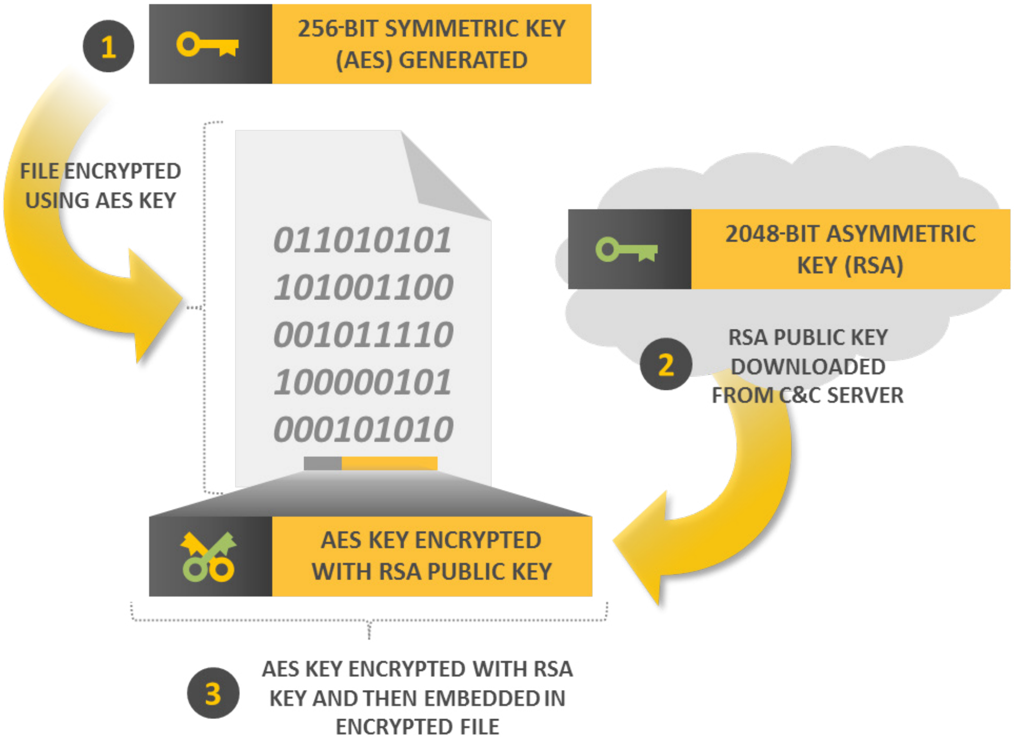

1
256-BIT SYMMETRIC KEY (AES) GENERATED
FILE ENCRYPTED USING AES KEY
011010101
101001100
001011110
100000101
000101010
2048-BIT ASYMMETRIC KEY (RSA)
2
RSA PUBLIC KEY DOWNLOADED FROM C&C SERVER
AES KEY ENCRYPTED WITH RSA PUBLIC KEY
3
AES KEY ENCRYPTED WITH RSA KEY AND THEN EMBEDDED IN ENCRYPTED FILE

Figure 18. CryptoDefense has to download a public key before encryption begins

Embedded public key

CTBLocker also uses both symmetric and asymmetric encryption techniques to encrypt the user's files but takes a slightly different approach. Samples of CTBLocker include an embedded public key for the RSA asymmetric encryption algorithm process. The attacker keeps the corresponding private key. During the infection process, CTBLocker generates a new symmetric key for the AES encryption process and uses it to encrypt the user's files. The 256-bit AES key is encrypted with the embedded public RSA key and the encrypted AES

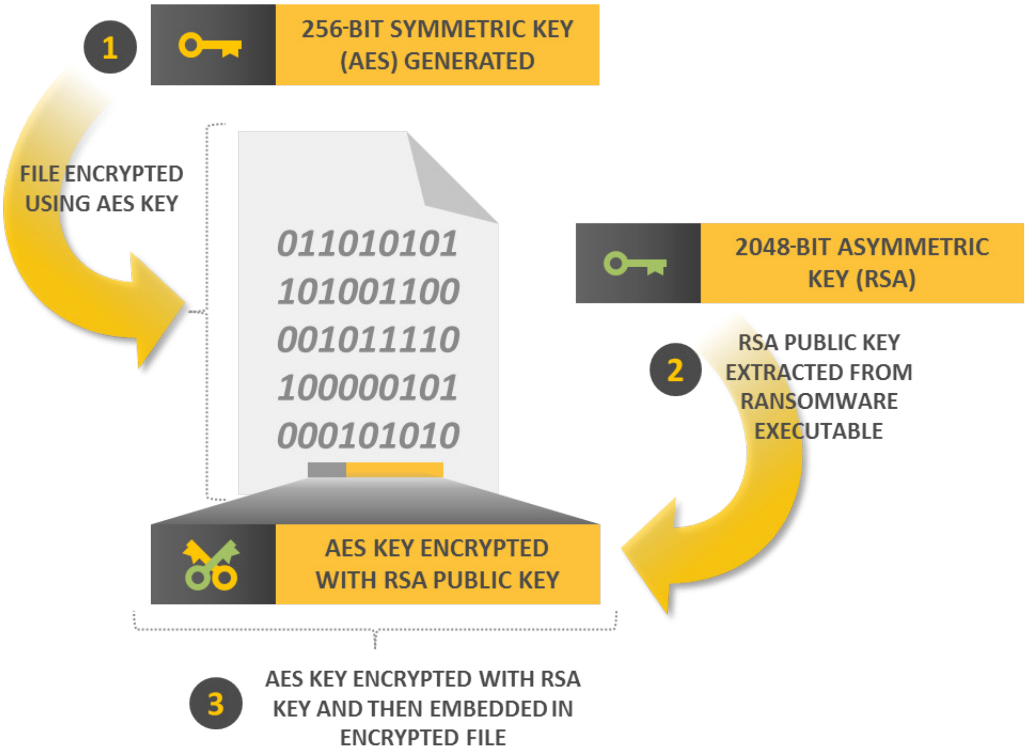

1
256-BIT SYMMETRIC KEY (AES) GENERATED
FILE ENCRYPTED USING AES KEY
011010101
101001100
001011110
100000101
000101010
2048-BIT ASYMMETRIC KEY (RSA)
2
RSA PUBLIC KEY EXTRACTED FROM RANSOMWARE EXECUTABLE
AES KEY ENCRYPTED WITH RSA PUBLIC KEY
3
AES KEY ENCRYPTED WITH RSA KEY AND THEN EMBEDDED IN ENCRYPTED FILE

Figure 19. CTBLocker can begin encrypting without contacting a server first as it already has a public key embedded

key is then added to the encrypted file's data. The user cannot recover the AES key to decrypt their files as they do not possess the private RSA key needed to decrypt the key.

The advantage of using this approach is that CTBLocker can begin its file-encryption process without requiring any internet access first. The weakness of using this approach is that attackers must use a different public key for each infection of CTBLocker. If they don't do this, then once the first user obtains the private RSA key, they could potentially share the key with other victims, allowing them to decrypt their files. For this scheme to be effective, the attacker must customize each copy of CTBLocker sent to victims.

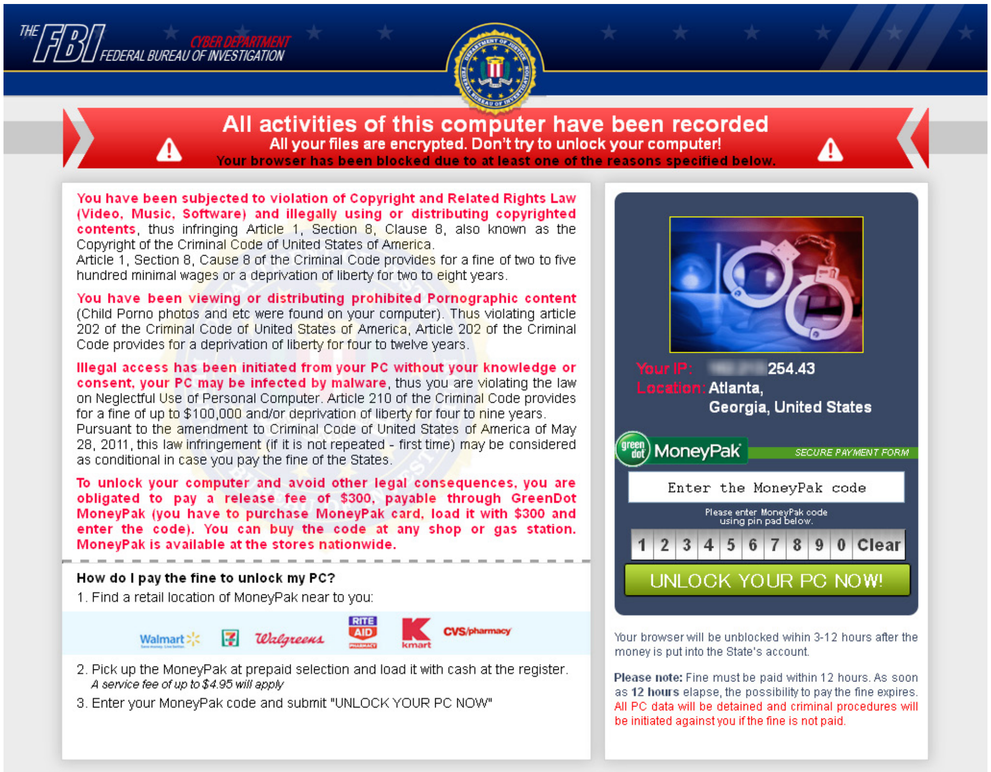
Embedded symmetric key

Android.Simplocker only uses the AES symmetric encryption algorithm to encrypt files on the user's mobile device. The 256-bit AES key is included in the application code itself so the malware does not need to reach out to a C&C server to download any additional keys or files. Instead, the attacker can instruct Simplocker by sending a command to it through an SMS message, for example, to direct the ransomware to encrypt or decrypt the user's files. As the key is included in the application, it is relatively straight forward to find the key and use it to decrypt the encrypted files.

Hard coding symmetric encryption keys in this way is not a common technique for modern crypto ransomware. The method is usually only seen in the most basic forms of crypto ransomware such as those from amateur newcomers who have not learned past lessons on cryptography.

Screen locking

Locker ransomware attempts to block infected users from accessing the operating system and services that are running on their computer or device. The approach that is most commonly used is to display a ransom message to the user in a continuous loop. This gives the impression that the message is constantly displayed even though there may be slight intervals where it is possible for the user to close the current display of the message. These ransomware threats mostly use features or APIs from the underlying operating system to perform this task.



All activities of this computer have been recorded

All your files are encrypted. Don't try to unlock your computer!

Your browser has been blocked due to at least one of the reasons specified below.

You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.
Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or deprivation of liberty for four to nine years.
Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

To unlock your computer and avoid other legal consequences, you are obligated to pay a release fee of $300, payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.

How do I pay the fine to unlock my PC?

1. Find a retail location of MoneyPak near to you:
2. Pick up the MoneyPak at prepaid selection and load it with cash at the register.
   A service fee of up to $4.95 will apply
3. Enter your MoneyPak code and submit "UNLOCK YOUR PC NOW"

Your IP: [redacted]254.43
Location: Atlanta,
Georgia, United States

Enter the MoneyPak code

Please enter MoneyPak code using pin pad below.

Your browser will be unblocked wihin 3-12 hours after the money is put into the State's account.

Please note: Fine must be paid within 12 hours. As soon as **12 hours** elapse, the possibility to pay the fine expires. All PC data will be detained and criminal procedures will be initiated against you if the fine is not paid.

Figure 20. FBI ransom screen from a computer infected with a Browlock variant

Windows locker ransomware

The locker ransomware threats that infect the Windows operating system, such as Trojan.Ransomlock.G, all employ similar strategies to lock the user's screen. The ransomware displays a full screen window that covers the entire desktop to display its message. The ransomware may create the window itself or use a browser window in full screen mode to show their ransom message. The window is usually shown as the only window on a new virtual desktop that the ransomware creates and makes active. The ransomware may use a background thread to monitor the system's desktops and ensure that their one is kept active and on top.

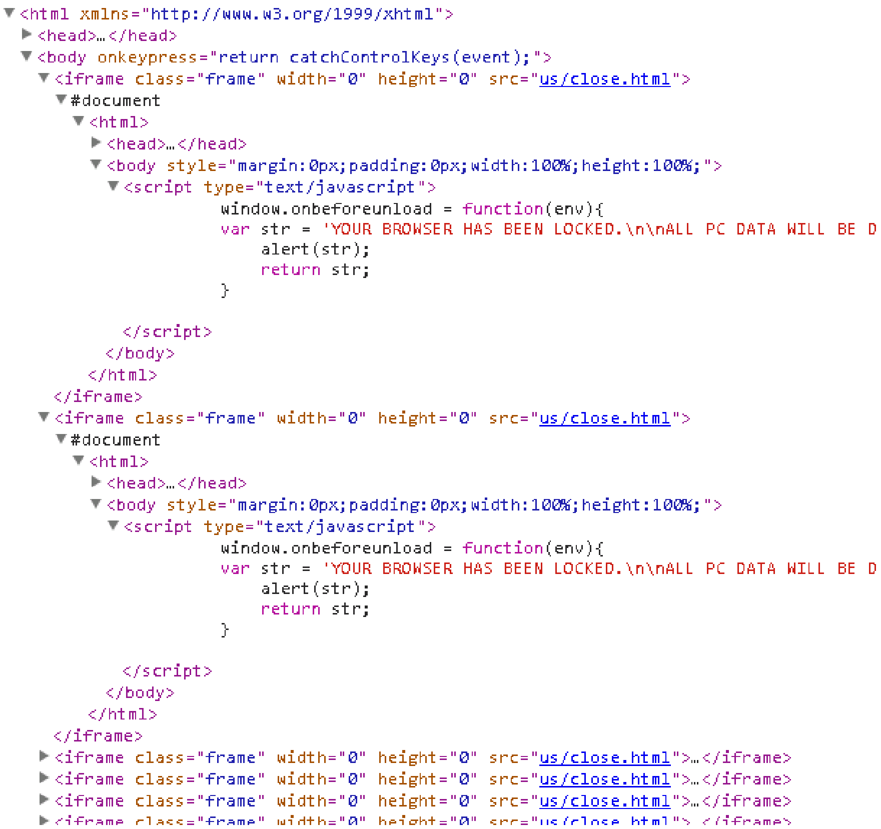
The contents of the messages are occasionally included in the ransomware executable itself but it is more common for the ransomware to download the contents from the attackers' server. This allows the attackers to serve localized messages using language and law-enforcement images relevant to the country where the infection has occurred.

For self-protection, locker ransomware on Windows often use background threads to monitor for processes and applications that the user may try to use to end the ransomware process, such as Task Manager. The ransomware process will end these processes if they are detected. Some variants have also used shutdown messages to try to signal to other windows that the system is shutting down. This may allow the ransomware to close other processes that may interfere with its activities.

Browser locking

Browlock is different to other locker Trojans in that it does not use binary executable files and it does not block access to the underlying operating system. To become "infected," the user must navigate to a server hosting Browlock through their web browser, where they are shown a page like the one shown in Figure 20.

Browlock is implemented entirely using client-side web technology. The ransom page contains HTML code and images that are used to display the ransom page contents to the user. The page contains JavaScript code that defines an onbeforeunload function. This function is called when the user attempts to exit the page and allows web developers to ask the user to confirm that they want to exit or display final messages.



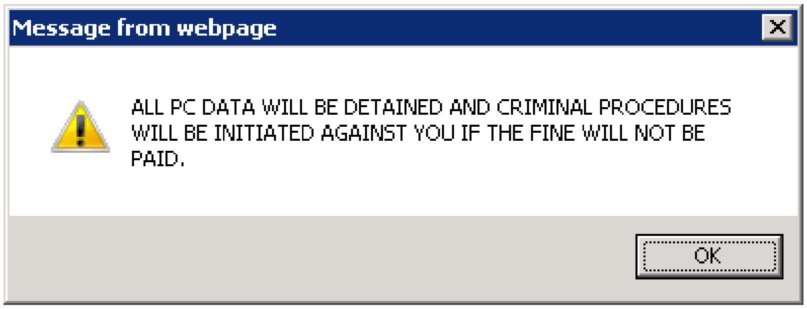
```
▼<html xmlns="http://www.w3.org/1999/xhtml">
  ▶<head>…</head>
  ▼<body onkeypress="return catchControlKeys(event);">
    ▼<iframe class="frame" width="0" height="0" src="us/close.html">
      ▼#document
        ▼<html>
          ▶<head>…</head>
          ▼<body style="margin:0px;padding:0px;width:100%;height:100%;">
            ▼<script type="text/javascript">
                         window.onbeforeunload = function(env){
                         var str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL PC DATA WILL BE D
                             alert(str);
                             return str;
                         }

             </script>
           </body>
         </html>
     </iframe>
    ▼<iframe class="frame" width="0" height="0" src="us/close.html">
      ▼#document
        ▼<html>
          ▶<head>…</head>
          ▼<body style="margin:0px;padding:0px;width:100%;height:100%;">
            ▼<script type="text/javascript">
                         window.onbeforeunload = function(env){
                         var str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL PC DATA WILL BE D
                             alert(str);
                             return str;
                         }

             </script>
           </body>
         </html>
     </iframe>
    ▶<iframe class="frame" width="0" height="0" src="us/close.html">…</iframe>
    ▶<iframe class="frame" width="0" height="0" src="us/close.html">…</iframe>
    ▶<iframe class="frame" width="0" height="0" src="us/close.html">…</iframe>
    ▶<iframe class="frame" width="0" height="0" src="us/close.html">…</iframe>
```

Figure 21. Source code from Browlock showing multiple iframes containing functions to display ransom message popups

The main Browlock page also contains multiple iframes that point to another page on the same Browlock server. This page also defines an onbeforeunload JavaScript function that displays the same message to the user. The

Browlock onbeforeunload function displays the dialog in Figure 22 when the user tries to exit the page.

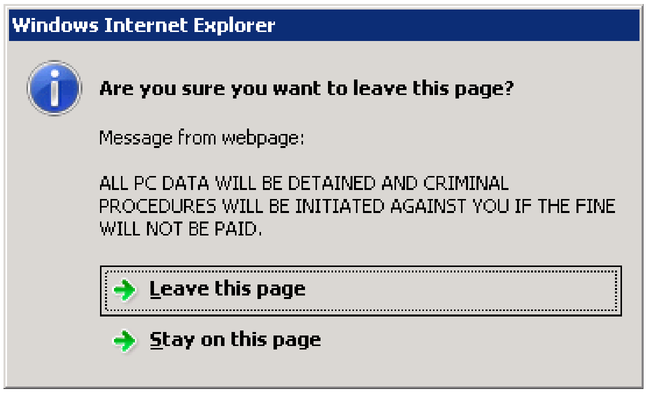
If the user clicks “OK” to close the dialog in Figure 22 then the dialog in Figure 23 is shown.



ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

Figure 22. First Browlock dialog box

If the user selects “Stay on this page,” then the main Browlock page in Figure 20 is kept open. If the user selects “Leave this page” in Figure 23, then the first and second dialog boxes will be displayed in turn for every onbeforeunload function in each iframe in the page. As the number of iframes is in the hundreds in most Browlock samples, the user may believe that they cannot exit the main Browlock page. The reality is that the user can actually exit if they persist in selecting “Leave this page” or if they close the browser process by another means such as through Windows Task Manager.



Are you sure you want to leave this page?

Message from webpage:

ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

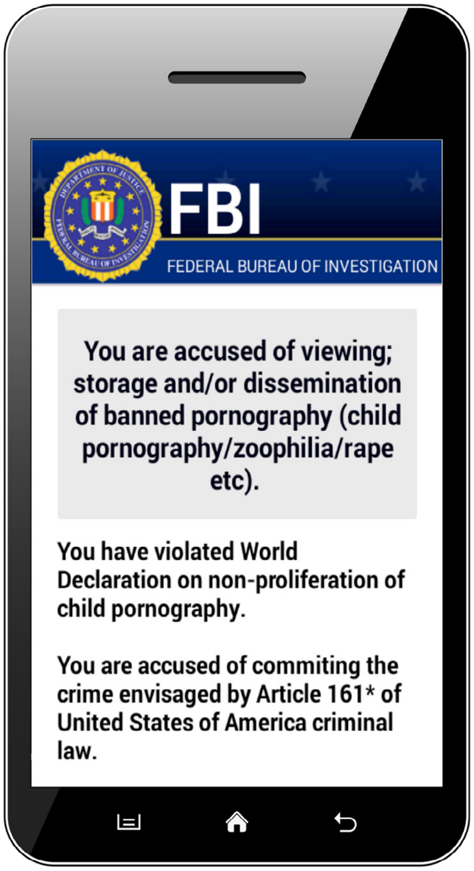
Figure 23. Second Browlock dialog box

As Browlock executes within the web browser, it can be considered a cross-platform ransomware as it will execute on any platform that provides a web browser supporting the JavaScript features it uses. This has allowed Browlock to be used as a fall-back ransomware as a last resort on malicious web servers used for serving up ransomware to unsuspecting web users. The way this works is that when a user is redirected to a malicious server, possibly through a malvertisement campaign, the server will fingerprint the victim’s computer and determine what type of computer it is. For victims running Windows, it may send ransomware that is designed for Windows but for users of other operating systems such as Linux or Mac OS X, it may send Browlock instead.

Browser locking is not a very effective technique, but doesn’t cost a lot to implement and its cross-platform capabilities make it useful to cybercriminals as an additional revenue-generating option.

Android locker ransomware

Android locker ransomware such as Android.Simplocker.B typically creates activity windows to display its ransom message. It periodically checks that the activity window is being displayed to the user by using techniques such as Android ExecutorService objects. The period is very short, which gives the user the impression that the activity window is never closed.



You are accused of viewing; storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc).

You have violated World Declaration on non-proliferation of child pornography.

You are accused of commiting the crime envisaged by Article 161* of United States of America criminal law.

Figure 24. Ransom message shown in an Android activity window

HOW WIDESPREAD IS THE PROBLEM OF RANSOMWARE

> “Even though it is a global problem, certain countries tend to be affected more than others.”

How widespread is the problem of ransomware

Today, the ransomware threat has become a global epidemic touching all corners of the world. Even though it is a global problem, certain countries tend to be affected more than others. By looking at our data for the past 12 months, we discovered that certain types of binary-based ransomware are more often targeted at particular countries.

Top 12 countries impacted by ransomware

Over the past 12 months, Symantec's telemetry has shown that the following countries are most affected by ransomware (Figure 25).

This telemetry shows that the cybercriminals behind ransomware are for the most part targeting more affluent or populous countries in the hope of finding rich pickings. As a result, 11 of the top 12 countries impacted by ransomware are members of the G20 organization, representing industrialized and developing economies that make up roughly 85 percent of the world's global domestic product (GDP).

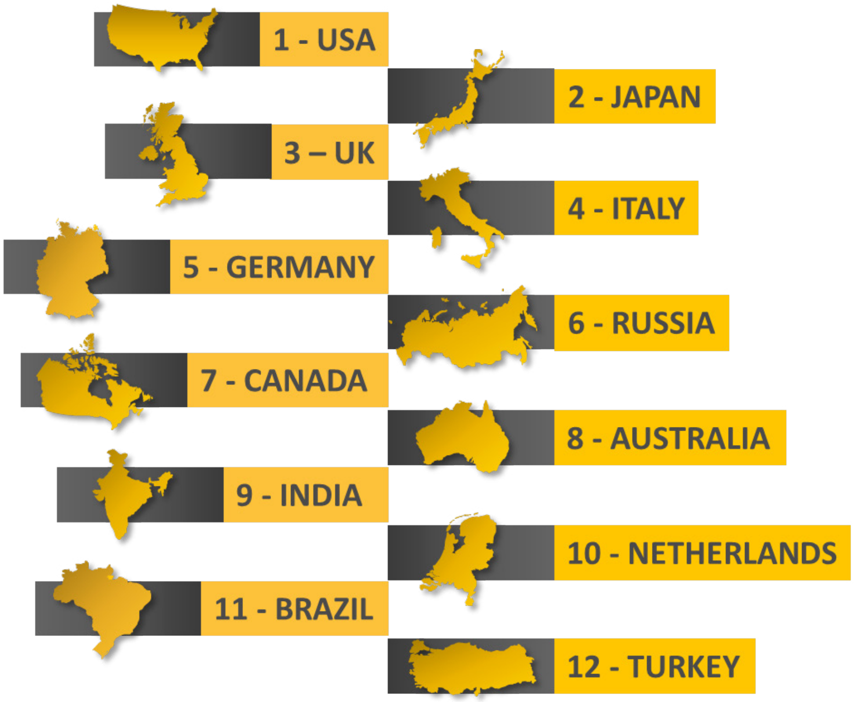


Figure 25. Top countries impacted by binary-based ransomware

The ransomware mix

Exploring the Symantec telemetry on binary-based ransomware (excluding browser lockers) in more detail reveals the dominance of file-encrypting ransomware such as Cryptowall, which turns out to be the most prevalent crypto ransomware during this time. The following chart shows the month-by-month mix of binary-file-based locker ransomware versus crypto ransomware in the past 12 months.

Our findings reveal that over the past 12 months, 64 percent of binary-based ransomware families observed have been crypto ransomware while locker ransomware made up the remaining 36 percent. This shows the dominance of binary-based crypto ransomware over binary-based locker ransomware. This is in line with Symantec's findings that between 2013 and 2014, there was a 250 percent increase in new crypto ransomware families on the threat landscape.

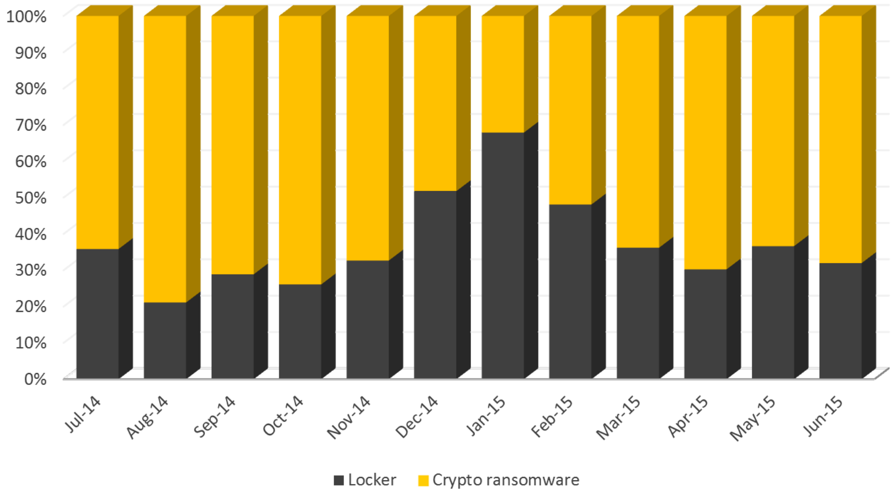


Figure 26. Detections for binary-based crypto ransomware dominate the ransomware threat landscape for past 12 months.

Top countries by ransomware type

While a wide range of countries are impacted by ransomware, the countries most impacted may vary depending on the type of ransomware. The following charts further break down the mix of binary-file-based ransomware and the top ten countries impacted. While the US retains top spot for both crypto ransomware and locker ransomware, there are some noticeable differences in the order of other countries most affected by each ransomware type. For crypto ransomware, Japan comes in at number two whereas for locker ransomware, it occupies the sixth spot.

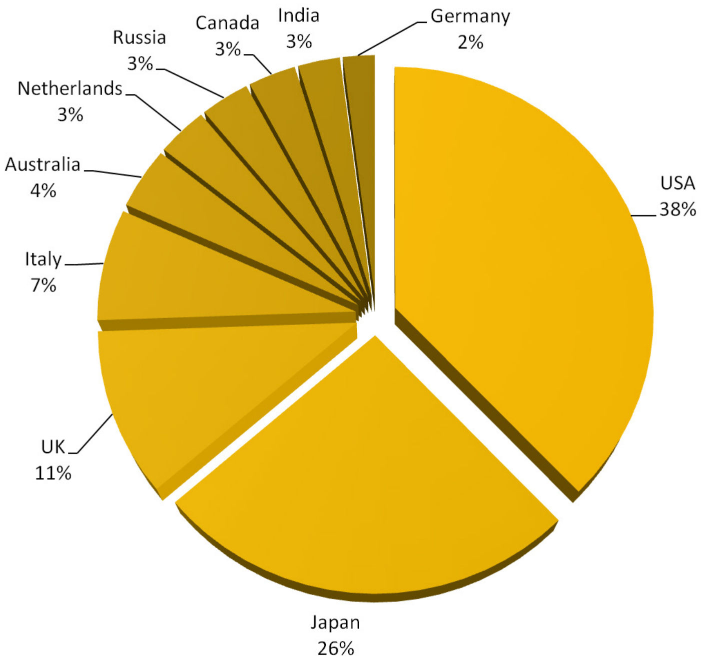


Figure 27. Top 10 countries for detections of binary file based crypto ransomware

The localization effect

The high prevalence of crypto ransomware in Japan is mostly due to Cryptowall. Since Cryptowall's discovery, Japan has ranked highly in the top countries targeted with this threat. In November 2014, we saw the first crypto ransomware variant (Trojan.Cryptolocker.H) designed to specifically target the Japanese-speaking population. The expenditure of effort to localize to Japanese shows that some cybercriminals have started to recognize that Japan is a potentially lucrative market worthy of investing time and effort into localizing their malware for.

Subsequent to that, even more crypto ransomware threats were seen localized to languages spoken in Asian countries, such as Korean. The high rankings of the UK, Italy, and Australia for crypto ransomware are also of no surprise. It is the result of several malware spam campaigns that have been targeting these regions in the last year, leading to crypto ransomware such as CTBLocker, among others.

Locker ransomware, down but not out

While binary-based locker ransomware may not be dominating the ransomware threat landscape today, its cousin the browser locker ransomware is still one of the most prevalent ransomware on the threat landscape. Through its use of social engineering and client-side web-browser-based tricks, browser locking remains a relatively effective technique without having to use a binary file to infect systems.

Today, the most prevalent binary-based locker ransomware in nearly all countries is Trojan.Ransomlock.G. This malware is controlled by a gang known as Reveton, , which has been active for several years and shows no signs of dissipating any time soon. The Reveton gang is also believed to control the browser locker ransomware known as Browlock.

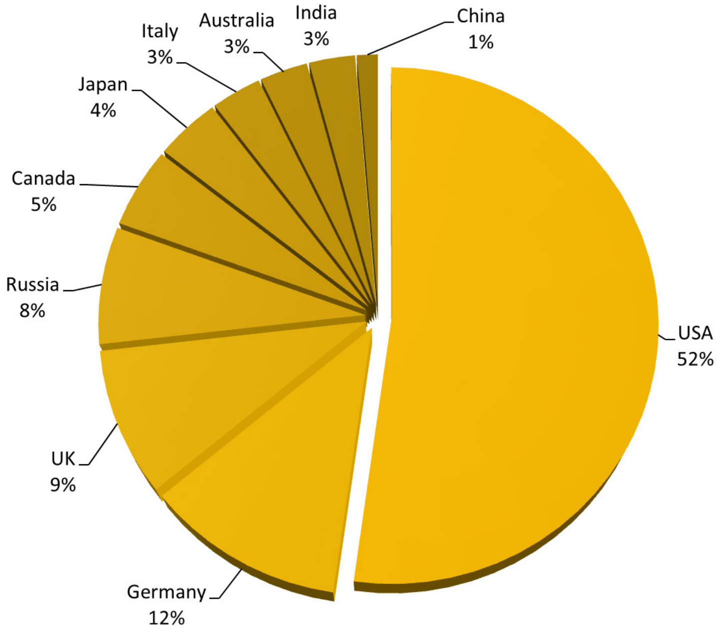


Figure 28. Top countries for detections of binary-based locker ransomware

Shifting focus of ransomware

The telemetry for the past year shows how certain countries have been targeted more than others with either binary-based crypto or locker ransomware over time. This is apparent in the monthly changing proportion of detections in the top countries impacted by ransomware. The following chart tracks the top countries for binary-based crypto ransomware and the proportion of detections for each country.

In the chart we can see that a few core countries tend to dominate the top of the list, namely the US, Japan and UK, save for a few exceptions. However, if we look at the position of Italy in the chart, we can clearly see that crypto ransomware activity has increased over the second half of the time period. In this case, Italians were the target of a malicious spam campaign leading to CTBLocker infections.

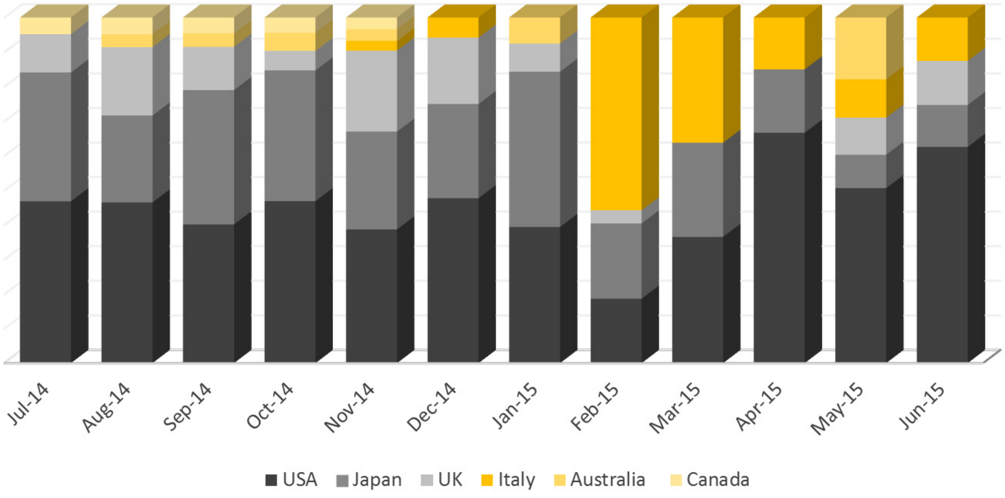


Figure 29. Countries most targeted by binary-based crypto ransomware by month

It's not unusual for ransomware to heavily target certain countries for a set period of time before moving onto others. The following chart tracks the top countries for binary-based locker ransomware and the proportion of detections for each country.

There has also been a gradual decline in binary-based crypto ransomware hitting Japan, particularly from April to June 2015. This may be a trend or a longer term fluctuation. We cannot be certain about the reasons for the fall. A possible reason may be because the effort has not proven to be as profitable as expected, so the cybercriminals have shifted their focus to other regions instead.

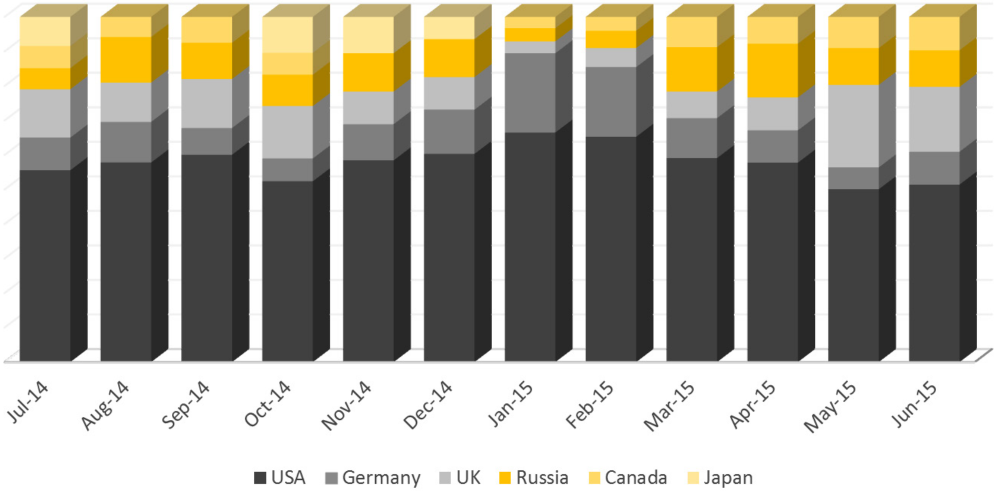


Figure 30. Countries most targeted with binary-based locker ransomware by month

On a similar note, we can see that the instances of binary-based locker ransomware hitting Japan has also declined relative to other regions, causing them to move out of the top 10.

WHAT DOES THE FUTURE HOLD FOR RANSOMWARE?

> “We believe that the ransomware concept has reached a high level of maturity...”

What does the future hold for ransomware?

It is never easy to predict what way the ransomware landscape will evolve in the future. We can look at the patterns of the past and try to speculate about what might happen in the future. We believe that the ransomware concept has reached a high level of maturity now. This is evident from the number of players in the space as well as the number and variety of variants that we see appearing. The emergence of RaaS implementations is another possible indicator that the crypto ransomware idea is close to maturity and market saturation.

In Figure 4, we saw that after approximately every two to three years of reaching a peak, the cybercriminals switched their focus to a different malware type. The patterns in the chart suggest that crypto ransomware growth is already at, or close to, its peak. This means it may soon plateau before finally entering a declining phase. This does not mean that it will go away. Instead it is likely that crypto ransomware may enter a decay phase within two years but the decay phase will be drawn out and never reach zero.

The decline may come about as a result of various factors such as increasing crackdown by law enforcement, better protection technology against crypto ransomware, increased awareness of these attacks, refusal of victims to pay, changes in international law and financial regulations. Cybercriminals may even find a better alternative to generate illicit income. What cybercriminals will focus on after crypto ransomware is uncertain, but they have proven themselves to be resourceful and will find another option to fill the void.

For now, we are aware of a number of trends that are going on in the ransomware threat landscape which will shape the near-term future of ransomware.

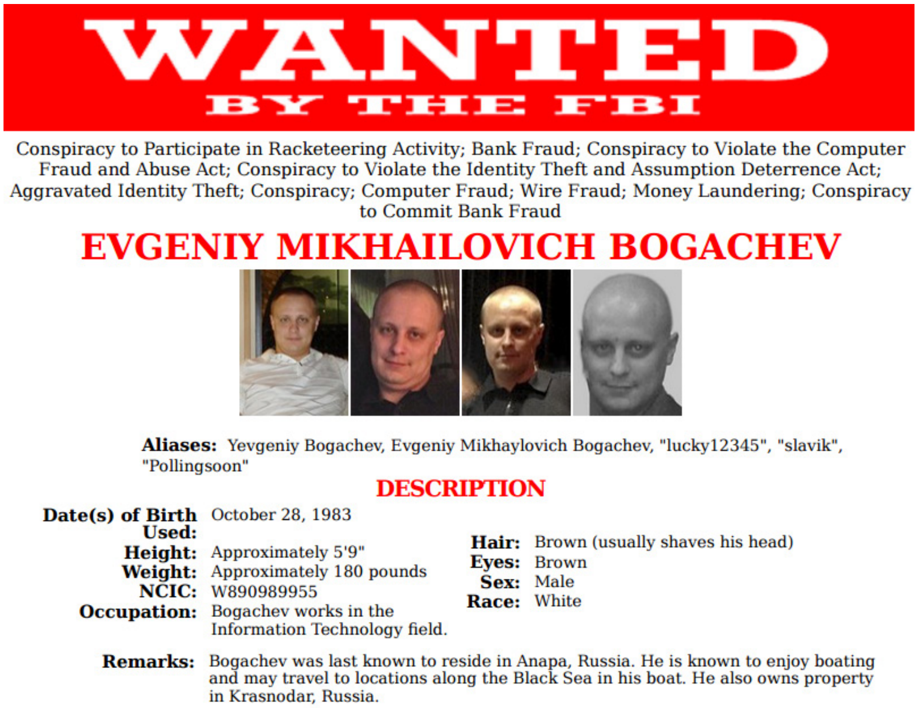
Focus on operational security

As security vendors and law enforcement pay closer attention to attack activities, cybercriminals behind ransomware will be forced to continually innovate and evolve the way they operate. With the FBI already offering a reward of up to US$3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev, the alleged mastermind behind the infamous Cryptolocker, other cybercriminals are paying attention and are already tightening operational security further to conceal their activities and identity.

Many groups have already implemented operational security measures such as the use of Tor and the Invisible Internet Project (I2P). These systems provide network-communication anonymity and concealment of their websites' location, which in turn provides resistance to any take-down efforts by law enforcement or security vendors.

Cybercriminals are using cryptocurrencies such as Bitcoin and Litecoin for ransom payments, making it more difficult for law enforcement to track any money laundering or spending of ill-gotten gains.

They are using bulletproof hosting, a service provided by some unscrupulous domain-hosting or web-hosting firms that allows their customers



WANTED

BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used:	October 28, 1983		
Height:	Approximately 5'9"	**Hair:**	Brown (usually shaves his head)
Weight:	Approximately 180 pounds	**Eyes:**	Brown
NCIC:	W890989955	**Sex:**	Male
Occupation:	Bogachev works in the Information Technology field.	**Race:**	White

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

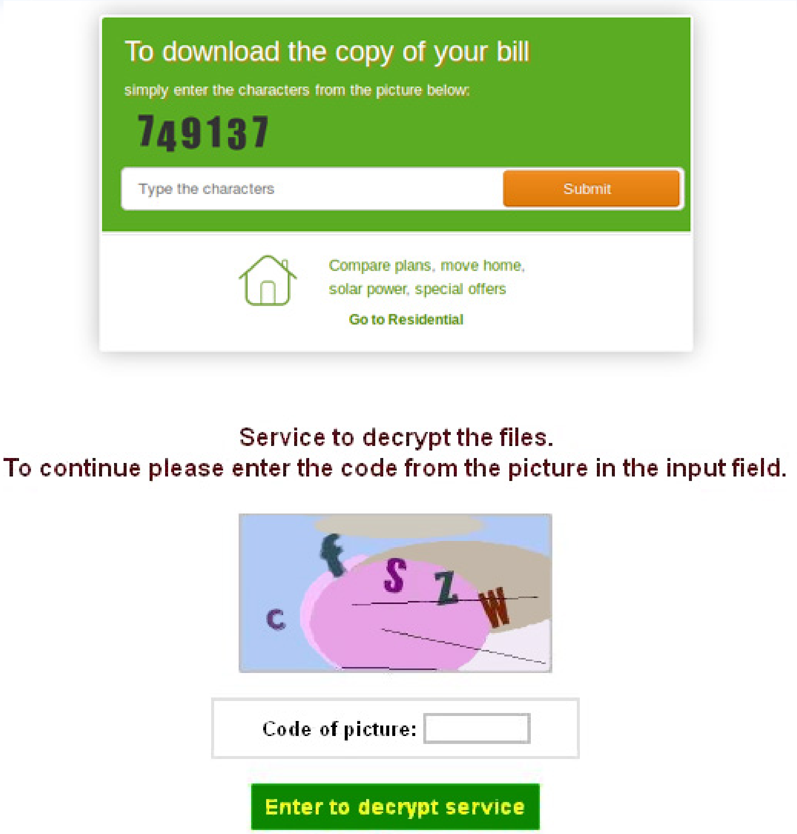
Figure 31. FBI wanted poster for the alleged creator of Cryptolocker ransomware

considerable leniency around matters of the law. Some of these cybercriminals use domain name generation algorithms (DGA) with multiple levels of redirection to increase obfuscation and decrease chances of takedown.

Some are also implementing CAPTCHA challenge responses into different parts of their operational activities, in an effort to make it more difficult for investigators. For example, Cryptolocker is using CAPTCHA challenges as gate keepers to prevent automated downloading of their malware. Cryptodefense is using CAPTCHA to limit access to payment details screens, again to make it harder for investigators on their trail.

IP address location lookups have also been used to prevent visitors from unintended locations from downloading the malware. Again this is done to prevent unwanted access to the malware, such as by malware investigators from countries outside of the targeted country/region.

As the challenges to ransomware operations increase, we expect cybercriminals to incorporate more ways to block and obfuscate attempts to track and thwart their activities.



To download the copy of your bill

simply enter the characters from the picture below:

749137

Compare plans, move home, solar power, special offers

Service to decrypt the files.
To continue please enter the code from the picture in the input field.

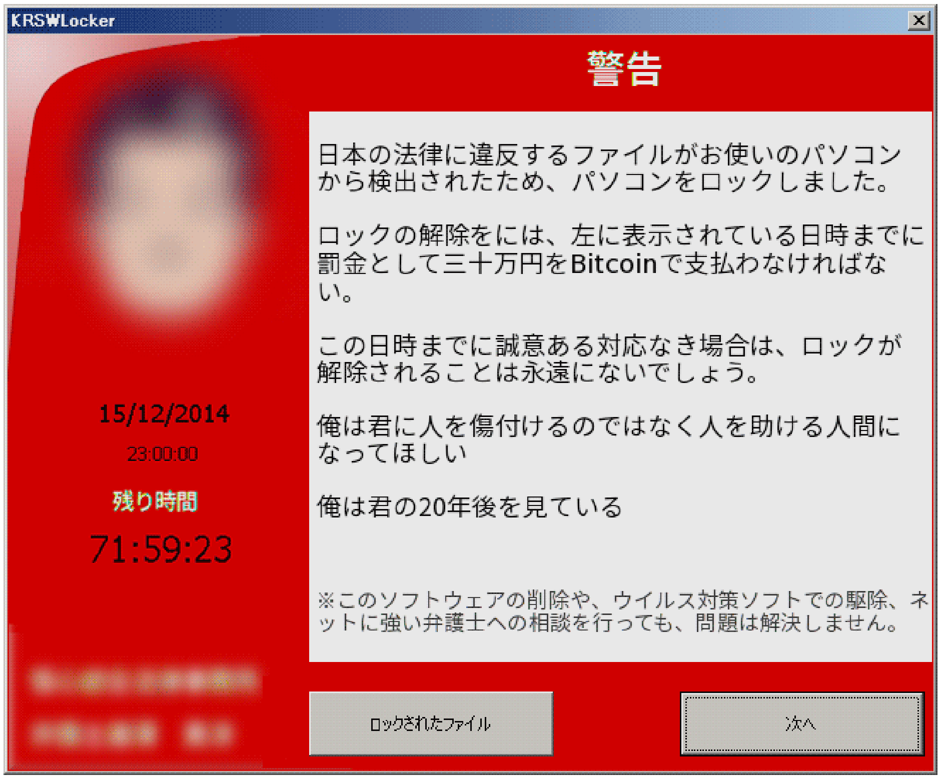
Code of picture:

Figure 32. Various CAPTCHA challenges to prevent automated access and analysis

Increasing localization

As we have noted previously in this report, ransomware is affecting many of the G20 nations but is particularly prevalent in the more affluent member countries. The challenge of catering to an international audience is the need to localize content for local languages and cultural norms in order to maximize chances of a return. Ransomware has been localized for European countries for many years now. Certain ransomware variants use localized language and law enforcement imagery, along with locally accessible payment options.

In December 2014, Symantec reported of a TorLocker



警告

日本の法律に違反するファイルがお使いのパソコンから検出されたため、パソコンをロックしました。

ロックの解除をには、左に表示されている日時までに罰金として三十万円をBitcoinで支払わなければならない。

この日時までに誠意ある対応なき場合は、ロックが解除されることは永遠にないでしょう。

俺は君に人を傷付けるのではなく人を助ける人間になってほしい

俺は君の20年後を見ている

※このソフトウェアの削除や、ウイルス対策ソフトでの駆除、ネットに強い弁護士への相談を行っても、問題は解決しません。

15/12/2014
23:00:00
残り時間
71:59:23

Figure 33. Localized crypto ransomware targeted at Japanese users

variant that was specifically localized for Japanese targets. Not only was the user interface's language translated to Japanese, the image used was also changed to a cartoon character that has cultural relevance to the local population. This suggests that the cybercriminals in this case are aware of the popular culture of Japan and are likely to be Japanese nationals or are a foreign-based group with Japanese partners (perhaps affiliates) who provide the localization services.

The use of bitcoins for payment holds additional advantages for cybercriminals seeking out international victims, as the cryptocurrency is not a national currency and is relatively easy to purchase from any of the existing Bitcoin exchanges online.

Since the initial reporting of the Japanese crypto ransomware, we have seen increased efforts by cybercriminals to create localized ransomware with more ransomware attacks hitting Japanese and Korean speaking users. In the future, we can expect to see more localized ransomware hitting countries such as China, considering its increasing GDP, and massive computer and mobile market.

Ransomware everywhere

Ransomware was initially a problem that mainly existed for users of the Windows operating system in mostly traditional computer form factors. As Windows is by far the most widely used operating system in the world, this comes as no surprise. Ransomware specifically designed for the other major desktop operating systems such as Linux or Mac OS X have been thin on the ground. This is most likely due to the low market share of those operating systems, making ransomware investment in them unattractive.

Multi-platform locker ransomware such as Browlock has been created as a sort of catch-all solution to target non-core victims. However, ransomware such as Browlock has limited effectiveness, since it only targets the web browser and can be relatively easily overcome.

We have already seen ransomware appear on mobile phones but where else are ransomware likely to appear?

Ransomware on your wrist

In terms of consumer electronics, the wearables market is an area that manufacturers continue to push for growth. In the wearables market, the smartwatch is a category that's gathering momentum. The two main players in the mobile OS space are also battling for the number one spot in this emerging market segment. Google has a specially tailored version of its mobile OS called Android Wear for devices such as smartwatches. Apple released its Apple Watch this year, which is equipped with a custom operating system called watchOS. Android Wear smartwatches are gaining in popularity and typically retail from around US$100 to several hundred. According to research firm Canalys, 720,000 Android Wear devices were shipped in 2014, with the Moto 360 being the leading device in the Android end of the market.

This year may be considered by many to be the year when the smartwatch finally becomes mainstream with the arrival of many more Android Wear models as well as the much anticipated Apple Watch, though its shipment numbers are still unknown. With so much growth and hype in this technology, the wearable device market is likely to attract the attention of ransomware creators.

When we considered smartwatches in the context of ransomware, we came to the conclusion that there are no particular reasons why ransomware would not work on them. Android Wear is a limited subset of the Android OS. They typically feature a small touch screen that allows a wearer to use touch gestures to interact with the device. Android Wear devices also support voice commands which can be activated by saying "OK Google" to the smartwatch followed by a command or question. Hardware buttons are not often used or have very limited functionality in these devices as the bulk of the functionality is accessed through touch- or voice-activated menus.

Most Android Wear devices do not have the ability to make their own direct internet connections such as through Wi-Fi. This issue was resolved for some devices that were built using system on chip (SoC) hardware which already had the Wi-Fi equipment built in through later updates to the operating system. Due to their inherent limitations, devices running the Android Wear OS are designed to be paired with a separate Android device such as a mobile phone to access the internet for data transfer and install specially designed apps for the smartwatch.

To ensure support for the smartwatch OS, Android Wear was designed to enable existing phone-based apps to work with Android Wear in order to show notifications and alerts without any changes to the existing app's code. App developers can also write apps specifically for Android Wear or they can extend existing phone apps to take

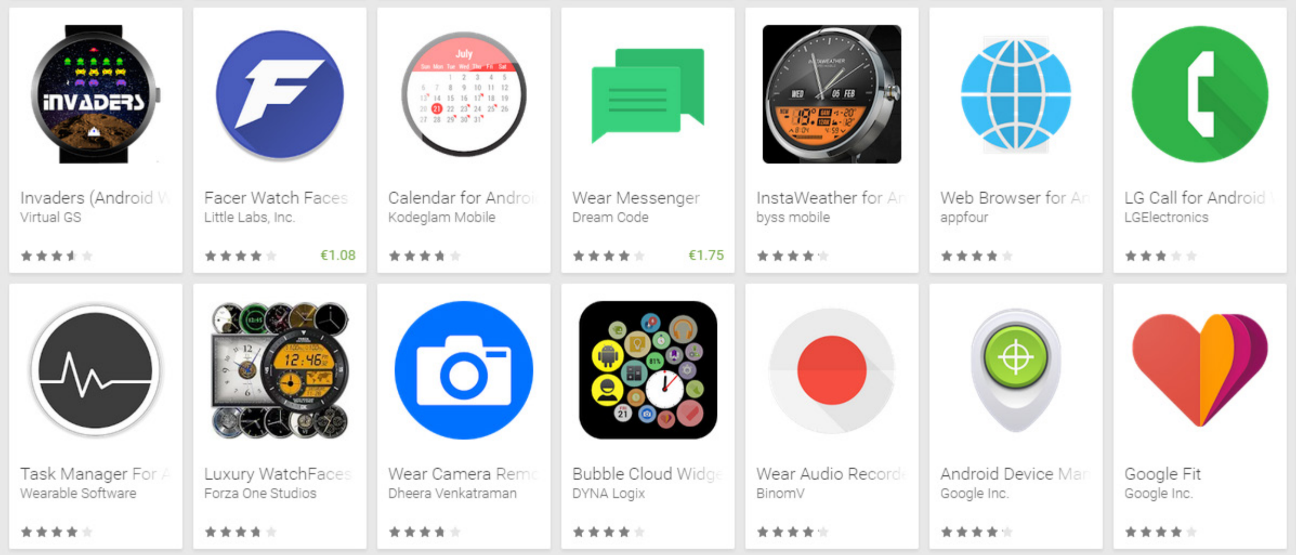


Figure 34. A selection of Google and third-party apps designed for Android Wear

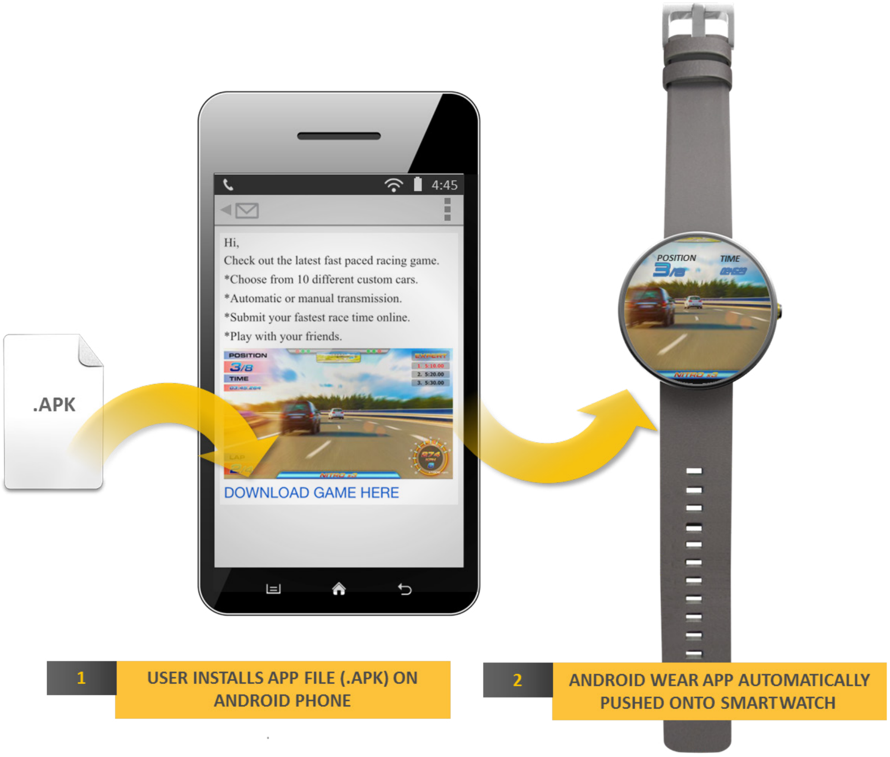
full advantage of extra features enabled by the smartwatch.

Based on our understanding of how ransomware typically works and how these devices operate, we believe that the most likely form of ransomware to appear for smartwatches is locker ransomware. We don’t believe that smartwatches are likely to hold much data that is of great value to the wearer, so holding data to ransom on these devices is of little use. A device-locking ransomware could potentially be more successful due to the way many of these devices are designed. Given the limited options for interacting with a smartwatch and the lack of hardware interfaces, we believe that these devices may be more susceptible to a locker ransomware attack. At best, locker ransomware attacks on smartwatches may be highly inconvenient, forcing the user to resort to factory resets to recover the device. At worse, the ransomware infection could potentially render the device unusable.

Installing an Android Wear app

To install an app on an Android Wear smartwatch, the device must first be paired with an Android mobile phone or tablet through a Bluetooth connection. Once this is done, the user can simply discover and install smartwatch apps in the normal way using their mobile device. They can browse for apps through Google Play, other unofficial app markets, or even by direct links to .apk files. There is a small but growing collection of apps for Android Wear available on Google Play as more developers begin to take advantage of the new platform.

From a user’s point of view, the process of installing an app onto the smartwatch is seamless and is no different from installing an app on the phone. If the



Hi,
Check out the latest fast paced racing game.
*Choose from 10 different custom cars.
*Automatic or manual transmission.
*Submit your fastest race time online.
*Play with your friends.

DOWNLOAD GAME HERE

1 USER INSTALLS APP FILE (.APK) ON ANDROID PHONE

2 ANDROID WEAR APP AUTOMATICALLY PUSHED ONTO SMARTWATCH

Figure 35. How Android Wear apps are installed

app being installed on the mobile phone has an Android Wear component, the component will be automatically pushed by the phone onto the smartwatch through the Bluetooth link without the user having to take any extra steps.

This means that apps can also be installed through alternative sources, such as unofficial market places, as well as directly from other alternative sources, such as through links in an email or on a website.

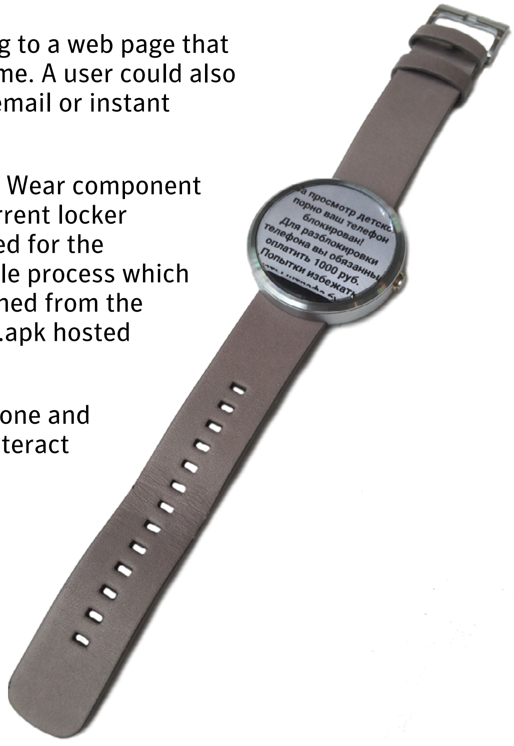
Ransomware on a smartwatch

A typical ransomware installation scenario may involve the user browsing to a web page that redirects them to download ransomware disguised as a useful app or game. A user could also potentially be tricked into installing the ransomware if they are sent an email or instant messaging notification with a link to download a new app.

After the .apk file is downloaded and installed on the phone, the Android Wear component of the ransomware is automatically pushed onto the smartwatch. For current locker ransomware to work on Android Wear devices, they have to be repackaged for the platform to allow them to run on the Android Wear Device. This is a simple process which is not difficult to achieve. In our testing, we had Android.Simplocker pushed from the phone to the smartwatch by having the user install a fake game from an .apk hosted on a web server.

Once the installation process was completed and the app started, the phone and the watch both became locked and could not be used. Any attempts to interact with the device were blocked by a modal ransom notification message in Russian language.

This prevents the user from being able to perform any meaningful interaction, as every time they try to swipe or tap on the menu, the ransom message is pushed onto the screen again. Voice-activated commands may also be impacted as many voice commands still require some touch interaction.



а просмотр детско
порно ваш телефон
блокирован!
Для разблокировки
телефона вы обязанны
оплатить 1000 руб.
Попытки избежать

Figure 36. Ransom message from Android.Simplocker as seen on a Moto 360 smartwatch

Bricked smartwatch?

Under normal circumstances, if there is an unwanted app on the smartwatch, the user can simply uninstall the app from the phone, causing the app to be removed from the smartwatch too. However, because this is a screen-locker ransomware, it is not possible to uninstall the ransomware from the phone using the normal app uninstallation method through the menu.

Faced with this situation, it may seem easier to just reset the phone to factory settings to start afresh, but this option may not be reachable on the smartwatch. Earlier, we mentioned that for many smartwatches, access to the functionality of the watch is made through the touchscreen or to a more limited extent with voice commands. But when a locker ransomware is running on the smartwatch, it continuously blocks and interrupts user interactions, making it extremely difficult for the user to reach any of the functionally of the smartwatch including access to the factory reset option.

If the user is unable to reset or disinfect the smartwatch, the smartwatch may be rendered useless.

Fortunately with our Moto 360 test smartwatch, we were able to force a cold reboot by holding the side hardware button down for 30 seconds. Upon reboot, the ransomware was slow to restart allowing just enough time for us to reach the factory reset option on the watch menu before the ransomware kicked in again. This meant that we could wipe the smartwatch and start afresh; not convenient, but at least we could recover the watch. If the ransomware was able to restart quicker after the cold reboot or if the watch did not have a cold boot option, then things may not have worked out quite so well.

Ransomware meets Internet of Things

One undeniable shift that we see in the world today is the increasingly mobile, connected, and ubiquitous nature of computing. The IoT and wearable computing are trends that will bring growth to the IT industry, but this growth also brings new opportunities for ransomware creators. We already have smart TVs, smartwatches, smart clothing, smart fridges, smart locks, and internet-enabled cars, and the list continues to grow by the day. All of these devices are effectively connected computers which could potentially be hijacked by cybercriminals and held to ransom. Some device types may be more susceptible than others due to the nature of their usage or by design. For example, we have already seen crypto ransomware target data-rich devices such as network attached storage (NAS) devices. Trojan.Synolocker is just one such threat that targeted Synology NAS products.

Imagine a scenario your smart house lock refuses to allow entry to your own house or where your car is taken over by ransomware and refuses to start, allow entry, speed up, or slow down until a ransom is paid.

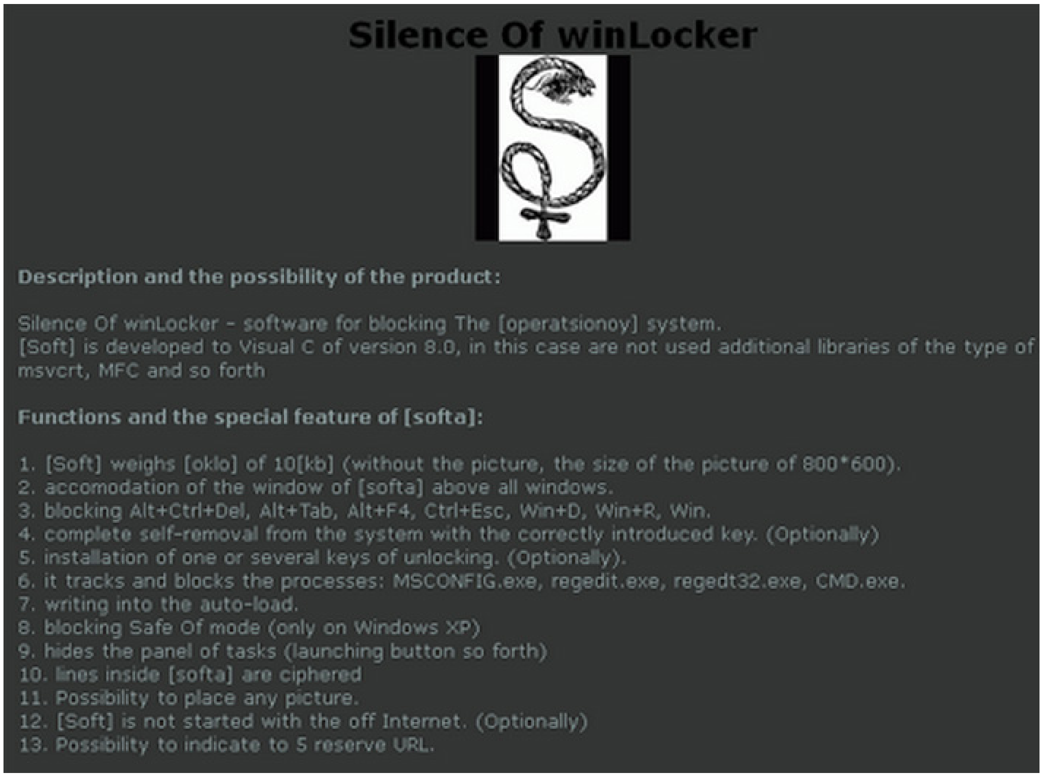
This scenario may not be as farfetched as it may seem. We have recently seen that researchers can remotely gain access to a moving Jeep Cherokee vehicle and take over control from the driver. The researchers were able to control virtually all aspects of the car's functionality, including lights, air circulation, wipers, entertainment system, the steering, transmission, and brakes. As more cars become dependent on connected computing technology, we may inevitably see more malware attacks against them unless their design and implementation is better secured.

In the past, ransomware infections did not necessarily put lives at risk. In the future, this frightening prospect may just become that bit closer to reality.

Increased franchising and co-operations

For the novice cybercriminal with limited knowledge and skills, there is a thriving underground marketplace selling crimeware toolkits. These toolkits allow easy entry into the world of ransomware extortion for the uninitiated. Over the last few years, a number of ransomware toolkits have emerged. While initially sold on underground forums, several of these tools can now be found for free on underground forums.

Tools such as Silence of winLocker (Trojan.Ransomlock.K) have provided non-technical cybercriminals with access to everything they need to commit ransomware attacks for the price of 2500 WMZ. This includes the builder to create the malicious binary that holds the compromised computer hostage and the backend C&C server control panel software, which allows attackers to create and choose which extortion demand image they wish to serve to their victims.



Silence Of winLocker

Description and the possibility of the product:

Silence Of winLocker - software for blocking The [operatsionoy] system.
[Soft] is developed to Visual C of version 8.0, in this case are not used additional libraries of the type of msvcrt, MFC and so forth

Functions and the special feature of [softa]:

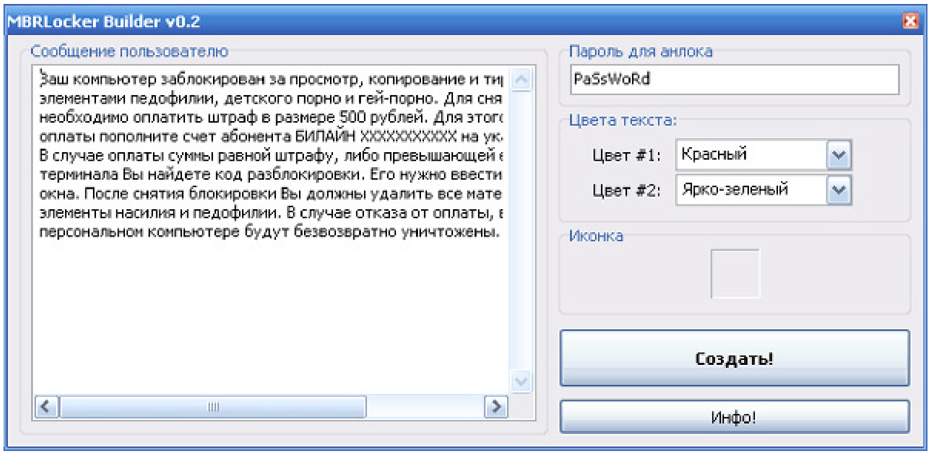
1. [Soft] weighs [oklo] of 10[kb] (without the picture, the size of the picture of 800*600).
2. accomodation of the window of [softa] above all windows.
3. blocking Alt+Ctrl+Del, Alt+Tab, Alt+F4, Ctrl+Esc, Win+D, Win+R, Win.
4. complete self-removal from the system with the correctly introduced key. (Optionally)
5. installation of one or several keys of unlocking. (Optionally).
6. it tracks and blocks the processes: MSCONFIG.exe, regedit.exe, regedt32.exe, CMD.exe.
7. writing into the auto-load.
8. blocking Safe Of mode (only on Windows XP)
9. hides the panel of tasks (launching button so forth)
10. lines inside [softa] are ciphered
11. Possibility to place any picture.
12. [Soft] is not started with the off Internet. (Optionally)
13. Possibility to indicate to 5 reserve URL.

Figure 37. Forum post advertising the availability of the "Silence Of winLocker" ransomware toolkit for sale

Other freely available toolkits,

such as MBRLocker (Trojan.Bootlock.B), infect a compromised computer’s master boot record (MBR). This prevents the operating system from booting up until the ransom is paid and the unlock code is entered.

With attackers seeing cybercrime as a business venture, it is not uncommon for them to take successful business models and implement them into their own malicious campaigns. As standalone offline ransomware toolkits are commonly leaked and found online for free after release, it is not surprising that ransomware authors look for a different business model approach to monetize their product and opt for the affiliate/franchise model.



MBRLocker Builder v0.2

Сообщение пользователю

Ваш компьютер заблокирован за просмотр, копирование и тир
элементами педофилии, детского порно и гей-порно. Для сня
необходимо оплатить штраф в размере 500 рублей. Для этого
оплаты пополните счет абонента БИЛАЙН XXXXXXXXXX на ук
В случае оплаты суммы равной штрафу, либо превышающей е
терминала Вы найдете код разблокировки. Его нужно ввести
окна. После снятия блокировки Вы должны удалить все мате
элементы насилия и педофилии. В случае отказа от оплаты, в
персональном компьютере будут безвозвратно уничтожены.

Пароль для анлока: PaSsWoRd

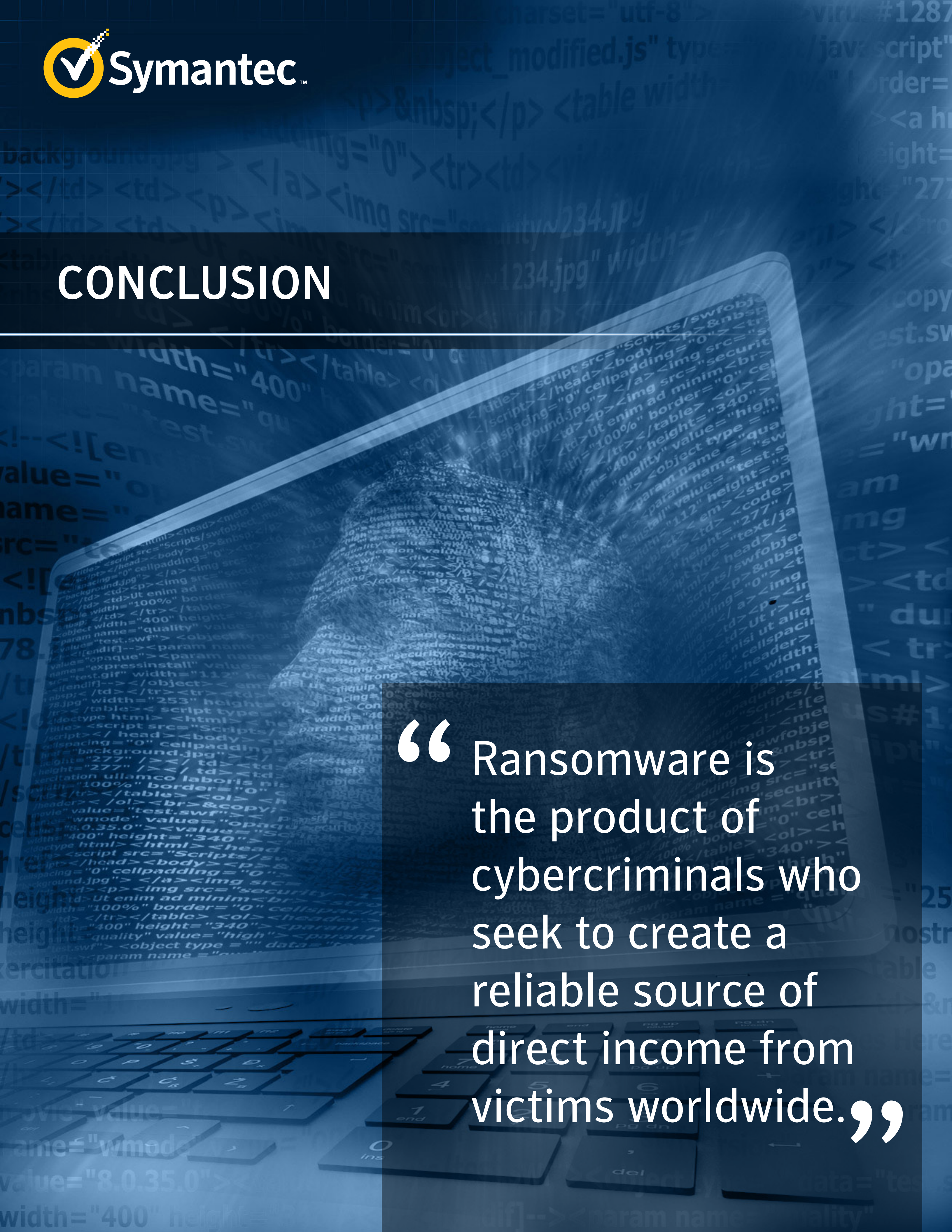
Цвета текста:

Цвет #1: Красный

Цвет #2: Ярко-зеленый

Figure 38. MBRLocker Builder is a ransomware-builder kit available for free on underground forums

The malware authors behind toolkits such as Torlocker and Tox looked to cloud services for inspiration on how to model their business. Their business models effectively provide RaaS, signing up users and offering them a cut of the profit for distributing the ransomware. This allows the ransomware author to maintain control and generate an income stream from the threat’s use. In this business model, work and risk is shared between the ransomware affiliates and the toolkit provider. It is also an approach to the division of labor, allowing experts to do what they do best. Coders stick with ransomware development and those who are best at malware distribution stick with doing that. It also gives each business partner in crime more control over their respective activities. Given the success of affiliate business models in all other aspects of business and crime, it would be reasonable to expect more of this type of activity in ransomware in the future.



CONCLUSION

> “Ransomware is the product of cybercriminals who seek to create a reliable source of direct income from victims worldwide.”

Conclusion

In this report, we have looked at the origins and evolution of ransomware and charted the many twists and turns in its history. We saw how ransomware is the product of cybercriminals who seek to create a reliable source of direct income from victims worldwide. Starting from less persuasive forms of direct revenue generation using misleading applications such as PC performance tools, cybercriminals learned and iterated over the years and with each step, ratcheted up the levels of aggression. They progressed from misleading apps to fake antivirus scams and then later moved onto pure ransomware in the form of locker and crypto ransomware threats that are so prevalent today. In this study, we have learned that crypto ransomware has now emerged as the most common form of binary-based ransomware, making up 64 percent of binary-file-based ransomware detected so far in 2015. We saw that between 2013 and 2014, there was a 250 percent increase in new crypto ransomware families on the threat landscape.

Ransomware is not cheap; the average ransom demand hitting individual users now stands at a hefty US$300. In the past 12 months, we saw ransom demands range from US$21 to US$700. The exact amounts may vary depending on the ransomware family and the location of the victim. Striking a balance between volume and pricing is a continuing challenge for cybercriminals and some even offered to return data for free after a set period.

We also looked at the different factors that are contributing to the growth in ransomware, how they are spread, and how they are the experts at leveraging human psychology to press home their demands. We considered how widespread the problem of ransomware is, hitting the majority of the nations that make up the G20 group. Increasing localization of ransomware shows that the problem is both global and local at the same time. We also looked at how technological trends such as IoT and the growth in the wearables market can allow cybercriminals to target new areas with ransomware. In our research, we have demonstrated how existing Android ransomware can be easily retargeted at Android Wear smartwatches, potentially opening up new revenue streams for cybercriminals.

What this research shows more than anything else is that attention to security is paramount for all. Battling ransomware is a major task and we all have a role to play in it. For product designers creating new technology or products, just considering the normal benign use cases is not enough anymore. If there are weaknesses that allow products to be subverted or functionality denied to owners, cybercriminals will find them. The challenge to designers of products is to improve security and take malicious usage and scenarios into consideration. Potential victims of ransomware need to practice basic security practices to protect their data, such as avoiding clicking malicious links or attachments and patching exploitable software vulnerabilities. Learn about the threat of ransomware and take steps to prepare for and minimize risk from these ransomware attacks.

APPENDIX

Appendix

Ransomware victim manipulation techniques

To understand how ransomware attacks can succeed in extracting payment from a rational population, we must consider some of the behavioral economic, psychological, and social-engineering techniques used in ransomware. Behavioral economics refers to the study of the effects of psychological, social, cognitive, and emotional factors on the economic decisions of individuals.

Psychology in this case refers to the scientific study of the human mind and its functions, especially those affecting behavior in a ransomware context. In information security, social engineering has long been known to be a powerful tool in any attacker's arsenal. It refers to the psychological manipulation of people through techniques based on specific attributes of decision-making known as cognitive and motivational biases.

For the purpose of understanding how they can be used in different ransomware attacks, we will see how they apply to the two different types of ransomware: locker ransomware and crypto ransomware. The locker ransomware example we will examine runs on the Android platform and is known as Android.Lockdroid.G and for the crypto ransomware example, we will look at Trojan.Cryptolocker.

Locker ransomware manipulation

Lockdroid.G is typical of modern locker ransomware and employs a range of psychological tricks to convince victims to pay.

Deception

The human cognitive mechanism is known to take representational shortcuts (assumptions that we generally hold to be true) in order to gain efficiency. Deception is designed to exploit this tendency in the cognitive system. The use of legitimate-looking themes such as those mimicking law enforcement agencies helps to deceive victims.

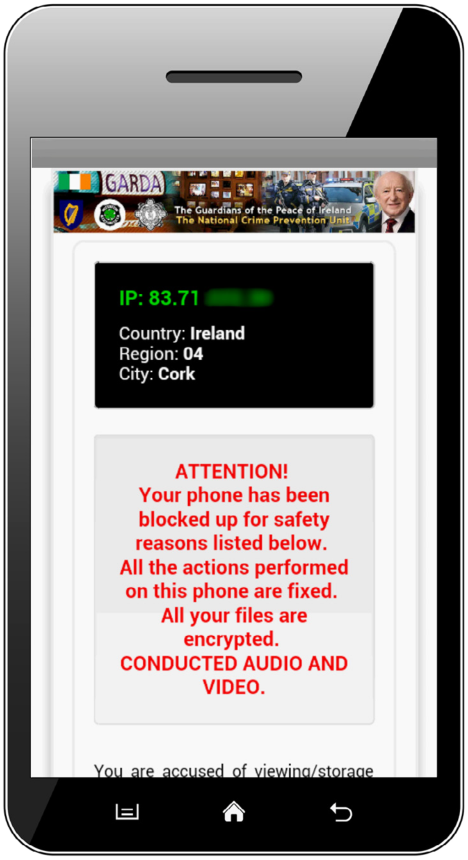
Central and peripheral route to persuasion

The Elaboration Likelihood Model (ELM) proposes that there is a central route and a peripheral route to persuasion. With persuasion through the central route, an individual is persuaded through careful and thoughtful considerations of the merits presented. With peripheral persuasion, an individual is persuaded through associations with positive or negative cues in the stimulus. Positive associations may be that of a reward for carrying out some action, while a negative association is the threat of punishment for not complying.

Through the types of themes, imagery, and wording seen in Figure 39, we can see that Lockdoid.G, like a large number of its peers, is designed to persuade using both the central and peripheral routes of persuasion.

Authority & social compliance

Society has trained people to behave in accordance with established patterns and norms, such as trusting and obeying known authorities like the police. The use of nationally localized law enforcement themes along with other relevant authority cues makes the extortion demand seem all the more real.


GARDA
The Guardians of the Peace of Ireland
The National Crime Prevention Unit

IP: 83.71 [redacted]

Country: Ireland
Region: 04
City: Cork

ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.

You are accused of viewing/storage

Figure 39. Example of the lock screen shown by Android.Lockdroid.G employing many psychological tricks

In an infamous experiment by Stanley Milgram in 1963, he showed just how willing people are to hurt another human being in order to comply with a recognized authority. This show how powerful the technique is when trying to convince victims of their wrongdoing and payment of a fine.

Visceral triggers

The accusation of committing a crime and the authorities knowing their location can provoke an intuitive reaction of fear within a victim. This can influence the victim's cognitive information processing and their decision-making abilities, making it less likely that they will make a rational decision when it comes to the ransom payment.

We can see Lockdroid.G taking advantage of this effect through the display of country/location-specific law enforcement banners, the user's IP address, and the city in which they are located. Location information can be easily obtained by correlating IP address ranges to entries in IP address location libraries or online IP location services that are freely available.

Influence of framing

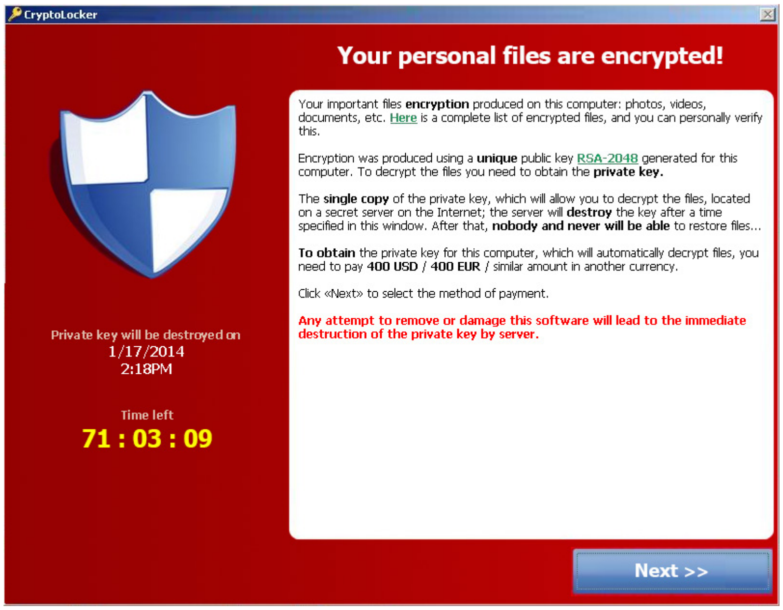
The way in which a risk is framed or described can influence the individual's perception of risk. Prospect theory is a behavioral economic theory that states that people make decisions that are risk-adverse over prospects involving gains, while they become risk-loving over prospects involving losses. This means people are more likely to take risks when they are given a proposition that plays up risk of losses. False messages threatening the deprivation of liberty for 5 to 11 years are designed to take advantage of these human characteristics and could unduly influence a victim into paying the ransom.

Dishonesty principle

If you have broken the law, it can be used against you. With ransomware messages threatening prosecution for "downloading of pirated music, video, warez", some victims are less likely to seek help from others or to contact law enforcement once they realize they have been scammed.

Preference for confirmatory rewarding information

Information search bias describes a tendency for individuals to seek information that confirms their initial hypothesis, rather than seeking out information to disprove it. This has been found to be a persistent human error and reduces the quality of decision outcomes. After the initial shock of seeing the ransomware message, victims may erroneously seek out information to confirm the existence of the organizations and laws presented in the ransomware messages, rather than trying to disprove the claims. This can lead to a bias and influence the decision to make a ransom payment.



Your personal files are encrypted!

Private key will be destroyed on
1/17/2014
2:18PM

Time left
71 : 03 : 09

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **400 USD** / **400 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Figure 40. Ransom demand screen presented by Trojan.Cryptolocker

It should also be noted that most ransomware threats that use law enforcement themes tend to quote official-looking legislation and use lots of legal jargon as part of the scam. Since most people are not legal experts, they can be confused and, instead of seeking help (as mentioned in the dishonesty principle), resort to paying the ransom instead.

Crypto ransomware manipulation

While locker ransomware relies more heavily on psychological factors within the extortion message to convince victims to make a payment, crypto ransomware relies more on the users' sentiments towards the encrypted data and what effect the loss of this information might have. To that end, crypto ransomware targets a different set of psychological factors and effects which we will now have a look at.

Time

Time pressure has been shown to influence the decision strategy used. When under time pressure, an individual is more likely to reduce the cognitive resources available for an analytic judgment. In Figure 40, we can see that the crypto ransomware employs time-pressure tactics accompanied with temporal monetary penalties in an effort to force payment of the ransom.

Endowment effect

As a result of ownership, people ascribe more value to their own possessions. This can lead to people paying more to retain something they already own rather than obtaining something owned by someone else. For example, having a victim's personal photos encrypted by ransomware could potentially invoke this effect.

Loss aversion

People have a stronger tendency to avoid losses than to acquire gains. This relates to Prospect theory, in which people tend to make decisions that are risk-adverse over prospects involving gains, while they become risk-loving over prospects involving losses. If a victim is unsure what risks are associated with the loss of their information, it can lead to loss-aversion decision-making which increases the likelihood of the victim making the ransom payment

Sunk costs

This is a cost in terms of time or money that has already been incurred and cannot be recovered. In behavioral economics, evidence suggests that sunk costs influence decisions and can lead to irrational behavior because individuals are prone to loss aversion and framing effects. If a victim's personal work which they have invested a lot of time and effort into has been encrypted and is threaten with loss, it can unduly influence the ransom payment. The decision-making process in this case is a tradeoff between the value of the work that is potentially lost versus the ransom amount.

Ellsberg paradox

This is the idea of how people make decisions under conditions of ambiguity or uncertainty. Basically people overwhelmingly prefer and will choose known probabilities of winning in risky situations. Without fully knowing how the loss of data might affect a victim, they may opt for the safer probability of paying the ransom to get their data back. In ransomware situations, the victim is potentially faced with two unequal probabilities. On the one hand, they are unsure about whether they would actually get the data back even if they paid the ransom. On the other hand, they could be even more uncertain about how the loss of data would impact them. Faced with these unequal uncertainties, people have a tendency to choose the option that they perceive to have a more definite outcome. At least as presented by the ransomware, the payment of the ransom is supposed to return the original files.

Fear of regret

When faced with an ambiguous decision, individuals may take into account the possibility of feeling regret and may attempt to reduce this possibility through the choice that they make. Fear of regret around the possible loss of data may influence any decisions around the ransomware payment.

Anxiety, risk and decision making

It has been shown that surges in anxiety can be correlated with surges in general risk perception, which can lead to errors in risk assessment. A victim's anxiety around the potential loss of data may affect their risk perception and assessment, leading to a higher probability of paying the ransom demand.

MITIGATION STRATEGIES

Mitigation strategies

With ransomware, prevention is definitely better than cure. This section details a number of useful tips that can help to reduce the risk of ransomware.

Educate and inform

Read up on ransomware, how they work, and how they spread. Ransomware is a constantly evolving threat so it is important to keep up to date with new developments. Ensure that users are aware of the techniques that the malware uses such as the social-engineering tricks in the spam emails. Awareness of these attacks can help users recognize and avoid future attacks.

Use security intelligence sources such as Symantec DeepSight Intelligence and the Symantec Security Response blog to learn about the latest attacks. You can also follow us on Twitter (@threatintel) for the latest security news.

Patching software

One of the most common methods for ransomware to make its way onto a computer is through drive-by-downloads caused by accidentally visiting websites rigged with exploits. Bear in mind that you don't have to enter in the URL of the malicious website yourself. Your browser could be redirected to the malicious site by a malvertisement or hidden iframe even by simply visiting well-known and legitimate sites. The best defense against an exploit-based infection scenario is to ensure that your software and operating system is up to date with security patches.

Some of the most common software is also the most targeted through exploit kits. If you use any of the following software, we recommend that you use automatic updates if possible.

Adobe

Users of Adobe Acrobat/Reader, Flash Player, and Shockwave Player should ensure that they are up to date with patches. Adobe releases software updates on the second Tuesday of each month. The following resource provides more information and details of patches:

- https://helpx.adobe.com/security.html

Microsoft

Users of Microsoft products such as Windows, Office, and Internet Explorer are often targeted by exploit kits. Users of these software products should ensure that they are up to date with security patches. Microsoft normally releases software updates on the second Tuesday of each month.

The following resource provides more information and details of patches:

- https://technet.microsoft.com/en-us/security/bulletin/

Oracle

Oracle Java is frequently targeted by exploit kits. User of the software should ensure that they are up to date with patches. Oracle normally releases software patches once every quarter. You can find out more about Oracle software updates at the following location:

- http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Use a layered defense approach

Most of today's ransomware attacks involve many different elements. An attack could start with a spam email that includes a link to a malicious website which exploits multiple vulnerabilities to download the ransomware. A multi-layered defense strategy addresses each of these attack vectors at various points in an organization's infrastructure. For example, using a messaging protection solution such as Symantec Messaging Gateway or

Email Security.cloud could provide protection against many messaging-based attacks before the malicious message could even reach a user at the endpoint.

Network protection could help prevent users from visiting malicious websites and file-based protection could block malicious code from executing at the endpoint computer. Each layer creates an extra obstacle for the malware to overcome, making it much more difficult for the ransomware attack to be successful.

Use a comprehensive endpoint security solution

We recommend the use of an endpoint security solution that incorporates not only signature-based protection mechanisms but also heuristic-, behavioral-, and reputation-based protection. Norton Security and Symantec Endpoint Protection provide a comprehensive security solution to help protect against known and unknown attacks.

Advice for mobile/tablet device users

If using a mobile/tablet device, be sure to install a suitable mobile security solution such as Symantec Mobility Suite for enterprises or Norton Security with support for mobile devices.

Be wary of installing apps from untrusted sources such as unofficial markets and messages or websites offering free apps for installation.

When installing a new app, check the list of permissions to see if it is appropriate for the app that you are installing.

Enable a remote-wipe facility to allow you to delete all data and perform a full factory reset on the mobile/tablet device even if it is locked by ransomware. This feature will also come in handy should the device be lost or stolen.

Use network protection

Many ransomware infections today are a result of malicious network traffic. A drive-by-download attack scenario could potentially be prevented by using a suitable network protection solution. Network protection can help prevent users from accessing malicious websites as well as providing protection against remote exploits from zero-day vulnerabilities.

Network protection could also help prevent network encryption which is what could happen with some crypto ransomware threats that attempt to reach out over network shares to encrypt files on other computers.

Comprehensive endpoint protection products such as the Norton Security and Symantec Endpoint Protection have an integrated network protection (IPS) component which can prevent a large number of these attacks. Users of these products should ensure that the protection layer is not turned off so that they continue to receive protection against network-based attacks.

Make backups and have a plan

Making backups is always a good idea, even without the threat of ransomware. Backups are also an essential part of a business continuity and disaster recovery plan, which all businesses should have. At a minimum, we recommend that users at least make backups of the files that are important to them and do it regularly. How often backups are made and to which storage solutions are all things that need to be considered, depending on your own risk profile.

If the worst should happen...

If all else fails and your system become infected with crypto ransomware, hopefully you have already made backups. If not, there are at least a number of things that you can do to try to recover your files.

Use tools to remove the ransomware

Symantec provides tools such as Norton Power Eraser to help users remove all types of persistent malware from infected computers. You can learn more about this tool by visiting these resources:

- Remove FBI Virus: Steps to remove Moneypak Malware using Norton Power Eraser (Video)
- SymHelp tool (Symantec Power Eraser)
- Norton Power Eraser

Shadow Copies

Sometimes crypto ransomware can have weaknesses in their implementation which could allow victims to recover at least some of their files without paying. For example, Windows can be set up to make recovery points at regular intervals. These backups are called shadow copies. If this service is enabled and if a crypto ransomware does not interfere with this feature, it may be possible recover some files using this method. This blog details various Windows tools that can be useful to aid recovery in case of a crypto ransomware attack.

File recovery software

Another point worth noting is that when a file is deleted in Windows, the contents of the file are not usually scrubbed from the physical disk itself. Instead, the entries defining the file are removed from the disk allocation tables, freeing up the space. The original data in the freed space is not overwritten until a new file is written to the same space on the disk. This makes it possible to recover delete files if the disk space has not already been overwritten by another file. Victims can use file recovery software such as PhotoRec to scan for deleted files and recover them.

No bullet-proof solution

It should be noted that the more advanced crypto ransomware groups are aware of these techniques and take steps to prevent their successful use. As a result, some crypto ransomware threats delete shadow copies to prevent victims from being able to recover files. Similarly, other crypto ransomware threats such as Trojan.Ransomcrypt.R use a secure deletion tools such as SDelete to ensure that original files are securely erased from the disk after encryption. In this situation, the only answer is to have a backup of the files as there is no practical way for the files to be recovered or decrypted without the right key.

Symantec detections for common ransomware families

The following is a list of commonly known names of recent ransomware families along with Symantec’s detection names for them. The ransom demands priced in US dollars reflect the currency value at the time that the ransomware was released:

Table. Names and Symantec detections for recent ransomware families

Discovered	Type	Common name/Alias	Ransom demand	Symantec detection
July 2015	Crypto	Encryptor RaaS	0.174911 BTC (US$50)	Trojan.Crytolocker.W
June 2015	Crypto	Troldesh	1 BTC (US $250)	Trojan.Ransomcrypt.T
May 2015	Crypto	Locker	0.1 BTC (US $25)	Trojan.Cryptolocker.V
May 2015	Crypto	Tox	1 BTC (US $250)	Trojan.Cryptolocker.U
May 2015	Crypto	Pollcrypto	1 BTC (US $250)	Trojan.Pollcrypto
May 2015	Crypto	Breaking Bad	AUD $450 (US $350)	Trojan.Cryptolocker.S
April 2015	Crypto	Alpha Crypt		Trojan.Cryptolocker.N
April 2015	Crypto	Threat Finder		Trojan.Ransomcrypt.S
April 2015	Crypto	Kriptovor		Trojan.Cryptolocker.R
April 2015	Crypto	PClock2	0.5 BTC (US $118)	Trojan.Cryptolocker.Q
March 2015	Crypto	Pacman		Trojan.Cryptolocker.P
March 2015	Crypto	VaultCrypt		Trojan.Ransomcrypt.R
March 2015	Crypto	BandChor		Trojan.Ransomcrypt.Q
March 2015	Crypto	CryptoFortress	1 BTC (US $250)	Trojan.Cryptolocker.H
February 2015	Crypto	TeslaCrypt	2 BTC (US $500)	Trojan.Cryptolocker.N
February 2015	Crypto	Coin Locker		Trojan.Ransomcrypt.H
January 2015	Crypto	CryptoTorLocker2015	BTC (US $100)	Trojan.Cryptolocker.M
January 2015	Crypto	Ransomweb		Php.Ransomcrypt.A
January 2015	Crypto	Pclock	1 BTC (US $291)	Trojan.Ransomcrypt.P
December 2014	Crypto	Keyholder	1.5 BTC (US $450)	Trojan.Cryptolocker.L
December 2014	Crypto	Ophionlocker	BTC (US $300)	Trojan.Ransomcrypt.O
December 2014	Locker	Virlock	BTC (US $250)	W32.Ransomlock. AOW32. Ransomlock. AO!inf
November 2014	Crypto	CoinVault	0.7 BTC (US $350)	Trojan.Cryptolocker.K
November 2014	Locker	Tech Support Scam		Trojan.Ransomlock.AM
October 2014	Locker	Porndroid	Money Pak (US $500)	Android.Lockdroid.E
October 2014	Locker	Koler Android Worm	Money Pak(US $300)	Android.Lockdroid.F
September 2014	Crypto	KRSWLocker	BTC 40,000 YEN (US $500)	Trojan.Ransomcrypt.H
September 2014	Crypto	CryptoGraphic Locker	0.2 BTC (US $100)	Trojan.Cryptolocker.I
August 2014	Crypto	Synolocker	0.6 BTC (US $300)	Trojan.Synolocker
August 2014	Crypto	TorrentLocker	BTC (US $500)	Trojan.Cryptolocker.H
August 2014	Crypto	Zerolocker	BTC (US $300)	Trojan.Ransomcrypt.N
July 2014	Crypto	KeyBTC	BTC (US $190)	Trojan.Rnsomcrypt.L

July 2014	Crypto	CTB/Onion /Critroni	0.5 BTC (US $320)	Trojan.Cryptolocker.G
July 2014	Crypto	Simplocker Android English	Money Pak (US $300)	Android.Simplocker.B
June 2014	Locker	Department of Justice (DOJ)	Money Pak (US $300)	Trojan.Ransomlock.AL
June 2014	Crypto	Simplocker Android Russian	MoneXy (US $21)	Andorid.Simplocker
June 2014	Crypto	Casinomtgot		Trojan.Ransomcrypt.K
June 2014	Crypto	Cryptolocker (Copying name)		Trojan.Cryptolocker.F
June 2014	Crypto	PoshCoder		Trojan.Ransomcrypt.J
May 2014	Locker	Koler Android	MoneyPak (US $300)	Android.Lockdroid.G
May 2014	Crypto	BitCrypt V 2.0		Trojan.Ransomcrpt.I
April 2014	Locker	Kovter	MoneyPak (US $300)	Trojan.Ransomlock.AK
April 2014	Crypto	Cryptolocker (Copying name)	0.6 BTC (US $300)	Trojan.Cryptolocker.E
March 2014	Crypto	TorLocker	0.1 BTC (US $100)	Trojan.Ransomcrypt.H
March 2014	Crypto	Cryptodefense/Cryptowall	BTC (US $500)	Trojan.Cryptodefense
March 2014	Crypto	OMG		Trojan.Ransomcrypt.G
January2014	Crypto	Cryptobit	BTC (US $500)	Trojan.Naymaim.B
December2013	Crypto	Cryptolocker 2.0		Trojan.Cryptolocker.B
September 2013	Locker	QQ Coins		Trojan.Ransomlock.AI
September 2013	Crypto	Cryptolocker	1 BTC (US $500)	Trojan.Cryptolocker
August 2013	Crypto	Power Loader		Trojan.Ransomcrypt.E
August 2013	Locker	Contact QQ		Trojan.Ransomlock.AF
July 2013	Cryptor	Dirty Alert		Trojan.Ransomcrypt.D
May 2013	Cryptor	MBL Advisory		Trojan.Ransomcrypt.C
March 2013	Cryptor	ACCDFISA		Trojan.Ransomcrypt.B

Resources

Cryptolocker: A Thriving Menace
http://www.symantec.com/connect/blogs/ransomcrypt-thriving-menace

Recovering Ransomlocked Files Using Built-In Windows Tools
http://www.symantec.com/connect/articles/recovering-ransomlocked-files-using-built-windows-tools

Cryptolocker Q&A: Menace of the Year
http://www.symantec.com/connect/blogs/cryptolocker-qa-menace-year

Ransomware – A Growing Menace (Video)
http://www.symantec.com/tv/products/details.jsp?vid=1954285164001

Ransomware – A Growing Menace (Blog)
http://www.symantec.com/connect/blogs/ransomware-growing-menace

Ransomware: Extorting Money by Panic and Pressure
http://www.symantec.com/connect/blogs/ransomware-extorting-money-panic-and-pressure

Cryptolocker Alert: Millions in the UK Targeted in Mass Spam Campaign
http://www.symantec.com/connect/blogs/cryptolocker-alert-millions-uk-targeted-mass-spam-campaign

SymHelp tool (Symantec Power Eraser)
SymHelp tool (Symantec Power Eraser)

Norton Power Eraser
https://security.symantec.com/nbrt/npe.aspx

Trojan.Ransomlock
http://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99

Trojan.Cryptolocker
http://www.symantec.com/security_response/writeup.jsp?docid=2013-091122-3112-99

Trojan.Cryptodefense
http://www.symantec.com/security_response/writeup.jsp?docid=2014-032622-1552-99

Android.Simplocker
http://www.symantec.com/security_response/writeup.jsp?docid=2014-060610-5533-99

Trojan.Synolocker

http://www.symantec.com/security_response/writeup.jsp?docid=2014-080708-1950-99

Authors

Kevin Savage
Princ Threat Analysis Engineer

Peter Coogan
Princ Security Response Manager

Hon Lau
Mgr, Development

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/social/.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.