TOP 10 RANSOMWARES

SECURITY PLAN FOR IDENTIFICATION PROTECTION AND DEFENSE FROM RANSOMWARES

Prepared by: (TEAM G)

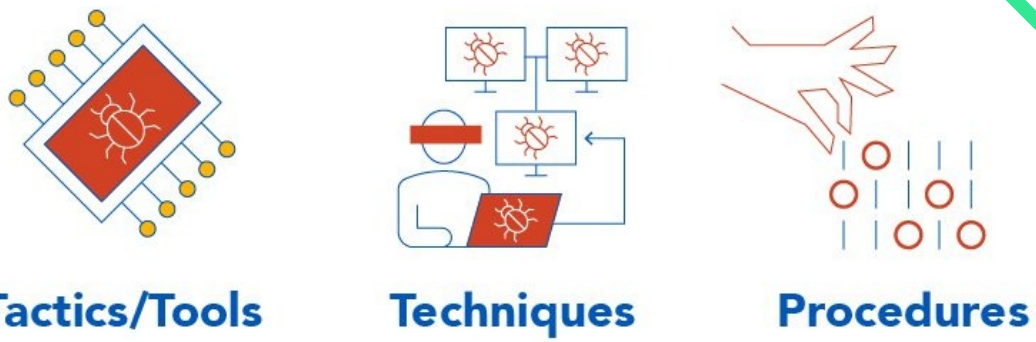
ANUSHKKA DHAMIJA
SHLOK SHARMA
MD HAMID MURTUZA
SHRUTIKA SONI
SAURABH CHAUHAN
MUGILAN ELUMALAI

REPORT 4

MILESTONE : TTPs of ATTACK

This report contains the TTPs used by the attacker in each attacker.

OVERVIEW



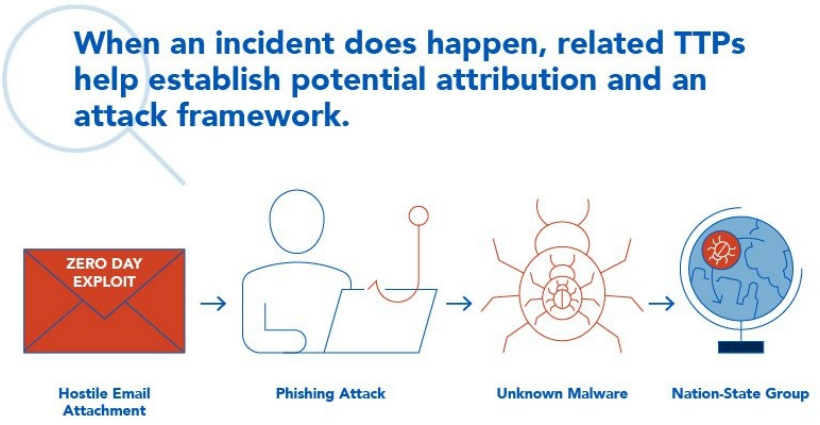
Whenever any cyber attack occurs the procedure is not as simple as seen by paying the ransom to the attackers and getting the decrypt key. Instead the attack infects the embedded system when the attacker uses the TTPs. Tactics, techniques and procedures (TTPs) are the "patterns of activities or methods associated with a specific threat actor or group of threat actors."

Analysis of TTPs aids in counterintelligence and security operations by describing how threat actors perform attacks.TTPs describe how threat actors (the bad guys) orchestrate, execute and manage their operations attacks. ("Tactics" is also sometimes called "tools" in the acronym.)

Specifically, TTPs are defined as the "patterns of activities or methods associated with a specific threat actor or group of threat actors,

DETAILS ABOUT TTPs

TTPs can significantly aid in contextualizing threats and fueling rapid research and response. Post-incident TTPs boost strategic research and response and, as such, are essential to the cyber threat intelligence process. Lessons learned, additional research into the campaign and related attack data all help mature an understanding of TTPs, allowing implementation of more proactive measures and controls for future attacks using those TTPs.



Some threat actors, for example, may use the same payload through multiple campaigns while others will drastically alter the main payload with each new operation. Understanding the TTPs of a particular threat actor helps endpoint security teams better harden against specific threats.

TTPs of WannaCry & GOLDEN-EYE

WANNACRY:

The WannaCry ransomware attack was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.[5] It propagated through EternalBlue, an exploit developed by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers at least a year prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. These patches are imperative to an organization's cyber-security but many were not applied because of needing 24/7 operation, risking having applications that used to work break, inconvenience, or other reasons.

GOLDEN_EYE :

The GoldenEye ransomware is a combination of two attack strategies. First, two viruses get downloaded together. These are called Mischa and Petya. Second, like all ransomware, these viruses encrypt data and then demand a payment to get the decryption key. An intermediate release, version 2.5, fix bugs in the ransomware. This was still running as Green Petya. As the fourth version of Petya, release 3.0, GoldenEye was the perfected system. GoldenEye launches both Mischa and Petya, with Mischa running first. So, this is a double encryption system. Marking the change from Green Petya, the livery of GoldenEye is yellow and black.

TTPs of WannaCry & GOLDEN-EYE

WORKING OF WANNACRY AND GOLDEN-EYE :

1.WannaCry contains a thread that will attempt to scan for new attached drives every few seconds. If one is identified, it will encrypt the files on the attached device
2. WannaCry scans its local network segment for remote systems to try to exploit and copy itself to.
3. WannaCry utilizes wmic to delete shadow copies.
4. We can see the DLL Injection is very easy to be exploited by an attacker. Attacker can also gain shell and escalate privileges using the method. We can also create reverse shell using msfvenom to take a step further

TTPs of WannaCry & GOLDEN-EYE

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	
	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting			Multilayer Encryption
Bootkit	DLL Injection					Service Execution		Scheduled Transfer	Peer Connections
Change Default File Association		Indicator Removal from Tools		Process Discovery	Shared Webroot	Windows Management Instrumentation			Remote File Copy
Component Firmware		Indicator Removal on Host		Query Registry	Taint Shared Content				Standard Application Layer Protocol
Hypervisor				Remote System Discovery	Windows Admin Shares				Standard Cryptographic Protocol
Logon Scripts		InstallUtil		Security Software Discovery					
Modify Existing Service		Masquerading		System Information Discovery					Standard Non-Application Layer Protocol
Redundant Access		Modify Registry							
Registry Run Keys / Start Folder		NTFS Extended Attributes		System Owner/User Discovery					Uncommonly Used Port
Security Support Provider		Obfuscated Files or Information		System Service Discovery					Web Service
Shortcut Modification		Process Hollowing							
Windows Management Instrumentation Event Subscription		Redundant Access							
		Regsvcs / Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

THIS IS FOR WANNACRY.

THIS IS FOR GOLDEN EYE.

THIS IS FOR BOTH WANNACRY AND GOLDENEYE.

TTPs of BAD-RABBIT and LOCKY

BADRABBIT:

Bad Rabbit first appeared in 2017 and has similarities to ransomware strains called WannaCry and Petya.
Disguised as an Adobe Flash installer, Bad Rabbit spreads through drive-by downloads on compromised websites, meaning 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."

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

TTPs of BAD-RABBIT and LOCKY

WORKING OF BADRABBIT:

- 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 then inject the infected websites with a malicious script. This script prompts the visitors to download a fake Adobe Flash Installer Update.
- 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.
- 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.

WORKING OF LOCKY :

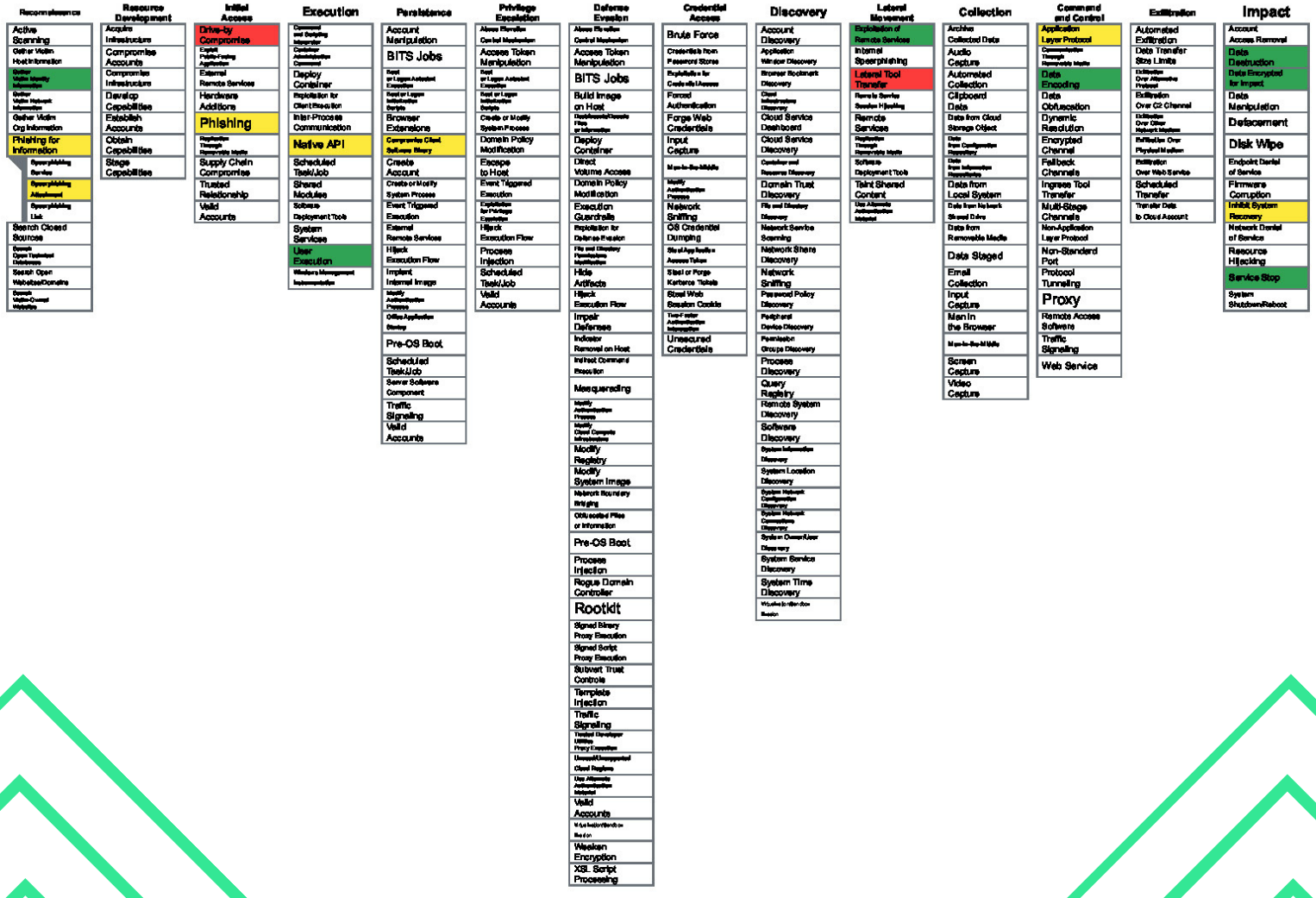
- The malware authors deliver this ransomware through email asking for payment through an attached invoice of a malicious Microsoft Word document that runs infectious macros.
- The document when opened by the user would not be in a readable format and a dialog box opens with a phrase “Enable macro if data encoding is incorrect.” This is a simple social engineering technique to used as bait to trick the user and pass on the infection.
- 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.
- 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.

TTPs of BAD-RABBIT and LOCKY

about
BAD RABBIT & LOCKY RANSOMWARE
BADRABBIT-RED,
LOCKY-YELLOW & COMMON-GREEN

domain
Enterprise
ATT&CK v9

platforms
Linux, macOS, Windows,
Azure AD, Office 365,
SaaS, IaaS, Google Workspace,
PRE, Network, Containers



TTPs of RYUK & GANDCRAB

GANDCRAB :

Gandcrab is a ransomware family that has been linked to the GOLD SOUTHFIELD group and operated as ransomware-as-a-service (RaaS) since at least April 2019. GandCrab is highly configurable and shares code similarities with the GandCrab RaaS.

RYUK :

Ryuk is a ransomware designed to target enterprise environments that has been used in attacks since at least 2018. It is similar to Hermes ransomware. It is a type of ransomware used in targeted attacks, where the threat actors make sure that essential files are encrypted so they can ask for large ransom amounts.

TTPs of RYUK & GANDCRAB

WORKING OF RYUK :

- GandCrab uses a lot of lists. It kills the process of some programs in order to correctly encrypt the data files they might have open.
- It of course has a target list of filetypes to encrypt, and files and paths to whitelist. It deletes the Volume Shadow Copy of the drives, and enumerates all mounted drive letters.
- The encryption takes a little time to complete, depending on how full the drive is. Free decryptor tools have been released for some versions of GandCrab, but the authors quickly update to another version, and the decryptor tools stop working.
- All the ransom notes include a GandCrab key you must provide if you meet their demand for payment.
- The business model for GandCrab gives the franchisee the option of choosing their ransom amount, among other features. Some victims report ransoms as low as $300 but they can run an order of magnitude higher.

WORKING OF RYUK :

- A typical Ryuk attack begins when a user opens a weaponized
- Microsoft Office document attached to a phishing email.
- Opening the document causes a malicious macro to execute a PowerShell command that attempts to download the banking Trojan Emotet.
- This further leads to additional malware download - executing a spyware payload (Trickbot).
- Then, the admin credentials and other details are collected, allowing attackers to move laterally to critical assets connected to the network.
- The attack chain concludes when the attackers execute Ryuk on each of these assets.

Ryuk has the ability to identify and encrypt network drives and resources, as well as delete shadow copies on the endpoint. This means the attackers can then disable Windows System Restore for users, making it impossible to recover from an attack without external backups or rollback technology.

TTPs of RYUK & GANDCRAB

About-

RYUK-VS-GANDCRAB

domain
Enterprise ATT&CK v9

platforms
Linux, macOS, Windows, Azure AD, Office 365, SaaS, IaaS, Google Workspace, PRE, Network, Containers

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Lognon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command-and-Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	Multilayer Encryption
Bootkit	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting			
Change Default File Association	DLL Injection	Indicator Removal from Tools		Process Discovery	Shared Webroot	Service Execution		Scheduled Transfer	Peer Connections
Component Firmware		Indicator Removal on Host		Query Registry	Taint Shared Content	Windows Management Instrumentation			Remote File Copy
Hypervisor				Remote System Discovery	Windows Admin Shares				Standard Application Layer Protocol
Logon Scripts		InstallUtil		Security Software Discovery					Standard Cryptographic Protocol
Modify Existing Service		Masquerading		System Information Discovery					Standard Non-Application Layer Protocol
Redundant Access		Modify Registry							
Registry Run Keys / Start Folder		NTFS Extended Attributes		System Owner/User Discovery					Uncommonly Used Port
Security Support Provider		Obfuscated Files or Information		System Service Discovery					Web Service
Shortcut Modification		Process Hollowing							
Windows Management Instrumentation Event Subscription		Redundant Access							
Winlogon Helper DLL		Regsvcs / Regasm							
		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

Ryuk-

Gandcrab-

Both-

TTPs of PETYA & NOT-PETYA

PETYA :

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. Later in 2016, another Petya variant emerged that contained an additional capability to be used if the virus could not gain administrator access to a machine.

NOT-PETYA:

Variants of Petya were first seen in March 2016, which propagated via infected e-mail attachments. In June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine. The new variant propagates via the Eternal Blue exploit, which is generally believed to have been developed by the U.S. National Security Agency (NSA), and was used earlier in the year by the WannaCry ransomware. 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 several governments.

TTPs of PETYA & NOT-PETYA

WORKING OF PETYA AND NOT-PETYA:

Petya exploits the vulnerability CVE-2017-0144 in Microsoft's implementation of the Server Message Block protocol. After it exploits the vulnerability, this attack encrypts the master boot record, among other files. It sends a message to the user to conduct a system reboot, after which the system is inaccessible. This makes the operating system incapable of locating files and there is no way to decrypt the files, which makes Petya a wiper rather than ransomware, which it was first believed to be.

The new variant has further increased its capabilities by adding a spreading mechanism similar to what we saw in WannaCry in May 2017. A set of critical patches was released by Microsoft on March 14 to remove the underlying vulnerability in supported versions of Windows, but many organizations may not have yet applied these patches.

Both PETYA and NOT-PETYA have same working

TTPs of PETYA & NOT-PETYA

adminetworkPersistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration over command-and-control channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	
	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting			Multilayer Encryption
Bootkit	DLL Injection					Service Execution		Scheduled Transfer	Peer Connections
Change Default File Association		Indicator Removal from Tools		Process Discovery	Shared Webroot	Windows Management Instrumentation			Remote File Copy
Component Firmware		Indicator Removal on Host		Query Registry	Taint Shared Content				Standard Application Layer Protocol
Hypervisor				Remote System Discovery	Windows Admin Shares				Standard Cryptographic Protocol
Logon Scripts		InstallUtil		Security Software Discovery					
Modify Existing Service		Masquerading		System Information Discovery					Standard Non-Application Layer Protocol
Redundant Access		Modify Registry							
Registry Run Keys / Start Folder		NTFS Extended Attributes		System Owner/User Discovery					Uncommonly Used Port
Security Support Provider		Obfuscated Files or Information		System Service Discovery					Web Service
Shortcut Modification		Process Hollowing							
Windows Management Instrumentation Event Subscription		Redundant Access							
		Regsvcs / Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

Red	PETYA
Yellow	NOT PETYA
Green	COMMON

TTPs of SHADE/TROLDESH & B0R0NT0K

SHADE/TROLDESH :

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.

B0R0NT0K:

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.

Some extensions were as follows:-

.PNG, .PSD, .PSPIMAGE, .TGA, .THM, .TIF, .TIFF, .YUV, .AI, .EP , S, .PS, .SVG

TTPs of SHADE/TROLDESH & B0R0NT0K

WORKING OF SHADE/TROLDESH :

Troldesh Ransomware attack is encrypting the victim's data and then demanding payment of a ransom to obtain the decryption key. This adds an additional layer of inconvenience to the attack, since the Troldesh Ransomware will replace the files' names with random characters and add the XTBL extension. The Troldesh Ransomware will drop text files on the victim's computer with the same payment instructions. The Troldesh Ransomware will drop about twenty copies of the text file on the victim's desktop as well as a copy of this text file on each of the folders containing encrypted files. Essentially, the Troldesh Ransomware attacks may have the following characteristics:

- The Troldesh Ransomware attack displays a warning message on the victim's computer.
- The Troldesh Ransomware replaces files on the victim's computer with encrypted copies in XTBL format.
- The Troldesh Ransomware drops text files on the victim's computer. These text files contain information on the attack and contact information for the attackers.

WORKING OF B0R0NT0K:

Rontok ransomware virus is mainly targeting websites and servers like Linux, but the threat may also be able to encrypt data on devices running Windows. This is a serious cyber infection that can affect more than your files because it makes additional changes to ensure the persistent that may include:

- added files or programs;
- disabled functions or applications;
- changed startup settings;
- added registry entries.

TTPs of SHADE/TROLDESH & B0R0NT0K

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	
	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting			Multilayer Encryption
Bootkit	DLL Injection					Service Execution		Scheduled Transfer	Peer Connections
Change Default File Association		Indicator Removal from Tools		Process Discovery	Shared Webroot	Windows Management Instrumentation			Remote File Copy
Component Firmware		Indicator Removal on Host		Query Registry	Taint Shared Content				Standard Application Layer Protocol
Hypervisor				Remote System Discovery	Windows Admin Shares				
Logon Scripts		InstallUtil		Security Software Discovery					Standard Cryptographic Protocol
Modify Existing Service		Masquerading		System Information Discovery					Standard Non-Application Layer Protocol
Redundant Access		Modify Registry							
Registry Run Keys / Start Folder		NTFS Extended Attributes		System Owner/User Discovery					Uncommonly Used Port
Security Support Provider		Obfuscated Files or Information		System Service Discovery					Web Service
Shortcut Modification		Process Hollowing							
Windows Management Instrumentation Event Subscription		Redundant Access							
		Regsvcs / Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

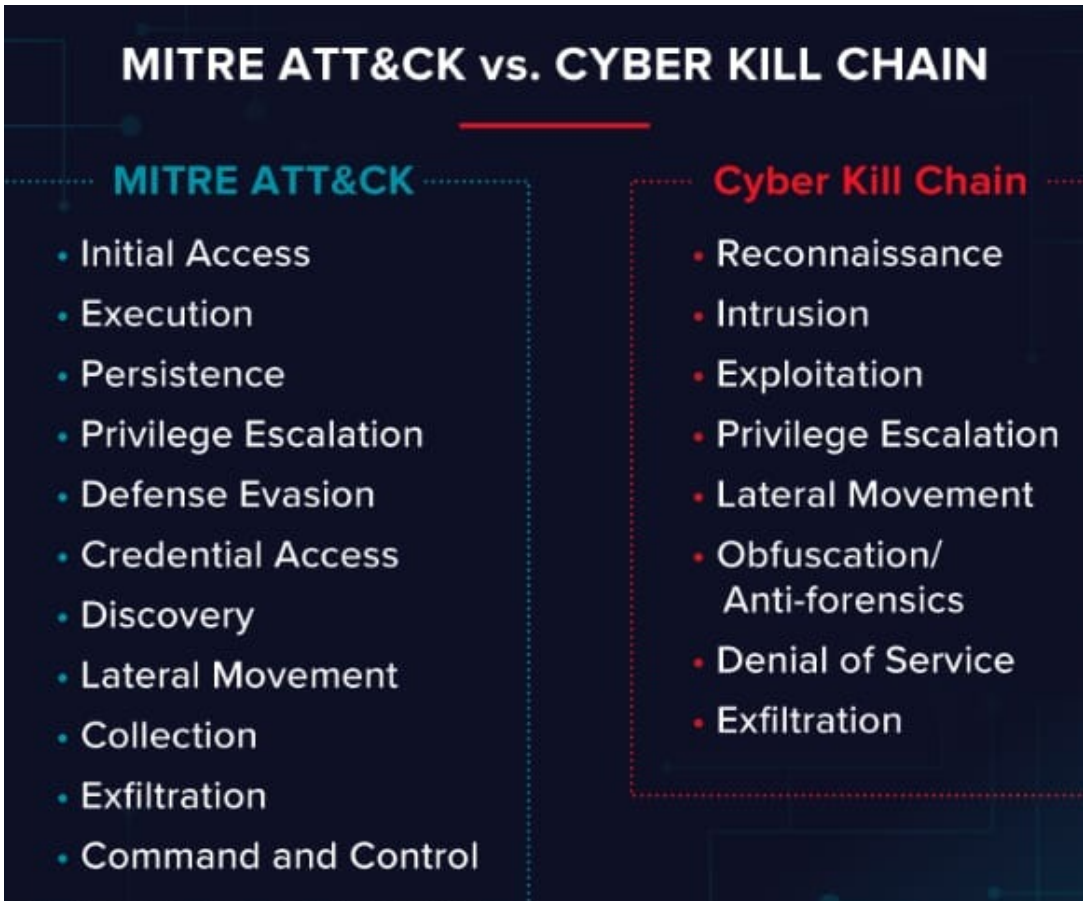
Shade

B0r0nt0k

Both Shade and B0r0nt0k

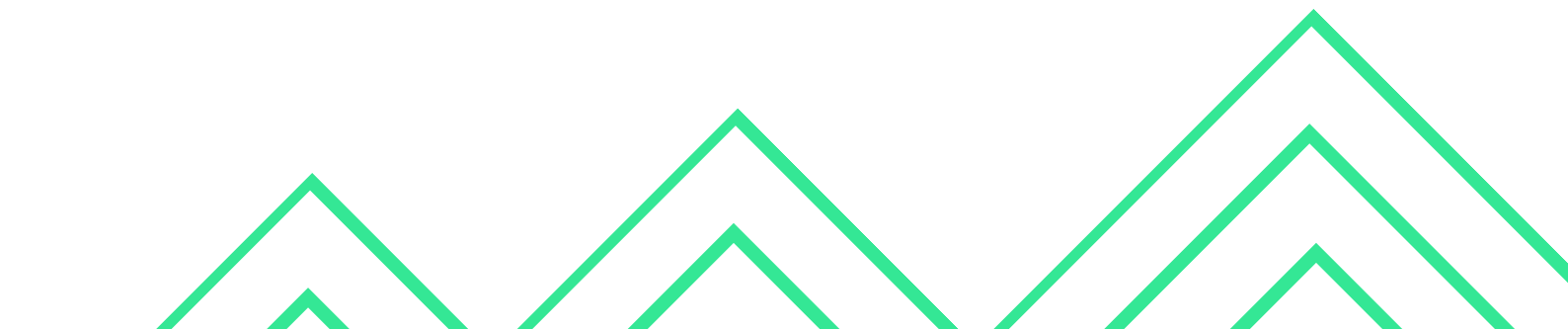
CONCLUSION

While the concept of an attacker leveraging ransomware affiliate programs is not new, ransomwares proved just how easy and successful these programs can be in practice. Key to this success is creating a low barrier for entry into the cybercrime ecosystem, while also distributing funds across affiliate program membersThe evolution was not only in the malware, but in the affiliates used to distribute and their TTP to compromise enterprise victims.Whether cyber kill chain or mitre att&ck both have deep rooted impact on systems which to more targeted victims and unfortunately higher ransoms



REFERENCES

- https://mitre-attack.github.io/attack-navigator/
- https://redskyalliance.org/xindustry/conti-ryuk-ransomware
- https://news.sophos.com/en-us/2019/03/05/gandcrab-101-all-about-the-most-widely-distributed-ransomware-of-the-moment/
- attack.mitre.org
- attackevals.mitre-engenuity.org
- kb.mazebolt.com
- https://www.elastic.co/blog/badrabbit-technical-analysis
- https://mitre-attack.github.io/attack-navigator/
- attack.mitre.org
- https://heimdalsecurity.com/blog/locky-ransomware-101/
- Petya. A / Not Petya is an AI-powered cyber weapon, TTPs lead to Sandworm APT group - SOC Prime
- https://attack.mitre.org/techniques/T1114/
- https://blog.group-ib.com/troldesh
- https://threats.kaspersky.com/en/class/Email-Worm/



THANK YOU