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 2

MILESTONE : ATTACK FLOW

This report contains the ATTACK FLOWS of the top 10 ransomwares

What is an Attack Flow?

Malwares hide themselves deep inside infected to carry out their mission. Ransomware is a special type of malware which announces its presence to the user the moment it finishes its activity.

There is a particular flow in which any malware infect the machine i.e. infection and distribution vectors (this may include a phishing mail with a malicious download link or an RDP i.e. the stolen login credentials) followed by data encryption (which includes accessing file with an attacker controlled key and replacing the original one) which thereby leads to the economically disastrous step called Ransom Demand (which consist of ransom notes demanding a set amount of cryptocurrency in exchange for victim files).

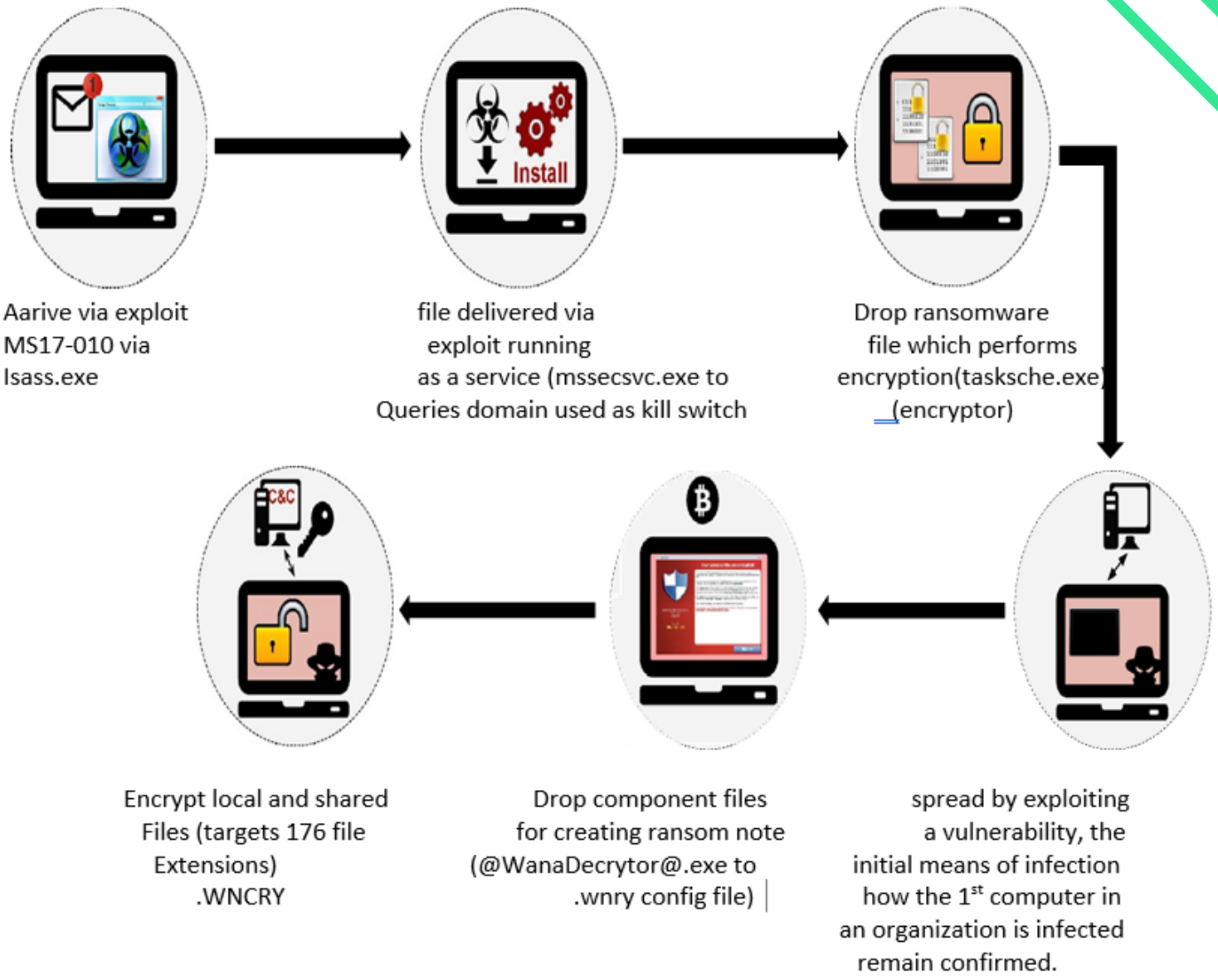
Decryption is a post attack procedure which is done via a descriptor program provided by the cyber criminal which is used as a private key to restore the access to users files once the ransom is paid

Attack Flow of WannaCry

WannaCry is a ransomware cryptoworm cyber attack that targets computers running the Microsoft Windows operating system. It was initially released on 12 May 2017. The ransomware encrypted data and demanded ransom of $300 to $600, paid in the cryptocurrency Bitcoin. WannaCry is also known as WannaCrypt, WCry, Wana Decrypt0r 2.0, WanaCrypt0r 2.0 and Wanna Decryptor.Once installed, WannaCry installed a backdoor in infected systems.WannaCry exploited a known vulnerability in older Windows systems called EternalBlue, which was found by the United States National Security Agency (NSA).EternalBlue was stolen and leaked by a group called The Shadow Brokers a few months prior to the attack. While EternalBlue was quickly patched, much of WannaCry's success was due to organizations not patching or using older Windows systems.Quick patching and the discovery of kill switch domains prevented infected computers from spreading WannaCry. That said, estimates from Europol peg the number of computers infected at more than 200,000 across 150 countries with damages ranging from hundreds of millions to billions of dollars.

Security experts, the United States, United Kingdom, Canada, Japan, New Zealand and Australia formally asserted that North Korea was behind the attack. In August 2018, a new variant of WannaCry forced Taiwan Semiconductor, a chip-fabrication company, to shut down several of its plants when the virus spread to 10,000 machines across its most advanced facilities.

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system called **ETERNAL BLUE** in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step 1:-
This ransomware attack is arrived via exploits shown in the attack flow .Microsoft word document that runs infectious macros MS 17-010 via lsass.exe and spread to other devices.

Step 2:-
As file delivered via exploit running as a service then entered mssecsvc.exe and queries domain used as kill switch. This is a simple social engineering technique to used as bait to trick the user and pass on the infection

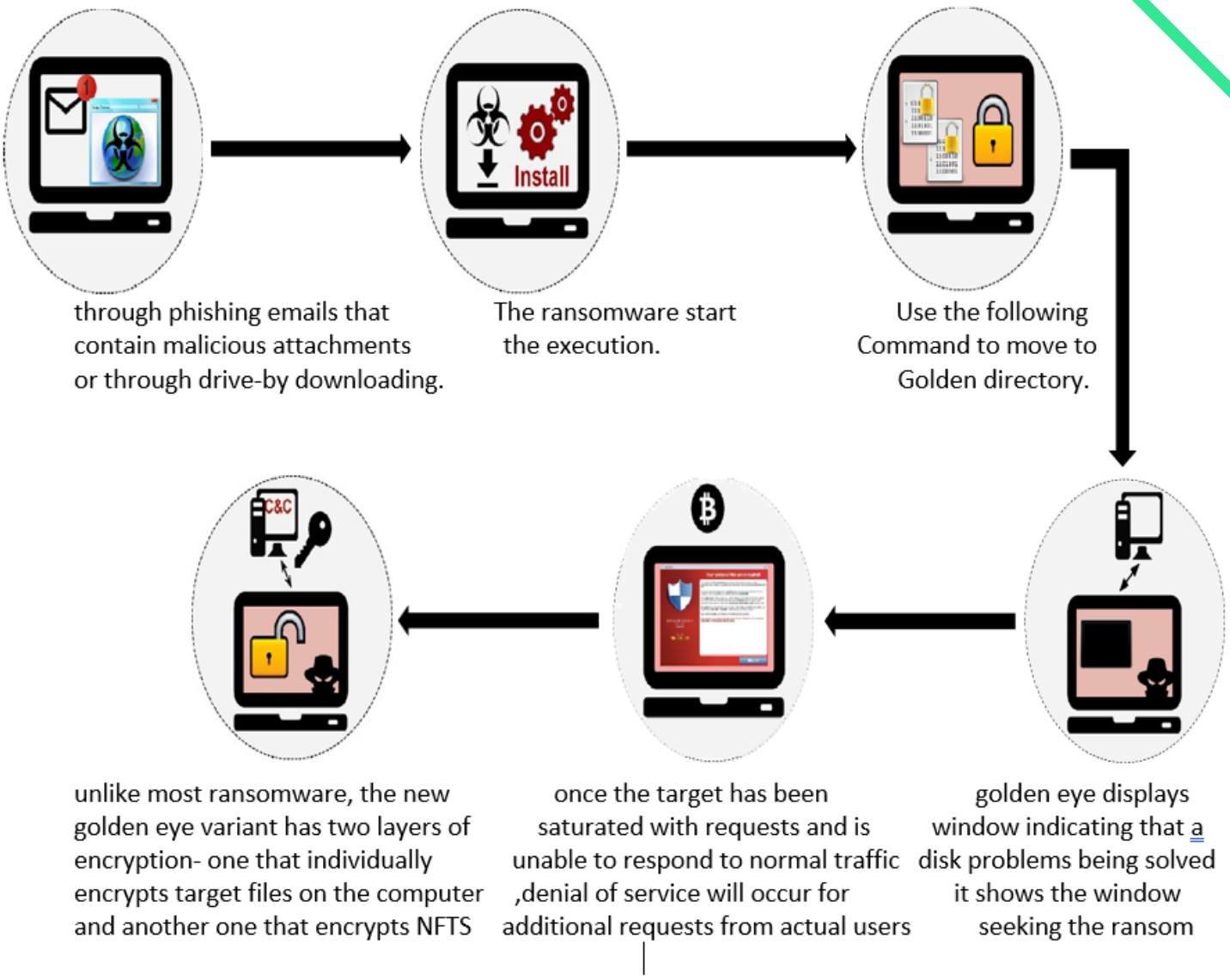
Step 3:-
Drop ransomware file which perform encryption is tracksache.exe(encrypt-or). When the computer gets infected, you would typically see a ransom note displayed either as a desktop wallpaper or a text file.

Step 4:-
Encrypt local and shared file and drop files about ransomware .Communicate with your users immediately to ensure that they are aware of the risk of this particular attack as well as being resistant to phishing attacks in general.

Attack Flow of Golden_Eye

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.

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step 1:-
In addition to encrypting files on the computer, this ransomware family is characterized by encrypting the MBR when it has permissions, thus blocking full access to the computer.

Step 2:-
When it runs, it encrypts certain files on compromised system drives. In turn, if it has administrator permissions, it also encrypts the system boot sector by preventing access to the computer unless an access key that decrypts the system is entered.

Step 3:-
That key is assumed to be delivered once payment of the ransom has been made.
The sample creates a scheduled task to shut down the computer afterwards.

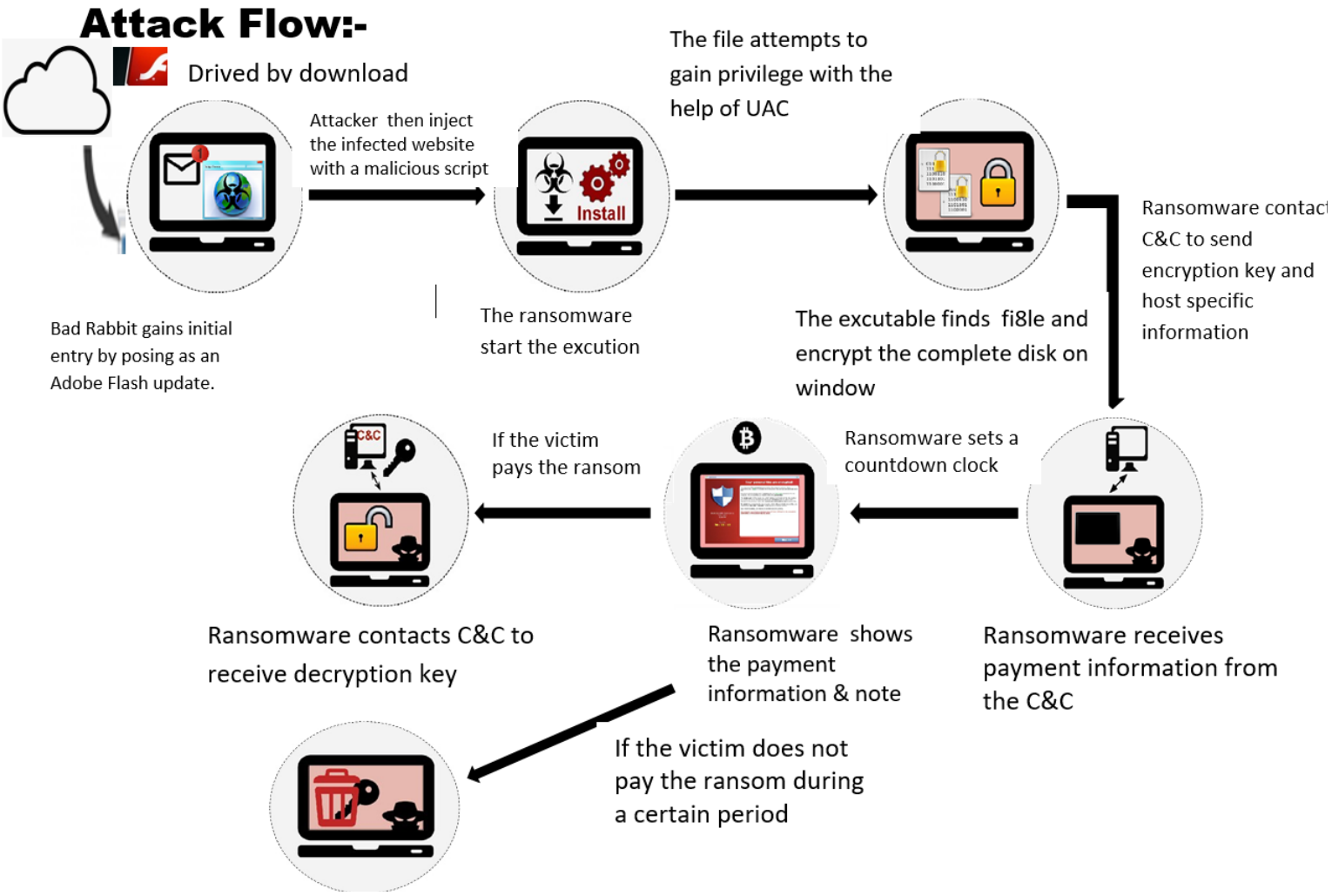
Step 4:-
Upon restarting the computer, GoldenEye displays a fake window indicating that a disk problem is being solved.

Attack Flow of Bad_Rabbit

Bad Rabbit is a strain of ransomware that first appeared in 2017 and is a suspected variant of Petya. Like other strains of ransomware, Bad Rabbit virus infects locks up victims' computers, servers, or files prevents them from regaining access until a ransom—usually in Bitcoin—is paid.

Like other strains of ransomware, Bad Rabbit virus locks up victims' computers, servers, or files prevents them from regaining access until a ransom—usually in Bitcoin—is paid.

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step – 1: Bad Rabbit gains initial entry by posing as an Adobe Flash update. Once inside a network it spreads by harvesting credentials with the Mimikatz tool as well as using hard coded credentials.
The attackers infect popular websites with a prime objective to attack their visitors with the help of a watering hole attack.
Step – 2: The attackers then inject the infected websites with a malicious script. This script prompts the visitors to download a fake Adobe Flash Installer Update. Once a user manually allows the browser for downloading the update, a file named install_flash_player.exe gets downloaded on the computer system of the visitor.
Step – 3: Once the downloaded file is executed manually by the user (i.e. the visitor), the ransomware starts the execution. It spreads onto the local network after infecting the target system. After the .exe file is executed on the target system, a chain of events takes place –

1. The file attempts to gain privilege with the help of standard User Access Control (UAC) prompt.
2. Once privileges are acquired, a file named infpub.dat is created under C:\Windows.
3. C:\Windows/infpub.dat is executed using rundll32 and it adds a file named dispci.exe in the same folder. This file is derived from DiskCryptor, an opensource tool for encrypting the complete disks on Windows. Apart from encrypting the data, this executable file also modifies the bootloader.
4. It overwrites MBR and installs its own bootloader. A restart is scheduled after rewriting process is completed.
5. Once the target system reboots, it displays the ransom note to the user by preventing the operating system from booting.

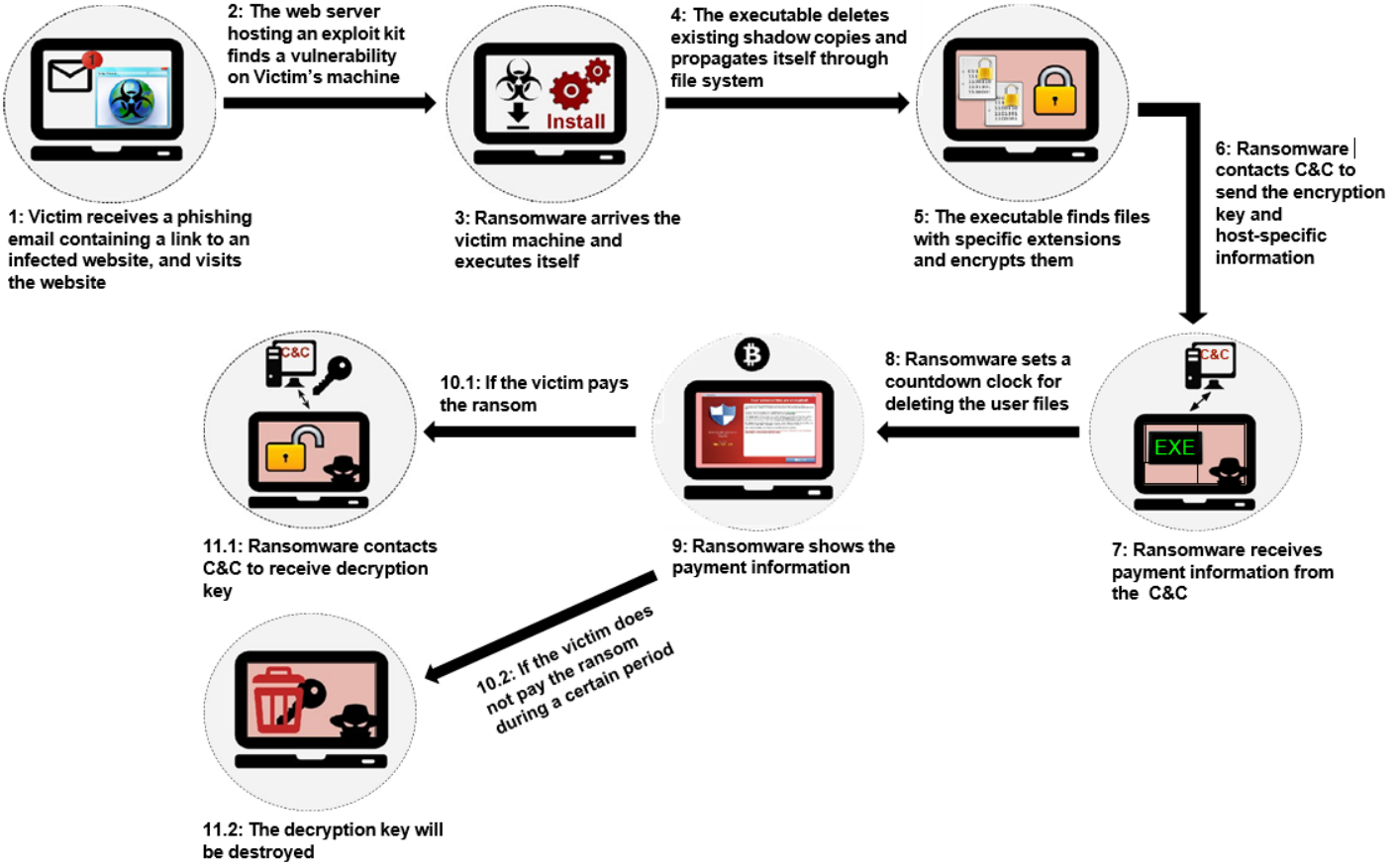
Step – 4: Once a target system is infected, the ransomware tries to spread to other systems in the network by using Server Message Block (SMB). To spread across the network, it uses Mimikatz, an open-source tool for extracting Windows passwords in plaintext and changing privileges. Along with Mimikatz, the malware also features a hardcoded list of commonly used credentials. This list of credentials is used to perform various attacks such as a dictionary attack to get access to the devices connected to the network i.e. lateral movement in the local network.

Attack Flow of 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

Flow Chart of Attack Flow

ATTACK FLOW :-



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step 1:- the malware authors deliver this ransomware through email asking for payment through an attached invoice of a malicious Microsoft Word document that runs infectious macros.

Step 2:- The document when opened by the user would not be in a readable format and a dialog box opens with a phrase “Enable macro if data encoding is incorrect.” This is a simple social engineering technique to used as bait to trick the user and pass on the infection.

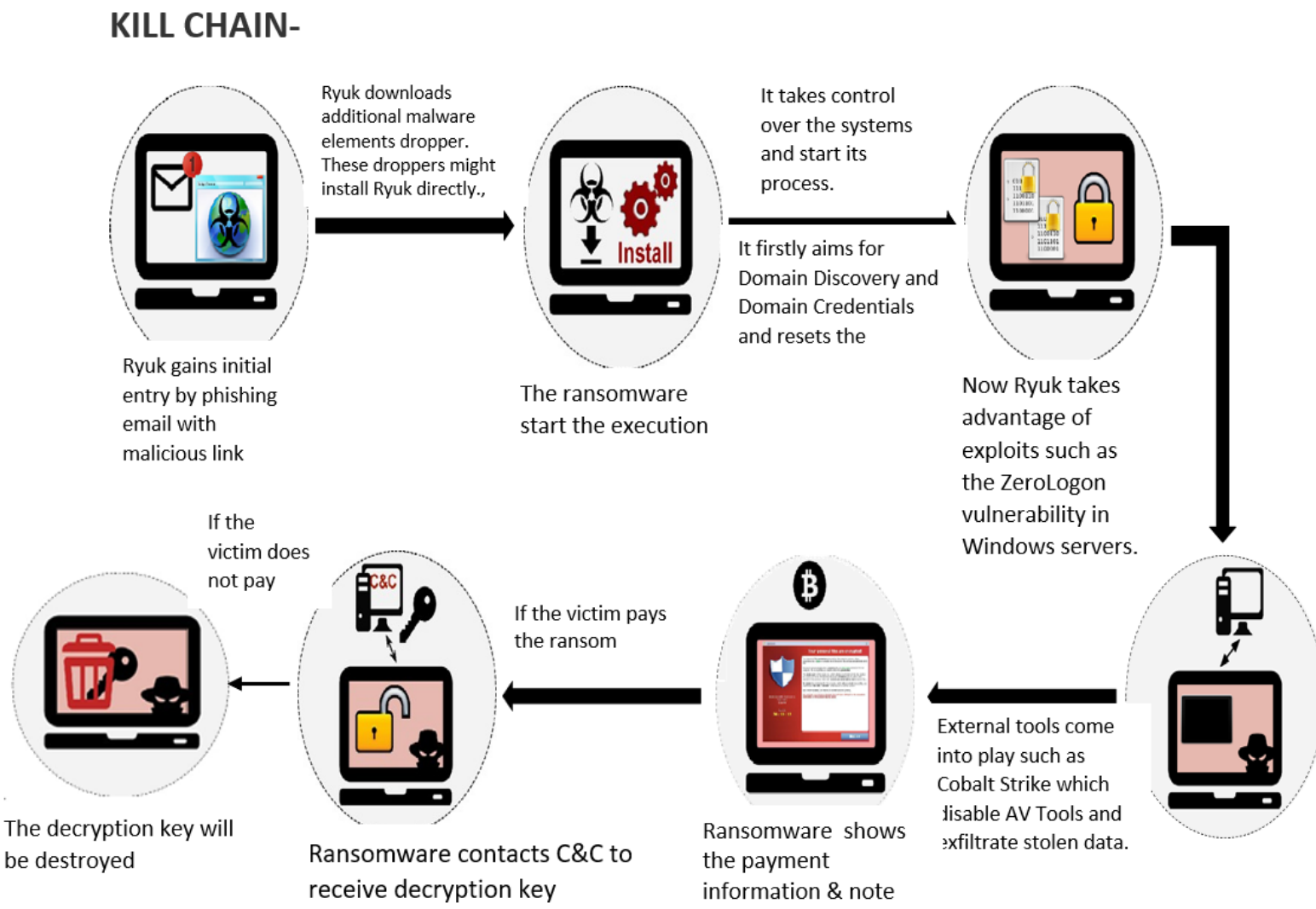
Step 3:- When the user enables the macros, the malware author runs a binary file which then installs the encryption trojan that locks all the files that have specific extensions. Later the filenames are changed to a combination of letters and numbers

Step 4 :- Once the files are encrypted, the malware demands to download the tor browser and enter a specific website which is actually malicious. It also demands to pay a ransom to unlock the encrypted file.When the computer gets infected, you would typically see a ransom note displayed either as a desktop wallpaper or a text file, just as seen on the picture below

Attack Flow of RYUK

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.

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step1- Ryuk can use download as a service (DaaS) to infect targeted systems. DaaS is a service one hacker offers to another. If a hacker develops ransomware but doesn't know how to distribute it, other hackers with those skills help distribute it.

Step2- Often, unwitting users fall prey to phishing attacks that facilitate the initial infection. AdvIntel reports that 91% of attacks begin with phishing emails. It is extremely important to train users to spot phishing emails. Training dramatically reduces the chance of infection.

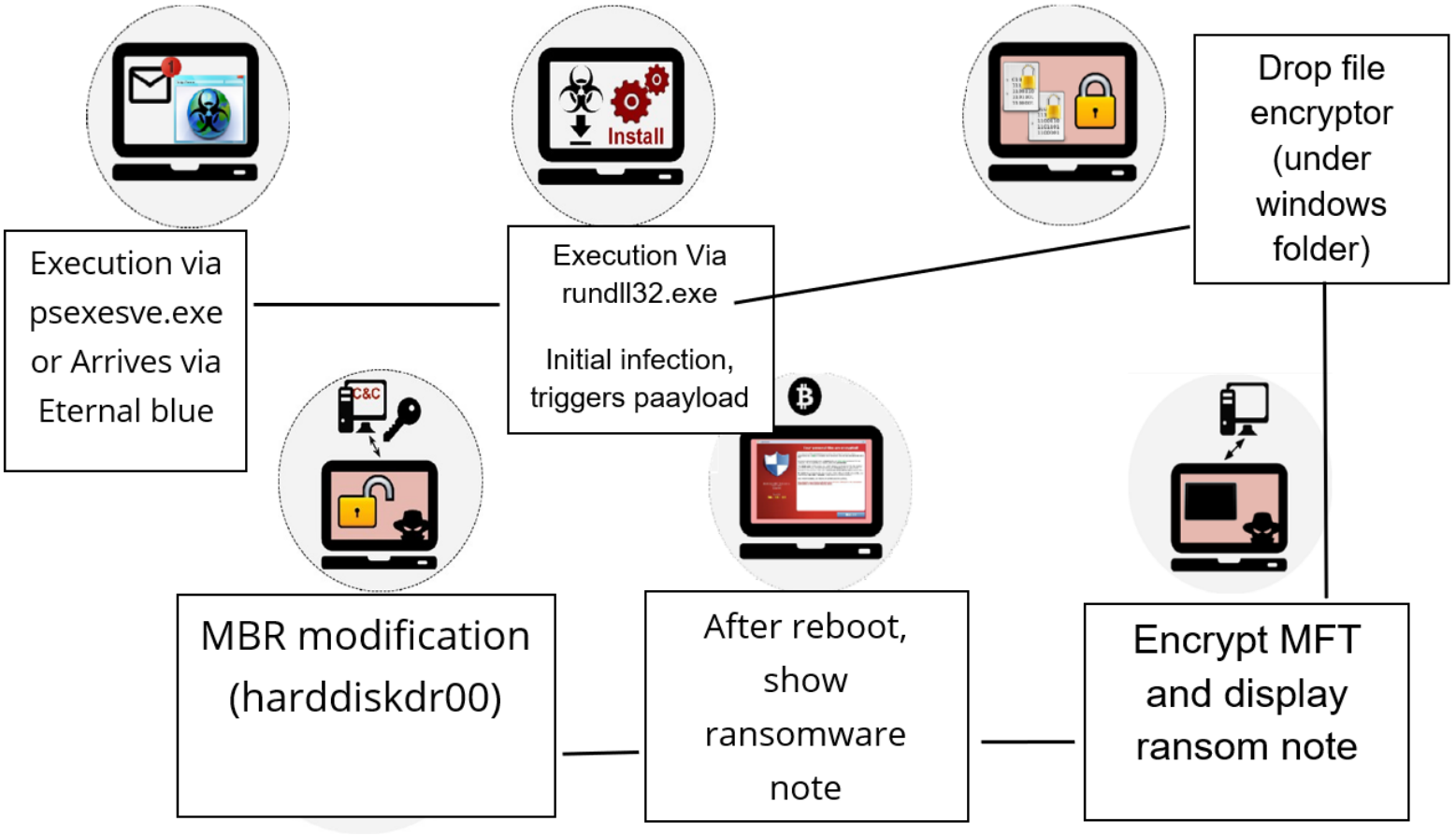
Step3- Once the user clicks on the phishing email, Ryuk downloads additional malware elements called droppers. The additional malware includes Trickbot, Zloader, BazarBackdoor, and others. These droppers might install Ryuk directly.

Step4- They could also install another piece of malware such as Cobalt Strike Beacon to communicate with a command and control (C2) network. Ryuk downloads once the malware is installed. Ryuk has also taken advantage of exploits such as the ZeroLogon vulnerability in Windows servers.

Attack Flow of PETYA

Petya is a family of encrypting malware that was first discovered in 2016. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system. The Petya malware had infected millions of people during its first year of its release. Like other strains of ransomware, Bad Rabbit virus locks up victims' computers, servers, or files prevents them from regaining access until a ransom—usually in Bitcoin—is paid

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step 1:
“MBR Overwrite” – Overwrite the hard-drive’s Master Boot Record and implanting custom boot-loader. After querying for the system drive name (for example “\\.\PhysicalDrive1”), the MBR is identified by directly using the DeviceIOControl code API IOCTL_DISK_GET_PARTITION_INFO_EX.
The overwriting operations are only performed for partitions returning the values PARTITION_STYLE_MBR or PARTITION_STYLE_GPT

Step 2:
loaded by the bootstrap code implanted in Stage 0. Its first operation is to try and locate the ONION_SECTOR structure so it can verify that Stage 0 was successfully completed. If this check returns a positive value, Petya begins enumerating the drive’s Master File Table (MFT) records, while masquerading as a legitimate file repair application. Petya uses an encryption method called SALSA20, which is where its second and more serious encryption flaw resides.
The original SALSA20 implementation uses a 32-byte encryption key and an 8-byte initialization vector to produce the final 512-bit key-stream
boots and displays the scary skull logo seen below. After the victim presses any key, the ransom note containing instructions for payment and decryption is displayed.

Steps of Attack Flow Continued

Step 3:
Specifically, Petya will check the avp.exe , NS.exe, ccSvcHst.exe
If avp.exe is found running, Petya will proceed with both MBR overwriting and file encryption. However, after rebooting the infected machine, it will not perform MFT encryption. In this case, if the user has somehow managed to back up their MBR, they can theoretically restore the system since the MFT was not encrypted. Despite this, the affected files will still be encrypted If the processes NS.exe or ccSvcHst.exe are found running, Petya will refrain from propagating using the SMB exploits EternalBlue and EternalRomance. The ransomware will still attempt to spread via other methods.

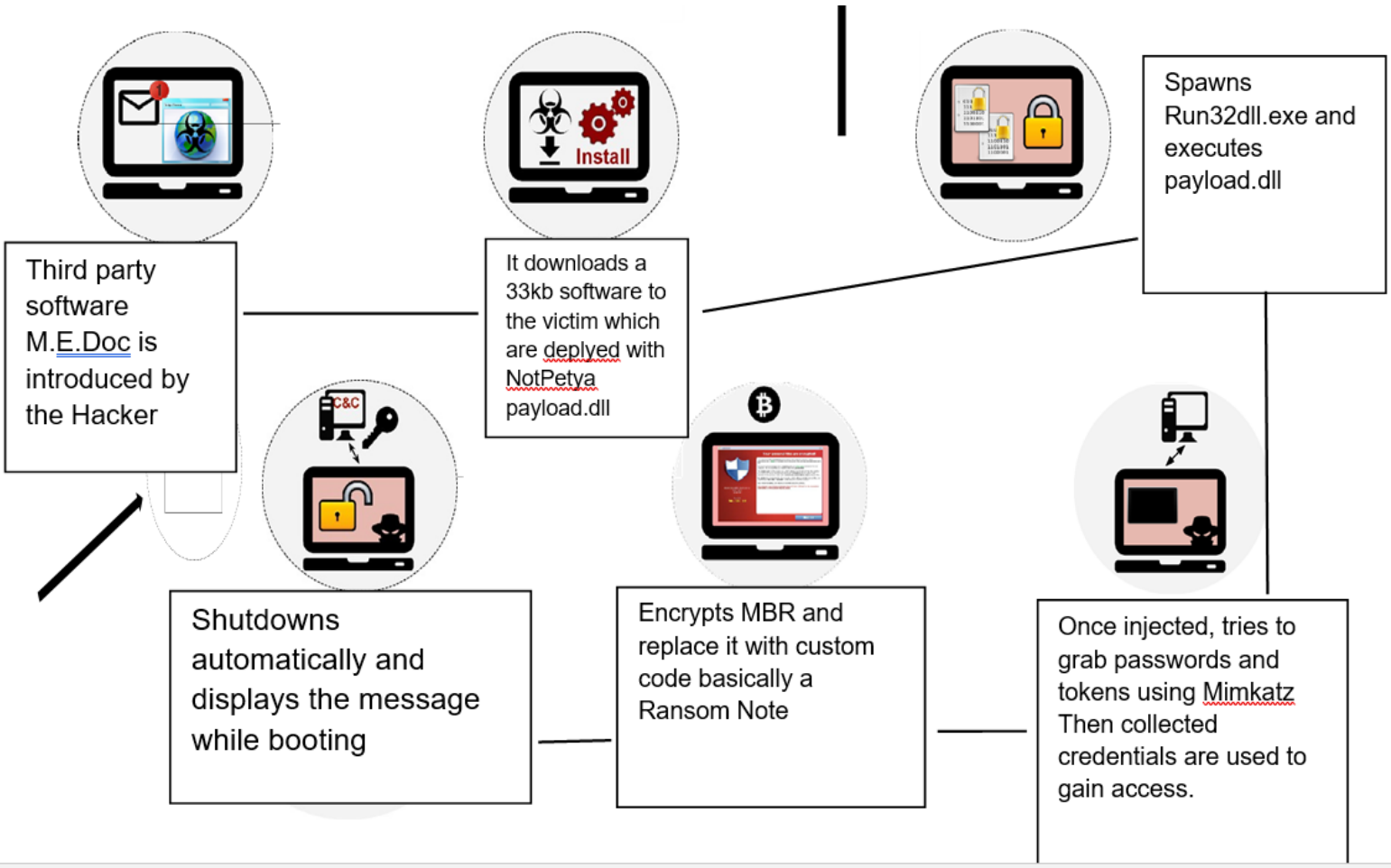
Step 4:
Then adds a scheduled task that reboots the system after at least an hour. Meanwhile, the Master Boot Record (MBR) is also modified so that the MFT encryption routine will display the ransom note upon reboot. A fake CHKDSK notice is initially displayed; this is when the MFT encryption happens.

Step 5:
This is Petya's most straight-forward stage. After MBR and MFT encryption is complete, the computer boots and displays the scary skull logo seen below. After the victim presses any key, the ransom note containing instructions for payment and decryption is displayed.

Attack Flow of NOT_PETYA

In June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine. Kaspersky Lab referred to this new version as Not Petya to distinguish it from the 2016 variants, due to these differences in operation. In addition, although it purports to be ransomware, this variant was modified so that it is unable to actually revert its own changes. The Not Petya attacks have been blamed on the Russian government, specifically the Sandworm hacking group within the GRU Russian military intelligence organization, by security researchers, Google, and severalgovernments.

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step 1:
Once Petya is dropped, it will drop psexec.exe as dllhost.dat on the target machine. The malware also drops a copy of itself to \\{remote machine name}\admin$\{malware filename}. It then executes the dropped copy by using dllhost.dat locally (which is the file name of the PSExec tool) with the following parameters:dllhost.dat \\{remote machine name} -accepteula -s -d C:\Windows\System32\rundll32 "C:\Windows\{malware filename}",#1 {randomnumber minimum 10} {enumerated credentials}

Step 2:
Petya variant uses an advanced method to extract information from the infected system. It makes use of a customised Mimikatz—a legitimate security tool—to extract usernames and passwords. The 32-bit and 64-bitMimikatz executables are encrypted and stored in the resource section of the ransomware.

Step 3:
This Petya variant is dropped into a system as perfc.dat, after which it uses the rundll32.exe process to run and carry out its file encryption routine. Unusually for ransomware, it does not change the extensions of any encrypted files. It targets more than 60+ file extensions to encrypt; it is worth noting that the file types it targets are typically used in enterprise settings; images and video files, which are usually targeted by other ransomware, are notablyabsent.

Steps of Attack Flow Continued

Step 4:
Specifically, Petya will check if the following processes are running:
•avp.exe
•NS.exe
•ccSvcHst.exe

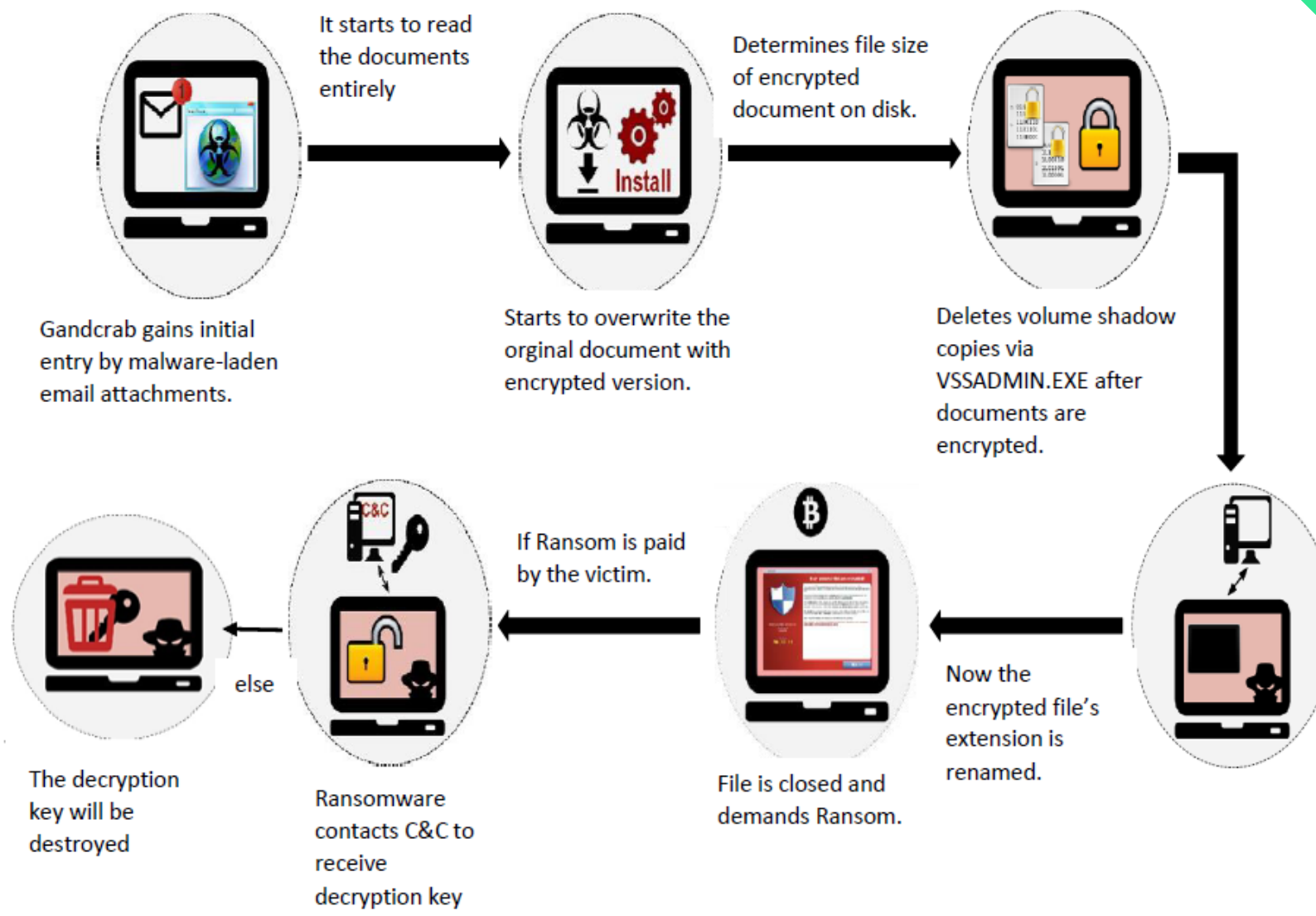
If avp.exe is found running, Petya will proceed with both MBR overwriting and file encryption. However, after rebooting the infected machine, it will not perform MFT encryption. In this case, if the user has somehow managed to back up their MBR, they can theoretically restore the system since the MFT was not encrypted. Despite this, the affected files will still be encrypted.If the processes NS.exe or ccSvcHst.exe are found running, Petya will refrain from propagating using the SMB exploits EternalBlue and EternalRomance. The ransomware will still attempt to spread via other methods.

Step 5:
Then adds a scheduled task that reboots the system after at least an hour. Meanwhile, the Master Boot Record (MBR) is also modified so that the MFT encryption routine will display the ransom note upon reboot. A fake CHKDSK notice is initially displayed; this is when the MFT encryption happens.

Attack Flow of GAND_CRAB

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.

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step1- GandCrab gains initial entry by malware-laden email attachments. It starts to read the documents entirely.

Step2- It Starts to overwrite the original document with encrypted version. Determines file size of encrypted document on disk.

Step3- Deletes volume shadow copies via VSSADMIN.EXE after documents are encrypted.

Step4- Now the encrypted file's extension is renamed. File is closed and demands Ransom.

Step5-If Ransom is paid by the victim, Ransomware contacts C&C to receive decryption key, and if ransom is not paid the decryption key will be destroyed.

Attack Flow of SHADE/TROLDESH

Shade or Troldesh is Malwarebytes detection name for a type of ransomware that is also known as Shade. It is thought to be of Russian origin and has been around since 2014. The Shade Ransomware has been in operation since around 2014 and they likely to target victims especially from Russia and Ukraine.

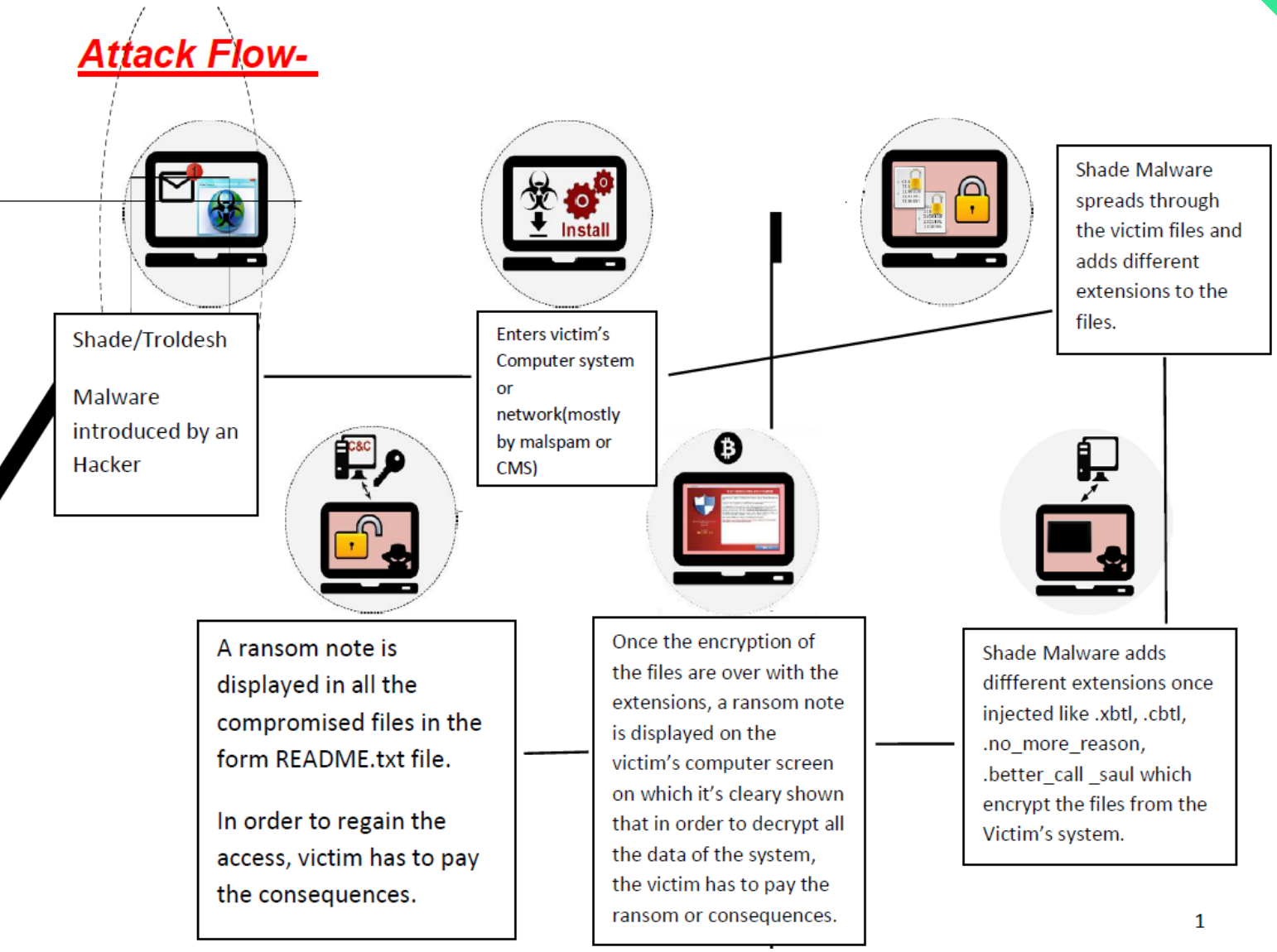
Troldesh or Shade malware is spread by malspam(malicious spam or spam email), typically in the form of attached .zip files. This ransomware sometimes uses a CMS on a compromised site to host downloads.

Troldesh/Shade adds different extensions to the encrypted files, depending on the version of the ransomware.

Some of the extensions are as follows-

- .xbtl
- .cbtl
- .no more reason

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step 1- Shade is introduced by an Hacker to a victim mostly in the form of Mailcious or spam mail which are mostly zip files.

Step 2- Once the Victim is baited, Shade enters the Victim's system and hence resulting in adding different extensions in the system files such as .cbtl, .xbtl, .no more reason and .better call saul.

Step 3- These extensions encrypt the data and other valuable information from the Victim's computer system hence making almost impossible to access the data.

Step 4- Here the files are compromised and encrypted using AEC 256 in CBC(Block Cipher) mode. All the data is now in hands of the Hacker hence forcing Victim to pay the Ransom.

Step 5- A ransom note is presented in all the files of the computer system in the form of Read Me.txt. Here all the details for the payment and stuff are displayed.

Step 6- Once the ransom is payed, the Victim will have the green flag to regain all the access of the it's computer system.

Attack Flow of B0R0NT0K

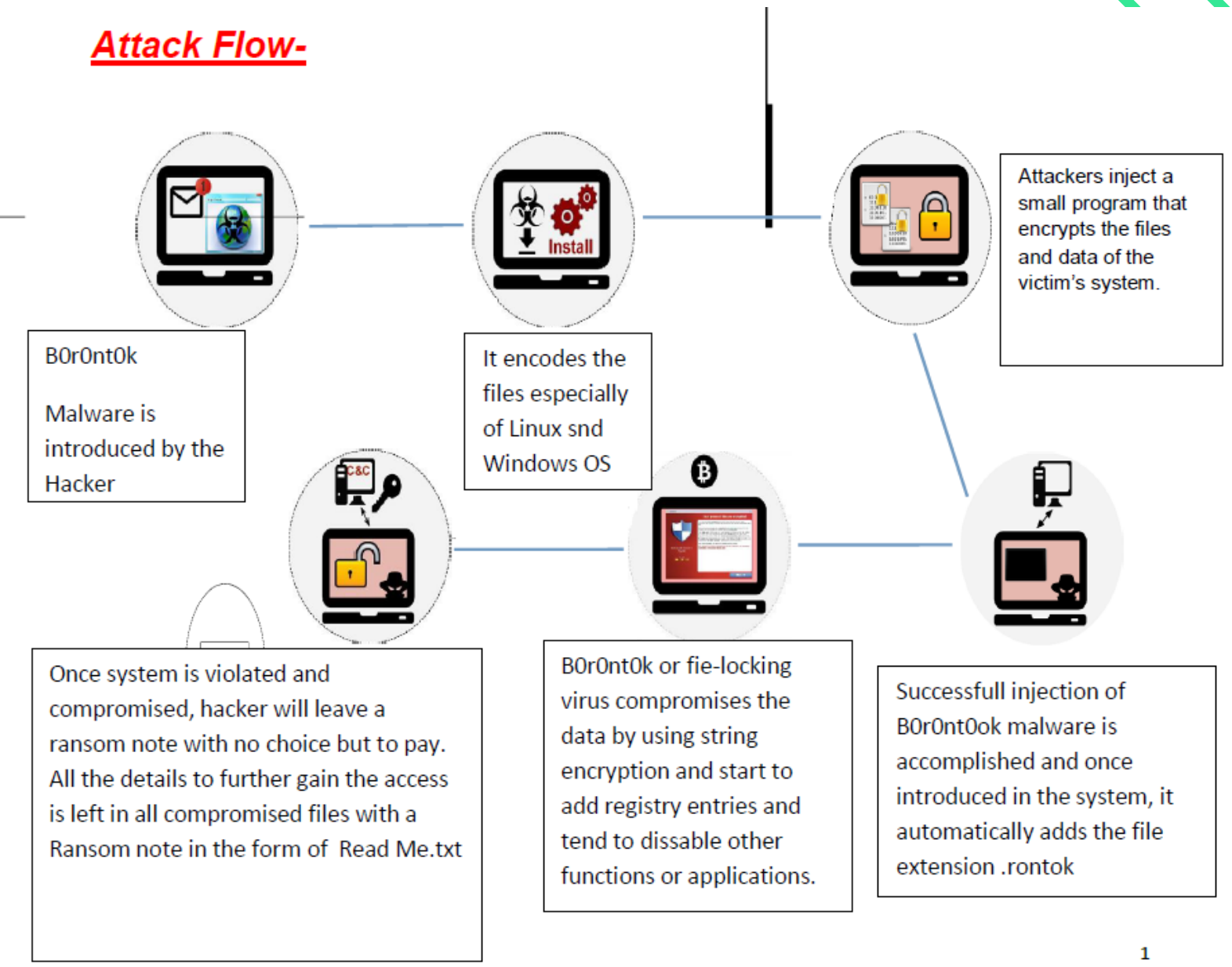
The B0r0nt0k Ransomware is a file encoder threat that emerged on February 25th, 2019 when site owners reported finding files with strange names and the '.rontok' extension. It is also known as CryptoVirus as it demands Crypto in return.

B0r0nt0K 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.

Here, Attackers inject a small program that encrypted generic data containers along with some site configuration files.

After injecting through the potential network, it encrypts victim's files and change their names adding the file extension .rontok and then B0r0nt0k 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'.

Flow Chart of Attack Flow



The above attack flow shows the exploitation of an operating system in the form of a flow chart which creates a map of the malware spread . The users don't have to activate the infected file in order to avoid the further spreading. This representation explains the specific vulnerabilities in the backend system and the detailed steps are given below.

Detailed Steps of Attack Flow

Step 1- B0r0nt0k malware is introduced by the Hacker to the Victim's system in order to gain access particularly of Linux servers.

Step 2- Once the malware is injected in the Victim's system, it harms and breaches the Linux servers and hence resulting in gaining access of the files to the Hacker.

Step 3- This type of malware once introduced, starts to expand itself and hence resulting in creating an harmful extension i.e .rontok. This extension then encrypts the file and compromises all the data of Victim's system.

Step 4- Now the data being compromised, Victim has to suffer and pay for the consequences. In order to regain the access of the system, Victim will pay the ransom to the Hacker.

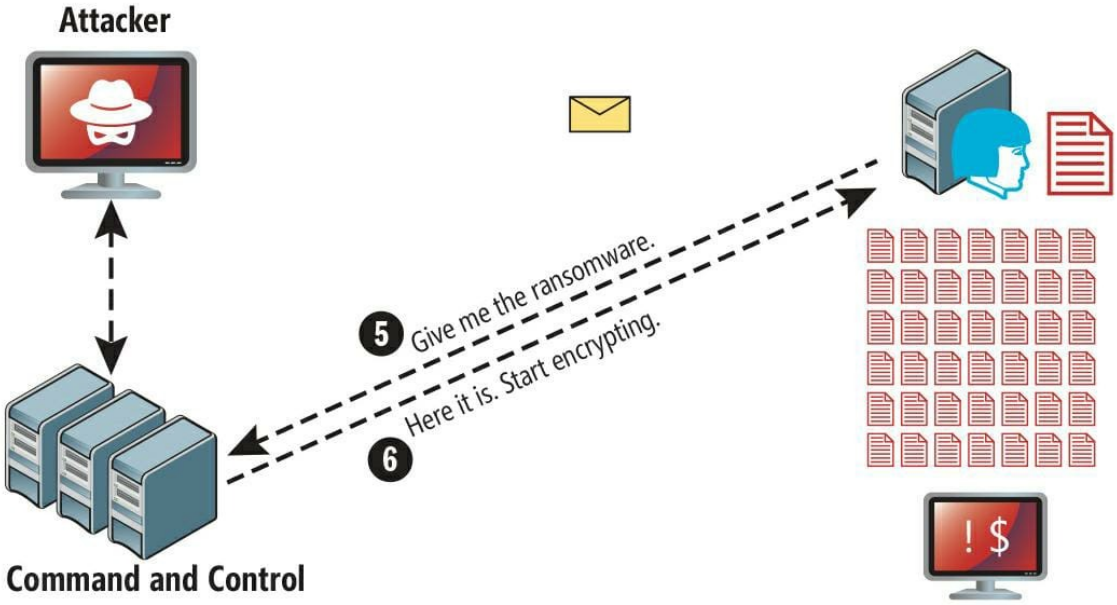
Step 5- All the details for the Ransom and other messages are present in all the files by the name
Read Me.txt. Once the Victim opens the file, it shall receive all the instructions for the payment.

Step 6- This ransomware or Crypto Virus mostly demand the ransom in the way of Bitcoins. Being a crypto currency, Victim is forced to pay the Hacker in Bitcoins in order to regain the access or full control of the system back.

CONCLUSION

There are various ways that an attacker can plant Ransomware on a victims machine or systems, the 2 most common methods of ransomware attack is through phishing emails and fraudulent websites. An attack can either be to a specific target or distributed randomly distributed to different users.

Ransomware has quickly become the most prominent and visible type of malware. Recent ransomware attacks have impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations.



REFERENCES

https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

WANNA_CRY

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

GOLDEN_EYE

https://kb.mazebolt.com/knowledgebase/goldeneye-http-flood/

BAD_RABBIT

https://www.elastic.co/blog/badrabbit-technical-analysis
https://lifars.com/wp-content/uploads/2017/12/Bad-Rabbit-Ransomware-Guide.pdf
https://www.proofpoint.com/us/threat-reference/bad-rabbit

LOCKY

https://heimdalsecurity.com/blog/locky-ransomware-101/
https://enterprise.comodo.com/blog/what-is-locky-ransomware/

RYUK

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

PETYA

https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/petya.html
https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
Decrypting the Petya Ransomware | Check Point Blog

NON-PETYA

https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/petya.html
https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

GAND_CRAB

https://www.sophos.com/
https://www.vmray.com/cyber-security-blog/gandcrab-ransomware-evolution-analysis/

SHADE/TROLDESH

https://securityboulevard.com/2020/05/shade-troldesh-ransomware-decryption-tool/
https://blog.malwarebytes.com/detections/ransom-troldesh/

B0R0NT0K

https://secure.wphackedhelp.com/blog/b0r0nt0k-ransomware/
https://linuxinsider.com/story/b0r0nt0k-ransomware-threatens-linux-servers-85870.html

THANK YOU