BLACK CELL
Protecting critical infrastructures

Annual Threat Intelligence based Retrospective TTP report for 2024

Table of Contents

1. Introduction

In an ever-evolving digital landscape, where threats constantly loom on the horizon, Black Cell stands at the forefront of the battle against cybercriminals. Our commitment to safeguarding digital interests compels us to maintain a vigilant stance against the dynamic threats that target our valued clientele. The diversity our clients, each unique in its structure and purpose, necessitates a nuanced approach to security. It's evident that adversaries wielding malicious intent are far from monolithic. Those who set their sights on one client employ tactics and techniques vastly dissimilar to those chosen by those with other targets in mind. Our mission extends beyond a mere infrastructure audit. To provide you with the most precise and effective recommendations, we embark on a comprehensive journey that takes us not only through the intricacies of your systems but also towards a broader understanding of the landscape in which you operate. In parallel with our infrastructure assessments, we delve deep into the annals of our ever-expanding repository of threat intelligence. Our focus remains on the most remarkable threats that have led to the successful compromise of other organizations. We meticulously collect, analyze, and methodically chart the Tactics, Techniques, and Procedures (TTPs) harnessed in these incidents. Our map, finely aligned with the esteemed MITRE ATT&CK framework, unveils a heatmap that vividly illustrates the techniques posing the most formidable threats to your organization.

This annual retrospective Threat Intelligence report represents our ongoing dedication to illuminate the evolving threat landscape, providing our valued customers with the knowledge to safeguard their digital domains. As we unveil the intricacies of adversary tactics and the dynamic spectrum of threats, we empower our customers to remain a step ahead in an ever-changing digital world.

1.1. Leveraging Annual Threat Intelligence Insights

The annual Threat Intelligence (TI) based retrospective TTP report is more than just a repository of knowledge; it's the cornerstone of our proactive defense strategy. At Black Cell, we understand that knowledge, when applied strategically, can be the most potent weapon against cyber threats. Our seasoned detection engineering team is at the heart of this operation. Armed with the insights gleaned from the annual TI-based retrospective TTP report, they embark on a mission to empower your defenses. The wealth of data contained within the report isn't merely an academic exercise; it's a blueprint for action. Detection rules, the frontlines of your digital security, are crafted and meticulously fine-tuned with precision. Each rule is tailored, honed, and adjusted to the nuances of your unique infrastructure.

This bespoke approach ensures that the security measures we employ are not just effective but efficient. We are in pursuit of a single goal – detection coverage that aligns seamlessly with the dynamic threat landscape, as unveiled in the annual TI-based retrospective TTP report.

It is in this synergy between comprehensive threat intelligence, data engineering and cutting-edge detection engineering that the true value of the report emerges. With each passing year, we refine our techniques, elevate our defenses, and stand ready to address emerging threats. The annual TI-based retrospective TTP report doesn't just inform our strategy; it shapes it. As we move forward, we remain steadfast in our commitment to providing you with detection

coverage that is not only informed by the latest intelligence but also backed by the power of adaptability. With this holistic approach, we empower your organization to thrive in the ever-evolving landscape of cybersecurity.

Our detection engineering services are an integral part of this ongoing commitment. In a world where cyber adversaries perpetually evolve, so must our defenses. The annual Threat Intelligence (TI) based retrospective TTP report lays the foundation, but it is in the constant vigilance and action that we find true resilience. Our expert detection engineering team, armed with the insights from the TI report, operates as your vanguard. Their mission doesn't stop at creating and fine-tuning detection rules based on historical data; it extends to monitoring the ever-shifting threat landscape, identifying new attack vectors, and crafting responsive solutions. In the dynamic arena of cybersecurity, the ability to swiftly adapt is the key to survival. With our ongoing detection engineering services, we stand ready to address emerging threats the moment they surface. Our team is ever-vigilant, ensuring that your security posture remains in lockstep with the evolving tactics, techniques, and procedures outlined in the TI report.

1.2. Analysis of Adversary TTPs

The usefulness of threat intelligence can be measured in its ability to deny cyber-attacks when adequate mitigations are in place. An excellent illustration of this concept is David Bianco's Pyramid of Pain. This simple diagram shows the relationship between the types of indicators we might use to detect an adversary's activities and how much effort or "pain" it will cause them when you are able to deny them the use of those indicators.

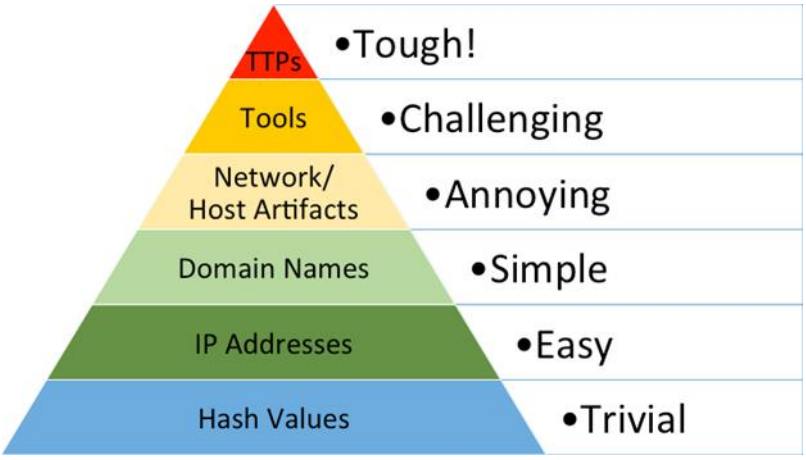

Figure 2: The Pyramid of Pain

When we are able to detect and mitigate TTPs, we are covering entire adversary behaviours, not just their tools. From a pure effectiveness standpoint, this is ideal. If we are able to prevent or react to adversary TTPs in a timely fashion, we can force them to do the most time-consuming thing possible, learn new behaviours. Therefore, with the results of this assessment in combination with the analysis of relevant and timely TTPs, you will receive actionable intelligence about where to focus your efforts, in order to cause as much possible headache for would-be attackers.

2. Methodology

There are numerous sources of historical data and high-quality analyses of cyber threats that can be used to map out TTPs. Therefore, out analysis starts with the aggregation of appropriate data in terms of quantity and quality from a range of sources. Our data gathering starts with a search of the clear web, which is essentially everything that is indexed by the most popular search engines. For our research we used Google Dork because it strongly supports targeted OSINT work. Dorking (or Google Hacking) is a technique used by security researchers that utilizes specialized queries written in Google's own query language, to find highly specialized resources. For further data enrichment we used a deep web metasearch engine and dark web crawlers for TOR, I2P, Zeronet/Freenet, Lokinet. Where applicable we also used cyber-attack information from various commercial threat intel sources in order to identify:

- **Most emerging malwares**
- **Most active threat actors**
- **Other high profile TTPs**

Following the identification of the above we used the previously described data collection methodologies to determine the specific approaches and procedures that led to the successful cyber-attack. Mapping these procedures to ATT&CK techniques is trivial and is sometimes even included in publicly available analyses. We also collected any available data to identify the malwares and tools that were used. These threat profiles may contain exploitation tools, malwares, and typical techniques that they have used in previous attacks.

Finally, it is also necessary to review the security gaps that victimized the affected entity. Often times searches for such information will not be fruitful, however when this information can be gathered, it is incredibly useful. The security gaps and inadequacies that resulted in successful cyber-attacks, serve as excellent points of reflection, allowing us to consider how these gaps apply to our own environments and enable us to learn from others' mistakes.

In summary our data collection process can be broken down into the following steps.

1. Find the most performing malwares, threat actors, adversarial frameworks, AI threats and other high profile TTPs.

2. Gather all available information about the incidents.
2.1. Pinpoint the tools or malwares that were used.
2.2. Determine and/or extract attack procedures and methodologies that were used.
2.3. Map this information to ATT&CK techniques.

3. Identify the threat actors (APT, criminal groups) and build a threat profile.
3.1. Collect information about their tools and attack procedures.
3.2. Map this information to ATT&CK techniques.

4. Determine the inadequacies of the victim.
4.1. Map these security gaps to ATT&CK techniques.

Not all the information collected holds equal significance. Within our repository of gathered data, a discerning eye distinguishes between highly impactful attack data and less relevant details. Thus, it becomes imperative to categorize and quantify the collected information in a form conducive to further analysis. While one aspect of this process involves the alignment of attack data with ATT&CK techniques, another crucial facet involves the assignment of numerical scores to each cyber threat.

To facilitate this, we've designed a comprehensive scoring system. We evaluate each threat on multiple dimensions that represent a layer in MITRE ATT&CK Navigator:

- **Impact Score (1-5):** This metric gauges the potential consequences of an incident. A score of 1 suggests that the threat could be resolved in a matter of days, while a score of 3 indicates substantial and lasting damage to the victim. At the extreme end, a score of 5 signifies a significant risk to human life or lasting societal damage.
- **Evasion Score (1-5):** This score measures how effectively the threat eluded detection. A score of 1 indicates that relatively simplistic, signature-based detection tools could have identified the threat, whereas a score of 5 implies that highly sophisticated evasion methods were employed.
- **Complexity Score (1-5):** This score assesses the competency, experience, and knowledge level of the adversary. A score of 1 denotes an adversary limited to using existing tools, colloquially known as a 'script kiddie,' while a score of 5 indicates an adversary capable of crafting custom-tailored malware.
- **Historical Success Score (1-5):** This metric evaluates the past performance of the threat. A score of 1 implies little or partial success, while a score of 5 signifies perfect execution and complete success in achieving the threat's objectives.

Considering the sheer volume of data and the diversity of data sources, we further enhance our analysis by assigning an accuracy multiplier. This multiplier reflects our certainty and confidence in our findings. The final scores are meticulously mapped to ATT&CK techniques and are subsequently normalized on a scale ranging from 0.5 to 1.5. These normalized scores culminate in a comprehensive heatmap, providing a visual representation of the threat landscape's intricacies and priorities.

3. Datasets

3.1. Most emerging malwares

1. **AgentTesla**

   Description: Agent Tesla is a sophisticated remote access trojan (RAT) focused on stealing and infiltrating sensitive information from compromised systems. It can gather various data types, such as keystrokes and credentials used in web browsers (e.g., Google Chrome and Mozilla Firefox) and email clients on infected devices.

   Scores:

   - Impact: 3
   - Evasion: 4
   - Complexity: 3
   - Successfulness: 4
   - Accuracy: 1.3

2. **ALPHV/BlackCat Ransomware**

   Description: ALPHV Ransomware is another variant of ransomware that encrypts data and demands a ransom for decryption. Ransomware attacks are a common method used by cybercriminals to extort money from victims.

   Scores:

   - Impact: 4
   - Evasion: 4
   - Complexity: 4
   - Successfulness: 4
   - Accuracy: 1.5

3. **Androxgh0st**

   Description: Androxgh0st predominantly targets Laravel applications, a leading PHP framework used in numerous web applications. By scanning .env files, Androxgh0st can detect and retrieve sensitive data, including crucial login details for platforms like Amazon Web Services.

   Scores:

   - Impact: 2
   - Evasion: 3
   - Complexity: 3

- Successfulness: 3
- Accuracy: 1.0

4. **AsyncRAT**

   Description: AsyncRAT is an open-source remote access tool initially available on the NYANxCAT GitHub repository, which has been leveraged in malicious campaigns.

   Scores:

   - Impact: 2
   - Evasion: 3
   - Complexity: 2
   - Successfulness: 3
   - Accuracy: 1.1

5. **Black Basta**

   Description: Black Basta is a ransomware written in C++ that has been operating under the ransomware-as-a-service (RaaS) model since at least April 2022, with variants designed to target both Windows and VMware ESXi servers. The group's operations often involve a double extortion tactic, where they not only demand a ransom to decrypt an organization's files but also threaten to release sensitive data on a leak site if payment is not made. Black Basta affiliates have targeted several high-value organizations, with most victims located in the U.S.

   Scores:

   - Impact: 4
   - Evasion: 4
   - Complexity: 4
   - Successfulness: 4
   - Accuracy: 1.3

6. **Cactus**

   Description: CACTUS ransomware is a malware strain first identified in March 2023. The name comes from the ransom note "cAcTuS.readme.txt" it leaves on victims' machines. It also encrypts files with a .cts1 extension, where the number at the end can vary.

   Scores:

   - Impact: 3
   - Evasion: 3
   - Complexity: 3

- Successfulness: 3
- Accuracy: 1.0

7. **Clop**

   Description: Clop is a ransomware strain first identified in February 2019. It has been used in attacks against a variety of sectors, including retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, mining, financial services, aerospace, telecommunications, professional and legal services, healthcare, and high-tech industries. Clop is a variant of the CryptoMix ransomware family.

   Scores:

   - Impact: 4
   - Evasion: 4
   - Complexity: 4
   - Successfulness: 4
   - Accuracy: 1.4

8. **Cobalt Strike**

   Description: Cobalt Strike is a popular post-exploitation framework used by penetration testers and red teamers. However, it is also favored by malicious actors for its advanced capabilities in evading detection and controlling compromised systems.

   Scores:

   - Impact: 4
   - Evasion: 5
   - Complexity: 5
   - Successfulness: 5
   - Accuracy: 1.5

9. **CryptBot**

   Description: CryptBot is an information-stealing malware that captures browser credentials, cryptocurrency wallet details, cookies, credit card information, and screenshots from infected systems. The stolen data is consolidated into a zip file and uploaded to a command-and-control (C2) server.

   Scores:

   - Impact: 3
   - Evasion: 4
   - Complexity: 3

- Successfulness: 4
- Accuracy: 1.2

10. **DarkGate**

Description: First documented in 2018, DarkGate is a commodity loader with features that include the ability to download and execute files to memory, a Hidden Virtual Network Computing (HVNC) module, keylogging, information-stealing capabilities, and privilege escalation. DarkGate makes use of legitimate AutoIt files and typically runs multiple AutoIt scripts. New versions of DarkGate have been advertised on a Russian language eCrime forum since May 2023.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.3

11. **FormBook**

Description: FormBook is an infostealing malware discovered in 2016. It collects various data from infected machines, including browser-cached credentials, screenshots, and keystrokes, and can also serve as a downloader for other malicious files.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 2
- Successfulness: 4
- Accuracy: 1.3

12. **GuLoader**

Description: GuLoader, a trojan discovered in December 2019, often serves as an initial stage in multi-step malware infections. After compromising a host, it downloads and installs additional malware, originally distributing Parallax RAT but has since branched into delivering ransomware and banking trojans, such as Netwire, FormBook, and Agent Tesla.

Scores:

- Impact: 3
- Evasion: 5

- Complexity: 4
- Successfulness: 4
- Accuracy: 1.4

13. **LockBit**

Description: LockBit ransomware first emerged in September 2019 and has since evolved through several versions, with LockBit 3.0 being the latest. LockBit is one of the most active ransomwares globally, targeting mainly small-to-medium-sized organizations and demanding lower ransom payments compared to the industry average.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.5

14. **Lokibot**

Description: Lokibot is a popular information-stealing malware first identified in 2015, designed to extract usernames, passwords, cryptocurrency wallet data, and other credentials. It can also create a backdoor in infected systems, allowing attackers to deploy additional payloads.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 2
- Successfulness: 4
- Accuracy: 1.2

15. **Lumma Stealer**

Description: Lumma Stealer (also known as LummaC2 Stealer) is a C-based information stealer available via Malware-as-a-Service (MaaS) on Russian-speaking forums since at least August 2022. It primarily targets cryptocurrency wallets and two-factor authentication (2FA) browser extensions, stealing sensitive information and exfiltrating it to a C2 server using HTTP POST requests with a "TeslaBrowser/5.5" user agent. It also includes a non-resident loader capable of delivering additional payloads via EXE, DLL, and PowerShell.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.1

16. **Metastealer**

Description: MetaStealer is an info-stealing malware that targets sensitive data, such as login credentials, payment information, and browser history. Often spread through phishing emails or malicious downloads, it can exfiltrate data to a command-and-control (C2) server and employs stealth techniques for evasion and persistence, making detection challenging.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.0

17. **NanoCore**

Description: NanoCore is a modular remote access tool developed in .NET, used since 2013 for spying on victims and stealing information.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.2

18. **njRAT**

Description: njRAT is a remote access tool (RAT) first observed in 2012, commonly used by threat actors in the Middle East.

Scores:

- Impact: 2
- Evasion: 2
- Complexity: 2
- Successfulness: 3
- Accuracy: 1.0

19. **Phorpiex**

Description: Phorpiex is a botnet malware recognized as a major malware threat in 2021. The Phorpiex botnet is well-established and supports various purposes, including spam email distribution, malware delivery, and cryptomining.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.1

20. **PLAY**

Description: Play ransomware was first detected in June 2022. The group employs multi-extortion tactics by not only encrypting the data of target organizations but also threatening to expose it on their public TOR-based sites. Play attackers do not show a preference for specific victims, though they tend to focus on large enterprises. Known targets include medical institutions, as well as organizations in the financial, manufacturing, real estate, and education sectors.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.0

21. **Qbot**

Description: Qbot, also known as QakBot, is a modular banking trojan with a history dating back to at least 2007. Over time, it has evolved from an information stealer into a delivery agent for ransomware, such as ProLock and Egregor.

Scores:

- Impact: 4
- Evasion: 3
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.2

22. **Ramnit**

Description: Ramnit is a banking trojan discovered in 2010. It ranks among the top 5 banking trojans globally and is notably prevalent in the Asia-Pacific region, where it is the third most common malware and the second most common banking trojan.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 3
- Successfulness: 5
- Accuracy: 1.3

23. **Raspberry Robin**

Description: Raspberry Robin is a malware variant known for its moderate evasion capabilities and effectiveness in data exfiltration. It may be associated with financially motivated cybercriminals.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 4
- Successfulness: 3
- Accuracy: 1.0

24. **RedLine Stealer**

Description: RedLine Stealer extracts information from browsers, such as saved credentials, autocomplete data, and credit card details. When running on a target machine, it also collects system information, including username, location, hardware configuration, and security software details. Recent versions can steal cryptocurrency, and the malware targets FTP and IM clients, with capabilities to upload/download files, execute commands, and periodically report back on the infected machine.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.1

25. **Remcos RAT**

Description: Remcos RAT (Remote Administration Tool) is a type of remote access malware that allows attackers to gain control of a victim's computer or network. It's often used for unauthorized access and data theft.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 2
- Successfulness: 2
- Accuracy: 1.0

26. **RisePro**

Description: RisePro is a stealer that spreads through downloaders like win.privateloader, capable of stealing credit card information, passwords, and personal data once deployed on a system.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 2
- Successfulness: 4
- Accuracy: 1.0

27. **SocGholish**

Description: SocGholish is a sophisticated malware known for its high success rate in evading security measures. It targets sensitive information and is often used in cyber espionage and data theft.

Scores:

- Impact: 3
- Evasion: 4

- Complexity: 3
- Successfulness: 4
- Accuracy: 1.4

28. **StealC**

Description: StealC is an information-stealing malware written in C that uses WinAPI functions to target data from web browsers, browser extensions, desktop cryptocurrency wallet applications, and other programs like messengers and email clients. It downloads seven legitimate third-party DLLs, such as sqlite3.dll, nss3.dll, and vcruntime140.dll, to gather sensitive data from browsers, exfiltrating the information to its C2 server via HTTP POST requests.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.0

29. **STOP**

Description: STOP ransomware encrypts user data with AES-256 and appends one of several available extensions to the encrypted file's name. Rather than encrypting entire files, it only encrypts the first 5 MB. Originally, it could operate offline using a hard-coded key, which allowed for decryption under certain conditions.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.0

30. **Vidar**

Description: Vidar is an information-stealing malware operating under the malware-as-a-service model, first detected in late 2018. Vidar runs on Windows and collects various types of sensitive information from browsers and digital wallets. The malware is also used as a downloader for ransomware, becoming one of the most successful info-stealers since its inception.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.2

31. **WannaCry**

Description: WannaCry is ransomware with a worm component that exploits vulnerabilities in the Windows SMBv1 server to remotely compromise systems, encrypt files, and spread to additional hosts.

Scores:

- Impact: 5
- Evasion: 4
- Complexity: 4
- Successfulness: 5
- Accuracy: 1.5

32. **XMRig Miner**

Description: XMRig Miner is not malware itself, but a legitimate cryptocurrency mining software. However, it can be abused by cybercriminals to mine cryptocurrency on victims' computers without their consent.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.3

3.2. Most active threat actors

1. **8Base**

Description: 8Base is a ransomware group that appeared in 2022 but escalated its activities and improved its tactics significantly by 2023. Initially a crypto-ransomware, the malware has since evolved into a tool for multi-extortion attacks. The group targets companies across various industries, including finance, manufacturing, IT, and

healthcare, focusing primarily on small to medium-sized businesses (SMBs) in the United States, Brazil, and the United Kingdom.

Scores:

- Impact: 2
- Evasion: 2
- Complexity: 3
- Successfulness: 2
- Accuracy: 1.5

2. **Akira Ransomware Group**

Description: Akira is a ransomware variant and operator active since at least March 2023. It gains initial access by exploiting compromised credentials and single-factor external access points such as VPNs, then uses publicly available tools and techniques for lateral movement. Akira engages in "double extortion," where data is exfiltrated before encryption, with threats to publish it if a ransom is not paid. Technical analysis of Akira shows multiple similarities and overlaps with Conti ransomware.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.5

3. **Anonymous Russia**

Description: A collective of pro-Russian hacktivists often engaged in politically motivated cyber-attacks. Known for DDoS and data leak operations targeting NATO, governments, and companies opposing Russian interests.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.2

4. **Anonymous Sudan**

Description: Anonymous Sudan is a hacktivist group that emerged in early 2023 and claims to target entities perceived to oppose Sudan or Islam. The group primarily conducts distributed denial-of-service (DDoS) attacks and data leaks, often claiming to support Sudanese or Islamic interests.

Scores:

- Impact: 3
- Evasion: 2
- Complexity: 2
- Successfulness: 3
- Accuracy: 1.3

5. **BianLian**

Description: BianLian is a ransomware group involved in developing and deploying ransomware and extorting data. Active since June 2022, it has targeted critical infrastructure sectors in the U.S. and Australia, including a data breach in 2024 affecting Northern Minerals.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.5

6. **BlackSuit**

Description: The BlackSuit ransomware group surfaced in spring of 2023, employing a multi-faceted extortion strategy that combines data encryption with exfiltration. For victims who do not meet their demands, BlackSuit hosts public data leak sites. They are notably active in attacking healthcare, education, and other essential industries.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.3

7. **Cicada3301**

Description: Cicada3301 group has posed significant risk since its discovery in June 2024, primarily targeting essential industries across the US and UK. Written in Rust, Cicada3301's ransomware is cross-platform, compatible with Windows, Linux, ESXi, and even rare architectures like PowerPC. Advanced encryption is used, integrating ChaCha20 and RSA algorithms with customizable modes: Full, Fast, and Auto.

Scores:

- Impact: 5
- Evasion: 5
- Complexity: 5
- Successfulness: 5
- Accuracy: 1.1

8. **Cyber Army of Russia**

Description: A pro-Russian hacker group actively involved in cyber warfare, primarily using DDoS and defacement tactics against organizations and governments deemed adversaries to Russian interests.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.1

9. **CyberDragon**

Description: The CyberDragon hacker group is known for its pro-Russian stance, evident from both public statements and Russian-language communications. They are known for coordinating attacks with other pro-Russian groups.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.0

10. **dAn0n**

Description: dAn0n group stands out by engaging in both data brokerage and ransomware activities. They gain access primarily through phishing, deploying custom ransomware binaries and obfuscated scripts. The group uses privilege escalation and defense evasion to establish persistence and avoid detection.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.0

11. **DragonForce**

Description: DragonForce group runs a Ransomware-as-a-Service (RaaS) program using two main ransomware strains: one is a LockBit3.0 variant, and the other, while initially claimed as unique, is based on ContiV3. Double extortion methods are used, encrypting data and threatening leaks to coerce ransom payments.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.2

12. **Helldown**

Description: Helldown ransomware group has quickly made a name for itself, using advanced encryption methods like AES, Salsa20, and RSA. Known for its stealth through the dark web and cryptocurrencies, Helldown exploits vulnerabilities to penetrate networks and disable defenses, especially in IT, telecom, and manufacturing. They exfiltrate and threaten to release sensitive data unless ransoms are paid, often causing extensive damage.

Scores:

- Impact: 4
- Evasion: 5
- Complexity: 4
- Successfulness: 4

- Accuracy: 1.1

13. **Hunters International**

Description: Hunters International is a cybercrime group that targets organizations across various sectors. The group is involved in ransomware operations and is known for its methodical approach to compromising networks and extorting victims through data leaks and encryption.

Scores:

- Impact: 3
- Evasion: 2
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.4

14. **Inc. Ransomware Group**

Description: Inc. Ransomware is a relatively new ransomware group that focuses on targeting organizations in critical infrastructure sectors. Known for its aggressive tactics, the group employs a combination of ransomware attacks and data theft, threatening to release sensitive information unless a ransom is paid.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.3

15. **Lazarus Group**

Description: Lazarus Group is a North Korean state-sponsored cyber threat group associated with the Reconnaissance General Bureau. Active since at least 2009, the group is notorious for the Sony Pictures attack in 2014 and has conducted multiple campaigns targeting sectors like energy and finance.

Scores:

- Impact: 5
- Evasion: 5
- Complexity: 5
- Successfulness: 5

- Accuracy: 1.5

16. **Lynx**

Description: Lynx, a ransomware group discovered in July 2024, has claimed over 20 victims across different sectors. They use both single and double extortion tactics but refrain from targeting government entities, hospitals, non-profits, and other socially critical areas.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 3
- Accuracy: 1.2

17. **Mad Liberator**

Description: The Mad Liberator ransomware group targets AnyDesk users by initiating unsolicited connections. Once a connection is approved, the attackers drop a fake Windows update binary, distracting victims while stealing data from OneDrive, network shares, and local storage using AnyDesk's File Transfer feature. Victims' keyboards are disabled to prevent interruption. While not encrypting data, the group leaves ransom notes in shared folders, threatening data publication if demands are unmet.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.0

18. **Medusa**

Description: The Medusa Ransomware-as-a-Service (RaaS) group mainly distributes its ransomware by exploiting unpatched vulnerabilities in public-facing systems. Medusa affiliates also buy system credentials from initial access brokers (IABs) and take over legitimate accounts to infiltrate networks. The group employs Living off the Land (LoTL) techniques to bypass defenses and mimic normal system activity, indicating that the operators are technically skilled and highly experienced.

Scores:

- Impact: 4

- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.5

19. **Meow**

Description: Meow ransomware group maintains a data leak site for their victims. Using ChaCha20 to encrypt data on compromised servers, they direct victims to contact them via email or Telegram for ransom payment instructions.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 2
- Successfulness: 4
- Accuracy: 1.0

20. **NoEscape Ransomware Group**

Description: NoEscape ransomware group, also known as N0_Esc4pe, has intensified its cyber-attack activities recently, targeting key sectors globally.

Scores:

- Impact: 4
- Evasion: 3
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.4

21. **NoName057(16)**

Description: NoName057(16) is a pro-Russian hacktivist group that emerged in the context of the Russian invasion of Ukraine. The group primarily engages in DDoS attacks targeting Western and Ukrainian entities, often coordinating its operations through social media and other public platforms.

Scores:

- Impact: 4
- Evasion: 3
- Complexity: 3

- Successfulness: 3
- Accuracy: 1.1

22. **Qilin**

Description: Qilin operates as a Ransomware-as-a-Service (RaaS) criminal network, working with affiliates to encrypt and exfiltrate data from compromised organizations, followed by a ransom demand.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.1

23. **Ra Group**

Description: RA Group adopts double extortion, threatening to publish exfiltrated data from uncooperative victims, enhancing the pressure for ransom payments.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.0

24. **Ransomed.VC**

Description: Ransomed.VC made a notable entrance with a structured PR campaign, featuring a clearnet website and channels on Telegram and Twitter/X. They exploit GDPR penalties as leverage in their extortion schemes, warning victims of potential legal penalties if data is leaked.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 5

- Accuracy: 1.3

25. **RansomHub**

Description: RansomHub has become a prominent ransomware group, relying on double extortion. Affiliates gain initial access, steal data, and launch ransomware, leaving victims to recover both systems and deal with the threat of data publication.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.4

26. **Rhysida**

Description: The Rhysida ransomware group first appeared in May 2023, with a victim support chat hosted on TOR (.onion). They present themselves as a "cybersecurity team," claiming to highlight security weaknesses by targeting victims' systems.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.1

27. **Server Killers**

Description: Server Killers collaborates with other notorious hacker groups, escalating cyber threats in Eastern Europe. They include gangs like NoName057(16), Digital Revolt, 2CC, Cyber Army of Russia, Phoenix, Coup Team, Lulzsec Muslims, and CyberDragon.

Scores:

- Impact: 4
- Evasion: 4
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.1

28. **SiegedSec**

Description: SiegedSec is an emerging cyber threat group that gained traction during Russia's invasion of Ukraine. Known for data leaks, they now target various global sectors.

Scores:

- Impact: 3
- Evasion: 4
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.0

29. **Türk Hack Team**

Description: Türk Hack Team, established in 2004, is one of Turkey's oldest and most notable hacking collectives. The group claims responsibility for nearly 30 widely publicized attacks on foreign government and corporate websites, often focusing on targets of national or cultural significance. Their campaigns are high-profile and frequently aim to disrupt international corporations and government institutions through defacements and data breaches.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 4
- Accuracy: 1.0

30. **UserSec**

Description: UserSec is a pro-Russian hacking group active since at least 2022, recognized for its DDoS attacks and collaborations with other pro-Russian groups. In May 2023, UserSec launched a cyber campaign against NATO member states, joining forces with KillNet to execute coordinated attacks on NATO.

Scores:

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3

- Accuracy: 1.0

4. Scores

The following scores were assigned to each cyber threat:

Threat/Threat Actor	Impact	Evasion	Complexity	Successfulness	Accuracy	**Sum**
AgentTesla	3	4	3	4	1.3	**18.2**
ALPHV/BlackCat Ransomware	4	4	4	4	1.5	**24**
Androxgh0st	2	3	3	3	1.0	**11**
AsyncRAT	2	3	2	3	1.1	**11**
Black Basta	4	4	4	4	1.3	**20.8**
Cactus	3	3	3	3	1.0	**12**
Clop	4	4	4	4	1.4	**22.4**
Cobalt Strike	4	5	5	5	1.5	**28.5**
CryptBot	3	4	3	4	1.2	**16.8**
DarkGate	3	4	4	4	1.3	**19.5**
FormBook	3	3	2	4	1.3	**15.6**
GuLoader	3	5	4	4	1.4	**22.4**
LockBit	4	4	4	4	1.5	**24**
Lokibot	3	3	2	4	1.2	**14.4**
Lumma Stealer	3	4	3	4	1.1	**15.4**
Metastealer	3	4	3	4	1.0	**14**
NanoCore	3	3	3	4	1.2	**15.6**
njRAT	2	2	2	3	1.0	**9**
Phorpiex	3	3	3	4	1.1	**14.3**

PLAY	3	3	3	3	1.0	**12**
Qbot	4	3	4	4	1.2	**18**
Ramnit	4	4	3	5	1.3	**20.8**
Raspberry Robin	3	3	4	3	1.0	**13**
RedLine Stealer	3	3	3	4	1.1	**14.3**
Remcos RAT	3	3	2	2	1.0	**10**
RisePro	3	3	2	4	1.0	**12**
SocGholish	3	4	3	4	1.4	**19.6**
StealC	3	4	3	4	1.0	**14**
STOP	3	3	3	3	1.0	**12**
Vidar	3	3	3	4	1.2	**15.6**
WannaCry	5	4	4	5	1.5	**27**
XMRig Miner	3	3	3	3	1.3	**15.6**
8Base	2	2	3	2	1.5	**13.5**
Akira Ransomware Group	4	4	4	4	1.5	**24**
Anonymous Russia	3	4	3	4	1.2	**16.8**
Anonymous Sudan	3	2	2	3	1.3	**13**
BianLian	4	4	4	4	1.5	**24**
BlackSuit	4	4	4	4	1.3	**20.8**
Cicada3301	5	5	5	5	1.1	**22**
Cyber Army of Russia	4	4	4	4	1.1	**17.6**
CyberDragon	3	3	3	4	1.0	**13**
dAn0n	3	4	4	4	1.0	**15**

DragonForce	4	4	3	4	1.2	**18**
Helldown	4	5	4	4	1.1	**18.7**
Hunters International	3	2	3	3	1.4	**15.4**
Inc. Ransomware Group	4	4	3	4	1.3	**19.5**
Lazarus Group	5	5	5	5	1.5	**30**
Lynx	4	4	4	3	1.2	**18**
Mad Liberator	3	3	3	3	1.0	**12**
Medusa	4	4	4	4	1.5	**24**
Meow	3	3	2	4	1.0	**12**
NoEscape Ransomware Group	4	3	4	4	1.4	**21**
NoName057(16)	4	3	3	3	1.1	**14.3**
Qilin	3	4	4	4	1.1	**16.5**
Ra Group	4	4	4	4	1.0	**16**
Ransomed.VC	4	4	4	5	1.3	**22.1**
RansomHub	4	4	4	4	1.4	**22.4**
Rhysida	3	4	4	4	1.1	**16.5**
Server Killers	4	4	3	4	1.1	**16.5**
SiegedSec	3	4	3	3	1.0	**13**
Türk Hack Team	3	3	3	4	1.0	**13**
UserSec	3	3	3	3	1.0	**12**

4.1. Other high profile TTPs

In our recent detections, we observed that several adversarial techniques were closely associated with zero-day attack based incidents. These techniques highlighted the use of previously unknown software vulnerabilities. Threat actors leveraged these vulnerabilities to

gain unauthorized access to systems and execute malicious code without relying on known exploits or patches. Exploiting zero-day vulnerabilities allowed adversaries to evade traditional security measures and remain undetected, posing a significant challenge for organizations in defending against such emerging threats. This underscores the critical need for proactive security strategies, such as vulnerability management and threat intelligence, to effectively protect against zero-day attacks and their associated adversarial techniques.

The following techniques can be considered as the core detection stack that needs to be addressed. Therefore, these techniques' scores are retrofitted in proportion to the highest-scoring technique of the threat landscape based on their relevance.

Technique ID	Score	Technique ID	Score
T1553.002	119.7	T1485	61.3
T1021.002	112.5	T1070	56.4
T1572	106.3	T1573.002	55.5
T1053	102.4	T1587.001	54
T1490	101	T1218.007	53.4
T1070.001	97.3	T1059.006	49.5
T1095	94.5	T1078.002	49.3
T1021.004	91.5	T1056	39.6
T1021	90.3	T1087	35.3
T1203	88.7	T1003.001	34.5
T1210	80.4	T1588.002	30
T1027.013	78.1	T1595.002	27.8
T1059	75.7	T1053.005	21
T1074.001	67.6	T1218.011	13
T1129	66.9	T1505.003	11
T1071.004	64.5	-	-

Understanding these techniques and their contexts is essential for organizations to enhance their threat detection and response capabilities, as well as to bolster their cybersecurity defenses.

5. Heatmap

Below you can find the MITRE ATT&CK heatmap. Red techniques indicate critical threats, while green techniques are less severe.

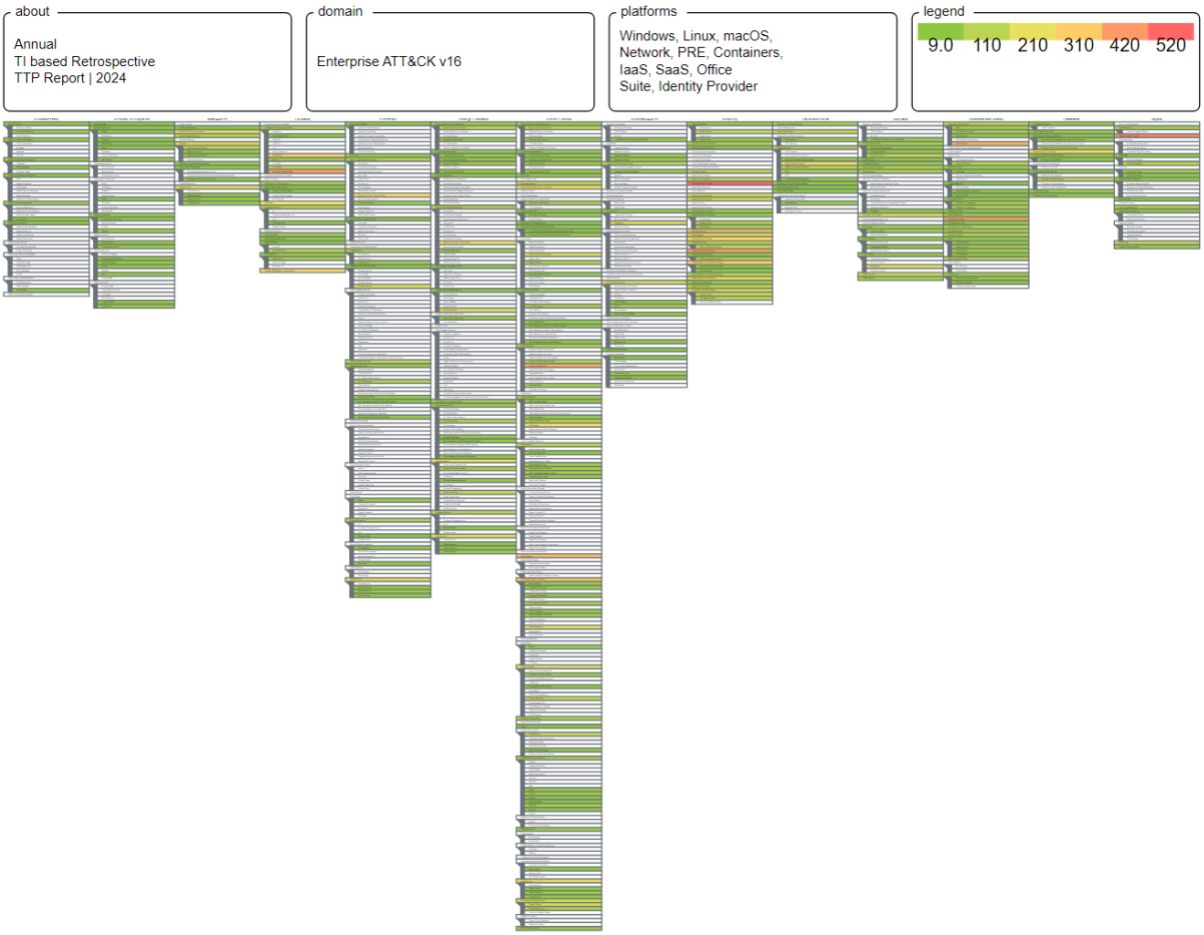

Figure 1: Annual_TI_based_Retrospective_TTP_report_heatmap

6. Results

Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access. Since there are 203 techniques and 453 Sub-techniques, we need to prioritize them in a descending order based on their score. For detection engineering purposes, we defined the baseline at 120 points. This means that that we need to cover, have visibility, proper date source, detection rules and playbooks for all these techniques and sub-techniques. Most of the followings have multiple procedures.

1. T1083: File and Directory Discovery

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the

information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Score: 517.8

2. T1486: Data Encrypted for Impact

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

Score: 448.2

3. T1082: System Information Discovery

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Score: 406.1

4. T1105: Ingress Tool Transfer

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as ftp. Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. Lateral Tool Transfer).

Score: 402.2

5. T1059.003: Command and Scripting Interpreter: Windows Command Shell

Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via Remote Services such as SSH.

Score: 393.3

6. T1562.001: Impair Defenses: Disable or Modify Tools

Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information. Adversaries may also disable updates to prevent the latest security patches from reaching tools on victim systems.

Score: 369.9

7. T1071.001: Application Layer Protocol: Web Protocols

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Score: 367.3

8. T1057: Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Administrator or otherwise elevated access may provide better process details. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Score: 339.2

9. T1112: Modify Registry

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.

Score: 334.6

10. T1059.001: Command and Scripting Interpreter: PowerShell

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of

actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

Score: 314

11. T1027: Obfuscated Files or Information

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

Score: 309

12. T1016: System Network Configuration Discovery

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.

Score: 306.2

13. T1041: Exfiltration Over C2 Channel

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Score: 284.7

14. T1047: Windows Management Instrumentation

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is designed for programmers and is the infrastructure for management data and operations on Windows systems. WMI is an administration feature that provides a uniform environment to access Windows system components.

Score: 281.5

15. T1021.001: Remote Services: Remote Desktop Protocol

Adversaries may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.

Score: 280.9

16. T1018: Remote System Discovery

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as Ping or net view using Net.

Score: 272.7

17. T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.

Score: 261.9

18. T1106: Native API

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations.

Score: 249.4

19. T1070.004: Indicator Removal: File Deletion

Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: Ingress Tool Transfer) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

Score: 246.6

20. T1140: Deobfuscate/Decode Files or Information

Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that

information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

Score: 244.4

21. T1055: Process Injection

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

Score: 218

22. T1078: Valid Accounts

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

Score: 208.2

23. T1027.002: Obfuscated Files or Information: Software Packing

Adversaries may perform software packing or virtual machine software protection to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory. Virtual machine software protection translates an executable's original code into a special format that only a special virtual machine can run. A virtual machine is then called to run this code.

Score: 204.4

24. T1033: System Owner/User Discovery

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do

this, for example, by retrieving account usernames or by using OS Credential Dumping. The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from System Owner/User Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Score: 197.7

25. T1564.001: Hide Artifacts: Hidden Files and Directories

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a 'hidden' file. These files don't show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (dir /a for Windows and ls –a for Linux and macOS).

Score: 196.6

26. T1190: Exploit Public-Facing Application

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

Score: 193.7

27. T1003: OS Credential Dumping

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password. Credentials can be obtained from OS caches, memory, or structures. Credentials can then be used to perform Lateral Movement and access restricted information.

Score: 192.9

28. T1056.001: Input Capture: Keylogging

Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when OS Credential Dumping efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. In order to increase the likelihood of capturing credentials quickly,

an adversary may also perform actions such as clearing browser cookies to force users to reauthenticate to systems.

Score: 192.2

29. T1046: Network Service Discovery

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.

Score: 182.7

30. T1497.001: Virtualization/Sandbox Evasion: System Checks

Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors.

Score: 177.7

31. T1543.003: Create or Modify System Process: Windows Service

Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions. Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.

Score: 176.7

32. T1012: Query Registry

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

Score: 171.4

33. T1489: Service Stop

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.

Score: 167

34. T1135: Network Share Discovery

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

Score: 164.9

35. T1566: Phishing

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Score: 161.2

36. T1005: Data from Local System

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.

Score: 153.5

37. T1566.001: Phishing: Spearphishing Attachment

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

Score: 150

38. T1497: Virtualization/Sandbox Evasion

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors.

Score: 149

39. T1113: Screen Capture

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as CopyFromScreen, xwd, or screencapture.

Score: 137.4

40. T1087.002: Account Discovery: Domain Account

Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior such as targeting specific accounts which possess particular privileges.

Score: 135

41. T1518.001: Software Discovery: Security Software Discovery

Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. This may include things such as cloud monitoring agents and anti-virus. Adversaries may use the information from Security Software Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Score: 134.4

42. T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control

Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.

Score: 133.4

43. T1055.012: Process Injection: Process Hollowing

Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Process hollowing is a method of executing arbitrary code in the address space of a separate live process.

Score: 127.2

44. T1570: Lateral Tool Transfer

Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e., Ingress Tool Transfer) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation.

Score: 126.2

45. T1059.005: Command and Scripting Interpreter: Visual Basic

Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as Component Object Model and the Native API through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.

Score: 126

46. T1133: External Remote Services

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.

Score: 125.8

47. T1555: Credentials from Password Stores

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Score: 124.1

48. T1622: Debugger Evasion

Adversaries may employ various means to detect and avoid debuggers. Debuggers are typically used by defenders to trace and/or analyze the execution of potential malware payloads.

Score: 123.7

49. T1560.001: Archive Collected Data: Archive via Utility

Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to compress, encrypt, or otherwise package data into a format that is easier/more secure to transport.

Score: 122.1

50. T1071: Application Layer Protocol

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Score: 120.2

7. Sources

- https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
- https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q2-2024-threat-landscape-report-threat-actors-ransomware-cloud-risks-accelerate
- https://www.avast.com/c-new-computer-viruses
- https://www.gendigital.com/blog/news/innovation/q2-2024-threat-report
- https://blog.checkpoint.com/research/july-2024s-most-wanted-malware-remcos-and-ransomhub-run-rampant/
- https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-groups
- https://blog.checkpoint.com/research/june-2024s-most-wanted-malware-ransomhub-takes-top-spot-as-most-prevalent-ransomware-group-in-wake-of-lockbit3-decline/
- https://securelist.com/it-threat-evolution-q2-2024-pc-statistics/113683/
- https://go.recordedfuture.com/hubfs/reports/cta-2024-0910.pdf
- https://blog.checkpoint.com/research/august-2024s-most-wanted-malware-ransomhub-reigns-supreme-while-meow-ransomware-surges/
- https://cyberint.com/blog/research/ransomware-trends-2024-report/
- https://www.globalsecuritymag.fr/january-2024-s-most-wanted-malware-major-vextrio-broker-operation-uncovered-and.html
- https://spycloud.com/resource/2024-malware-ransomware-defense-report/
- https://www.reliaquest.com/blog/q3-2024-ransomware/
- https://www.cyfirma.com/research/tracking-ransomware-august-2024/
- https://attack.mitre.org/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a
- https://any.run/cybersecurity-blog/cryptbot-infostealer-malware-analysis/
- https://www.fortinet.com/blog/threat-research/deconstructing-an-evasive-formbook-campaign-leveraging-covid-19-themes
- https://www.cyfirma.com/research/lumma-stealer-tactics-impact-and-defense-strategies/
- https://blog.netmanageit.com/content/files/2023/12/Report-New-MetaStealer-malvertising-campaigns.pdf
- https://threats.kaspersky.com/en/threat/Trojan-Dropper.Win32.Phorpiex.gt/
- https://malware.news/t/threat-analysis-unit-tau-threat-intelligence-notification-ramnit-banking-trojan/34825
- https://www.cyfirma.com/research/redline-stealer-a-new-variant-surfaces-deploying-using-batch-script/
- https://blogs.blackberry.com/en/2024/06/threat-analysis-insight-risepro-information-stealer
- https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/
- https://brandefense.io/blog/ransomware/stop-djvu-ransomware-analysis/

- https://darktrace.com/blog/a-surge-of-vidar-network-based-details-of-a-prolific-info-stealer
- https://tria.ge/240705-c7mmzs1amk
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
- https://www.vectra.ai/threat-actors/cicada3301
- https://socradar.io/dark-web-profile-meow-ransomware/
- https://socradar.io/dark-web-profile-noescape-ransomware/
- https://socradar.io/dark-web-profile-qilin-agenda-ransomware/
- https://www.trendmicro.com/en_us/research/24/c/multistage-ra-world-ransomware.html
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
- https://socradar.io/threat-actor-profile-siegedsec/
- https://socradar.io/dark-web-profile-usersec/