BLACK CELL
Protecting critical infrastructures

# Annual Threat Intelligence based Retrospective TTP report for 2023

# 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.

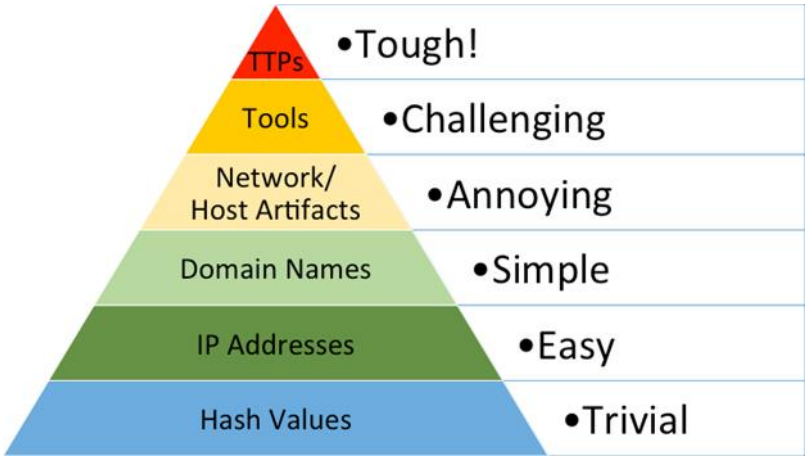


*Figure 2: The Pyramid of Pain*

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. **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

2. **Impacket**:

- **Description**: Impacket is an open-source collection of Python modules used for programmatically constructing and manipulating network protocols. It includes tools for remote service execution, Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks.
- **Scores**:
    - Impact: 3
    - Evasion: 4
    - Complexity: 4
    - Successfulness: 3
    - Accuracy: 1.1

3. **Gootloader**:

- **Description**: Gootloader is a type of malware responsible for distributing various payloads, including ransomware. It uses complex evasion techniques and is moderately successful in compromising systems.
- **Scores**:
    - Impact: 2
    - Evasion: 4
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 0.8

4. **Mimikatz**:

- **Description**: Mimikatz is a powerful post-exploitation tool that specializes in stealing credentials and access tokens from Windows operating systems. It's widely used by attackers to escalate privileges and maintain access to compromised systems.
- **Scores**:
    - Impact: 3
    - Evasion: 4
    - Complexity: 4
    - Successfulness: 3
    - Accuracy: 1.0

5. **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: 2
    - Evasion: 5
    - Complexity: 4
    - Successfulness: 4
    - Accuracy: 1.3

6. **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

7. **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: 4
    - Complexity: 4
    - Successfulness: 4
    - Accuracy: 1.1

8. **BloodHound**:

- **Description**: BloodHound is a tool used for Active Directory reconnaissance. While not inherently malicious, it can aid attackers in identifying vulnerabilities and lateral movement paths within a network.
- **Scores**:
    - Impact: 2
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.0

9. **Gamarue**:

- **Description**: Gamarue is a worm that spreads through removable drives and network shares. It has been used for various malicious purposes, including the distribution of other malware.
- **Scores**:
    - Impact: 3
    - Evasion: 2
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 0.8

10. **Yellow Cockatoo**:

- **Description**: Yellow Cockatoo is an activity cluster involving a remote access trojan (RAT) that filelessly delivers various other malware modules.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 2
    - Successfulness: 3
    - Accuracy: 0.9

11. **Emotet**:

- **Description**: Emotet is a prominent malware strain primarily used as a delivery mechanism for other types of malware, such as ransomware and information stealers. It has been a significant threat in the past.
- **Scores**:
    - Impact: 3
    - Evasion: 4
    - Complexity: 4
    - Successfulness: 4
    - Accuracy: 1.2

12. **PlugX**:

- **Description**: PlugX is a remote access trojan (RAT) commonly associated with cyber espionage campaigns. It provides attackers with control over compromised systems and the ability to steal sensitive information.
- **Scores**:
    - Impact: 4
    - Evasion: 4
    - Complexity: 4
    - Successfulness: 4
    - Accuracy: 1.2

13. **BloodAlchemy**:

- **Description**: BLOODALCHEMY is an x86 backdoor written in C and found as shellcode injected into a signed benign process. It was discovered in our analysis and is part of the REF5961 intrusion set
- **Scores**:
    - Impact: 2
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 2
    - Accuracy: 1.2

14. **RagnarLocker**:

- **Description**: RagnarLocker is a type of ransomware known for encrypting a victim's files and demanding a ransom for their decryption. It has been used in various cyber attacks and data extortion incidents.
- **Scores**:
    - Impact: 3
    - Evasion: 2
    - Complexity: 2
    - Successfulness: 3
    - Accuracy: 1.0

15. **Akira Ransomware**:

- **Description**: Akira Ransomware is a type of malicious software that encrypts a victim's data, rendering it inaccessible until a ransom is paid to the attackers for a decryption key.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.0

16. **ALPHV 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: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.0

17. **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

18. **Casper Stealer**:

- **Description**: Casper Stealer is a malware designed to steal sensitive information from infected systems. This information can include login credentials, payment data, and other valuable details.
- **Scores**:
    - Impact: !
    - Evasion: !
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.0

19. **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: 2
    - Evasion: 2
    - Complexity: 2
    - Successfulness: 2
    - Accuracy: 0.9

22. **Fletchen Stealer**:

- **Description**: Fletchen Stealer is a type of malware designed to steal sensitive data from compromised systems. This stolen data can be used for malicious purposes.
- **Scores**:
    - Impact: 2
    - Evasion: 2
    - Complexity: 2
    - Successfulness: 2
    - Accuracy: 0.9

23. **Lapsus$ Ransomware**:

- **Description**: Lapsus$ Ransomware is a variant of ransomware known for encrypting files and demanding a ransom payment in cryptocurrency for decryption.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.0

27. **SwiftSpy**:

- **Description**: SwiftSpy is permutation of Swift-Keylogger which is a macOS keylogger.
- **Scores**:
    - Impact: 3
    - Evasion: 2
    - Complexity: 2
    - Successfulness: 2
    - Accuracy: 0.9

28. **Nightmangle**:

- **Description**: Nightmangle highlights the versatility of Telegram as a C2 server for communication between attackers and their target clients in a covert and effective manner. Telegram's suitability for this purpose is underpinned by several advantages.
- **Scores**:
    - Impact: 2
    - Evasion: 4
    - Complexity: 3
    - Successfulness: 4
    - Accuracy: 1.2

29. **ZenRAT (Zen Remote Access Trojan)**:

- **Description**: ZenRAT is a type of remote access Trojan used by cybercriminals to gain unauthorized access to victims' systems and steal sensitive information.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.0

30. **Kinsing**:

- **Description**: Kinsing is malware known for targeting cloud environments and abusing them for cryptocurrency mining without authorization.
- **Scores**:
    - Impact: 3
    - Evasion: 4
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.1

31. **Vega Stealer**:

- **Description**: Vega Stealer malware contains stealing functionality targeting saved credentials and credit cards in the Chrome and Firefox browsers, as well as stealing sensitive documents from infected computers.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.0

32. **INC. Ransomware**:

- **Description**: Inc. ransomware is a multi-extortion operation, stealing victim data and threatening to leak said data online should the victim fail to comply with their demands.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.0

33. **Nagogy Grabber**:

- **Description**: Nagogy Grabber is a powerful virus that steals passwords, credit cards, cookies, browsing history from 20+ browsers and apps. It also targets anti-virus software, takes screenshots, captures Roblox cookies, Wi-Fi passwords, system info. Comes with a cool HTML UI and is fully undetectable (FUD).
- **Scores**:
    - Impact: 3
    - Evasion: 2
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 0.9

35. **BumbleBee Loader**:

- **Description**: The Bumblebee malware loader appeared in September 2021 and surged in popularity in late March 2022. This uptick came after threat actors who previously distributed a loader known as BazarLoader shifted their focus to Bumblebee (a compilation of vendor reports and resources related to Bumblebee can be found on Malpedia).
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 0.9

36. **Nobit**:

- **Description** NoBit RAAS builder, the malicious software is being promoted by an elusive threat actor and is being called the “hottest product” on the dark web.
- **Scores**:
    - Impact: 4
    - Evasion: 2
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 0.8
    -

37. **Sphynx**

- **Description**: Sophos discovered the Sphynx variant in March 2023 during an investigation into a data breach that shared similarities with another attack described in an IBM-Xforce report published in May (the ExMatter tool was used to extract the stolen data in both instances).
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 2
    - Successfulness: 3
    - Accuracy: 1

38. **Caro-Kann:**

- **Description**: Evading Kernel Scans with Encrypted Shellcode. In the ever-evolving game of cybersecurity, encrypted shellcode injection emerges as a formidable method to sidestep defenses.
- **Scores**:
    - Impact: 2
    - Evasion: 2
    - Complexity: 2
    - Successfulness: 3
    - Accuracy: 0.8

40. **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: 2
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 2
    - Accuracy: 0.7

41. **TeamsPhisher**:

- **Description**: A weakness has been discovered in Microsoft Teams that allows attackers to deliver malicious files to users if Microsoft Teams is configured to allow external parties to establish chat. There is a simple fix for the exploit called TeamsPhisher. Businesses should disable external access and allow only trusted domains to initiate chats from external parties, as by default, when Microsoft Teams is configured to enable external access, it allows access to anyone.
- **Scores**:
    - Impact: 2
    - Evasion: 2
    - Complexity: 2
    - Successfulness: 2
    - Accuracy: 0.8

42. **SeroXen**:

- **Description**: SeroXen is a fileless Remote Access Trojan (RAT) that excels in evading detection through both static and dynamic analysis methods. The malware incorporates various open-source projects, including Quasar RAT, r77-rootkit, and the command line tool NirCmd, to enhance its functionalities and capabilities.
- **Scores**:
    - Impact: 3
    - Evasion: 4
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.3

43. **SocketSilence**:

- **Description**: SocketSilence advertised the source code for a Google Chrome malware loader on the predominantly Russian language Deep Web forum "XSS." The loader allows threat actors to install malicious Chrome extensions on target machines running 64-bit architecture versions of Windows 10 or 11. The generated payloads do not require any interaction from the victims to execute.
- **Scores**:
    - Impact: 4
    - Evasion: 5
    - Complexity: 4
    - Successfulness: 4
    - Accuracy: 1.4

## 3.2. Most active threat actors

1. **Grayling**:

- **Description**: A previously unknown threat actor used custom malware and multiple publicly available tools to target a number of organizations in the manufacturing, IT, and biomedical sectors in Taiwan.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 4
    - Successfulness: 2
    - Accuracy: 1.0

2. **Darkhalo**

- **Description**: Dark Halo started its malicious operations at the end of 2019. The group launched several attacks against the unnamed US think tank to steal the emails of its senior executives. Presumably, Dark Halo searched for valuable data to enhance further reconnaissance operations against major US vendors and governmental organizations.
- **Scores**:
    - Impact: 5
    - Evasion: 4
    - Complexity: 4
    - Successfulness: 4
    - Accuracy: 0.7

3. **Cuba Ransomware Gang**:

- **Description**: The Cuba Ransomware Gang is a group of cybercriminals who specialize in ransomware attacks. They are known for encrypting victims' data and demanding ransoms for decryption.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.2

4. **Medusa Ransomware Group**:

- **Description**: The Medusa Ransomware Group is an organized cybercriminal entity known for deploying the MedusaLocker ransomware, which encrypts victims' files and demands payment for decryption.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 4
    - Successfulness: 3
    - Accuracy: 1.2

5. **Ragnar Locker Group**:

- **Description**: The Ragnar Locker Group is responsible for the RagnarLocker ransomware, which encrypts files and demands a ransom for decryption. They have been involved in various high-profile attacks.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 4
    - Accuracy: 1.2

6. **Akira Ransomware Group**:

- **Description**: The Akira Ransomware Group is responsible for the Akira ransomware, which follows the typical ransomware model of encrypting files and demanding ransoms for decryption.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.2

7. **Lapsus$ Ransomware**:

- **Description**: Lapsus$ Ransomware is not a group but rather a ransomware strain. It encrypts data and demands a ransom from victims for the release of their files.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.2

8. **ALPHV Ransomware Group**:

- **Description**: The ALPHV Ransomware Group is responsible for deploying the ALPHV ransomware, which encrypts victims' files and demands ransoms for decryption.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.2

9. **INC Ransomware Group**:

- **Description**: The INC Ransomware Group is responsible for a ransomware variant that follows the common pattern of encrypting files and demanding ransoms for decryption.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.2

10. **BianLian Ransomware Group**:

- **Description**: The BianLian Ransomware Group is another cybercriminal entity that operates ransomware. They encrypt victims' data and seek payments for decryption.
- **Scores**:
    - Impact: 3
    - Evasion: 3
    - Complexity: 3
    - Successfulness: 3
    - Accuracy: 1.2

11. **MoustachedBouncer**:

- **Description**: MoustachedBouncer's activities indicated a well-coordinated and persistent effort to gather intelligence, revealing their advanced capabilities and strategic interests.
- **Scores**:
    - Impact: 4
    - Evasion: 4
    - Complexity: 5
    - Successfulness: 5
    - Accuracy: 1.4

12. **NoEscape Ransomware Group**:

- **Description**: NoEscape ransomware group, also known as N0_Esc4pe, intensified its cyber-attack activities, targeting key sectors globally.
- **Scores**:
    - Impact: 4
    - Evasion: 3
    - Complexity: 4
    - Successfulness: 4
    - Accuracy: 1.4

# 4. Scores

The following scores were assigned to each cyber threat:

| Threat/Threat Actor | Impact | Evasion | Complexity | Successfulness | Accuracy | Sum |
|---|---|---|---|---|---|---|
| Qbot | 4 | 3 | 4 | 4 | 1.2 | 19.2 |
| Impacket | 3 | 4 | 4 | 3 | 1.1 | 15.8 |
| Gootloader | 2 | 4 | 3 | 3 | 0.8 | 7.7 |
| Mimikatz | 3 | 2 | 3 | 3 | 1.0 | 11.0 |
| SocGholish | 2 | 5 | 4 | 4 | 1.3 | 27.3 |
| Raspberry Robin | 3 | 3 | 4 | 3 | 1.0 | 18.0 |
| Cobalt Strike | 4 | 4 | 4 | 4 | 1.1 | 21.1 |
| BloodHound | 2 | 3 | 3 | 3 | 1.0 | 12.0 |
| Gamarue | 3 | 2 | 3 | 3 | 0.8 | 8.6 |
| Yellow Cockatoo | 3 | 3 | 2 | 3 | 0.9 | 7.2 |
| Emotet | 3 | 4 | 4 | 4 | 1.2 | 19.2 |
| PlugX | 4 | 4 | 4 | 4 | 1.2 | 25.9 |
| BloodAlchemy | 2 | 3 | 3 | 2 | 1.2 | 9.6 |
| RagnarLocker | 4 | 3 | 3 | 3 | 1.0 | 10.0 |
| Akira Ransomware | 3 | 2 | 3 | 2 | 1.0 | 10.0 |
| ALPHV Ransomware | 3 | 3 | 3 | 3 | 1.0 | 9.0 |
| Remcos RAT | 3 | 3 | 4 | 3 | 1.0 | 10.0 |
| Casper Stealer | 4 | 4 | 3 | 3 | 1.0 | 14.0 |
| XMRig Miner | 2 | 2 | 2 | 2 | 0.9 | 3.2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Fletchen Stealer | 2 | 2 | 2 | 2 | 0.9 | 3.2 |
| Lapsus$ Ransomware | 3 | 4 | 3 | 3 | 1.2 | 12.9 |
| SwiftSpy | 3 | 2 | 2 | 2 | 0.9 | 7.6 |
| Nightmangle | 2 | 4 | 3 | 4 | 1.2 | 19.2 |
| ZenRAT | 3 | 3 | 3 | 3 | 1.0 | 9.0 |
| Kinsing | 3 | 4 | 3 | 3 | 1.1 | 11.9 |
| Vega Stealer | 3 | 3 | 3 | 3 | 1.0 | 9.0 |
| INC. Ransomware | 3 | 3 | 3 | 3 | 1.0 | 9.0 |
| Nagogy Grabber | 3 | 2 | 3 | 3 | 0.9 | 7.2 |
| BumbleBee Loader | 3 | 3 | 3 | 3 | 0.9 | 7.3 |
| Nobit | 4 | 2 | 3 | 3 | 0.8 | 7.7 |
| Sphynx | 3 | 3 | 2 | 3 | 1.0 | 9.0 |
| Caro-Kann | 2 | 2 | 2 | 3 | 0.8 | 4.8 |
| Darkgate | 2 | 3 | 3 | 2 | 0.7 | 2.9 |
| TeamsPhisher | 2 | 2 | 2 | 2 | 0.8 | 2.5 |
| SeroXen | 3 | 4 | 3 | 3 | 1.3 | 18. |
| SocketSilence | 3 | 3 | 4 | 4 | 1.0 | 14 |
| Grayling | 3 | 3 | 4 | 2 | 1.0 | 12.0 |
| Darkhalo | 5 | 4 | 4 | 4 | 0.7 | 13.3 |
| Cuba Ransomware Gang | 3 | 3 | 3 | 3 | 1.2 | 13 |
| Medusa Ransomware Group | 3 | 3 | 4 | 3 | 1.2 | 14.4 |
| Ragnar Locker Group | 3 | 3 | 3 | 4 | 1.2 | 14.4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Akira Ransomware Group | 3 | 3 | 3 | 3 | 1.2 | 12.9 |
| Lapsus$ Ransomware | 3 | 3 | 3 | 3 | 1.2 | 12.9 |
| ALPHV Ransomware Group | 3 | 3 | 3 | 3 | 1.2 | 13 |
| INC Ransomware Group | 3 | 3 | 3 | 3 | 1.2 | 13 |
| BianLian Ransomware Group | 3 | 3 | 3 | 3 | 1.2 | 13 |
| MoustachedBouncer | 4 | 4 | 5 | 5 | 1.4 | 56.0 |
| NoEscape Ransomware Group | 4 | 3 | 4 | 4 | 1.4 | 33.6 |

## 4.1. Other high profile TTPs

In our recent detections, we observed that several adversarial techniques were closely associated with incidents some of these were involved in 0 day. These techniques, including T1055 (Process Injection), T1217 (Browser Bookmark Modification), and T1555.003 (Web Shell), 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 0-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 0-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 of their relevance.

| Technique ID | Score | Technique ID | Score |
|---|---|---|---|
| T1059.003 | 56 | T1112 | 20 |
| T1059.001 | 49.6 | T1553.001 | 20 |
| T1047 | 43.7 | T1553.005 | 20 |
| T1555.003 | 42 | T1548.001 | 20 |
| T1217 | 37 | T1021.002 | 20 |
| T1027 | 34 | T1621 | 20 |
| T1082 | 33 | T1105 | 12 |
| T1552.001 | 33 | T1033 | 9 |
| T1055 | 29 | T1622 | 9 |
| T1569.002 | 27 | T1203 | 7 |
| T1106 | 26 | T1071.001 | 7 |
| T1587.001 | 26 | T1592.001 | 7 |
| T1115 | 22 | T1546.015 | 4 |
| T1560 | 22 | T1574.002 | 4 |
| T1057 | 22 | T1001 | 4 |
| T1036.003 | 20 | - | - |

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 to this sector, while green techniques are less severe.

https://github.com/blackcellltd/Heatmaps/blob/07f8f6e1c275741f6eccb39c093aec27008c1ff1/annual_ti_based_retrospective_ttp_report__2023.json

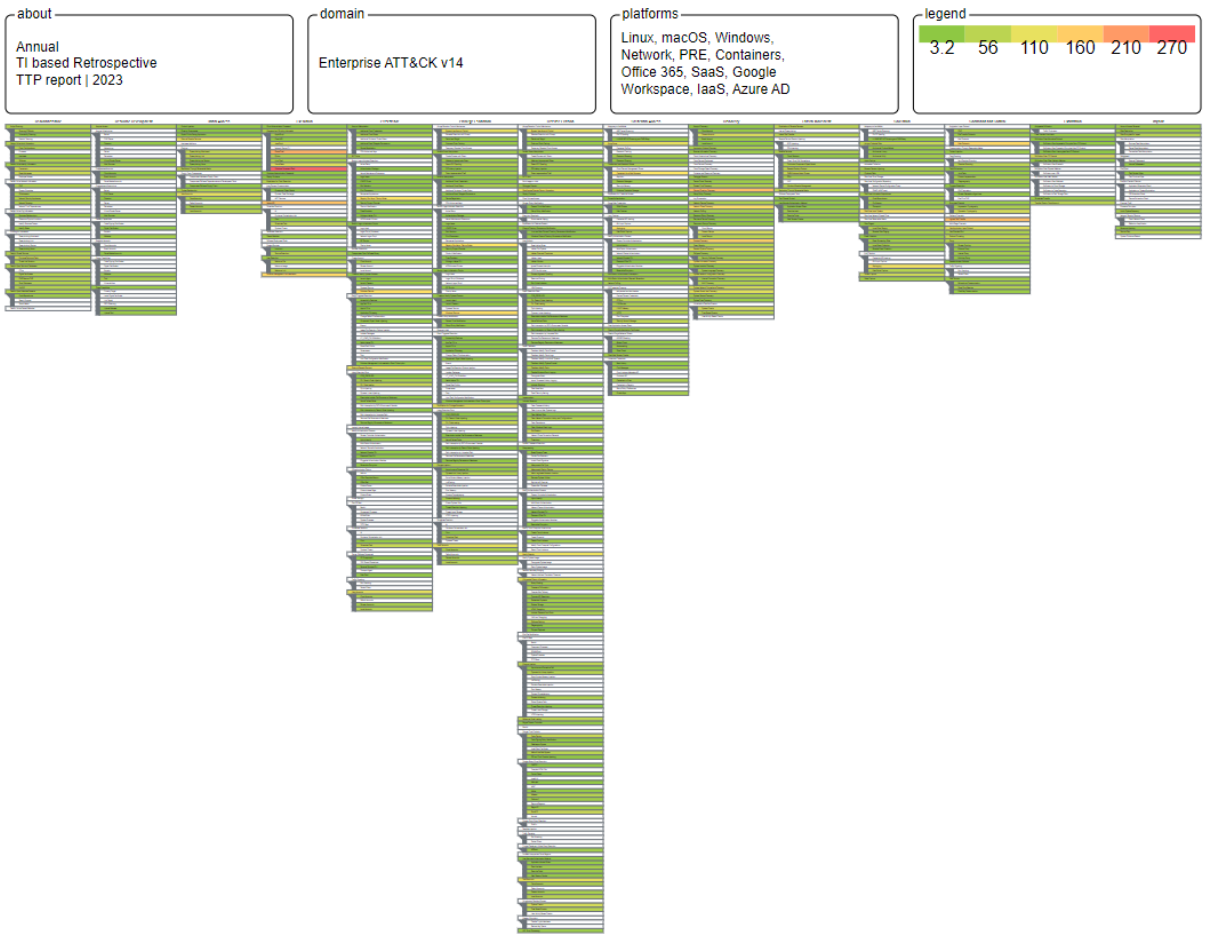


*Figure 1: Annual_TI_based_Retrospective_TTP_report_heatmap*

# 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 201 techniques and 424 Sub-techniques exist, we need to prioritize them in a descending order based on their score. For detection engineering purposes, we defined the baseline at 60 points. This mean that that we need to cover, have visibility, proper date source, detection rules and playbook for all these techniques and sub-techniques. Most of the followings have multiple procedure.

1. **T1059: 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:266.9

2. **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:186.7

3. **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:173.6

4. **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:173.4

5. **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: 168.3

6. **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. 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:153.9

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:148.6

8. **T1047: Windows Management Instrumentation**
   Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by Remote Services such as Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM). Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS

   Score: 145.2

9. **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.[1] Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.

   Score:141.6

10. **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:138

11. **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.[1] These programs will be executed under the context of the user and will have the account's associated permissions level.

    Score:133.2

**12. T1555.003: Credentials from Password Stores: Credentials from Web Browsers**

Adversaries may acquire credentials from web browsers by reading files specific to the target browser.[1] Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.

Score:132.8

**13. 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:122

**14. 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: 112.2

**15. 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. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility Reg may be used for local or remote Registry modification. [1] Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API.

Score: 110.9

16. **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: 107.9

17. **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:107.8

18. **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.[1] 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: 104.5

19. **T1110: Brute Force**

    Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

    Score:103.5

**20. 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:95.6

**21. T1095: Non-Application Layer Protocol**

Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

Score:94.6

**22. 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:95.5

**23. 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:94.1

24. **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:92.7

25. **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:90.6

26. **T1069.002: Permission Groups Discovery: Domain Groups**
    Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.

    Score:88.8

27. **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:88.8

28. **T1059.007: Command and Scripting Interpreter: JavaScript**
    Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.

    Score: 87.6

29. **T1589.001: Gather Victim Identity Information: Credentials**

    Adversaries may gather credentials that can be used during targeting. Account credentials gathered by adversaries may be those directly associated with the target victim organization or attempt to take advantage of the tendency for users to use the same passwords across personal and business accounts.

    Score: 87

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: 86

31. **T1573.001: Encrypted Channel: Symmetric Cryptography**

    Adversaries may employ a known symmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Symmetric encryption algorithms use the same key for plaintext encryption and ciphertext decryption. Common symmetric encryption algorithms include AES, DES, 3DES, Blowfish, and RC4.

    Score:84.2

32. **T1049: System Network Connections Discovery**

    An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate. Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services.

    Score:79.2

**33. T1003.001: OS Credential Dumping: LSASS Memory**

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

Score:76.7

**34. 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: 76.6

**35. 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:76.3

**36. T1574.002: Hijack Execution Flow: DLL Side-Loading**

Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to DLL Search Order Hijacking, side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s).

Score:74.7

37. **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:74.5

38. **T1597.002: Search Closed Sources: Purchase Technical Data**
    Adversaries may purchase technical information about victims that can be used during targeting. Information about victims may be available for purchase within reputable private sources and databases, such as paid subscriptions to feeds of scan databases or other data aggregation services. Adversaries may also purchase information from less-reputable sources such as dark web or cybercrime blackmarkets.

    Score:73.8

39. **T1589.002: Gather Victim Identity Information: Email Addresses**
    Adversaries may gather email addresses that can be used during targeting. Even if internal instances exist, organizations may have public-facing email infrastructure and addresses for employees.

    Score:73.8

40. **T1021.002: Remote Services: SMB/Windows Admin Shares**
    Adversaries may use Valid Accounts to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user. SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba.e Services: SMB/Windows Admin Shares

    Score: 73.5

41. **T1053.005: Scheduled Task/Job: Scheduled Task**
    Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The schtasks utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task.

    Score: 69.6

**42. T1566.002: Phishing: Spearphishing Link**

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

Score: 68.3

**43. 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:64.6

**44. 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: 63

**45. 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: 61.9

**46. T1003.002: OS Credential Dumping: Security Account Manager**

Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. The SAM is a database file that contains local accounts for the host, typically those found with the net user command. Enumerating the SAM database requires SYSTEM level access.

Score: 61.1

**47. T1572: Protocol Tunneling**

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet.

Score:60.4

# 7. Sources


- https://www.picussecurity.com/resource/blog/key-threat-actors-malware-and-exploited-vulnerabilities-august-2023
- https://otx.alienvault.com/
- https://socradar.io/dark-web-profile-medusa-ransomware-medusalocker/
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks
- https://www.zerofox.com/blog/the-underground-economist-volume-3-issue-20/
- https://top-attack-techniques.mitre-engenuity.org/
- https://redcanary.com/threat-detection-report/techniques/
- https://redcanary.com/threat-detection-report/threats/
- https://attack.mitre.org
- https://top-attack-techniques.mitre-engenuity.org/
- https://www.trendmicro.com/en_nl/research/23/f/seroxen-mechanisms-exploring-distribution-risks-and-impact.html
- https://www.elastic.co/security-labs/disclosing-the-bloodalchemy-backdoor
- https://socradar.io/nightmangle-telegram-c2-agent-and-new-fud-crypter-with-windows-defender-bypass/
- https://www.proofpoint.com/us/threat-insight/post/new-vega-stealer-shines-brightly-targeted-campaign
- https://www.sentinelone.com/anthology/inc-ransom/
- https://dreamyoak.xyz/
- https://connect.fidelissecurity.com/rs/884-ZRZ-648/images/Fidelis%20TRT%20Threat%20Intelligence%20Summary%202020%20December.pdf
- https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/
- https://www.data3.com/knowledge-centre/blog/microsoft-teamsphisher-exploit-alert/
- https://malpedia.caad.fkie.fraunhofer.de/details/win.darkgate
- https://www.bleepingcomputer.com/news/security/blackcat-ransomware-hits-azure-storage-with-sphynx-encryptor/
- https://thecyberexpress.com/nobit-raas-new-generation-ransomware-builder/