deep instinct™

2023 Mid-Year Threat Report

# Navigating the Threat Landscape

deepinstinct.com

# What's Inside



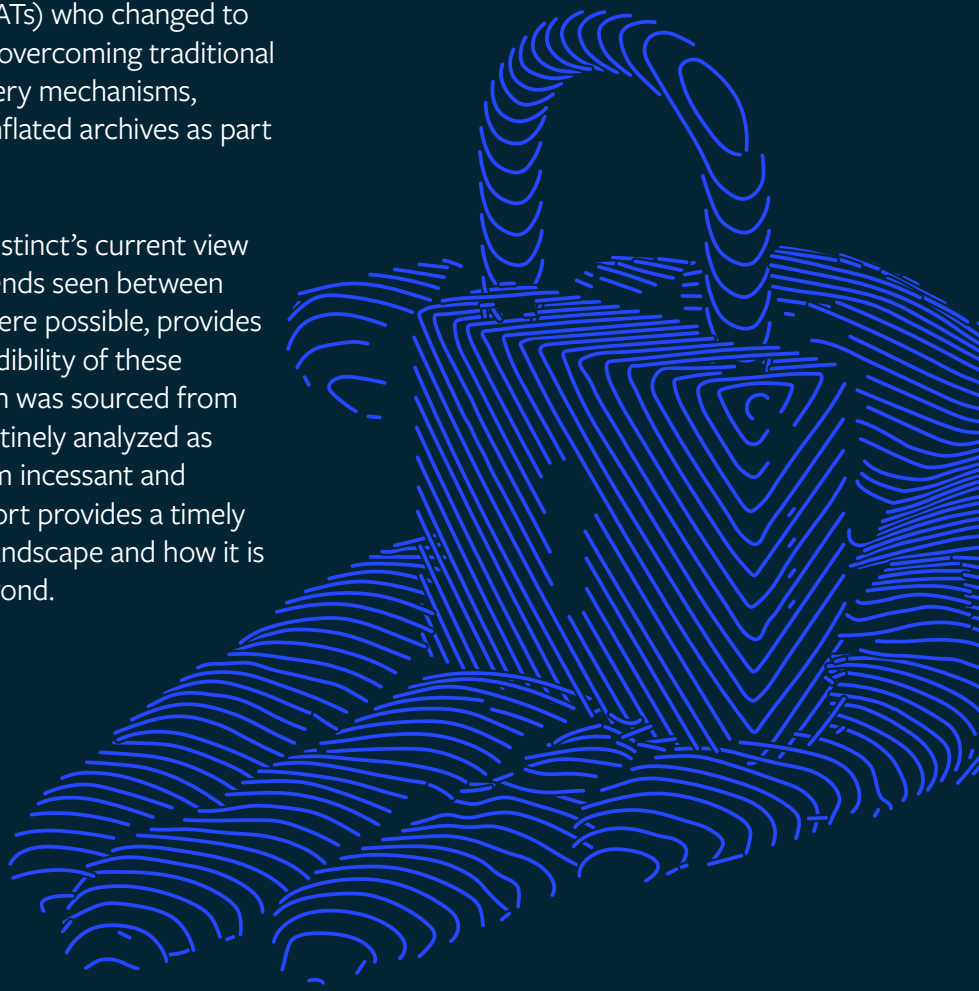
# Introduction

Welcome to Deep Instinct's interim threat report, which details the most important cyber threats of the year along with overall trends to be aware of as 2024 draws nearer. We have seen several major developments throughout the year, with the proliferation of Ransomware-as-a-Service (RaaS) being one of the most concerning. From the launch of LockBit's affiliate program to new languages featured within BlackCat's latest family, the impact and scale RaaS can offer ransomware gangs has proven irresistible.

State-sponsored cyber attacks have evolved as the war between Russia and Ukraine continues. Cybercriminal gangs fragmented and regrouped for a variety of reasons, with the various Conti splinter groups being particularly high profile following their inception. Adaptation by criminal gangs has not been limited to their organizational structures. As vendors have made changes to their software suites to increase their resistance to malware, gangs have also evolved their leading malware.

Examples of this evolution include nearly all stealers and Remote Access Trojans (RATs) who changed to maintain their effectiveness in overcoming traditional defenses by varying their delivery mechanisms, adopting LNK, HTML, JS and inflated archives as part of their malware strategy.

This report represents Deep Instinct's current view of the threat landscape and trends seen between January - August 2023, and where possible, provides concrete data to verify the credibility of these developments. The information was sourced from our repositories, which are routinely analyzed as we protect our customers from incessant and ever-evolving attacks. This report provides a timely perspective of today's threat landscape and how it is likely to evolve in 2024 and beyond.



# The Top Malware Trends of H1 2023

## Ransomware Trends

Total number of ransomware victims in 2023 compared to 2022 is significantly higher. In fact, the number of victims in the first half of 2023 already exceeds *all* victims in 2022. As you can see in Figure 1, there are several spikes during 2023 caused by vulnerabilities that are often used for large-scale campaigns affecting a significant number of victims at once – such as the Zimbra and MOVEit vulnerability.

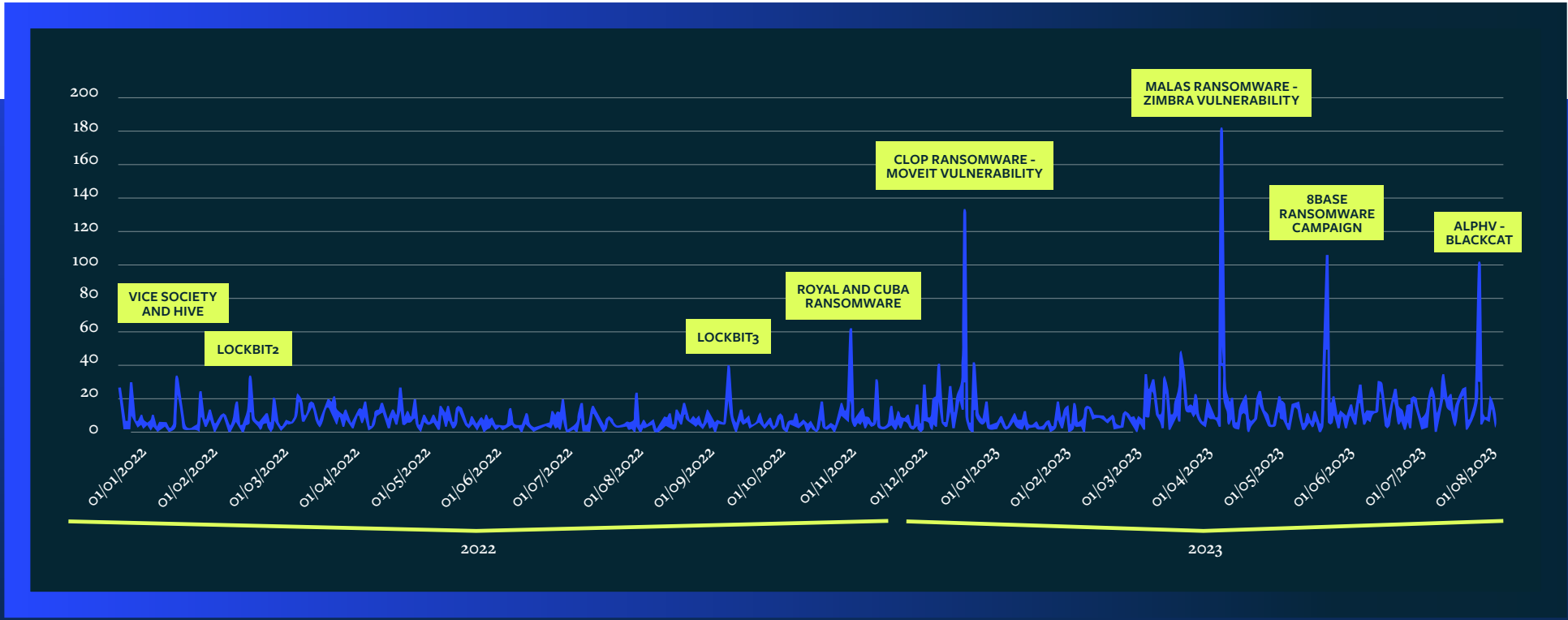



**FIGURE 1:** RANSOMWARE VICTIMS DURING 2022 AND 2023

# 2023 H1 vs 2022 H1 and H2

Large-scale ransomware campaigns were mentioned as a prediction in our last interim report. As you can see in Figure 1 and 2, no matter how you compare it with previous timeframes, ransomware operators are working harder and breaking records for victims.

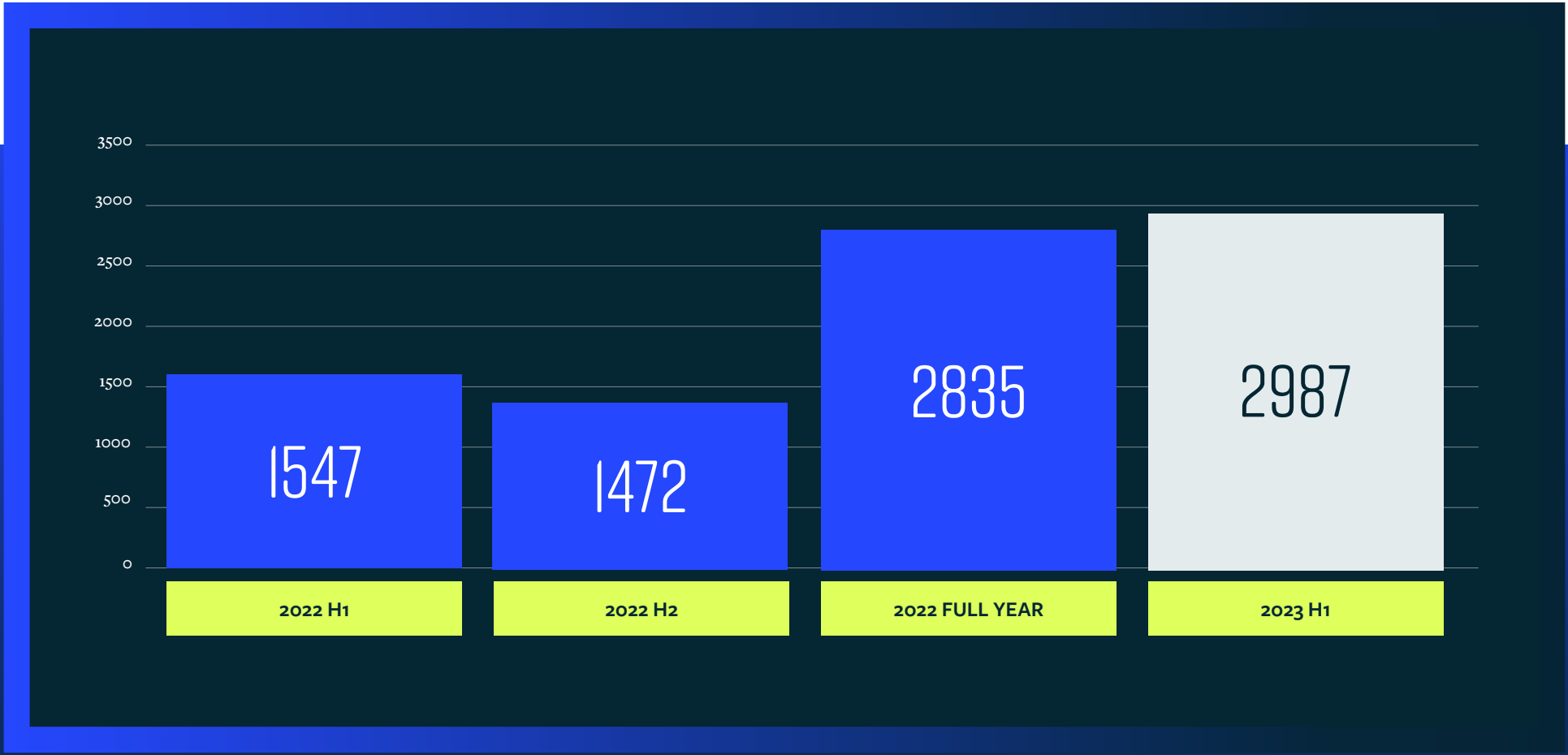



**FIGURE 2: NUMBER OF RANSOMWARE VICTIMS IN 2022 VS 2023**

## Ransomware threat actors:

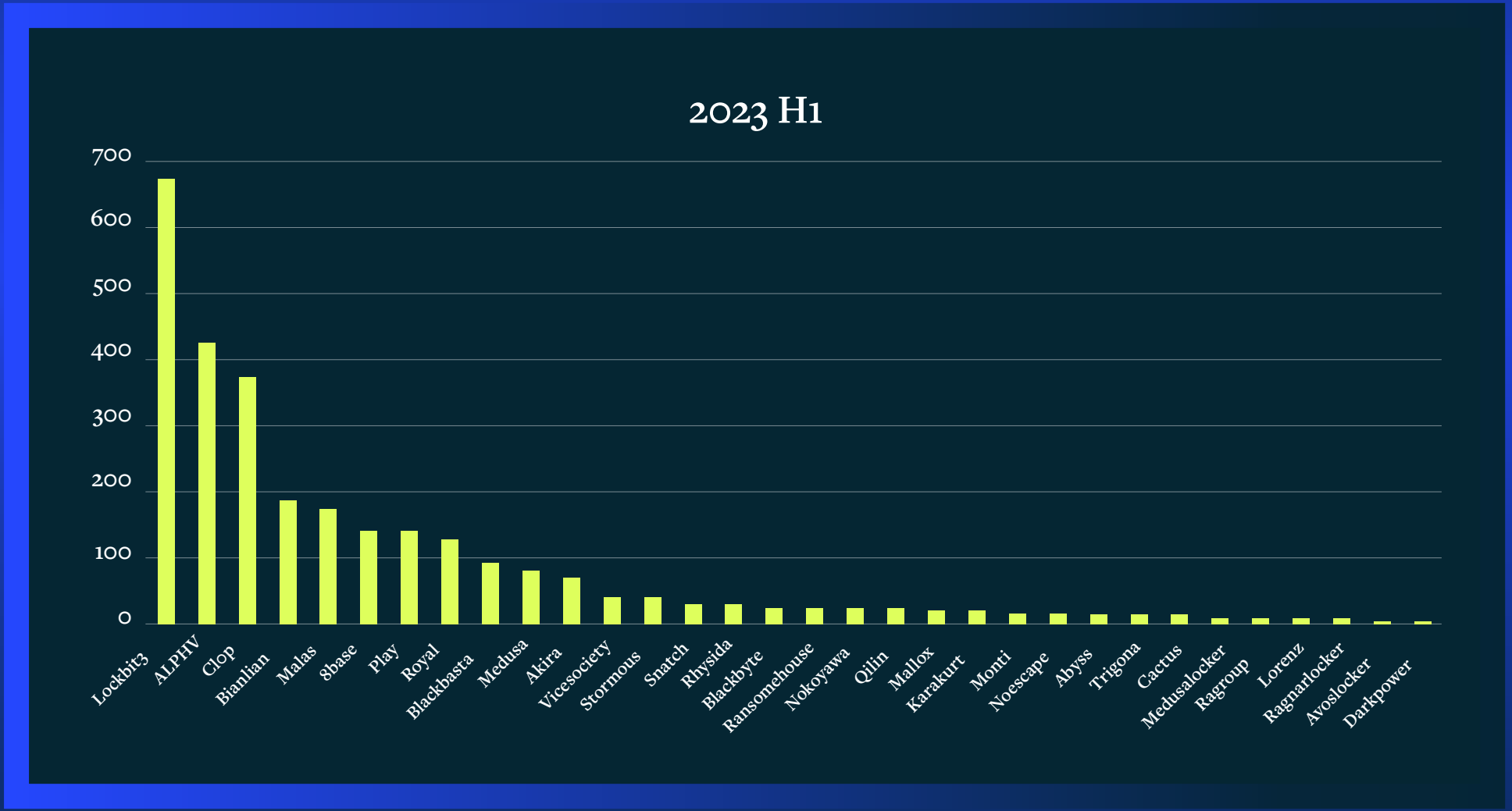



FIGURE 3: RANSOMWARE VICTIMS BY THREAT GROUP DURING 2023

# Ransomware Descriptions by Family and Activity Overview

## 01 LOCKBIT

In January 2020, LockBit posted an announcement that they had opened an affiliate program, becoming a RaaS. They noted that the development of the locker started in September 2019.

About a year after launching the service, in 2021, LockBit upgraded to version 2.0. According to their advert on underground forums, it is "the fastest encryption software all over the world." Some of the new features included an option to print ransom notes on network printers, automatically remove shadow copies, and clear logs. They also offer the option to use Wake-on-LAN (WoL) to power-on switched off computers.

After another year of operation, LockBit announced that they were working on version 3.0, also known as "LockBit Black." In July 2022, the first LockBit 3.0 attacks were reported. LockBit continues to claim to be the fastest ransomware to attract affiliates to use their software.

## 02 ALPHV

BlackCat (aka AlphaVM or AlphaV) is a ransomware family created in the Rust programming language and operated under a RaaS model.

BlackCat is primarily delivered via third-party frameworks and toolsets (for example, Cobalt Strike) and uses exploitation of exposed and vulnerable applications (for example, Microsoft Exchange Server) as an entry point. BlackCat has variants that work on both Windows and Linux operating systems, as well as in VMware ESXi environments.

In most of the attacks, BlackCat exfiltrates data from the victim using a BlackMatter exfiltration tool. If the ransom is unpaid, they either publish the data or sell it via their data leaks site.

BlackCat continues to make gains in popularity because it's paying most of the money earned from successful ransomware attacks to affiliates and insiders.

## 03 CLOP

Mainly known as Clop, this ransomware targets various industries and organizations, extorting data for a considerable ransom. It advances actively with new emerging campaigns. The Clop ransomware is associated with the Russian threat group TA505, which primarily operates as a RaaS. The threat group has been using various zero-day exploits for its campaigns, which include the latest MOVEit Transfer exploitation.

The ransomware is primarily Cryptomix ransomware, making its first appearance since 2019. Its leader is on the FBI's Most Wanted list and is communicating mainly using his Twitter (X) account, "ransomboris." Clop recently moved to use torrents to leak data and evade takedowns of their leak sites.

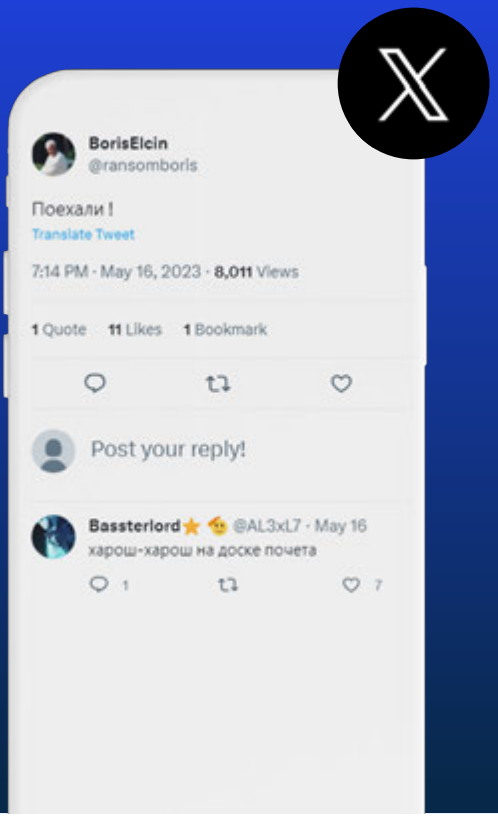



FIGURE 4: CLOP RANSOMWARE MEMBER TWEETED "LET'S GO!" AFTER THE FBI IDENTIFIED HIM AS WANTED FOLLOWING SEVERAL MAJOR CAMPAIGNS IN THE US.

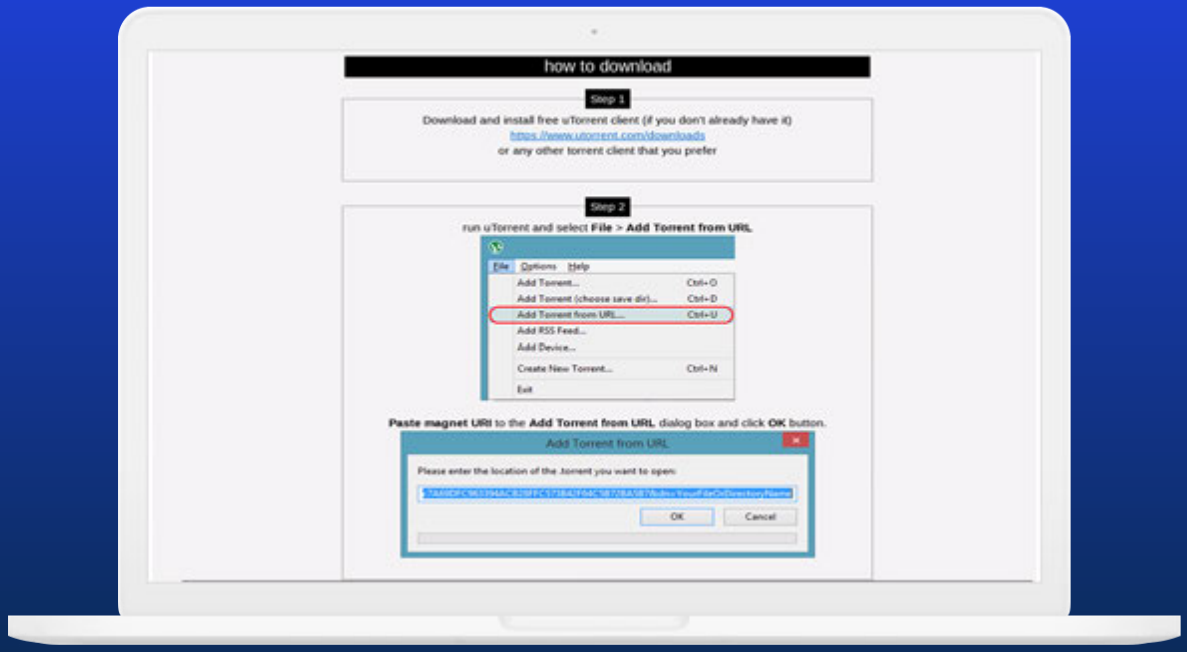



FIGURE 5: CLOP USING TORRENTS TO LEAK DATA

## 04 BIANLIAN

BianLian is a ransomware developer, deployer, and data-extortion cybercriminal group that has targeted organizations in multiple U.S. critical infrastructure sectors since June 2022. They have also targeted Australian critical infrastructure sectors, in addition to professional services and property development.

The group gains access to victim systems through valid Remote Desktop Protocol (RDP) credentials, uses open-source tools and command-line scripting for discovery and credential harvesting, and exfiltrates victim data via File Transfer Protocol (FTP), Rclone, or Mega. BianLian group actors then extort money by threatening to release data if payment is not made. The BianLian group originally employed a double-extortion model in which they encrypted victims' systems after exfiltrating the data; however, around January 2023, they shifted to primarily exfiltration-based extortion. The ransomware itself is Golang malware with several anti-analysis features.

## 05 MALAS

Also known as MalasLocker, this is a new ransomware group that was first observed at the end of March, 2023. Instead of demanding a typical ransom, the group claims to donate to a charity they approve of to provide a decryption tool and prevent data leakage of its victims. Their demand strategy may change in the future.

The threat group is using an open-source tool known as "age" for encryption. The threat group was at the top of the list of ransomware operators in 2023 H1 due to the massive attack campaign exploiting vulnerable Zimbra servers.

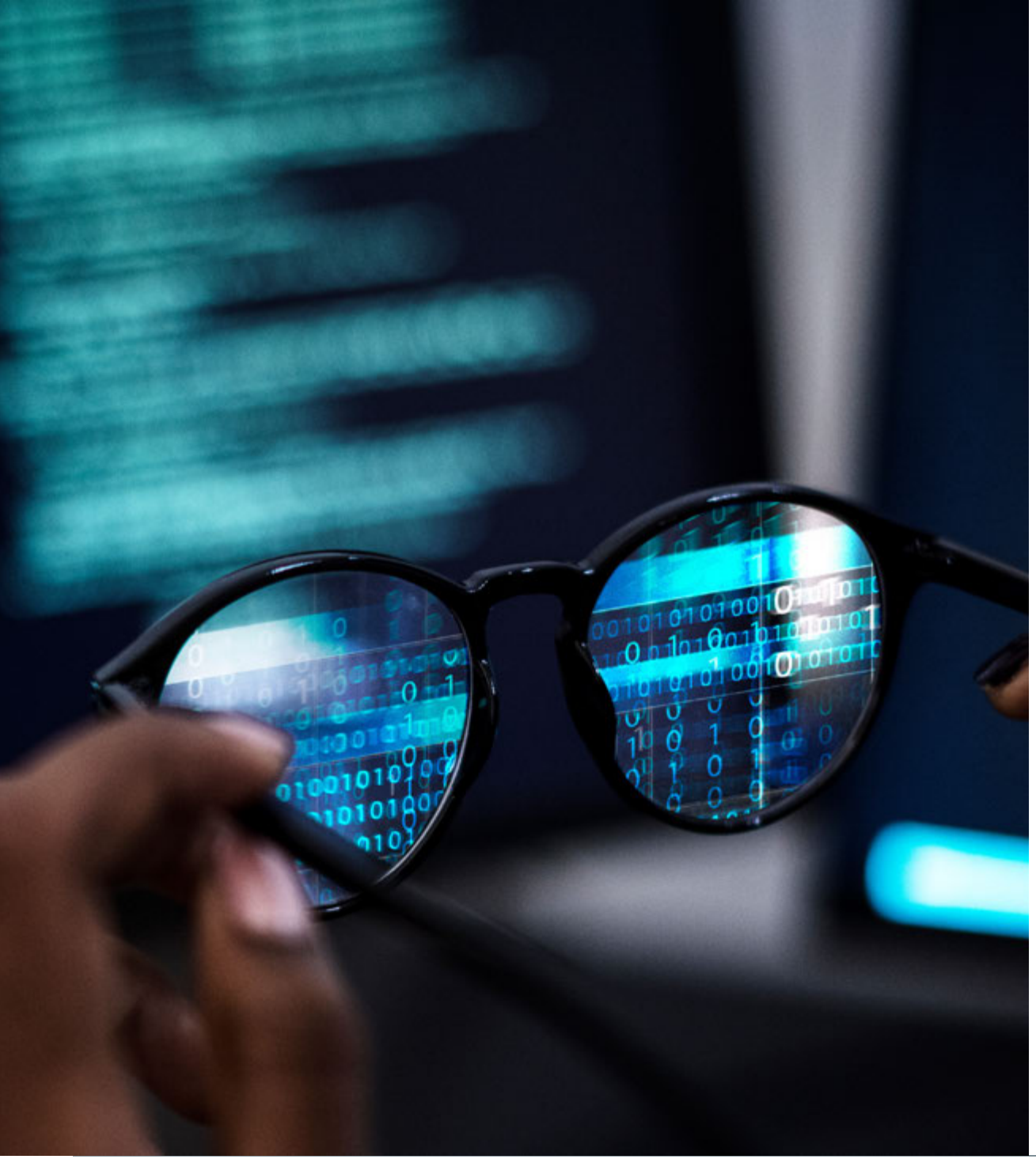
## 06 8BASE

8Base is a ransomware group that emerged in April 2022 and quickly became infamous for its aggressive approach attacking mainly small to medium-sized businesses across various industries. Although much about 8Base remains unknown, their communication style and information from their leak site hint at similarities with RansomHouse, a group known for buying compromised data and partnering with data leak sites for extortion. This has sparked rumors that 8Base might be linked to RansomHouse. Additionally, there are indicators that 8Base may have originated from the leaked Babuk builder.

## 07 PLAY

The Play ransomware, also known as PlayCrypt, often uses techniques to neutralize anti-malware and monitoring systems before performing the ransomware execution by employing tools such as Process Hacker, GMER, IOBit, and PowerTool. In 2023, this group was identified exploiting two specific vulnerabilities in Microsoft Exchange. Interestingly, there are distinct similarities between Play ransomware and two other strains: Hive and Nokoyawa.

This has led to hypothesizing a connection, especially considering that Hive, once among the top-three most active ransomware groups in 2022, has since vanished from the prominent ransomware threat list. The underlying links might provide insights into the shifting landscape of these ransomware groups.



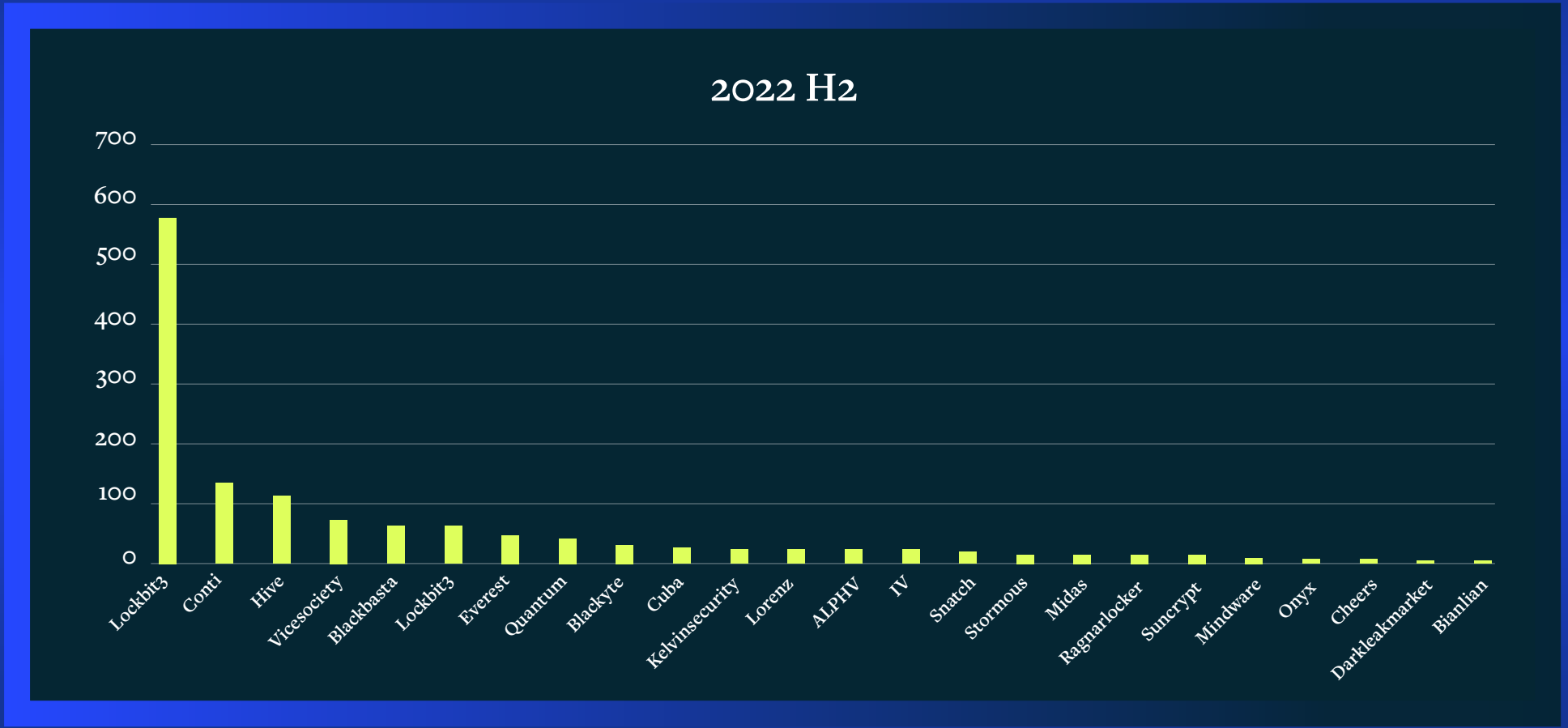
## 08 ROYAL

The Royal ransomware group, first observed in September 2022, is known for its distinct encryption method. Unlike standard practices, they employ a unique partial encryption tactic, enabling them to encrypt only a specified percentage of data within a file. This method, particularly beneficial for larger files, helps evade detection by security systems. However, their menace doesn't end at encryption; the Royal actors also utilize double extortion by threatening victims with the public disclosure of their encrypted data unless a ransom is paid.

Royal mainly uses phishing as their initial attack vector, but they've also been spotted exploiting valid Remote Desktop Protocol (RDP) credentials, as well as compromising web applications and brokers. Their activities have notably targeted critical infrastructure, with the healthcare sector being particularly vulnerable to their attacks.

What sets the Royal ransomware group apart is their organizational structure. Eschewing the prevailing model of recruiting affiliates for RaaS, Royal operates privately, comprising former members from the notorious Conti ransomware group.

**FIGURE 6: TOP THREAT GROUPS IN 2022 H2**




There are several other Ransomware operators still in business but no longer making a significant impact.

## 09 EVEREST

Known primarily as the result of targeting NASA partners, the Everest ransomware group emerged around December 2020, concentrating its attacks on organizations in the Americas and particularly focusing on the capital goods, healthcare, and public sectors. Among their most notable targets are telecommunications giant AT&T and several South American government entities.

Unlike many other ransomware factions that directly extort their targets, Everest has been increasingly functioning as an "Initial Access Broker." These are cybercriminals who sell entry points into organizations to other miscreants rather than executing the attack themselves. This modus operandi is relatively uncommon since ransomware attacks generally yield more profit than merely selling access.

## 10 LORENZ

This is a threat group that has similarities to ThunderCrypt. To pressure victims into paying the ransom, Lorenz first makes the data available for sale to other threat actors or possible competitors. Eventually, they start releasing password-protected Roshal Archive (RAR) archives containing the victim's data.

## 11 MIDAS

Also known as Midas Touch, Midas is one of the Thanos ransomware variants. The name Midas may come from the mythical king of Phrygia, known for the ability to turn everything he touched into gold. The ransomware is written in C# and obfuscated using SmartAssembly.

# Additional Known Threats

### 12 SNATCH RANSOMWARE

This ransomware group leverages an old, yet still working technique of rebooting the PC into Safe Mode to evade security products.

### 13 LV RANSOMWARE

LV ransomware mainly targets manufacturing, retail, and technology organizations in Europe, North America, and Asia. It has similarities with REvil crypter, first seen in 2020.

### 14 STORMOUS

This pro-Russian threat group is composed of ex-Conti members. The group recently showed up again with a new leak site.
Its partnerships and messages typically threaten Ukraine.

### 15 MINDWARE

Mindware is likely a rebrand of SFile ransomware. It was used mainly for attacking not-for-profit mental health providers.

### 16 DARKLEAKMARKET

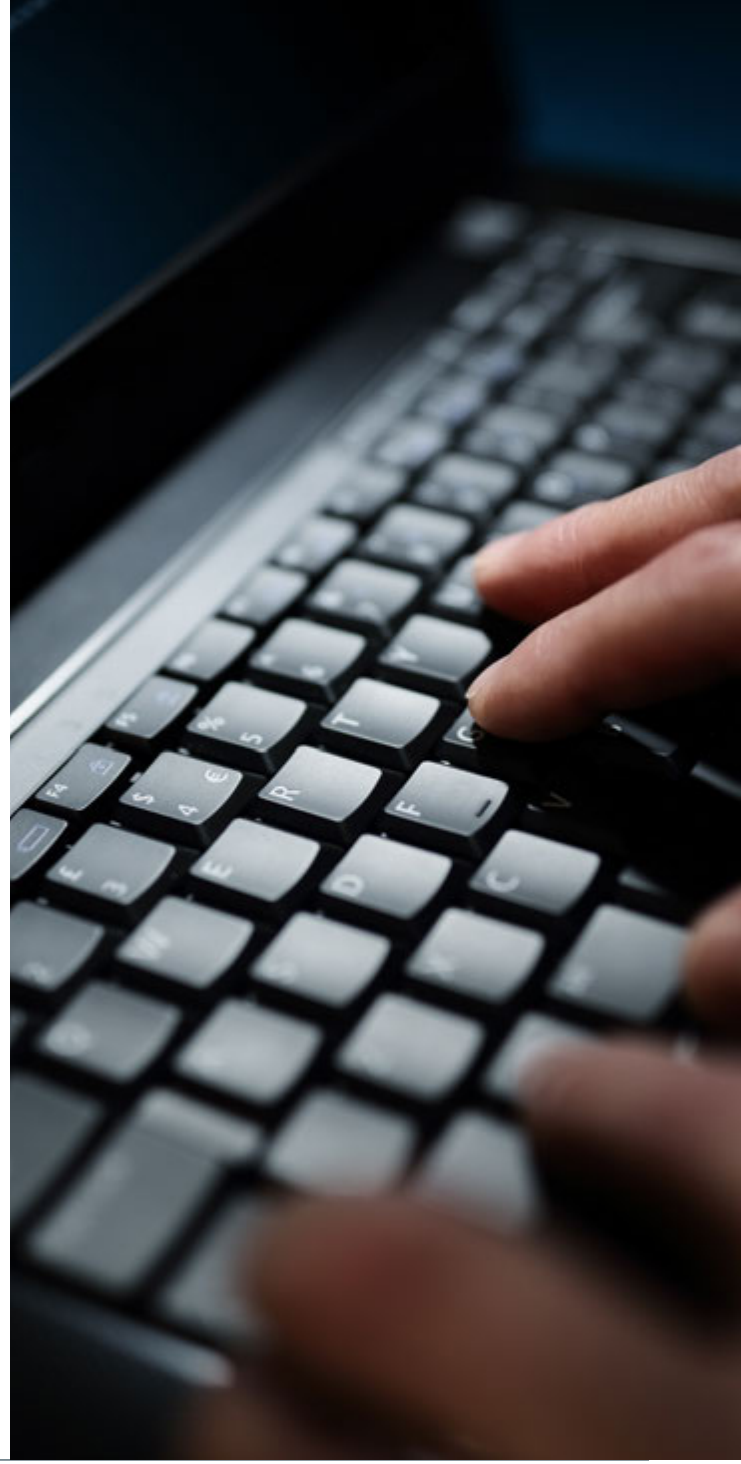
Darkleakmarket is known mainly as the result of attacking India's largest private bank.

### 17 CHEERS

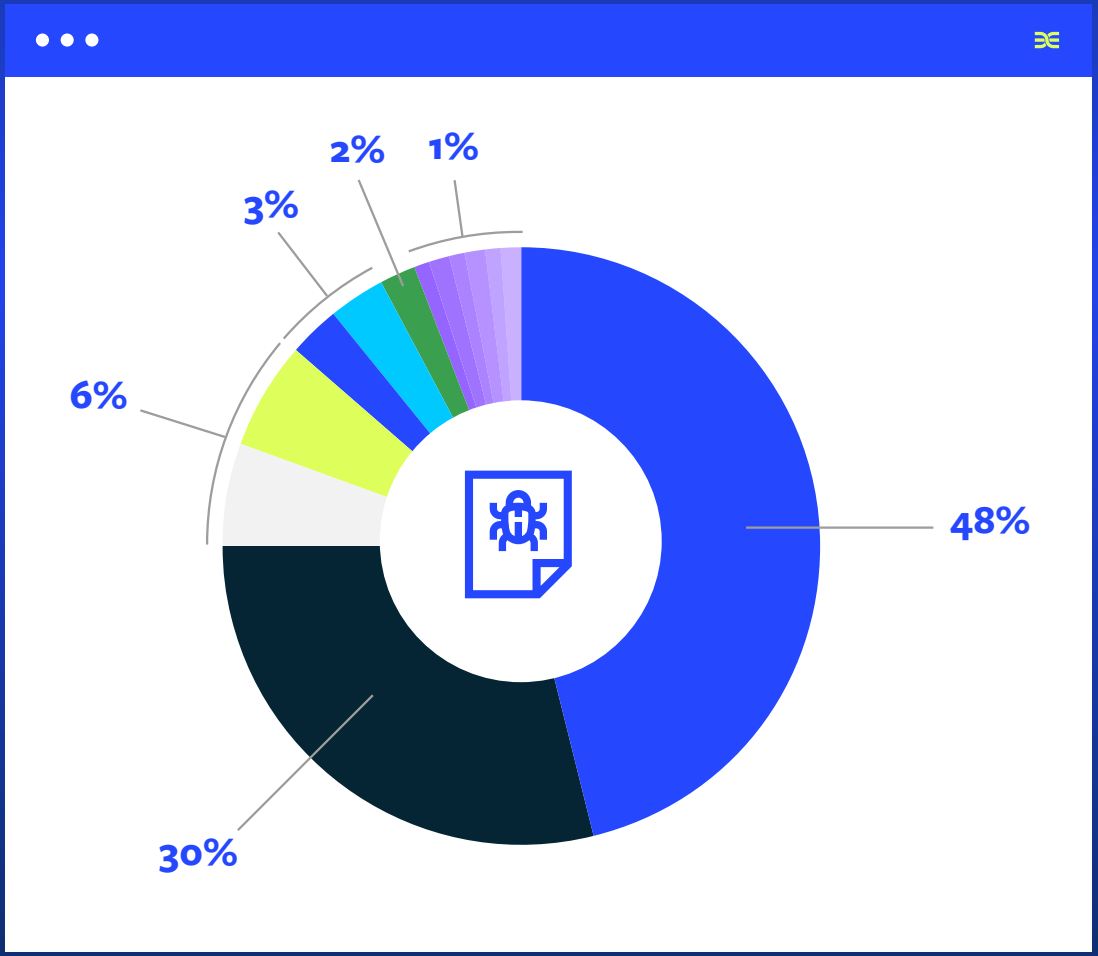
Cheers is a ransomware group targeting mainly Linux ESXi.

### 17 ONYX

Onyx is a .NET-based ransomware that switched to wiper mode.



# Top 5: Banking Trojans/Stealers/Spyware




**LEGEND**

- Emotet
- Agent Tesla
- NanoCore
- Redline Stealer
- Remcos
- Qbot
- IcedID
- LokiBot
- Njrat
- Vidar
- Ursnif
- Racoon
- Bumblebee

FIGURE 7: BANKING TROJANS/STEALERS/SPYWARE

# Top Stealers and RATs Overview

## 01 EMOTET

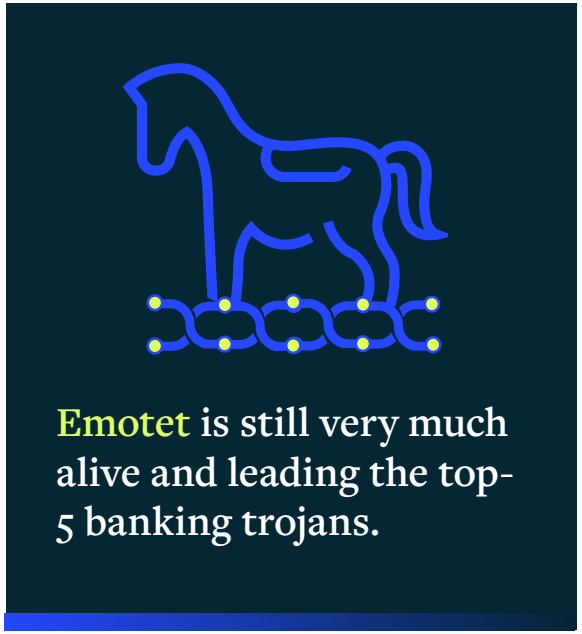
Emotet made its debut in 2014 as a banking trojan. It was spread via spam campaigns, imitating financial statements, transfers, and payment invoices. Emotet is propagated mostly via Office email attachments containing macros. If enabled, it downloads a malicious PE file (Emotet) which is then executed. Once executed, it can intercept and log network traffic, inject into browsers, and access banking sites to exfiltrate and store financial data.

In 2017, Emotet operators redesigned the trojan to work mainly as a Dropper, a type of malware that is designed to deliver other malware to a victim's computer. Other players in the cybercrime world, such as the TrickBot banking malware and Ryuk ransomware, utilize Emotet Dropper capabilities to infect countless other users.

Emotet evades security measures and moves laterally by leveraging a server message block (SMB) exploit or brute force of admin credentials, making it one of the most dangerous and dominant malware families in the wild. In early 2021, an international taskforce coordinated by Europol and Eurojust seized Emotet infrastructure, comprising several hundred servers located around the world, and arrested some of its operators. Additionally, in April 2021, law enforcement used the Emotet infrastructure to automatically uninstall the malware from infected systems. These actions stopped Emotet operations for a period, but in November 2021 new variants of Emotet were again spotted in the wild.

In early 2022, the notorious threat actor launched a massive phishing campaign in which it implemented highly-obfuscated VBA macros to avoid detection. In May 2022, Emotet started experimenting with LNK files, as a replacement for their Microsoft Office droppers. This change of approach, which is not unique to Emotet, is the result of Microsoft's decision to disable macros.

During 2023, Emotet added OneNote to its arsenal as an initial attack vector. That didn't last long as Microsoft deprecated the use of scripts inside OneNote. Later in 2023, Emotet adopted the recent trend of binary padding and artificial inflation to avoid detection.



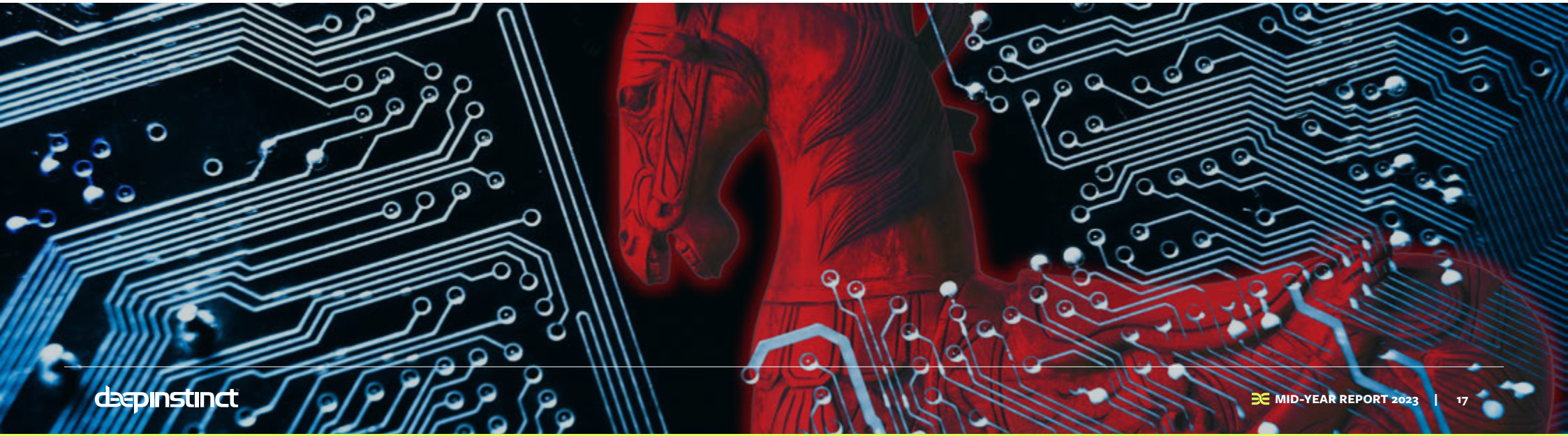
## 02 AGENT TESLA

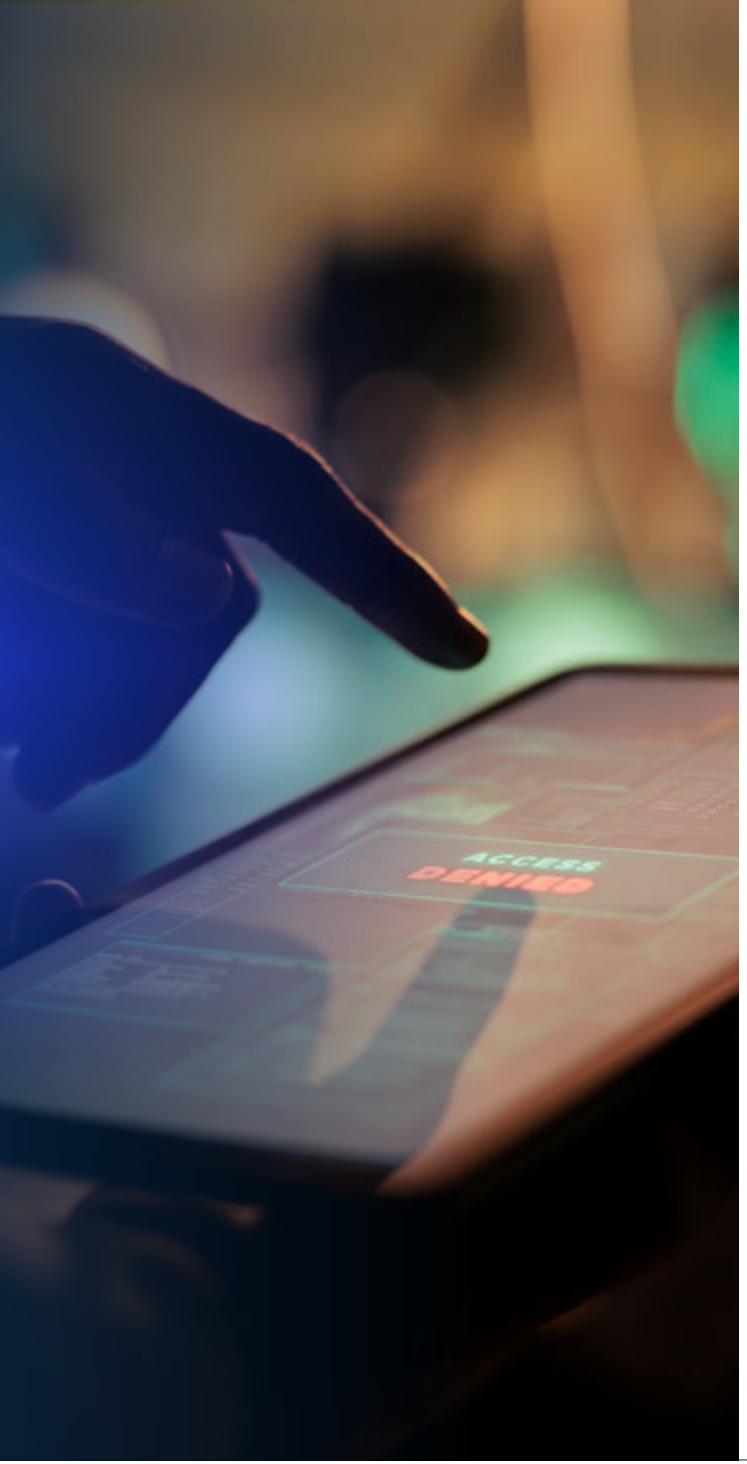
What started as keylogger in 2014 later became one of the most advanced and popular .NET-based RAT and data stealers. It facilitates initial access for cybercriminals, and it's often utilized in the Malware-as-a-Service (MaaS) model. In this nefarious business setup, threat actors, referred to as initial access brokers (IAB), lend their specialized skills to exploit corporate networks, collaborating with affiliate criminal factions. This first-stage malware allows remote access to infiltrated systems, paving the way for downloading advanced second-stage tools, such as ransomware.

## 03 NANOCORE

Also known as Nancrat or NanoCore, and managed by the APT33 threat group, it's used by cybercriminals as well as by nation state threat actors. NanoCore is a customizable RAT developed using the .NET framework. Its modifiable plugins allow attackers to adjust its functionality based on their requirements. Introduced in 2013, this malware has since gained worldwide popularity due to its modular nature. With plugins, the capabilities of NanoCore can be enhanced significantly, posing a heightened threat to organizational cybersecurity.

Remarkably, NanoCore is sold on its official website for a mere $25, inclusive of all official plugins, and comes with around-the-clock technical support. Moreover, "cracked" versions are available on hacking forums, further boosting its accessibility and usage. Despite the uncertainties surrounding its original purpose—whether developed as a legitimate commercial tool or with malicious intent—the creator, Taylor Huddleston, was apprehended by the FBI. The malware's affordability, simplicity, and widespread information have played a big role in its escalating prominence.





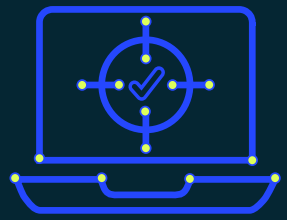

## 04 REDLINE STEALER

It is a type of malware available for purchase on illicit forums. Depending on the version, it's priced between $100 to $150 as a standalone product or can be accessed through a subscription model for $100/month. The malware is designed to extract data from browsers, including saved passwords, autocomplete details, and credit card information. Additionally, it conducts a system scan to gather information such as the user's name, location, hardware setup, and details about the security software in place. In its updated versions, RedLine has incorporated features to pilfer cryptocurrency. It also targets FTP and IM clients and can upload/download files, run commands, and routinely transmit data about the compromised system.

## 05 REMCOS

Short for "Remote Control & Surveillance," it's a RAT that provides cybercriminals with the ability to remotely control and monitor victim machines without the user's knowledge. It was first released around 2016 by BreakingSecurity, a European company that markets Remcos and other offensive security tools as legitimate software for remote administration but it's frequently abused by cybercriminals for malicious intent and sold on various underground forums.

Given its wide range of capabilities and its availability for purchase on the dark web, it has become popular among threat actors seeking to spy on, steal from, or otherwise exploit their victims.



During 2023 Remcos was detected in several major campaigns against European and US companies.

## 06 QBOT

Known as Qakbot, it's a popular information stealer and banking malware that has been active in the wild since 2009. Its main features enable it to steal online banking credentials and other financial information, though QakBot can also steal personal data such as files and keystrokes.

QakBot possesses worm features which allow it to spread through the network and removable drives. QakBot monitors the browser on the infected machine to detect when victims interact with an online banking website and then steals credentials. Additionally, QakBot collects additional information from the infected machine including IP address, country of origin, cookies, and other system information. QakBot's distribution methods vary and include malspam with specially crafted document attachments triggering the infection, or exploit kits deployed on compromised websites that deliver QakBot's payload to website visitors.

Qakbot has used different delivery methods over the years and refined their implementation to avoid detection. In early 2022, this process resulted in the adoption of Excel 4 Macros (XLM), VBA macros' older sibling, which gets less attention from anti-virus vendors, making it less likely to be detected. However, the use of XLM lasted only a few months, and in May 2022, the threat actor switched to LNK files because of Microsoft's intention to block all macros.

## 07 ICEDID

Also referred to as BokBot, it's a sophisticated banking trojan designed to steal users' financial details. It can also introduce other malware into the system. It employs a man-in-the-browser technique to snatch online banking login details. Once it obtains this information, it hijacks bank accounts to conduct unauthorized transactions.

While IcedID can spread through its own malicious email campaigns, it's frequently delivered as a follow-up payload by other malware, especially Emotet. To stay undetected, it employs strategies like embedding itself into the system's memory and standard processes.

Moreover, its creators consistently update it, enhancing its durability and ability to elude newer detection techniques. IcedID was first discovered in 2017 as a banking trojan and later evolved into a dropper and a second stage for many financially motivated cyber criminals.

During 2023, it adopted OneNote files as an initial vector, like many other threat actors. This technique didn't last for long. It was also detected dropping Nokoyawa ransomware, adding to the long list of ransomware that it has dropped over the years. The recent versions are using a custom socks5 named BackConnect.

## 08 LOKIBOT

Sometimes referred to as Loki PWS, it steals critical data, including usernames, passwords, and cryptocurrency wallet details. During 2023, it attempted to make a comeback with a campaign abusing Microsoft Office vulnerabilities.

# Top Takeaways

## STATE-SPONSORED ATTACKS

State-sponsored attacks continued to rise in 2023, breaking all records. Russia has become one of the leading threat actors in the world. After several cyberattacks in 2022, mostly on Ukrainian government websites, organizations, and companies, several Russian APT groups such as Sandworm, Callisto, and Gamaredon continued their campaigns against the Eastern European nation.

MuddyWater, also known as Mango Sandstorm (Mercury), is a cyber espionage group that is a subordinate element within the Iranian Ministry of Intelligence and Security (MOIS).

Deep Instinct's Threat Research team has identified a new C2 (command & control) framework.

This framework, named PhonyC2, is custom made, continuously in development, and has been used by the MuddyWater group since at least 2021. It is currently used in an active PaperCut exploitation campaign by MuddyWater

Another example for a state-sponsored attack is by Chinese threat actor Red Menshen (aka Red Dev 18), which has been observed targeting telecommunications providers across the Middle East and Asia, as well as entities in the government, education, and logistics sectors since 2021.

Deep Instinct's threat lab observed and analyzed a previously undocumented and fully undetected new variant of BPFdoor by Red Menshen APT.

## MACROS LEFT IN THE PAST, AS THREAT ACTORS WELCOME LNK, ARTIFICIAL INFLATION AND JAVASCRIPT

For years, macros in Office files were used as an initial stage by multiple threat actors. However, after Microsoft made macros automatically disabled by default, this became much less attractive as users needed to manually "enable content" to leverage this vector. That made threat actors search for a more hidden, evasive first step. Malicious LNK files, as a delivery method, is a technique that has been used for years.

This technique is efficient because it exploits a fundamental feature of Windows. Specifically, it automatically launches executables, such as PowerShell, using the metadata stored in the LNK file. Another technique that was recently raised is JavaScript. Deep Instinct researchers noticed their use recently in new campaigns of Bumblebee and IcedID. Both shared an obfuscated, minimally detected PindOS JS dropper.

This switch to JavaScript instead of PowerShell marks a significant change in more generalized and well established TTPs.

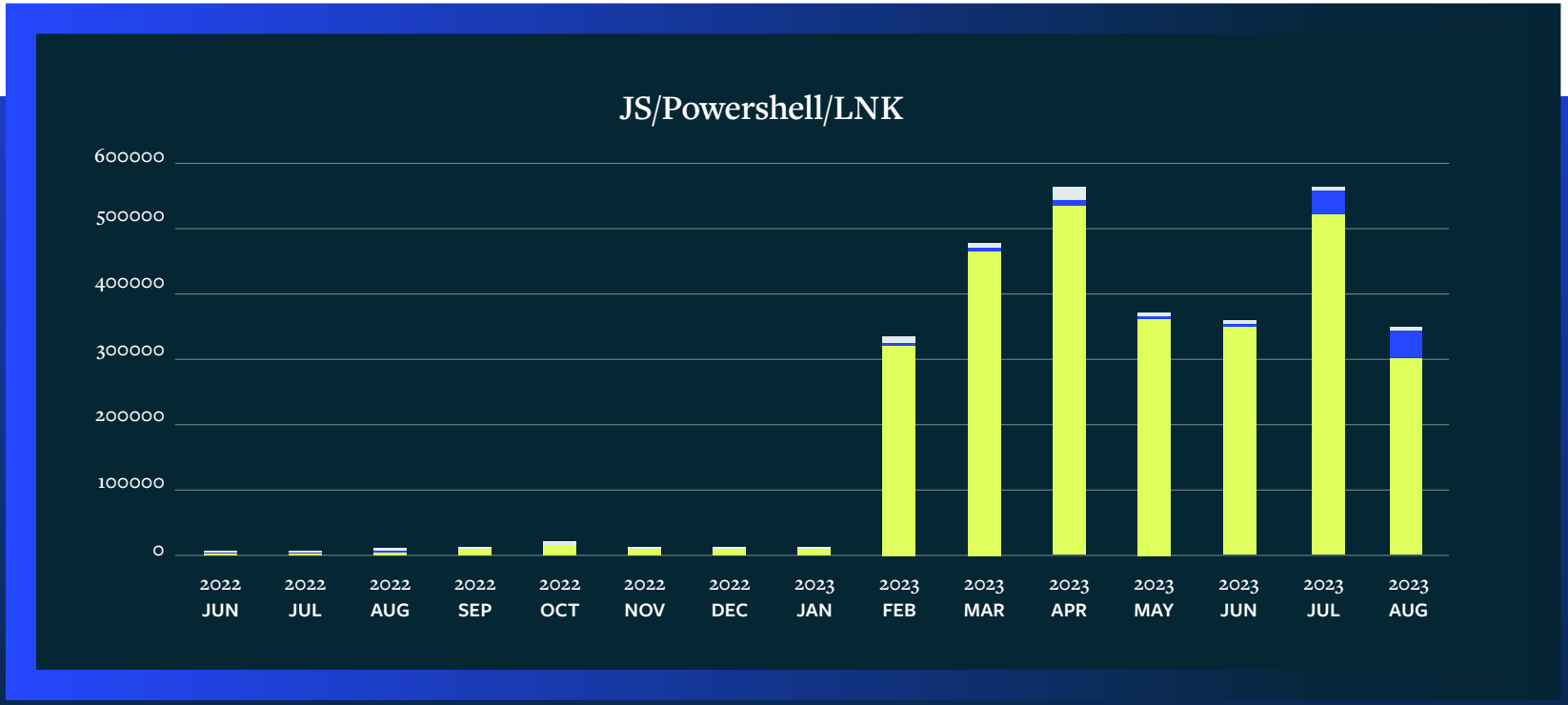



**FIGURE 8: THREAT ACTORS 2022 H2/2023 H1**

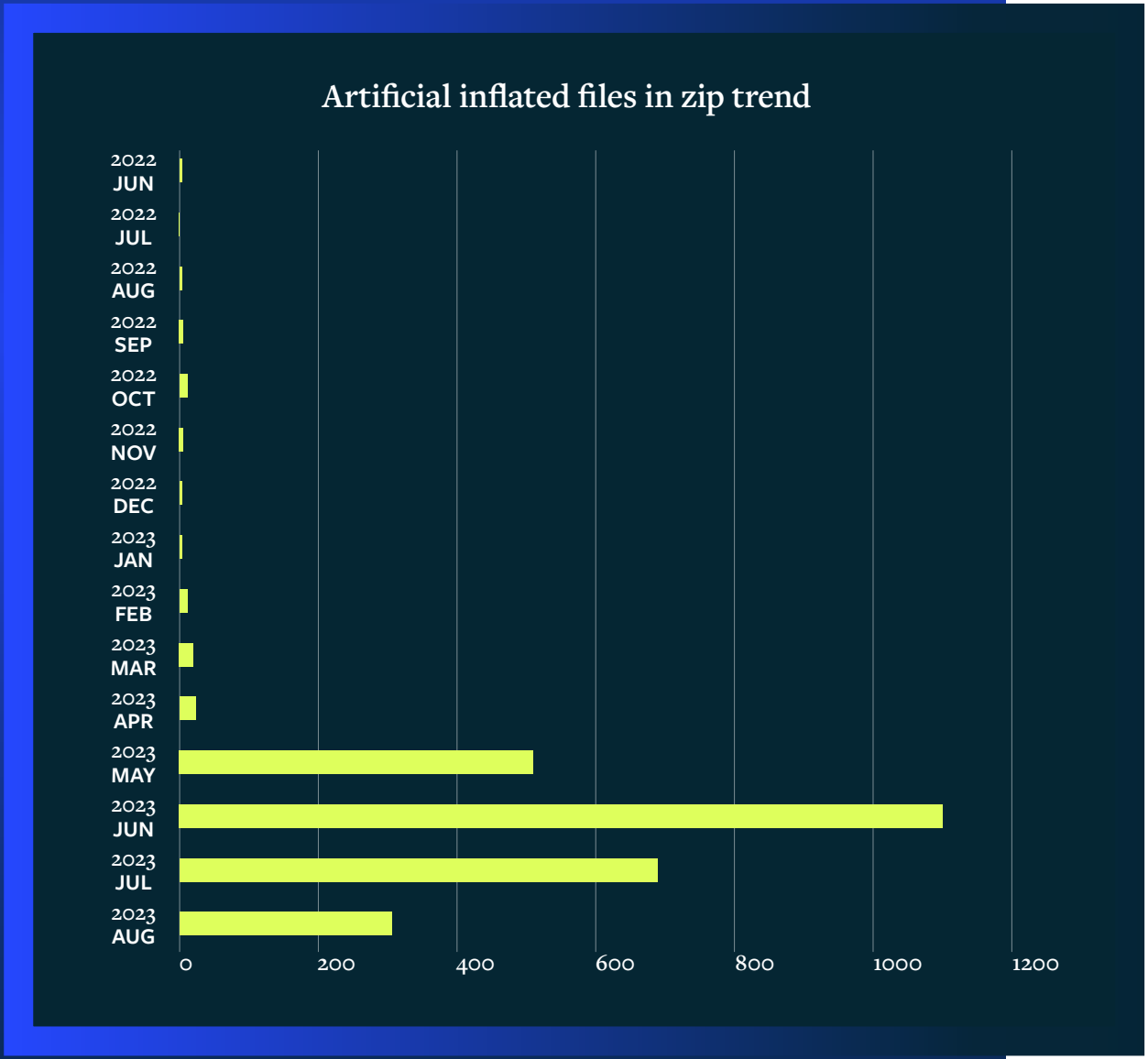



FIGURE 9: ARTIFICIAL INFLATED FILES IN ZIP TRENDS 2022 H2/2023 H1

Lastly, we've seen a rise in artificial inflation, which is padding the malicious file before or after the payload to make it large enough to evade security products (EPP and Sandboxes).

In addition, this technique changes the hash of the file and allows it to avoid hash-based detections. The technique uses zip files as the delivery method in order to keep the delivery files small. After extraction the files grow exponentially, expanding to hundreds of MBs in order to avoid anti-virus (AV) and Endpoint Detection and Response (EDR) scanning.


## UNDERGROUND FORUMS SHUT DOWN, BUT NEW ALTERNATIVE MARKETS EMERGE

Several large and known darknet and underground hacking forums were closed. Among those closed included the following:

- **RAID FORUMS**
- **GENESIS MARKET**
- **BREACHED FORUMS**
- **ASAP MARKET**

Additionally, several ransomware leak sites were seized by the FBI resulting in arrests of cyber threat actor gang members. Despite the arrests, growth continues. We're seeing a flow of new ideas to avoid seizure, including mirroring and alternative protocols. We're also seeing owners of the markets and forums that were closed open their own alternative markets.

While the leak sites have seen a significant increase in the number of victims on their sites, it's worth noting that in most cases victims are not paying quickly, or at all, and getting their leaked data published.

## POPULAR SYSTEMS BEING EXPLOITED

Vulnerabilities are still the most important component of large-scale cyber attacks. The usual flow is as follows:

- **A SEVERE VULNERABILITY IS PUBLISHED**
- **THREAT ACTORS SCANNING FOR VULNERABLE SERVERS FIND ONE**
- **THEY DEVELOP OR USE AN EXISTING POC FOR RANSOMWARE DELIVERY AND DATA EXFILTRATION**
- **THEY EXPLOIT IT ON ALL THE VULNERABLE SERVERS**

As we get closer to the end of the year, we typically see an increase of flows like this. A great recent example is the MOVEit vulnerability: a common platform with a vulnerability that has significant exposure to internet servers. For more information on MOVEit, see our blog. Also, note that a new SQL Injection vulnerability was recently found in MOVEit which has not yet been exploited in the wild. We expect to see more attacks abusing MOVEit, similar to what we saw with Log4j| and Log4Shell.

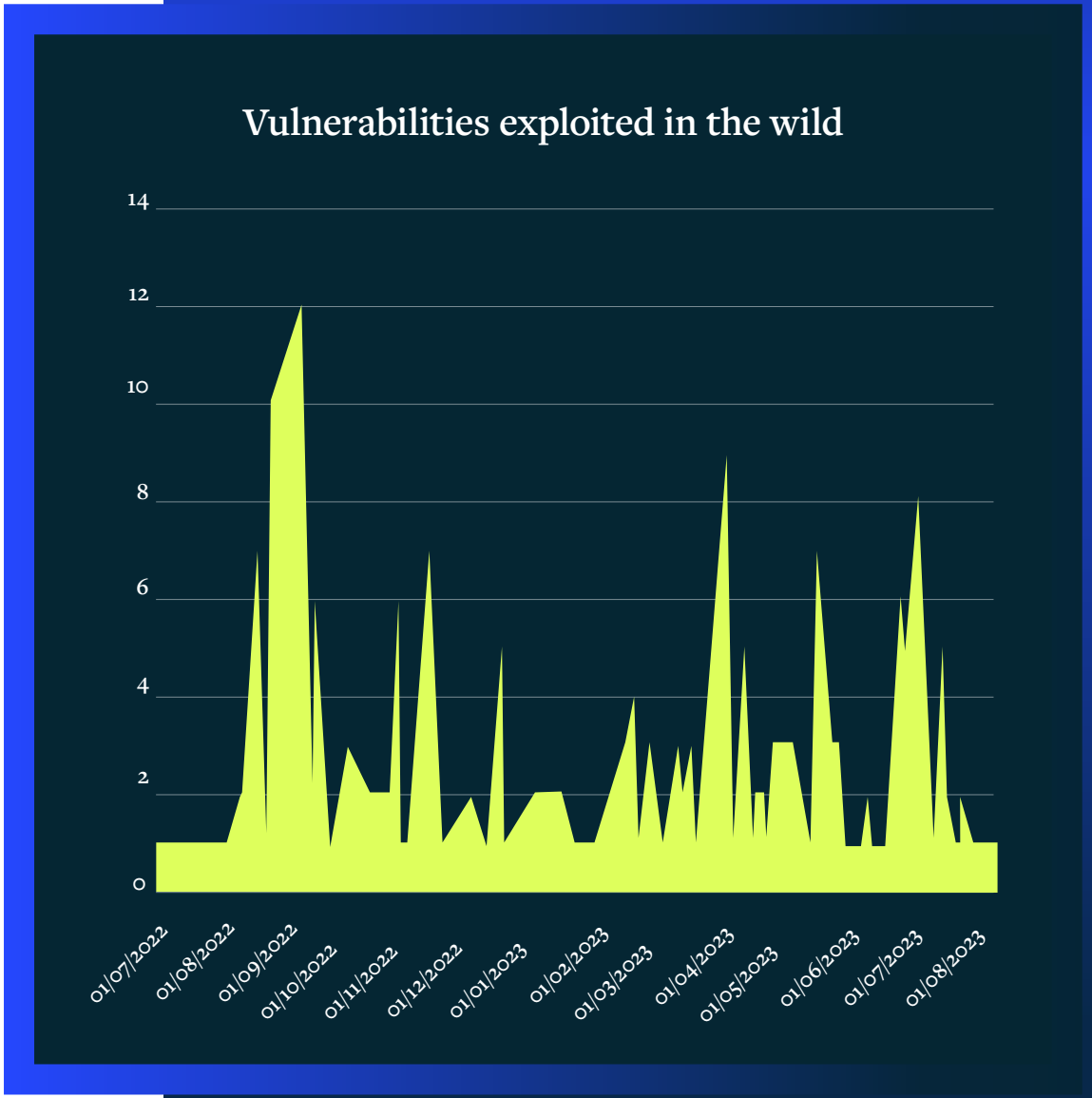



FIGURE 10: VULNERABILITIES EXPLOITED IN THE WILD

## LLMS INTRODUCE A NEW ERA FOR MALWARE BUILDERS

The year 2023 saw the rise of powerful Large Language Models (LLMs), and threat actors took advantage. They used ChatGPT and its alternatives using various "jailbreaking" guides in the underground and hacker forums and built their own LLMs for attack, including WormGPT.

Additionally, threat actors noted that ChatGPT was using "made up," non-existent, or deprecated code libraries in its responses. Threat actors decided to abuse those non-existent libraries by implementing them and adding malicious code. In the future, when ChatGPT suggests using those libraries, the user may be forced to download a code library with malicious code. We have demonstrated how ChatGPT can build nearly undetected malware.


**FIGURE 11: WORMGPT**

# Our Predictions for 2024

## THREATS BECOME EVEN MORE CUSTOMIZED AND SOPHISTICATED WITH AI

LLMs became a synonym for artificial intelligence (AI), which isn't accurate. We do believe that LLMs hold a lot of promise—but they are nowhere near their maximum potential yet. As public LLMs become more accurate and powerful, threat actors will leverage them aggressively.

We predict that LLMs will soon be able to perform standalone vulnerability research and exploit implementation and execute attacks, including custom obfuscation and custom malware builders like we've never seen before.

This is why it's critical to fight AI with a more advanced form of AI – specifically, deep learning. Only deep learning can combat these sophisticated and ever-increasing threats.

## LARGE-SCALE COMPROMISE ATTACKS WILL CONTINUE TO CAUSE FURTHER DAMAGE

Large-scale compromises are usually a result of a zero-day vulnerability exploit on a common system (SolarWinds, Log4j, MOVEit). Since vulnerability management is complex, especially in large organizations where it can take several months to patch systems, the best way to prevent damage is to block the payload before it can execute. In the first half of 2023, we have already seen a rapid increase in the exploitation of published vulnerabilities, especially in the first few weeks after a vulnerability is published.

## STEALTHY MALWARE AND AV SERVICE DISRUPTION BECOMES A CRITICAL COMPONENT IN THREAT ACTORS' ARSENAL

AV and EDR service disruption have become increasingly important to threat actors. Although most of the recent tools that were published used the same methodology of using vulnerable drivers (BYOD) and have a prerequisite of two highly privileged accounts, we believe that this path of development remains in focus for threat actors and security researchers.

## MACROS BECOME OBSOLETE, AS OTHER COMMON THREAT VECTORS TAKE PRECEDENCE

After a decade of macros and a very short spike of OneNote, it seems that LNKs, JS, and artificially inflated zipped files are here to stay. Those initial vectors are not easy to detect using classic AVs. We do not predict any new major initial vector to appear in the near future.

## STATE MOTIVATED CYBER ATTACKS BEGIN TO LEVERAGE AI

As the war between Russia and Ukraine continues, we expect to see the same level - or even more - state-motivated cyber attacks from threat actors on both sides.

After more than a year, several powerful threat groups from the ex-Soviet Union divided into pro-Russian and pro-Ukraine groups resulting in a full cyber warfield.

These cyber attacks mostly exist to leak sensitive data or disrupt services. Leak sites and underground forums are full of leaks from companies on both sides, with several leaks by pro-Ukraine threat groups.

Additionally, there are more state-scale attacks around the world in the U.S. and Europe by pro-Russian threat actors.

The cyber warfield will become very dangerous when AI and LLMs get included in large-scale cyber war. There are already some signs that Russia is using an AI scanner for "objectionable" material online, such as so-called propaganda named Oculus. It was launched in February 2023 and has already leaked source code. This type of tool can cause immense damage.

**This report was authored by members of the Deep Instinct Threat Research team:**

Shaul Vilkomir-Preisman

Bar Block

Simon Kenin

Mark Vaitzman

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt.

Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack — providing complete, multi-layered protection against threats across hybrid environments.



**deepinstinct.com**