BLACK CELL
Protecting critical infrastructures

WHITEPAPER

# THREAT INTELLIGENCE BASED RETROSPECTIVE TTP REPORT FOR 2025

## A Data-Driven Review of the 2025 Threat Landscape and Adversary Tactics

**Created by**

Zsófia Uszkay | Threat Intelligence Analyst

August 2026

# TABLE OF CONTENTS


**INTRODUCTION** 3
- LEVERAGING ANNUAL THREAT INTELLIGENCE INSIGHTS
- ANALYSIS OF ADVERSARY TTPS

**METHODOLOGY** 7

**DATASETS** 10
- MOST EMERGING MALWARE
- MOST ACTIVE THREAT ACTORS

**SCORES** 41

**HEATMAPS** 45

**RESULTS** 46
- TOP TECHNIQUES AND SUB-TECHNIQUES
- OTHER HIGH PROFILE TTPS

**SOURCES** 67

01

# 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.

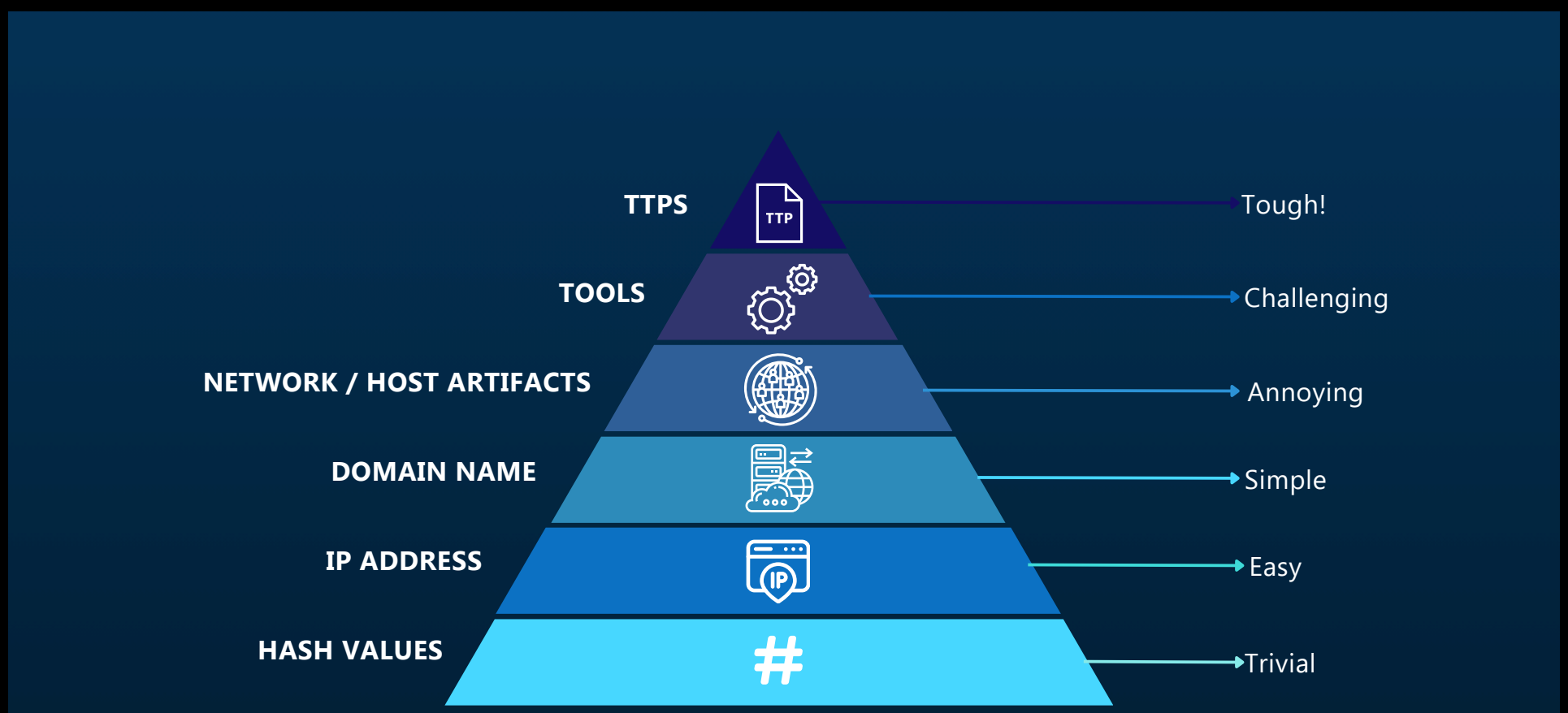



Figure 1: The Pyramid of Pain

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.

02

# 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 malware
- 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 malware and tools that were used. These threat profiles may contain exploitation tools, malware, 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 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 malware, threat actors, adversarial frameworks, AI threats and other high profile TTPs.
2. Gather all available information about the incidents.
3. Pinpoint the tools or malware that were used.
4. Determine and/or extract attack procedures and methodologies that were used.
5. Map this information to ATT&CK techniques.
6. Identify the threat actors (APT, criminal groups) and build a threat profile.
7. Collect information about their tools and attack procedures.
8. Map this information to ATT&CK techniques.
9. Determine the inadequacies of the victim.
10. 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.

03

# DATASETS

## 3.1. MOST EMERGING MALWARE

### 3.1.1. 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:** 3
- **Complexity:** 3
- **Successfulness:** 3
- **Accuracy:** 1.3

### 3.1.2. AMADEY

**Description:** Amadey is a modular botnet primarily targeting Windows systems, capable of executing a wide range of malicious functions such as data theft, malware deployment, and unauthorized network access. Discovered in 2018, it typically spreads through phishing campaigns, malicious ads, and infected files. Once established on a host, Amadey enables attackers to exfiltrate sensitive information, deliver additional payloads such as Trojans, and perform distributed denial-of-service (DDoS) attacks.

**Scores:**

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

### 3.1.3. 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: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.0

### 3.1.4. ASYNCRAT

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

### 3.1.5. BLACKLOCK

**Description:** BlackLock is a ransomware strain first detected in March 2024. It operates under a Ransomware-as-a-Service (RaaS) model and utilizes a double extortion technique, encrypting victim data while exfiltrating sensitive information for additional leverage. The ransomware is capable of infecting Windows, VMware ESXi, and Linux systems, and has been observed impacting organizations across a wide range of industries and regions.

**Scores:**

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 0.8

### 3.1.6. CLEARFAKE

**Description:** ClearFake is a malicious JavaScript framework injected into compromised websites to distribute additional malware through drive-by downloads. It relies heavily on social engineering, deceiving users into executing fake web browser updates that lead to system compromise

**Scores:**

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

### 3.1.7. 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: 1.5

### 3.1.8. 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

### 3.1.9. EMMENHTAL

**Description:** Emmenhtal is a malicious loader observed since early 2024. It is an obfuscated, multistage payload that uses the LOLBIN mshta.exe to execute an initial HTA stage containing malicious JavaScript. That JavaScript decodes and runs a PowerShell script, which in turn decrypts an obfuscated PowerShell loader that ultimately downloads and launches final-stage stealers and commodity RATs.

**Scores:**

- Impact: 2
- Evasion: 2
- Complexity: 2
- Successfulness: 2
- Accuracy: 0.7

### 3.1.10. FOG

**Description:** Fog ransomware surfaced in April 2024 and targets both Windows and Linux environments. The operation combines encryption with data extortion and operates a TOR-hosted data-leak site to list victims and publish stolen data when ransoms are not paid.

**Scores:**

- Impact: 2
- Evasion: 2
- Complexity: 2
- Successfulness: 2
- Accuracy: 0.7

### 3.1.11. 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: 3
- Successfulness: 3
- Accuracy: 1.3

### 3.1.12. HIJACKLOADER

**Description:** HijackLoader employs advanced evasion tactics such as Process Doppelgänging, DLL Search Order Hijacking, and the Heaven's Gate technique to bypass security defenses. Its payload is often embedded within the IDAT chunk of PNG image files, enabling stealthy delivery and execution on infected systems.

**Scores:**

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

### 3.1.13. INTERLOCK

**Description:** Interlock is a ransomware variant first observed in late 2024 that gained significant activity throughout 2025. It is distributed through opportunistic attacks involving compromised websites and multi-stage social engineering techniques. Unlike many Ransomware-as-a-Service (RaaS) variants, Interlock is operated privately without affiliates. It employs a double extortion model - encrypting victim data and threatening public exposure of stolen information via its dedicated leak site - to pressure victims into paying ransoms.

**Scores:**

- Impact: 2
- Evasion: 2
- Complexity: 2
- Successfulness: 2
- Accuracy: 0.7

### 3.1.14. LOCKBIT

**Description:** LockBit ransomware first emerged in September 2019 and has since evolved through several versions, with LockBit 4.0 and 5.0 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: 5
- Evasion: 4
- Complexity: 4
- Successfulness: 5
- Accuracy: 1.5

### 3.1.15. 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: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.3

### 3.1.16. MIRAI

**Description:** Mirai is one of the earliest and most notable botnets designed to compromise internet-exposed networking devices running Linux. The botnet primarily targets a wide array of networked embedded systems - including IP cameras, home routers from numerous vendors, and various Internet of Things (IoT) devices - to build large-scale networks used for distributed denial-of-service (DDoS) attacks.

**Scores:**

- Impact: 3
- Evasion: 2
- Complexity: 2
- Successfulness: 4
- Accuracy: 1.5

### 3.1.17. 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: 3
- Accuracy: 1.2

### 3.1.18. NETSUPPORT RAT

**Description:** NetSupport Manager, a legitimate remote administration tool, has been repurposed by threat actors as a Remote Access Trojan (RAT) to carry out malicious operations. Over time, multiple campaigns leveraging the tool have been observed, each iteration refining its evasion capabilities through successive layers of obfuscation and stealth techniques to avoid detection and improve persistence.

**Scores:**

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

### 3.1.19. 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: 3
- Accuracy: 1.2

### 3.1.20. 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: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.2

### 3.1.21. 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: 3
- Successfulness: 3
- Accuracy: 1.3

### 3.1.22. SNAKE KEYLOGGER

**Description:** Snake Keylogger is a .NET-based modular credential stealer and keylogger first observed in the wild in November 2020. Its capabilities include logging keystrokes, harvesting stored credentials, capturing screenshots, and collecting clipboard contents for exfiltration. Snake Keylogger is typically distributed via phishing and spear-phishing campaigns that include a malicious Office document or PDF attachment. When a recipient opens the document and enables macros or uses a vulnerable Office/PDF reader, an embedded downloader (often a PowerShell-based dropper) retrieves and executes the Snake Keylogger payload on the system.

**Scores:**

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

### 3.1.23. 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: 3
- Accuracy: 1.3

### 3.1.24. 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: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.2

### 3.1.25. VENOMRAT

**Description:** VenomRAT is a Remote Access Trojan (RAT) capable of numerous malicious actions, such as file theft, credential collection, keystroke capture, and remote webcam access. Like many RATs, it spreads through social-engineering techniques, including fake software download sites and phishing emails containing malicious attachments or files.

**Scores:**

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

### 3.1.26. 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: 3
- Accuracy: 1.3

### 3.1.27. XWORM

**Description:** XWorm is a widely distributed remote access trojan that has evolved into a flexible, feature-rich tool in cybercriminal arsenals. Its functions range from keylogging and remote desktop access to data exfiltration and arbitrary command execution. XWorm remains popular with threat actors because of its modular design, frequent updates, and ease of use, and is often used against targets in the software supply chain and the gaming industry.

**Scores:**

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

### 3.1.28. ZPHP

**Description:** ZPHP is a JavaScript-based downloader that infects users via fake browser-update pop-ups on compromised websites. When a user clicks the deceptive update prompt, ZPHP can fetch and install additional malware - for example, NetSupport RAT or Lumma Stealer.

**Scores:**

- Impact: 2
- Evasion: 2
- Complexity: 2
- Successfulness: 2
- Accuracy: 0.7

## 3.2. MOST ACTIVE THREAT ACTORS

### 3.2.1 ANDARIEL

**Description:** Andariel is an advanced persistent threat (APT) group linked to North Korea's Reconnaissance General Bureau (RGB), with activity traced to locations such as Pyongyang and Sinuiju. Active since around 2013, Andariel's objectives align with North Korean political and intelligence priorities. The group primarily targets defense, aerospace, nuclear, and engineering organizations for espionage, and has run ransomware operations against U.S. healthcare organizations to generate funding. Tactics include spear-phishing and exploiting web-server vulnerabilities for initial access, followed by system discovery, enumeration, and persistence via web shells and scheduled tasks. They deploy custom malware, RATs, and legitimate open-source tools to move laterally and exfiltrate data.

**Scores:**

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

### 3.2.2. 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: 1.3

### 3.2.3. APT28

**Description:** APT28 - commonly known as Fancy Bear and also tracked as Sofacy, Sednit, or Pawn Storm - is a sophisticated cyber-espionage actor with strong ties to the Russian GRU. First identified over a decade ago, the group continues to target government, military, and corporate entities worldwide. APT28 is notable for its technical sophistication, adaptability, and geopolitical motives, and is known to use bespoke malware families such as Hatvibe and CherrySpy.

**Scores:**

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

### 3.2.4. APT29

**Description:** APT29 is a highly capable, well-resourced cyber-espionage group believed to have operated on behalf of the Russian state since at least 2008. Its primary mission appears to be intelligence collection to support Russian foreign and security policy. APT29 predominantly targets Western governments and affiliated organizations - including ministries, agencies, think tanks, and contractors - but has also conducted operations against CIS countries and targets across Asia, Africa, and the Middle East.

**Scores:**

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

### 3.2.5. APT41

**Description:** Researchers assess APT41 as a China-linked espionage group that pursues financially motivated activity. Active since at least 2012, APT41 has targeted a broad set of industries - including healthcare, telecommunications, technology, finance, education, retail, and the video game sector - across multiple countries.

**Scores:**

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

### 3.2.6. CHAOS RANSOMWARE GROUP

**Description:** Chaos is a recently identified ransomware-as-a-service operation that has quickly increased its activity, carrying out double-extortion campaigns primarily in the United States and with victims also observed in the U.K., India, and New Zealand. The group employs voice phishing for initial access, abuses remote management tools to maintain persistence, and uses a rapid, selective encryption method to disrupt networks. Chaos avoids targets in BRICS/CIS countries and pressures non-paying victims via a public data-leak site, demanding ransoms reported as high as $300,000.

**Scores:**

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

### 3.2.7. DARK STORM TEAM

**Description:** Dark Storm Team is a pro-Palestinian cyber group that specializes in distributed denial-of-service (DDoS) attacks. While their operations are politically motivated, they have also commercialized their capabilities - offering DDoS-for-hire services and selling breached databases - turning ideological attacks into a revenue stream.

**Scores:**

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 0.8

### 3.2.8. DEVMAN

**Description:** DevMan began as an affiliate operating various RaaS families (notably Qilin, APOS, and DragonForce) but has increasingly positioned itself as an independent actor, later claiming its own eponymous ransomware, “DevMan.” The group announced plans to convert that ransomware into a RaaS offering (advertised on its onion DLS site to launch in late June 2025). As a RaaS operator, DevMan promises affiliates up to 90% profit per victim (70% if affiliates use DevMan-provided access). The group publicly states constraints - such as targeting organizations with revenue over $100M or medical-sector targets over $50M - but simultaneously shows lax or contradictory guidance around critical infrastructure, encourages attacks on such targets, and advertises bespoke support and custom builds for targeted operations.

**Scores:**

- Impact: 2
- Evasion: 2
- Complexity: 2
- Successfulness: 2
- Accuracy: 0.7

### 3.2.9. 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: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.0

### 3.2.10. FIN7

**Description:** FIN7 is a financially motivated cybercrime group active since 2013. Historically, FIN7 focused on retail and hospitality sectors - frequently leveraging point- of-sale malware - and used a front company known as Combi Security for some operations. Since 2020, the group has increasingly embraced a big-game-hunting (BGH) approach, deploying ransomware families such as REvil and operating RaaS services like Darkside. FIN7 is sometimes linked to the broader Carbanak ecosystem, though multiple distinct actors have used Carbanak tooling and are therefore tracked separately.

**Scores:**

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

### 3.2.11. FUNKSEC

**Description:** Funksec, also known as Funklocker, is a double-extortion ransomware actor that appeared in late 2024 and claims multiple victims. When it successfully compromises a host, it appends the ".funksec" extension to encrypted files and changes the desktop wallpaper to an image hosted remotely. The malware establishes persistence by creating a scheduled task named "funksec," attempts to disable Windows Defender real-time protection, clears event logs, detects and aborts in virtualized environments, and terminates a wide range of processes including browsers and productivity applications.

**Scores:**

- Impact: 2
- Evasion: 2
- Complexity: 2
- Successfulness: 2
- Accuracy: 0.7

### 3.2.12. 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: 4
- Successfulness: 4
- Accuracy: 1.2

### 3.2.13. KEYMOUS+

**Description:** Keymous+ specializes in high-volume DDoS operations, frequently leveraging commercial DDoS-for-hire platforms (for example, EliteStress). The group deliberately targets industrial and manufacturing sectors - including Israeli manufacturing - aiming to create process delays and operational disruption. They sometimes combine DDoS with data theft and website defacement to amplify media attention and psychological impact.

**Scores:**

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 0.8

### 3.2.14. KIMSUKY

**Description:** Kimsuky is a North Korea–linked cyber espionage group active since at least 2012. Initially focused on South Korean government entities, think tanks, and subject-matter experts, Kimsuky expanded to target organizations in the U.S., Japan, Russia, and Europe, including UN bodies and academic institutions. Their intelligence collection centers on Korean-peninsula policy, nuclear issues, and sanctions. Kimsuky's operations have occasionally overlapped with other North Korean actors, likely reflecting informal collaboration or resource sharing.

**Scores:**

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

### 3.2.15. 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

### 3.2.16. 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: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 0.8

### 3.2.17. 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: 1.2

### 3.2.18. MUSTANG PANDA

**Description:** Mustang Panda is a China-associated cyber espionage actor first observed publicly in 2017, although its operations may date back to at least 2014. The group targets government organizations, non-profits, religious entities, and other NGOs in the U.S., Europe, Mongolia, Myanmar, Pakistan, Vietnam, and elsewhere.

**Scores:**

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

### 3.2.19. NIGHTSPIRE

**Description:** NightSpire is a financially motivated ransomware group that emerged in early 2025. The group uses a double-extortion model: encrypting victims' systems while threatening to publish stolen data on a Dark Web data-leak site if ransoms are not paid. NightSpire demonstrates broad, cross-sector and multinational targeting.

**Scores:**

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 0.8

### 3.2.20. 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: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 1.0

### 3.2.21. 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: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.3

### 3.2.22. 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: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.4

### 3.2.23. RA RANSOMWARE GROUP

**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: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.2

### 3.2.24. 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: 4
- Evasion: 4
- Complexity: 4
- Successfulness: 4
- Accuracy: 1.3

### 3.2.25. SAFEPAY

**Description:** SafePay is a sophisticated ransomware group that emerged as a notable actor in 2025. First identified in September 2024, it rapidly accumulated victims and ranked among the top 10 active ransomware groups in Q1 2025. The group predominantly targets organizations in the United States, Germany, the United Kingdom, Australia, Canada, and several other countries. SafePay appears to avoid attacking current or former members of the Commonwealth of Independent States (CIS), a behavior that could suggest the group's operators are located in or originate from Eastern Europe or parts of Asia.

**Scores:**

- Impact: 3
- Evasion: 3
- Complexity: 3
- Successfulness: 3
- Accuracy: 0.8

### 3.2.26. SALT TYPHOON

**Description:** Salt Typhoon is a PRC-aligned state-backed actor active since at least 2019, credited with widespread compromises of network infrastructure at major U.S. telecommunications providers and internet service providers.

**Scores:**

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

### 3.2.27. SANDWORM TEAM

**Description:** Sandworm Team is a destructive cyber threat group attributed to Russia's GRU, specifically the Main Center for Special Technologies (GTsST), unit 74455. Active since at least 2009, the group has been linked to a series of high-profile disruptive operations, and in October 2020 the U.S. indicted six officers tied to Unit 74455 for involvement in incidents including the 2015–2016 attacks on Ukrainian electrical infrastructure, the 2017 NotPetya global outbreak, interference in the 2017 French presidential campaign, the 2018 Olympic Destroyer attack, operations against the OPCW, and attacks on Georgia. Some of these activities were conducted with assistance from GRU Unit 26165 (also associated with APT28).

**Scores:**

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

### 3.2.28. SCATTERED SPIDER

**Description:** Scattered Spider is an English-speaking criminal group active since at least 2022. Initially focused on customer-relationship-management and business-process- outsourcing firms, telecoms, and tech companies, the group expanded from 2023 onward to target gaming, hospitality, retail, MSPs, manufacturing, and financial services. Their campaigns rely heavily on targeted social engineering, efforts to bypass endpoint defenses, and more recently include deploying ransomware for financial gain.

**Scores:**

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

### 3.2.29. SHINYHUNTERS

**Description:** ShinyHunters is a financially motivated cybercriminal collective of uncertain origin, known for sophisticated intrusions against a diverse set of targets including commercial organizations and government agencies. The group commonly uses phishing and exploit kits to gain initial access, then exfiltrates large quantities of personally identifiable information (names, addresses, phone numbers, SSNs, payment card data, etc.).

**Scores:**

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

### 3.2.30. STORMOUS

**Description:** The Stormous Group is a relatively new, pro-Russian cybercriminal gang focused on ransomware and data theft. Operating internationally, they have targeted organizations of varying sizes, exfiltrated sensitive data, and demanded ransoms in exchange for non-publication or data return.

**Scores:**

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

### 3.2.31. TURLA

**Description:** Turla is a long-running cyber-espionage group attributed to Russia's FSB. Active since at least 2004, Turla has compromised victims in more than 50 countries across sectors such as government, embassies, military, education, research, and pharmaceuticals. The group is known for watering-hole and spear-phishing campaigns, and for leveraging bespoke tooling such as the Uroburos rootkit.

**Scores:**

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

### 3.2.32. VOLT TYPHOON

**Description:** Volt Typhoon is a PRC state-sponsored actor active since at least 2021 that primarily targets critical infrastructure organizations in the United States and its territories (including Guam). Their activities are widely assessed as pre-positioning to enable lateral movement toward operational-technology (OT) assets for potential disruptive or destructive operations. Volt Typhoon emphasizes stealth, using web shells, living-off-the-land binaries, credential theft, and hands-on-keyboard activity.

**Scores:**

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

04

# SCORES

The following scores were assigned to each cyber threat:

| Threat/Threat Actor | Impact | Evasion | Complexity | Successfulness | Accuracy | Sum |
|---|---|---|---|---|---|---|
| AgentTesla | 3 | 3 | 3 | 3 | 1.3 | 15.6 |
| Amadey | 2 | 2 | 2 | 3 | 1 | 9 |
| AndroxghOst | 3 | 3 | 3 | 3 | 1 | 12 |
| AsyncRAT | 3 | 3 | 3 | 3 | 1.3 | 15.6 |
| BlackLock | 3 | 3 | 3 | 3 | 0.8 | 9.6 |
| ClearFake | 3 | 3 | 3 | 3 | 1 | 12 |
| Clop | 4 | 4 | 4 | 4 | 1.5 | 24 |
| Cobalt Strike | 4 | 5 | 5 | 5 | 1.5 | 28.5 |
| FormBook | 3 | 3 | 3 | 3 | 1.3 | 15.6 |
| HijackLoader | 2 | 3 | 3 | 3 | 1 | 11 |
| Interlock | 2 | 2 | 2 | 2 | 0.7 | 5.6 |
| LockBit | 5 | 4 | 4 | 5 | 1.5 | 27 |
| Lumma Stealer | 3 | 3 | 3 | 3 | 1.2 | 14.4 |
| Mirai | 3 | 2 | 2 | 4 | 1.5 | 16.5 |
| NanoCore | 3 | 3 | 3 | 3 | 1.2 | 14.4 |
| NetSupport RAT | 3 | 3 | 3 | 3 | 1.3 | 15.6 |
| Phorpiex | 3 | 3 | 3 | 3 | 1.2 | 14.4 |

| Threat/Threat Actor | Impact | Evasion | Complexity | Successfulness | Accuracy | Sum |
|---|---|---|---|---|---|---|
| PLAY | 4 | 4 | 4 | 4 | 1.3 | 20.8 |
| Qilin | 4 | 4 | 4 | 4 | 1.4 | 22.4 |
| Raspberry Robin | 4 | 4 | 4 | 4 | 1.2 | 19.2 |
| Remcos RAT | 3 | 3 | 3 | 3 | 1.3 | 15.6 |
| SafePay | 3 | 3 | 3 | 3 | 0.8 | 9.6 |
| Snake Keylogger | 3 | 4 | 3 | 3 | 1.3 | 16.9 |
| SocGholish | 3 | 3 | 3 | 3 | 1.2 | 14.4 |
| StealC | 3 | 3 | 3 | 3 | 1.2 | 14.4 |
| VenomRAT | 3 | 3 | 3 | 3 | 1.3 | 15.6 |
| Vidar | 3 | 2 | 3 | 2 | 1 | 10 |
| XWorm | 2 | 2 | 2 | 2 | 0.7 | 5.6 |
| ZPHP | 4 | 3 | 4 | 4 | 1.3 | 19.5 |
| Andariel | 4 | 4 | 4 | 4 | 1.3 | 20.8 |
| Akira Ransomware Group | 4 | 4 | 4 | 4 | 1.5 | 24 |
| APT28 | 4 | 5 | 5 | 4 | 1.5 | 27 |
| APT29 | 4 | 4 | 5 | 4 | 1.5 | 25.5 |
| APT41 | 4 | 4 | 4 | 4 | 1.2 | 19.2 |
| Chaos Ransomware Group | 3 | 3 | 3 | 3 | 0.8 | 9.6 |
| Dark Storm Team | 2 | 2 | 2 | 2 | 0.7 | 5.6 |

| Threat/Threat Actor | Impact | Evasion | Complexity | Successfulness | Accuracy | Sum |
|---|---|---|---|---|---|---|
| Devman | 2 | 2 | 2 | 2 | 0.7 | 5.6 |
| DragonForce | 3 | 3 | 3 | 3 | 1 | 12 |
| Emmenhtal | 2 | 2 | 2 | 2 | 0.7 | 5.6 |
| FIN | 4 | 4 | 5 | 4 | 1.5 | 25.5 |
| FOG | 2 | 2 | 2 | 2 | 0.7 | 5.6 |
| FunkSec | 2 | 2 | 2 | 2 | 0.7 | 5.6 |
| INC Ransomware Group | 4 | 4 | 4 | 4 | 1.2 | 19.2 |
| Keymous+ | 3 | 3 | 3 | 3 | 0.8 | 9.6 |
| Kimsuky | 3 | 4 | 4 | 4 | 1.3 | 19.5 |
| Lazarus Group | 5 | 5 | 5 | 5 | 1.5 | 30 |
| Lynx | 3 | 3 | 3 | 3 | 0.8 | 9.6 |
| Medusa | 4 | 4 | 4 | 4 | 1.2 | 19.2 |
| Mustang Panda | 4 | 4 | 4 | 4 | 1.4 | 22.4 |
| NightSpire | 3 | 3 | 3 | 3 | 0.8 | 9.6 |
| NoName057(16) | 3 | 3 | 3 | 3 | 1 | 12 |
| RA Ransomware Group | 4 | 4 | 4 | 4 | 1.2 | 19.2 |
| Rhysida | 4 | 4 | 4 | 4 | 1.3 | 20.8 |
| Salt Typhoon | 4 | 3 | 3 | 3 | 1 | 13 |
| Sandworm Team | 5 | 4 | 5 | 4 | 1.5 | 27 |

| Threat/Threat Actor | Impact | Evasion | Complexity | Successfulness | Accuracy | Sum |
|---|---|---|---|---|---|---|
| Scattered Spider | 4 | 4 | 3 | 4 | 1.4 | 21 |
| ShinyHunters | 3 | 3 | 3 | 3 | 1.3 | 15.6 |
| Stormous | 3 | 3 | 3 | 3 | 1 | 12 |
| Turla | 4 | 5 | 5 | 4 | 1.5 | 27 |
| Volt Typhoon | 4 | 5 | 5 | 4 | 1.5 | 27 |

05

# HEATMAP

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

https://github.com/blackcellltd/Heatmaps/blob/main/annual_ti_based_retrospective_ttp_repo rt__2025.json




Figure 2: Annual_TI_based_Retrospective_TTP_report_heatmap

06

# RESULTS

## 6.1. TOP TECHNIQUES AND SUB-TECHNIQUES

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 216 techniques and 475 Sub-techniques, we need to prioritize them in a descending order based on their score. For detection engineering purposes, we defined the baseline at 200 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.

### 6.1.1. 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: 552.4**

### 6.1.2. 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: 545.5**

### 6.1.3. 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: 501.9**

### 6.1.4. 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: 488.9**

### 6.1.5. 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 this information to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. This behavior is distinct from Local Storage Discovery which is an adversary's discovery of local drive, disks and/or volumes.

**Score: 470.8**

### 6.1.6. 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: 467.8**

### 6.1.7. 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: 457**

### 6.1.8. 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: 457**

### 6.1.9. 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: 442.9**

### 6.1.10. 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: 440.2**

### 6.1.11. 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: 395.3**

### 6.1.12. 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: 383.8**

### 6.1.13. 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: 357**

### 6.1.11. 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: 395.3**

### 6.1.12. 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: 383.8**

### 6.1.13. 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: 357**

### 6.1.14. T1204.002: USER EXECUTION: MALICIOUS FILE

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Attachment. Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, .cpl, .reg, and .iso.

**Score: 347.4**

### 6.1.15. T1005: DATA FROM LOCAL SYSTEM

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

**Score: 339.9**

### 6.1.16. 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: 334**

### 6.1.17. 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: 332.7**

### 6.1.18. 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: 332.1**

### 6.1.19. 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: 329.4**

### 6.1.20. T1588.002: OBTAIN CAPABILITIES: TOOL

Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: PsExec).

**Score: 328.9**

### 6.1.21. T1112: MODIFY REGISTRY

Adversaries may interact with the Windows Registry as part of a variety of other techniques to aid in defense evasion, persistence, and execution.

**Score: 320.9**

### 6.1.22. 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, net view using Net, or, on ESXi servers, esxcli network diag ping.

**Score: 316.4**

### 6.1.23. 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: 311**

### 6.1.24. 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: 306.1**

### 6.1.25. 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: 301**

### 6.1.26. T1036.005: MASQUERADING: MATCH LEGITIMATE RESOURCE NAME OR LOCATION

Adversaries may match or approximate the name or location of legitimate files, Registry keys, or other resources when naming/placing them. This is done for the sake of evading defenses and observation.

**Score: 277.4**

### 6.1.27. 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: 274.3**

### 6.1.28. 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: 272.9**

### 6.1.29. 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: 267.3**

### 6.1.30. 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: 264.8**

### 6.1.31. 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: 260.9**

### 6.1.32. T1204.001: USER EXECUTION: MALICIOUS LINK

An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Link. Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via Exploitation for Client Execution. Links may also lead users to download files that require execution via Malicious File.

**Score: 258.2**

### 6.1.33. 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 and Windows Management Instrumentation (WMI) to create a scheduled task. Adversaries may also utilize the Powershell Cmdlet Invoke-CimMethod, which leverages WMI class PS_ScheduledTask to create a scheduled task via an XML path.

**Score: 258.1**

### 6.1.34. T1553.002: SUBVERT TRUST CONTROLS: CODE SIGNING

Adversaries may create, acquire, or steal code signing materials to sign their malware or tools. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. The certificates used during an operation may be created, acquired, or stolen by the adversary. Unlike Invalid Code Signature, this activity will result in a valid signature.

**Score: 257**

### 6.1.35. 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: 251.5**

### 6.1.36. 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.

**Score: 251.4**

### 6.1.37. T1203: EXPLOITATION FOR CLIENT EXECUTION

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

**Score: 250.3**

### 6.1.38. 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: 248.4**

### 6.1.39. T1049: SYSTEM NETWORK CONNECTIONS DISCOVERY

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

**Score: 245**

### 6.1.40. T1587.001: DEVELOP CAPABILITIES: MALWARE

Adversaries may develop malware and malware components that can be used during targeting. Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors (including backdoored images), packers, C2 protocols, and the creation of infected removable media. Adversaries may develop malware to support their operations, creating a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors.

**Score: 239.2**

### 6.1.41. T1567.002: EXFILTRATION OVER WEB SERVICE: EXFILTRATION TO CLOUD STORAGE

Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet.

**Score: 234.7**

### 6.1.42. 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: 232.8**

### 6.1.43. 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: 232.1**

### 6.1.44. T1218.011: SYSTEM BINARY PROXY EXECUTION: RUNDLL32

Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. Shared Modules), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations. Rundll32.exe is commonly associated with executing DLL payloads (ex: rundll32.exe {DLLname, DLLfunction}).

**Score: 231.8**

### 6.1.45. T1583.001: ACQUIRE INFRASTRUCTURE: DOMAINS

Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free.

**Score: 231.2**

### 6.1.46. 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: 226.1**

### 6.1.47. T1036.004: MASQUERADING: MASQUERADE TASK OR SERVICE

Adversaries may attempt to manipulate the name of a task or service to make it appear legitimate or benign. Tasks/services executed by the Task Scheduler or systemd will typically be given a name and/or description. Windows services will have a service name as well as a display name. Many benign tasks and services exist that have commonly associated names. Adversaries may give tasks or services names that are similar or identical to those of legitimate ones.

**Score: 223.1**

### 6.1.48. 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: 221.3**

### 6.1.49. T1583.006: ACQUIRE INFRASTRUCTURE: WEB SERVICES

Adversaries may register for web services that can be used during targeting. A variety of popular websites exist for adversaries to register for a web-based service that can be abused during later stages of the adversary lifecycle, such as during Command and Control (Web Service), Exfiltration Over Web Service, or Phishing. Using common services, such as those offered by Google, GitHub, or Twitter, makes it easier for adversaries to hide in expected noise. By utilizing a web service, adversaries can make it difficult to physically tie back operations to them.

**Score: 216.2**

### 6.1.50. T1490: INHIBIT SYSTEM RECOVERY

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. This may deny access to available backups and recovery options.

**Score: 215**

### 6.1.51. 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. 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: 214**

### 6.1.52. 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: 210.9**

### 6.1.53. T1012: QUERY REGISTRY

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

**Score: 208.7**

### 6.1.50. T1490: INHIBIT SYSTEM RECOVERY

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. This may deny access to available backups and recovery options.

**Score: 215**

### 6.1.51. 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. 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: 214**

### 6.1.52. 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: 210.9**

### 6.1.53. T1012: QUERY REGISTRY

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

**Score: 208.7**

### 6.1.54. T1505.003: SERVER SOFTWARE COMPONENT: WEB SHELL

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to access the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.

**Score: 203.6**

### 6.1.55. 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, vulnerability, and/or wordlist scans using tools that are brought onto a system.

**Score: 202.1**

## 6.2. 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 |
|---|---|
| T1543.003 | 194.4 |
| T1133 | 191.8 |
| T1059.007 | 182.9 |
| T1027.013 | 181.2 |
| T1003.003 | 178.1 |
| T1078.003 | 175.3 |
| T1218.005 | 171.4 |
| T1027.010 | 163 |
| T1489 | 157 |
| T1102 | 156 |
| T1110 | 152.7 |
| T1070 | 152 |
| T1078.002 | 151.5 |
| T1620 | 149.7 |
| T1622 | 147.2 |
| T1070.001 | 146.7 |
| T1059.006 | 144 |
| T1585.001 | 143.7 |
| T1564.001 | 142.7 |

| Technique ID | Score |
|---|---|
| T1539 | 138.9 |
| T1564.003 | 133.8 |
| T1566 | 127.2 |
| T1055.012 | 123.8 |
| T1119 | 121.5 |
| T1003.002 | 117 |
| T1598.003 | 113.9 |
| T1071 | 112.5 |
| T1555 | 110.7 |
| T1518 | 109.2 |
| T1003 | 108.8 |
| T1055.001 | 107.9 |
| T1529 | 106.4 |
| T1059.004 | 102.3 |
| T1078.004 | 87.6 |
| T1218 | 81 |
| T1070.003 | 74.7 |
| T1102.001 | 45 |
| T1530 | 42.2 |

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.

07

# SOURCES


- https://cyble.com/knowledge-hub/top-15-most-dangerous-malware-threats-in-2025/
- https://deepstrike.io/blog/ransomware-groups-2025
- https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf
- https://www.recordedfuture.com/research/h1-2025-malware-and-vulnerability-trends
- https://www.darktrace.com/blog/2025-cyber-threat-landscape-darktraces-mid-year-review
- https://go.cyberproof.com/hubfs/CyberProof_MidYear_Cyber%20Threat%20Landscape%20Report.pdf
- https://www.trellix.com/advanced-research-center/threat-reports/april-2025/
- https://www.surefirecyber.com/threat-actor-activity-q1-2025/
- https://reliaquest.com/blog/threat-spotlight-ransomware-cyber-extortion-q1-2025/
- https://beazley.security/insights/quarterly-threat-report-first-quarter-2025
- https://www.travelers.co.uk/insights/cyber/q1-2025-cyber-threat-report
- https://www.it-isac.org/post/q1-2025-our-newest-ransomware-report-update
- https://www.linkedin.com/pulse/top-threats-q1-2025-cybermaterial-vrkzc
- https://medium.com/@scottbolen/the-most-active-threat-actors-of-q1-2025-an-in-depth-analysis-325bebe12eb8

- https://circleid.com/posts/top-10-malware-of-q2-2025-a-deep-dive-into-the-iocs
- https://www.travelers.co.uk/insights/cyber/q2-2025-cyber-threat-report
- https://www.halcyon.ai/raas-mq/power-rankings-ransomware-malicious-quartile-q2-2025
- https://securelist.com/vulnerabilities-and-exploits-in-q2-2025/117333/
- https://www.rapid7.com/blog/post/q2-2025-ransomware-trends-analysis-boom-and-bust/
- https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2025
- https://www.asmag.com/showpost/35245.aspx
- https://research.checkpoint.com/2025/the-state-of-ransomware-q2-2025/
- https://bluefire-redteam.com/top-10-malware-q2-2025-what-hit-how-it-spread-and-how-to-stop-it/
- https://www.corvusinsurance.com/blog/q2-25-travelers-cyber-threat-report
- https://reliaquest.com/blog/ransomware-cyber-extortion-threat-intel-q2-2025/
- https://beazley.security/insights/quarterly-threat-report-second-quarter-2025
- https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of-january-2025/
- https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of-february-2025/
- https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of-march-2025/
- https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of-april-2025/
- https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of- may-2025/

- https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of- july-2025/
- https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of- august-2025/ •
- https://blog.checkpoint.com/research/january-2025s-most-wanted-malware- fakeupdates-continues-to-dominate-2/
- https://blog.checkpoint.com/security/february-2025s-malware-spotlight-asyncrat- emerges-targeting-trusted-platforms/
- https://blog.checkpoint.com/security/march-2025-malware-spotlight-fakeupdates- and-ransomhub-ransomware-group-dominate-cyber-threats/
- https://blog.checkpoint.com/research/april-2025-malware-spotlight-fakeupdates- dominates-as-multi-stage-campaigns-blend-commodity-malware-with-stealth/
- https://blog.checkpoint.com/research/may-2025-malware-spotlight-safepay-surges- to-the-forefront-of-cyber-threats/
- https://blog.checkpoint.com/research/june-2025-malware-spotlight-discord-exploits- lead-to-rising-threats/
- https://www.cm-alliance.com/cybersecurity-blog/january-2025-recent-cyber-attacks- data-breaches-ransomware-attacks
- https://www.cm-alliance.com/cybersecurity-blog/february-2025-major-cyber-attacks- ransomware-attacks-data-breaches
- https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-ransomware- attacks-data-breaches-of-march-2025
- https://www.cm-alliance.com/cybersecurity-blog/april-2025-major-cyber-attacks- ransomware-attacks-and-data-breaches
- https://www.cm-alliance.com/cybersecurity-blog/may-2025-biggest-cyber-attacks- ransomware-attacks-and-data-breaches
- https://www.cm-alliance.com/cybersecurity-blog/major-cyber-attacks-ransomware- attacks-and-data-breaches-of-june-2025
- https://www.cm-alliance.com/cybersecurity-blog/july-2025-biggest-cyber-attacks- ransomware-attacks-and-data-breaches
- https://www.cm-alliance.com/cybersecurity-blog/major-cyber-attacks-ransomware- attacks-and-data-breaches-august-2025

- https://www.cm-alliance.com/cybersecurity-blog/sept-2025-biggest-cyber-attacks- ransomware-attacks-and-data-breaches
- https://www.cyfirma.com/research/tracking-ransomware-january-2025/
- https://www.cyfirma.com/research/tracking-ransomware-february-2025/
- https://www.cyfirma.com/research/tracking-ransomware-march-2025/
- https://www.cyfirma.com/research/tracking-ransomware-april-2025/
- https://www.cyfirma.com/research/tracking-ransomware-may-2025/
- https://www.cyfirma.com/research/tracking-ransomware-june-2025/
- https://www.cyfirma.com/research/tracking-ransomware-july-2025/
- https://www.cyfirma.com/research/tracking-ransomware-august-2025/
- https://www.cyfirma.com/research/tracking-ransomware-september-2025/
- https://www.connectwise.com/blog/monthly-threat-brief-january-2025
- https://www.connectwise.com/blog/monthly-threat-brief-february-2025
- https://www.connectwise.com/blog/monthly-threat-brief-march-2025
- https://www.connectwise.com/blog/monthly-threat-brief-april-2025
- https://www.connectwise.com/blog/monthly-threat-brief-may-2025
- https://www.connectwise.com/blog/monthly-threat-brief-june-2025
- https://www.connectwise.com/blog/monthly-threat-brief-july-2025
- https://www.connectwise.com/blog/monthly-threat-brief-august-2025
- https://www.cisecurity.org/insights/blog/top-10-malware-q1-2025
- https://www.cisecurity.org/insights/blog/top-10-malware-q2-2025
- https://www.loginsoft.com/post/the-blacklock-breakdown-tools-tactics-and-the- rivalry-that-brought-it-down
- https://www.bridewell.com/insights/blogs/detail/clearfake-campaign
- https://blog.shieldsguard.com/dark-storm-ddos-tactics-infrastructure-and-campaign- profile/

- https://cyhawk-africa.com/news/mitre-attck-analysis-of-how-devman-breached-nssf- kenya/
- https://socradar.io/dark-web-profile-fog-ransomware/
- https://cyberflorida.org/funksec-a-top-ransomware-group-leveraging-ai/
- https://www.crowdstrike.com/en-us/blog/hijackloader-expands-techniques/
- https://socradar.io/dark-web-profile-interlock-ransomware/
- https://www.quorumcyber.com/wp-content/uploads/2023/06/Quorum-Cyber-_Mirai- Botnet-Report.pdf
- https://medium.com/@nirajbagde2004/netsupport-rat-analysis-and-with-a-path-of- fake-captcha-dd9a4b67fcef
- https://socradar.io/dark-web-profile-nightspire-ransomware/
- https://socradar.io/dark-web-profile-safepay-ransomware/
- https://socradar.io/dark-web-profile-shinyhunters/
- https://www.splunk.com/en_us/blog/security/under-the-hood-of-snakekeylogger- analyzing-its-loader-and-its-tactics-techniques-and-procedures.html
- https://dailysecurityreview.com/security-spotlight/stormous-ransomware-the-pro- russian-cyber-gang-targeting-global-networks/
- https://blog.netmanageit.com/content/files/2024/04/Report-VenomRAT-Deployed- with-Arsenal-of-Plugins.pdf
- https://www.splunk.com/en_us/blog/security/xworm-shape-shifting-arsenal- detection-evasion.html
- https://www.picussecurity.com/resource/blog/androxgh0st-malware-cloud-web- security-threat
- https://www.resecurity.com/blog/article/dragonforce-ransomware-reverse- engineering-report
- https://socradar.io/dark-web-profile-lynx-ransomware/
- https://socradar.io/dark-web-profile-noname05716/
- https://www.cybereason.com/blog/threat-analysis-phorpiex-downloader

- https://socradar.io/dark-web-profile-ra-world/
- https://socradar.io/threat-profile-rhysida-ransomware/
- https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in- popularity-part-1/

08

# CONTACT

Understanding how adversaries operate is essential to building stronger defenses. Black Cell combines threat intelligence, MITRE ATT&CK-based TTP analysis, and infrastructure assessments to identify the techniques that pose the greatest risk to your organization.

Contact our experts to turn threat intelligence into actionable security improvements.

Black Cell Hungary Zrt.
www.blackcell.io
tibor.luter@blackcell.io