CyberProof®
A UST Company

Top Malware Trends to Watch in 2023

Contents

2022’s arrival was plagued by multiple events including the ongoing COVID-19 pandemic and the inception of the Russian-Ukrainian conflict. These events were coupled with a flurry of high-profile cyber-related threats – with widespread Log4Shell and Follina exploitations chief among them.

Threat actors keep up with current events and advancements in technology and leverage the opportunities they represent. Alongside more methodical and calculated approaches that attackers take, they also incorporate current events into campaigns and attack chains.

While many types of attackers fall under the ever-blossoming threat actor umbrella, this eBook, based on data collected by the CyberProof Cyber Threat Intelligence (CTI) team, seeks to take a focused snapshot of the malware-related threat landscape from January to July 2022. Its aim is to attempt to analyze malware usage and trends as observed through the lens of a CyberProof analyst whose objective is to provide threat intelligence solutions to enterprise clients.

> **Alongside more methodical and calculated approaches, attackers also incorporate current events into campaigns and attack chains.**

MITRE techniques observed in malware attacks

The CyberProof CTI Team identified the following MITRE techniques most utilized in malware attacks:

Technique/Sub-technique	Tactic
Application Layer Protocol: Web Protocols	**Command and Control**
Scheduled Task/Job: Scheduled Task	**Execution/Persistence/Privilege Escalation**
Obfuscated Files or Information	**Defense Evasion**
Ingress Tool Transfer	**Command and Control**
Exfiltration Over C2 Channel	**Exfiltration**
Command and Scripting Interpreter: PowerShell	**Execution**
User Execution: Malicious File	**Execution**
Phishing: Spearphishing Link	**Initial Access**
Phishing: Spearphishing Attachment	**Initial Access**
Process Injection	**Defense Evasion/ Privilege Escalation**
Command and Scripting Interpreter: Windows Command Shell	**Execution**
System Information Discovery	**Discovery**
Boot or Logon Autostart Execution: Registry Run Keys/ Startup Folder	**Persistence/Privilege Escalation**
Credentials from Password Stores: Credentials from Web Browsers	**Credential Access**
Obfuscated Files or Information: Software Packing	**Defense Evasion**

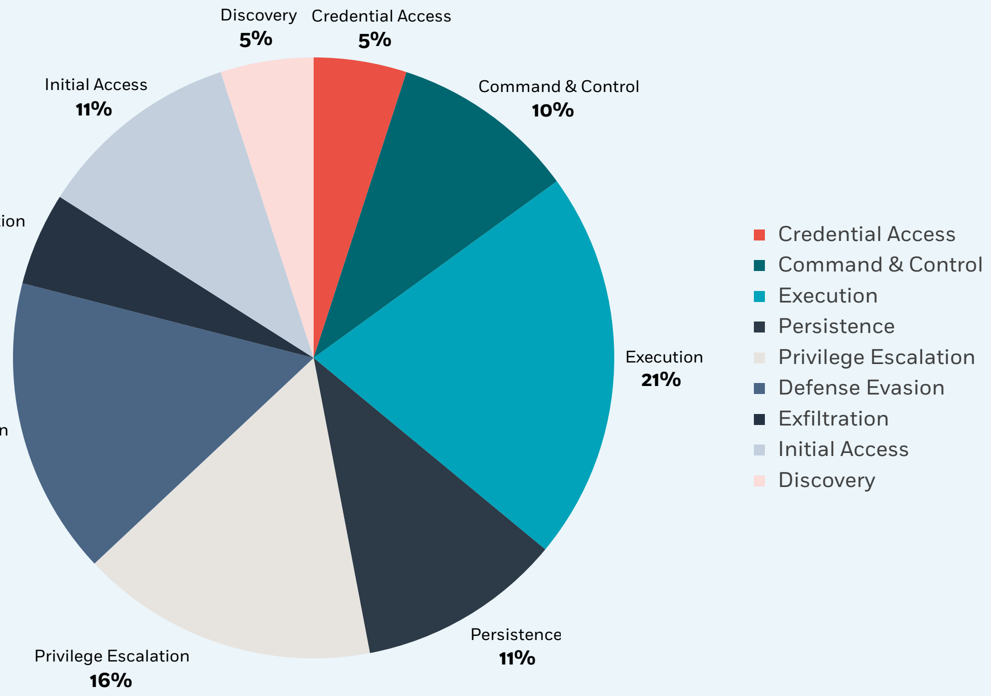
MITRE tactics

The MITRE techniques that were used were related to the following tactics:

21% of MITRE techniques used were related to Execution

16% pertain to Privilege Escalation

16% are related to Defense Evasion



TOP TACTICS RELATED TO THE MITRE TECHINQUES THAT WERE USED

A comparative analysis of data collected in previous years highlights an interesting trend:

In comparison to data collected by external sources in 2020, there was a large uptick in Scheduled Task usage, alongside a decrease in the volume of malware attacks using Process Injection, in the first half of 2022.

Interestingly, PowerShell exploitation has remained relatively consistent and is constantly being observed in attacks.

Unraveling the adversaries' motivation – User Execution

Now that we've laid out the top MITRE techniques used this year, we can attempt to understand why they were the most popular.

First, let's explore why malware was used most often for execution purposes. This notion is supported by several pieces of evidence:

WIPER MALWARE

Harnessed by threat actors hellbent on data destruction – is the most prominent type of malware utilized in the Russia-Ukraine conflict.

APT GROUPS

Advanced Persistent Threat (APT) groups have had the most individual malware strains attributed to their use. Seeing as these groups are acting to achieve a larger goal, their endgame usually culminates in user execution.

UNATTRIBUTED ATTACKS

Completely unattributed attacks – the "average Joes" of malware attacks – are most likely to have no ulterior motives save for user execution.

Why defense evasion techniques are so prevalent

Bearing in mind the fact that 21% of MITRE techniques used in the evaluated period were related to Execution – we can now try to figure out why Defense Evasion techniques were common. Generally, attackers nowadays are more inclined to bide their time and remain undetected for longer periods of time. This is underscored by the following:

- We observed an increasing number of malware strains that “managed to remain undetected,” are “elusive,” or have “gone under the radar.” The uptick in detecting such malware supports our initial hypothesis of a rise in more covert behavior from attackers– as seen, for example, with Symbiote and Tarrask.
- Attackers are incorporating advanced evasion techniques leveraging public cloud services such as Azure and AWS as part of their campaigns. Aside from obsoleting the need to host their own servers and maintain their infrastructure, this also acts as a cloaking mechanism for attempted attacks. We’ve seen this type of approach incorporated in ASyncRAT, Nanocore, and Netwire campaigns.
- Attackers are simply becoming smarter, more patient, and more up-to-date with new technology and the opportunities it presents. This extends to extensive usage of native Windows command-line and scripting tools such as PowerShell and VBScript.

> **Attackers nowadays are more inclined to bide their time and remain undetected for longer periods of time.**

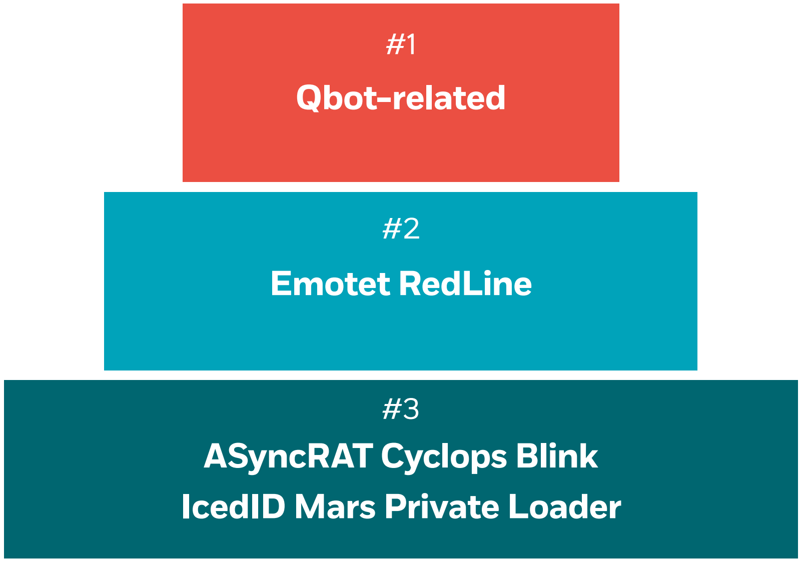
Top malware strains

In 2022, the CyberProof CTI Team reported:

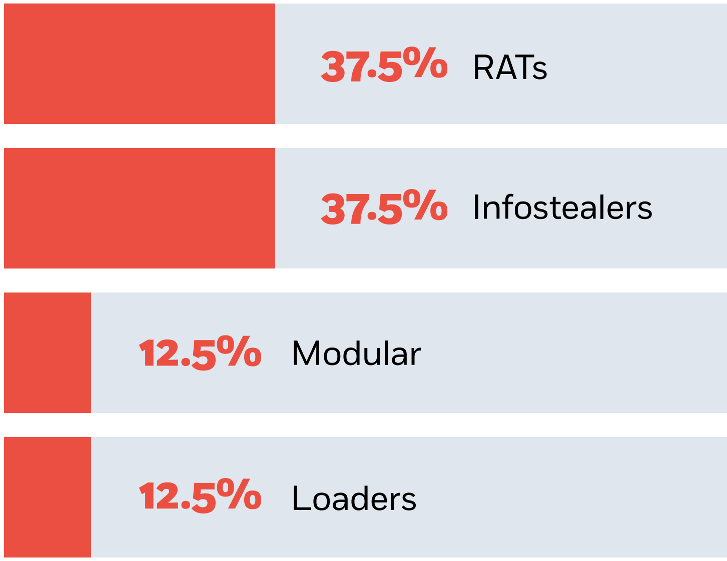
- Qbot-related campaigns were most frequent
- Emotet and RedLine incidents came in second place
- ASyncRAT, Cyclops Blink, IcedID, Mars, and PrivateLoader campaigns rounded out the rest of the top eight

It's worth noting that RATs and Infostealers each comprise 37.5% of the top eight, with Modular malware and Loaders making up 12.5% each.

Modular malware, such as wipers, saw a significant boost during the first half of 2022 due to its major role in attacks on Ukrainian organizations.



TOP MALWARE TREND FREQUENCY



TOP MALWARE STRAIN DISTRIBUTION

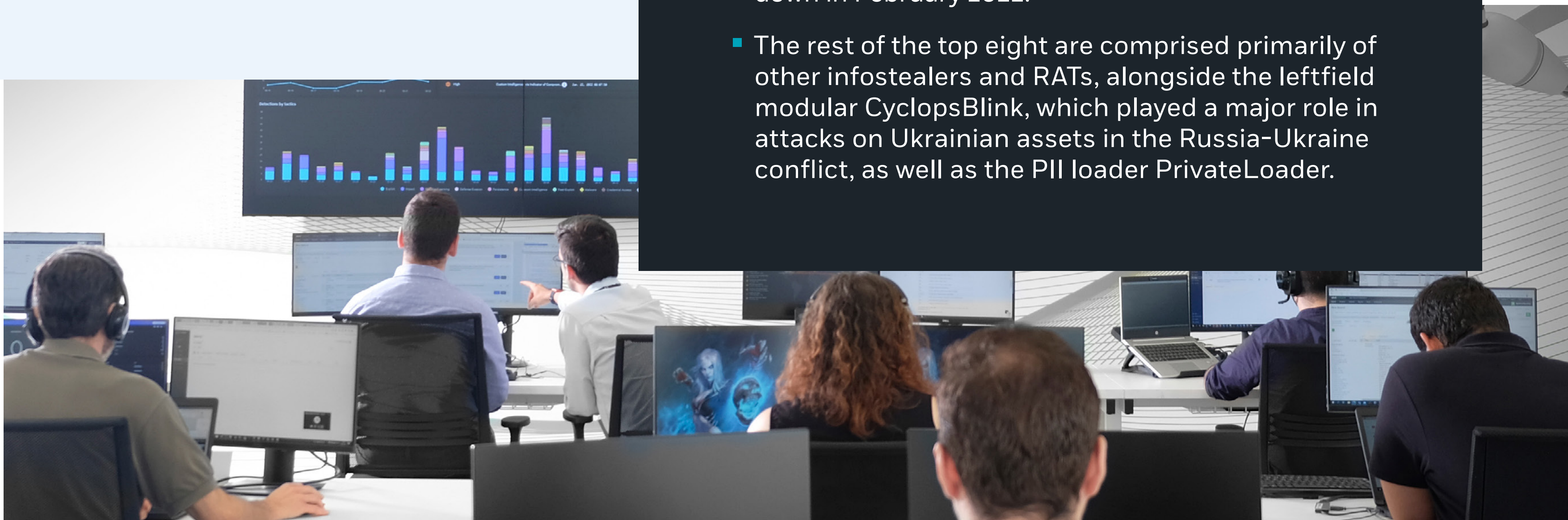
The most prevalent types of malware

We can attribute the fact that RATs and infostealers were the most prevalent pieces of malware due to the following causes:

- The prevalence of readily available infostealers on black market forums lowers the technical bar for newcomers, so greater numbers of adversaries are using them. AgentTesla and Netwire are prime examples of this.
- A surge in publicly available loaders makes it significantly easier to drop niche malware and technically unsophisticated malware. Matanbuchus and PrivateLoader are such loaders.

Insight into these malware types

- QBot and Emotet remain some of the heavy hitters in today's field. Extensive previous experience in running their respective operations, as well as solid technological infrastructure, enables them to resume their operations unfettered.
- Trickbot is interestingly absent from the top malware strains reported since the malware operation shut down in February 2022.
- The rest of the top eight are comprised primarily of other infostealers and RATs, alongside the leftfield modular CyclopsBlink, which played a major role in attacks on Ukrainian assets in the Russia-Ukraine conflict, as well as the PII loader PrivateLoader.



Malware trends & new techniques observed in 2022

As technology evolves – and as the technological infrastructure used by victims changes with the times – threat actors are quick to exploit and incorporate potential newfound "blind spots" as part of their attack chains.

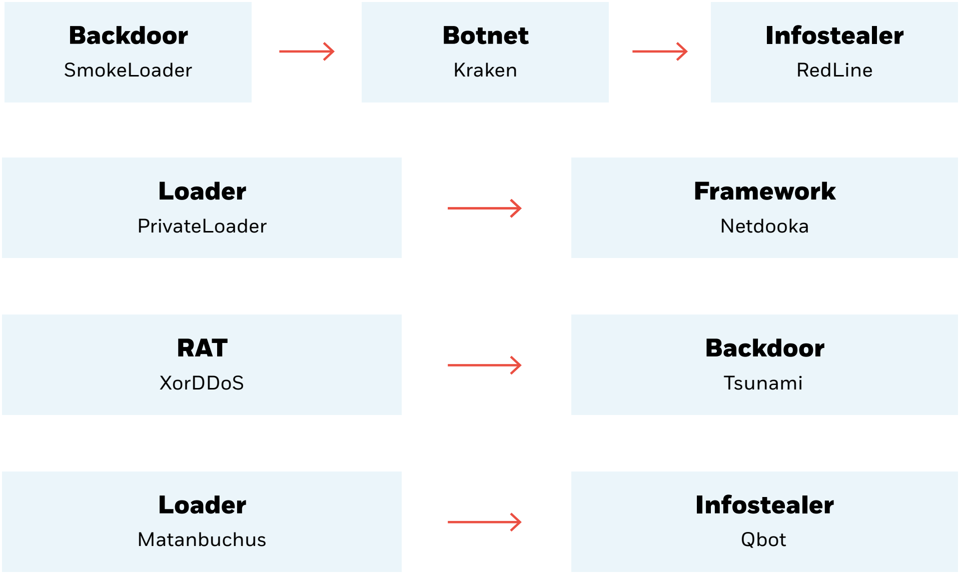
The CyberProof CTI team singled out the following emerging trends and new techniques that we expect to see more of in the second half of 2022 and beyond.

Malware	Technique	Description
Moonbounce	Targeting endpoints' UEFI	This malware is the third-most widely known malware delivery through a UEFI bootkit found in the wild.
Qakbot	Using new attack vectors	Using MSI Windows Installer packages as an infection vector is a first for Qbot operators, as Qbot is known to deliver payloads via malicious, macro-laced Microsoft Office attachments in phishing emails.
RedLine Infostealer	Coinciding with real-world events	The infostealers' operators were seen leveraging Windows 11's launch announcement to carry out attacks that coincided with the moment that Microsoft announced its broad development phase.
RedLine	Leveraging long-forgotten vulnerabilities and methods	RedLine was dropped via RIG exploit kits, even though such kits have dropped drastically in popularity.
ASyncRAT, Netwire, Nanocore, IcedID	Incorporating public cloud infrastructure	Threat actors are increasingly using cloud technologies to achieve their objectives without having to resort to hosting their own infrastructure. IcedID abused both Google Cloud and Google Firebase to deliver phishing links.
BazarLoader	Shifting familiar attack patterns	Threat actors were observed spreading malware via website contact forms as opposed to spreading via typical phishing emails.
Malicious NPM packages	Targeting a particular group of interest	Malicious NPM packages were released as part of a large-scale campaign targeting Azure developers. Several campaigns have involved malicious NPM packages uploaded to popular library archives.
Denonia	Deployed in attacks targeting AWS Lambda environments with cryptominers	The first known malware to specifically target AWS Lambda environments.
Spyder XMRig	Targeting unique technologies	Spyder was deployed in attacks targeting AMD devices. XMRig was dropped in a campaign targeting exposed Docker Engine API endpoints.

Linking different pieces of malware

While researching the threat landscape, the CTI team found it difficult to pinpoint the exact method threat actors might use to deliver the malicious payloads. Below is a non-exhaustive flowchart that showcases how the current delivery chain has no clear distribution pattern.

Between loaders dropping frameworks, RATs dropping backdoors, and other combinations – each threat actor working with complete agency to fulfill their own objectives – we find ourselves up against an ever-shifting "Wild West" of malware distribution.



Backdoor SmokeLoader → **Botnet** Kraken → **Infostealer** RedLine

Loader PrivateLoader → **Framework** Netdooka

RAT XorDDoS → **Backdoor** Tsunami

Loader Matanbuchus → **Infostealer** Qbot

VARIOUS DELIVERY CHAINS

Malware types used by APT, FIN, and UNC groups

Looking at malware distribution per threat actor type, we see that Advanced Persistent Threat (APT) groups utilize a wider array of malware types in comparison to other group types by quite a large margin.

This makes sense, as APT groups usually have a myriad of agendas, all using different means to achieve them. This stands in stark contrast to Financial Threat (FIN) groups, for example, who are only interested in financial profit.

Some of the types of malware that we observed being used by APT groups exclusively include:

FRAMEWORKS

BOOTKITS

MODULAR MALWARE

WEBSHELLS

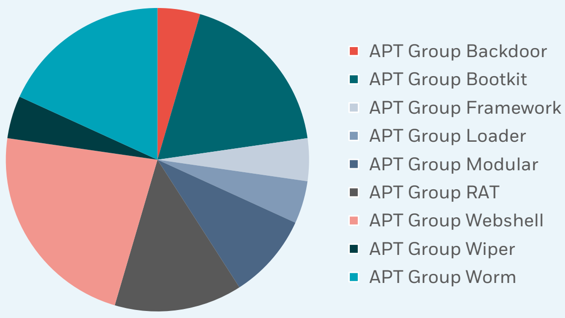
WORMS

While FIN groups were the only ones using cryptominers and APT groups were the only ones using wipers, the Uncategorized (UNC) groups have no "signature" malware.

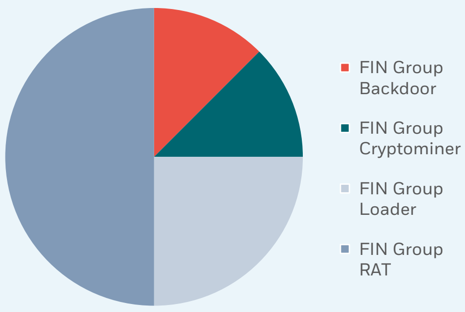
Malware types used by different kinds of threat actors

By taking a deeper dive into specific types of malware and how they're being leveraged by certain threat actors, we can see that loaders and RATs are being evenly employed by all types of groups, while wiper malware is being used almost only by APT groups – save for a single UNC group that is a suspected APT.

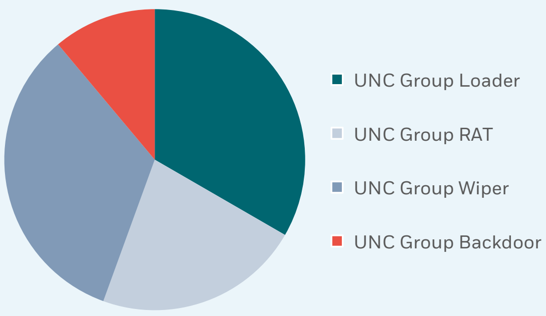
In contrast, backdoors saw use by all types of threat actors, though their use was heavily skewed towards APT groups. While APT groups were observed using backdoors in 50% of reported incidents, FIN groups were seen using them over 37% of the time.



MALWARE USED BY APT GROUPS



MALWARE USED BY FIN GROUPS



MALWARE USED BY UNC GROUPS

Key takeaways

- Execution was the most frequently observed tactic employed by threat actors, in part due to the prevalence of wiper malware in the Russian-Ukrainian conflict.
- Defense Evasion-related techniques were some of the most commonly observed, indicating that attackers are becoming more reserved, creating stealthier malware strains, and are incorporating public cloud infrastructure in attacks.
- RATs and Infostealers were the most common malware types we observed, in part due to the prevalence of readily available infostealers and loaders on the dark web.
- Qbot and Emotet remain the top actors in today's threat landscape, in part due to their rich experience and stable infrastructure.
- Attackers leveraged a plethora of new attack techniques, from an uptick in UEFI-targeting malware to targeting unique technologies in their attack chains.

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com.

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum

cyberproof.com