TOP 10 RANSOMWARES

SECURITY PLAN FOR IDENTIFICATION PROTECTION AND DEFENSE FROM RANSOMWARES

Prepared by: (TEAM G)

ANUSHKKA DHAMIJA
SHLOK SHARMA
MD HAMID MURTUZA
SHRUTIKA SONI
SAURABH CHAUHAN
MUGILAN ELUMALAI

REPORT 1

MILESTONE : REQUIREMENT GATHERING

This report contains the internet findings of the brief intro of the attacks

OVERVIEW

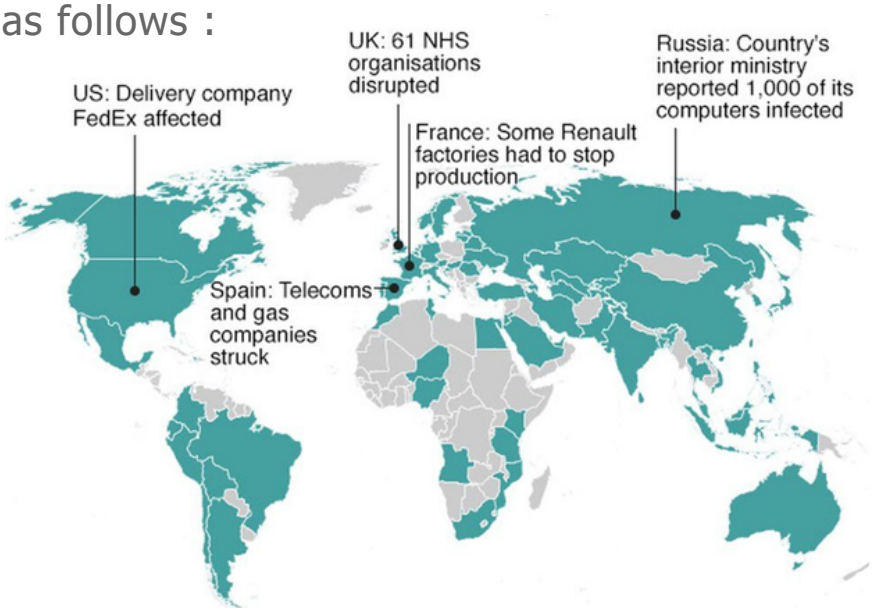
DEFINTION

Ransomware is a dangerous type of malware and viruses, and ransomware attacks are, unfortunately, on the rise now. These attacks cause significant financial losses and reputational damage

FREQUENTLY ATTACKED PLACES AND OPERATING SYSTEMS

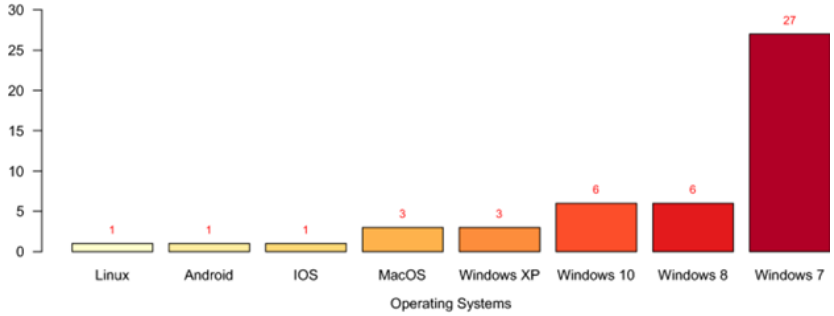
When it comes to ransomware statistics, attackers have been targeting North America, Asia and Europe more or less equally. North America is in the first position with about 33% of attacks. As for the number of ransomware attacks in different countries, the ranking presented in the State of Ransomware 2020 (BlackFog) is as follows :

1. USA
2. UK
3. Australia
4. Canada
5. Germany
6. Denmark
7. Japan
8. France



As for ransomware statistics of the most attacked operating systems, in the same Ransomware e-Statistics blog post, the figures are:

Windows – 85%
macOS – 7%
iOS – 7%
Android – 5%



Identifying ransomware – a basic distinction must be made

In particular, two types of ransomware are very popular:

Crypto ransomware

The aim of crypto ransomware is to encrypt your important data, such as documents, pictures and videos, but not to interfere with basic computer functions. This spreads panic because users can see their files but cannot access them. Crypto developers often add a countdown to their ransom demand: "If you don't pay the ransom by the deadline, all your files will be deleted." and due to the number of users who are unaware of the need for backups in the cloud or on external physical storage devices, crypto ransomware can have a devastating impact. Consequently, many victims pay the ransom simply to get their files back.

Locker ransomware

This type of malware blocks basic computer functions. For example, you may be denied access to the desktop, while the mouse and keyboard are partially disabled. This allows you to continue to interact with the window containing the ransom demand in order to make the payment. Apart from that, the computer is inoperable. But there is good news: Locker malware doesn't usually target critical files; it generally just wants to lock you out. Complete destruction of your data is therefore unlikely.

WHY THEY MAKE UP THE TOP 10 RANSOMWARES:

due to following features the TOP 10 RANSOMWARES are:

1. WANNA CRY
2. GOLDEN EYE
3. BAD RABBIT
4. LOCKY
5. RYUK
6. PETYA
7. NOT PETYA
8. GANDCRAB
9. SHADE/TROLDESH
10. B0R0NTOK

Locky

Locky is ransomware that was first used for an attack in 2016 by a group of organized hackers. Locky encrypted more than 160 file types and was spread by means of fake emails with infected attachments. Users fell for the email trick and installed the ransomware on their computers. This method of spreading is called phishing, and is a form of what is known as social engineering. Locky ransomware targets file types that are often used by designers, developers, engineers and testers.

WannaCry

WannaCry was a ransomware attack that spread to over 150 countries in 2017. It was designed to exploit a security vulnerability in Windows that was created by the NSA and leaked by the Shadow Brokers hacker group. WannaCry affected 230,000 computers worldwide. The attack hit one-third of all NHS hospitals in the UK, causing estimated damages of 92 million pounds. Users were locked out and a ransom payable in Bitcoin was demanded. The attack exposed the issue of outdated systems, because the hacker exploited an operating system vulnerability for which a patch had long existed at the time of the attack. The worldwide financial damage caused by WannaCry was approximately US$4 billion.

Bad Rabbit

Bad Rabbit was a ransomware attack from 2017 that spread via so-called drive-by attacks. Insecure websites were used to carry out the attacks. In a drive-by ransomware attack, a user visits a real website, unaware that it has been compromised by hackers. For most drive-by attacks, all that is required is for a user to call up a page that has been compromised in this way. In this case, however, running an installer that contained disguised malware led to the infection. This is called a malware dropper. Bad Rabbit asked the user to run a fake Adobe Flash installation, thereby infecting the computer with malware.

Ryuk

Ryuk is an encryption Trojan that spread in August 2018 and disabled the recovery function of Windows operating systems. This made it impossible to restore the encrypted data without an external backup. Ryuk also encrypted network hard disks. The impact was huge, and many of the US organizations that were targeted paid the ransom sums demanded. The total damage is estimated at over $640,000.

Shade/Troldesh

The Shade or Troldesh ransomware attack took place in 2015 and spread via spam emails containing infected links or file attachments. Interestingly, the Troldesh attackers communicated directly with their victims via email. Victims with whom they had built up a "good relationship" received discounts. However, this kind of behavior is an exception rather than the rule.

Petya & Not petya

Petya (not to be confused with ExPetr) is a ransomware attack that occurred in 2016 and was resurrected as GoldenEye in 2017. Instead of encrypting certain files, this malicious ransomware encrypted the victim's entire hard disk. This was done by encrypting the Master File Table (MFT), which made it impossible to access files on the hard disk. Petya ransomware spread to corporate HR departments via a fake application that contained an infected Dropbox link.

Another variant of Petya is Petya 2.0, which differs in some key aspects. In terms of how the attack is carried out, however, both are equally fatal for the device.

GoldenEye

The resurrection of Petya as GoldenEye resulted in a worldwide ransomware infection in 2017. GoldenEye, known as WannaCry's "deadly sibling," hit more than 2,000 targets – including prominent oil producers in Russia and several banks. In an alarming turn of events, GoldenEye forced the personnel of the Chernobyl nuclear power plant to manually check the radiation level there, after they were locked out of their Windows computers.

GandCrab

GandCrab is unsavory ransomware that threatened to disclose the porn habits of its victims. It claimed that it had hacked the victim's webcam and demanded a ransom. If the ransom wasn't paid, embarrassing footage of the victim would be published online. After its first appearance in 2018, GandCrab ransomware continued to develop in various versions. As part of the "No More Ransom" initiative, security providers and police agencies developed a ransomware decryption tool to help victims recover their sensitive data from GandCrab.

B0r0nt0k

B0r0nt0k is crypto ransomware that focuses specifically on Windows and Linux-based servers. This harmful ransomware encrypts the files of a Linux server and attaches a ".rontok" file extension. The malware not only poses a threat to files, it also makes changes to startup settings, disables functions and applications, and adds registry entries, files and programs.

WannaCry

DATE OF ATTACK : 12TH MAY 2017

DURATION : 4 DAYS

ATTACK ORIGIN : Pyongyang, North Korea

AFFECTED PLACES : WORLDWIDE

RANSOM DEMANDED : $300–600 USD (Via Bitcoin)

CAUSE : WannaCry worm

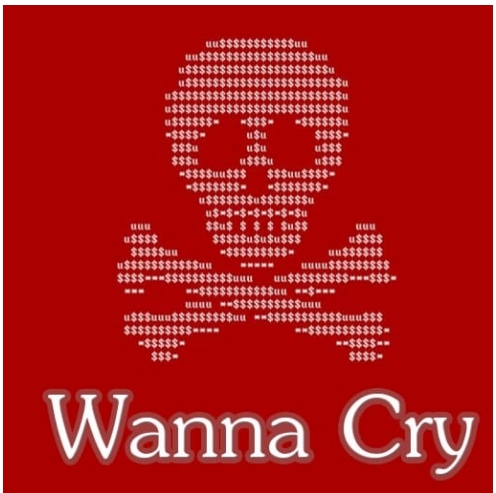
ABOUT THE ATTACK:

One of the most devastating ransomware attacks in history in terms of loss volume was caused by WannaCry, launched in 2017. The estimated value at the time was USD 4 billion in losses. The amount required to release each machine was around USD 300.

WannaCry spread via email scams, or phishing. Worldwide, more than 200 thousand people and companies were affected, such as, for example, FedEx, Telefonica, Nissan and Renault. WannaCry exploits a vulnerability in Windows. By the way, even today there are phishing emails claiming that you were infected by WannaCry, demanding ransom payment. But they’re plain emails, with no files. Pay attention!

SUSPECTED CYBER CRIMINALS : Lazarus Group

OUTCOME : 200,000 victims
300,000+ computers infected
The four most affected countries were Russia, Ukraine, India and Taiwan



GoldenEye

DATE OF ATTACK : June 27, 2017

DURATION : ------

ATTACK ORIGIN : Russia

AFFECTED PLACES : EUROPE

RANSOM DEMANDED : $3.5K USD ($3,500)

CAUSE : Telebots, Black energy (spread via SMB (Server Message Block))

ABOUT THE ATTACK:
The resurrection of Petya as GoldenEye resulted in a worldwide ransomware infection in 2017. GoldenEye, known as WannaCry's "deadly sibling," hit more than 2,000 targets – including prominent oil producers in Russia and several banks. In an alarming turn of events, GoldenEye forced the personnel of the Chernobyl nuclear power plant to manually check the radiation level there, after they were locked out of their Windows computers

SUSPECTED CYBER CRIMINALS : -------

OUTCOME :
the new GoldenEye variant has two layers of encryption—one that individually encrypts target files on the computer and another one that encrypts NTFS (New Technology File System—a proprietary file system of Microsoft) structures, according to Botezatu.
Just like Petya, GoldenEye encrypts the entire hard disk drive and denies the user access to the computer.

Bad Rabbit

DATE OF ATTACK : 24TH OCTOBER 2017

DURATION : 40 HOURS

ATTACK ORIGIN : Unidentified

AFFECTED PLACES :
Most of the targets are located in Russia. Similar but fewer attacks have also been seen in other countries – Ukraine, Turkey and Germany. Overall, there are almost 200 targets, according to the KSN statistics

RANSOM DEMANDED : 0.05 bitcoin, or about $275

CAUSE :
Drive-by attacks by compromising vulnerable websites from the stolen Petya kernel

ABOUT THE ATTACK:
Bad Rabbit is a strain of ransomware that first appeared in 2017 and is a suspected variant of Petya. Victims could be exposed to the virus simply by visiting a malicious or compromised website. The malware is embedded into websites using JavaScript injected into the site's HTML code. If a person clicks on the malicious installer, BadRabbit ransomware encrypts files and presents users with an austere black-and-red message. It reads in part: "If you see this text, your files are no longer accessible. You might have been looking for a way to recover your files. Don't waste your time. Victims reported that making the payment did unlock their files, though this isn't always the case in other ransomware attacks.

SUSPECTED CYBER CRIMINALS : Unidentified

OUTCOME :
Appeared to target media companiesspread by posing as an Adobe Flash media player update, persuading victims to click and open a malicious file.

LOCKY

DATE OF ATTACK : 16 FEB 2016

DURATION : Multiple Time

ATTACK ORIGIN : Unidentified

AFFECTED PLACES : Los Angeles

RANSOM DEMANDED : between 0.5 and 1 bitcoin

CAUSE : PHISHING MAIL , TROJAN

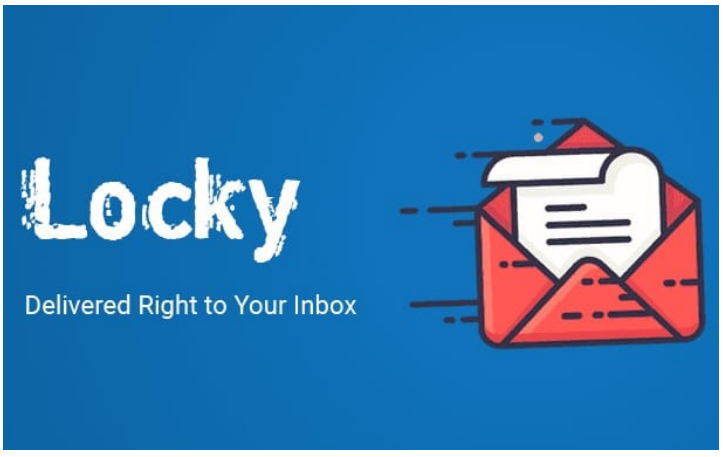
ABOUT THE ATTACK:

Locky is ransomware that was first used for an attack in 2016 by a group of organized hackers. Locky encrypted more than 160 file types and was spread by means of fake emails with infected attachments. Users fell for the email trick and installed the ransomware on their computers. This method of spreading is called phishing, and is a form of what is known as social engineering. Locky ransomware targets file types that are often used by designers, developers, engineers and testers

SUSPECTED CYBER CRIMINALS : NECURS

OUTCOME :

Sent to about a half-million users Filenames are converted to a unique 16 letter and number combination. Initially, only the .locky file extension was used for these encrypted files. Subsequently, other file extensions have been used, including .zepto, .odin, .aesir, .thor, and .zzzzz. After encryption, a message (displayed on the user's desktop) instructs them to download the Tor browser and visit a specific criminal-operated Web site for further information. It locks your computer



RYUK

DATE OF ATTACK : AUG 2018

DURATION : Multiple Attacks between 2018 and 2019

ATTACK ORIGIN : North Korean and Russian(Wizard Spider or Grim Spider)

AFFECTED PLACES :
Los Angeles , Paris , California , New York ,Germany , Florida (medical and school systems)

RANSOM DEMANDED :
$61 million (between 15 and 50 Bitcoins, or roughly between $100,000 and $500,000)

CAUSE : Emotet or TrickBot

ABOUT THE ATTACK:
Ryuk is ransomware version attributed to the hacker group WIZARD SPIDER that has compromised governments, academia, healthcare, manufacturing, and technology organizations.
Ryuk, pronounced ree-yook, is a family of ransomware that first appeared in mid-to-late 2018. In December 2018, the New York Times reported that Tribune Publishing had been infected by Ryuk, disrupting printing in San Diego and Florida.
The New York Times and the Wall Street Journal shared a printing facility in Los Angeles. They were also impacted by the attack, w hich caused distribution issues for the Saturday editions of the new spapers.

SUSPECTED CYBER CRIMINALS : NECURS

OUTCOME :
Targeting large, public-entity Microsoft Windows cybersystems

PETYA & NOT PETYA

Petya malware with the June 2017 attack unleashed a new variant, called Not-Petya due to changes in the malware's behavior. They use different keys for encryption & have unique reboot styles & displays & notes but both are equally as destructive.

DATE OF ATTACK : MARCH 2016 (PETYA)

DURATION : 2017 was followed by it's new varient NOT PETYA

ATTACK ORIGIN : ------

AFFECTED PLACES : globally specially UKRAINE, france, germany, italy, poland

RANSOM DEMANDED :
$61 million (between 15 & 50 Bitcoins, or roughly between $100,000 and $500,000)

CAUSE : Trojan horse/ crypto-virus (external blue exploit via email attachments)

ABOUT THE ATTACK:
The Petya ransomware attack on June 27, 2017 (which we analyzed in-depth in this blog) may have been perceived as an outbreak worse than last month's WannaCrypt (also known as WannaCry) attack. Petya was discovered in March 2016 by security researchers who noted that although the malware achieved fewer infections than other currently active strains, the virus was still unique in its operation, alerting many in the industry to keep a watchful eye on the advanced attack.

SUSPECTED CYBER CRIMINALS : TADEM hackers

OUTCOME :
White House assessment pegged the total damages brought about by NotPetya to more than $10 billion, the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline. Ukrainian ministries, banks and metro systems were also affected

DATE OF ATTACK : JUNE 27, 2017 (NOT PETYA)

DURATION : 4 year war

ATTACK ORIGIN : Russia

AFFECTED PLACES : globally specially UKRAINE, Europe, UK

RANSOM DEMANDED: $10 billion (lump sum)

CAUSE : modified petya versions(external blue & mimikatz)- sandworm

ABOUT THE ATTACK:

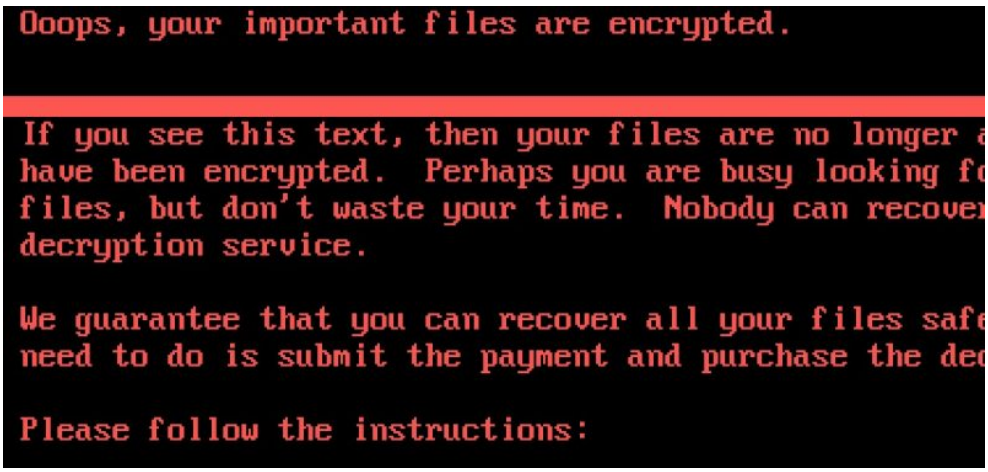
Tanother Petya variant emerged that contained an additional capability to be used if the virus could not gain administrator access to a machine. The updated capabilities of the new variant have some security professionals naming the virus NotPetya. NotPetya has been in the news a lately for being yet another ransomware attack that has spread like fire – affecting organizations in several verticals across 65+ countries, drawing comparisons with the WannaCry attack that recently hit over 200,000 machines globally. The ransom collection as of this writing is just over $10,000. Additionally, the email address used in the ransom request have since been shut down. NotPetya infects the master boot record (MBR) and prevents any system from booting. And even paying the ransom would not have recovered the machine! In that sense, it is also different from the 2016 Petya threat in that the damage from NotPetya is not reversible.

SUSPECTED CYBER CRIMINALS : ------

OUTCOME : WARLIKE

NotPetya wreaked havoc for some large companies, costing them billions of dollars in lost revenue, damaging computer systems, and requiring significant expense to restore global operations.

(1) NotPetya inflicted substantial economic damage on several companies, and (2) the US and UK governments attributed the NotPetya attack to the Russian military.



GandCrab

DATE OF ATTACK : MAY 31, 2019

DURATION : 10 MIN TIMER until ransom doubled

ATTACK ORIGIN : Russia/ Soviet Union

AFFECTED PLACES : globally specially UKRAINE, Europe, UK

RANSOM DEMANDED: $2 billion in illicit ransom

CAUSE : malvertizing (AIDS computer virus)

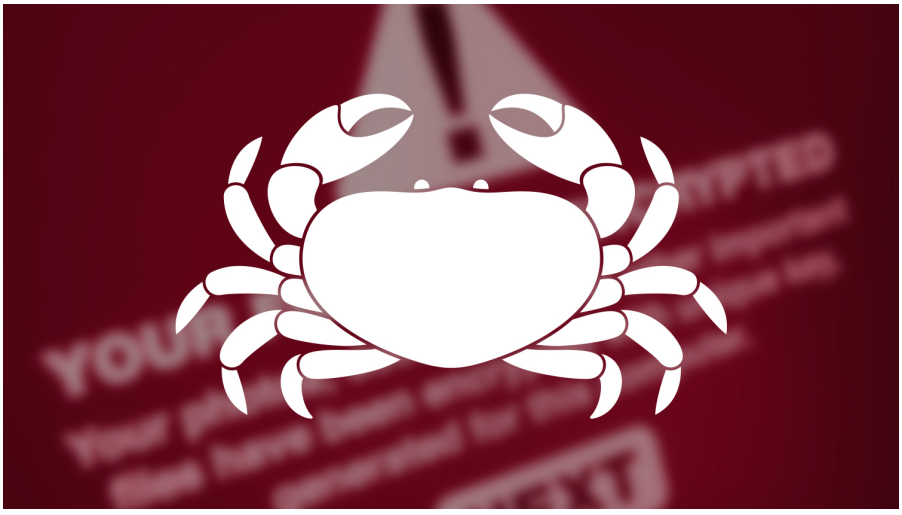
ABOUT THE ATTACK:

In the first half of 2019, GandCrab was the most popular ransomware used in large scale, untargeted attacks that use malicious websites or email attachments to infect as many victims as possible. Its creators peddled it to anyone who wanted to use it using the Ransomware-as-a-Service (RaaS) model, which netted them a percentage of each ransom it extorted. GandCrab operators choose the ransom they want to demand, typically somewhere between a few hundred to a few thousand dollars per computer. GandCrab follows an affiliate marketing business model, aka Ransomware-as-a-Service (RaaS), in which low-level cybercriminals do the heavy lifting of finding new victims while the threat authors are free to tinker with and improve their creation.

SUSPECTED CYBER CRIMINALS : ------

OUTCOME :

infected about 50,000 computers, most of them in Europe, asking each victim for ransoms. As of May 2019, cybercriminals behind GandCrab announced they were closing up shop and retiring after having allegedly earned more than $2 billion in extortion payments from victims



Shade/Troldesh

DATE OF ATTACK : 29 NOVEMBER, 2015

DURATION : Till 2019 when the attackers shutdown their shop

ATTACK ORIGIN : Russia

AFFECTED PLACES : global

RANSOM DEMANDED: 250 euros from each victim

CAUSE : encrypts a user's files with an ".xtbl" extension. Troldesh is spread initially via e-mail spam. (mexar - teamspy bot)

ABOUT THE ATTACK:

Troldesh is Malwarebytes detection name for a type of ransomware that is also known as Shade since 2014. It is likely to target victims especially from Russia and Ukraine. It is spread by malspam (malicious spam or spam email), typically in the form of attached .zip files. This uses a CMS on a compromised site to host downloads.

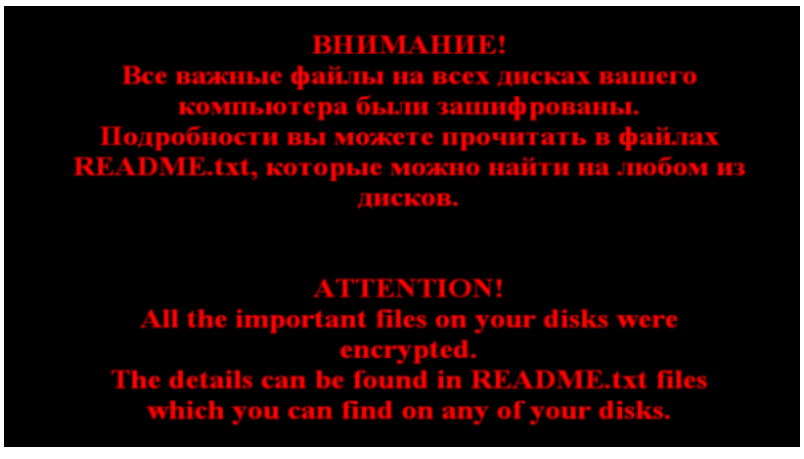
Attackers directly communicate with the victims

It adds different extensions to the encrypted files, depending on the version of the ransomware.

- .xbtl
- .cbtl
- .no_more_ransom
- .better_call_saul

OUTCOME :

Given the evidence found, it must be a cryptocurrency miner, used by the attackers to mine ZCash. This means that even if the victim pays the demanded ransom, attackers can still use the infected computer for cryptomining.



B0r0nt0k

DATE OF ATTACK : 25 FEBRUARY, 2019

DURATION : ------

ATTACK ORIGIN : Indonesia

AFFECTED PLACES : global

RANSOM DEMANDED: 20 BITCOINS

CAUSE : arrives as an attachment of e-mail named kangen.exe (kangen itself means "to miss someone/thing" TARGETS LINUX SERVERS

ABOUT THE ATTACK:

The B0r0nt0k Ransomware is a file encoder threat that emerged on February 25th, 2019 when site owners reported finding files with strange names and the 'rontok' extension. It is also known as Crypto Virus as it demands Crypto in return.
It has been putting Linux and possibly Windows Web servers at risk of encrypting all of the infected domain's files. It is encoded with base64 algorithm.
Attackers inject a small program that encrypted generic data containers along with some site configuration files.
.PNG, .PSD, .PSPIMAGE, .TGA, .THM, .TIF, .TIFF, .YUV, .AI, .EPS, .PS, .SVG
After injecting through the potential network, it encrypts victim's files and change their names adding the file extension. rontok and then it uses string encryption algorithm in order to deny the access to victim's files. After data being compromised, it delivers a Ransom note as a text file 'Read_Me.txt'.

OUTCOME :

cryptovirus like B0r0nt0k can disable security tools or other functions to keep running without interruption, warns 2-Spyware.com. The B0r0nt0k ransomware can alter more crucial parts of the computer if left untreated.

CONCLUSION

In conclusion ransomware attacks, has proved that their impact can be devastating to small business owners and organization. Ransomware is not only threats to small business and organization it has an impact on people as well. In its public service request report from the FBI,they urge anyone who's suffered a ransomware infection to never pay ransoms because it helps criminals refine their attacks and snare even more victims. The FBI says paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organizations are never provided with decryption keys after paying a ransom

Cybersecurity Ventures predicts global annual cybercrime costs will grow from $3 trillion in 2015 to $6 trillion by 2021, which includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

REFERENCES

https://searchsecurity.techtarget.com/definition/WannaCry-ransomware
https://www.irjet.net/archives/V7/i12/IRJET-V7I1266.pdf

https://www.coursehero.com/file/p2g9kc8/In-conclusion-ransomware-attacks-has-proved-that-their-impact-can-be/

https://secure.wphackedhelp.com/blog/b0r0nt0k-ransomware/

https://socprime.com/blog/security-advisory-bad-rabbit-ransomware-worm/

https://en.wikipedia.org/wiki/GoldenEye

https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/b0r0nt0k

https://blog.group-ib.com/troldesh

https://www.mimecast.com/content/locky-ransomware/

https://www.spiretech.com/blog/2016/08/rise-in-ransomware-attacks/

https://www.trendmicro.com/en_in/what-is/ransomware/ryuk-ransomware.html

https://success.trendmicro.com/solution/1114310-best-practice-configuration-against-ransomware-and-other-malware-threats-with-endpoint-application-c

https://portswigger.net/

https://www.itpro.co.uk/malware/34381/what-is-notpetya

https://thehackernews.com/?m=1

https://www.proofpoint.com/us/threat-reference/petya

THANK YOU