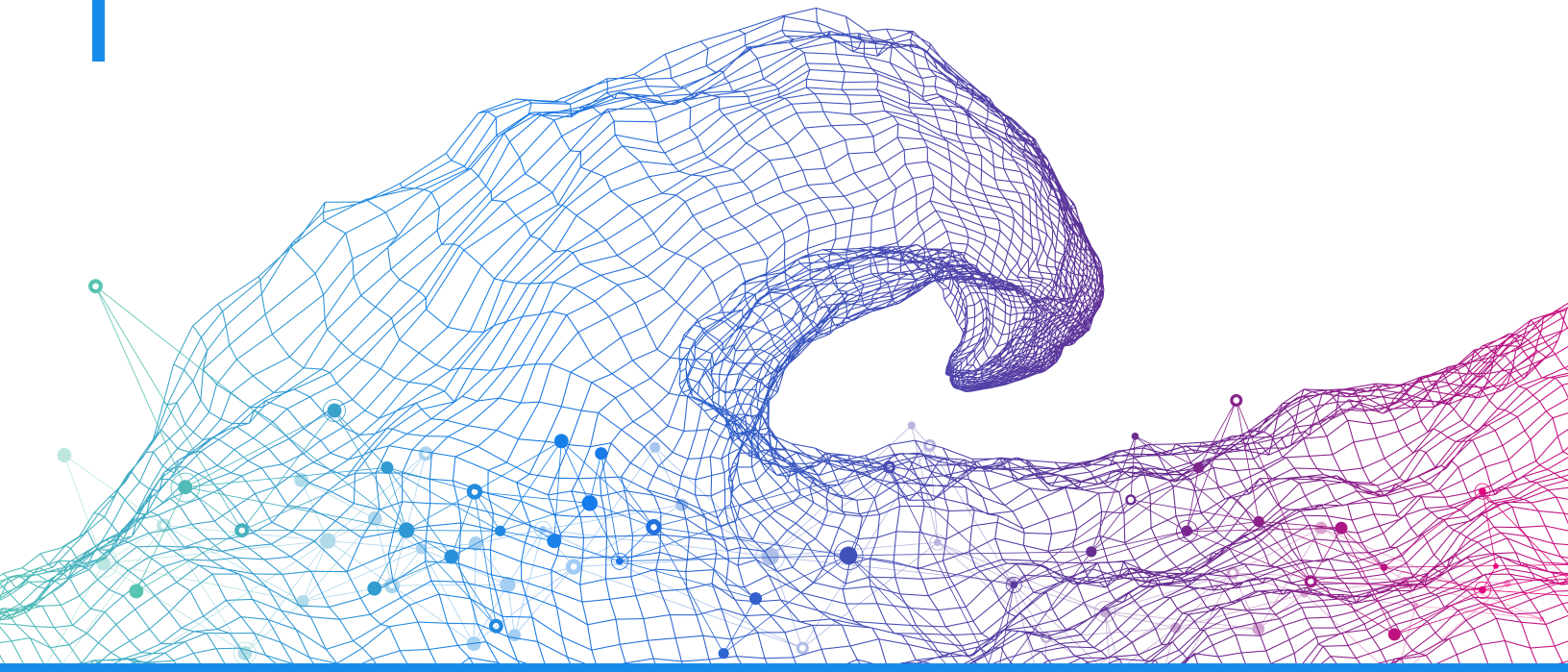
H1 2023
CRIMEWARE TRENDS
AND HIGHLIGHTS
AUGUST | 2023

Arete

Turning Tides

Navigating the Evolving World of Cybercrime

Executive Summary



In the first half of 2023, Arete observed several distinct trends and shifts in the cyber threat landscape. Leveraging the data collected during each incident response engagement, we can see the rise and fall of ransomware variants, notable trends in ransom demands and payments, industries targeted by ransomware attacks, and what may be coming next.

Looking back over the past few years, Arete has seen a pattern of action-reaction developing within cybersecurity. In response to several high-profile attacks in the past three years, many organizations invested in security tools, training, and services to reduce risk. To evade these standard security tools and common defense strategies, threat actors shifted their operations to target different types of operating systems with increasingly complex tactics.

The threat landscape continues to evolve with the widespread introduction of AI tools, lower barriers of entry into cybercrime, new vulnerabilities, and the socioeconomic effects of the Russia-Ukraine war. Ransomware operations thriving today are pushing the envelope in development and extortion techniques. Attrition, reorganization, and re-branding within cybercriminal groups have made attribution more challenging than ever.

However, as threat actors evolve, so do the threat hunters and organizations tracking them. Global law enforcement agencies have carried out several impactful arrests and seizures on multiple high-profile cybercriminal groups in the first half of 2023. We have seen a significant increase in collaboration between law enforcement agencies and civilian cybersecurity organizations, resulting in unprecedented information sharing on indicators and tactics, allowing for more accurate attribution, restoration, and potential disruption of ransomware threat actor activities.

Overview

FIRST HALF OF 2023 (H1 2023) HIGHLIGHTS FROM ARETE'S INCIDENT RESPONSE ENGAGEMENTS

- Mainstay actors prevail and new players arrive on the scene
- Professional services is the most targeted industry
- The percentage of incidents where a ransom is paid fell to 19%

OPENING THE FLOODGATES: LOWER BARRIER OF ENTRY INTO CYBERCRIME

- Cybercrime-as-a-Service on the rise
- Leaked source code skyrockets accessibility
- Artificial Intelligence changes the game

OTHER NOTABLE TRENDS

- Threat actors move to exfiltration-only operations
- Targeting of Linux and macOS systems increases attack surface
- Cascading effects of the Russia-Ukraine War continue
- Global law enforcement targets cybercriminals

* Disclaimer: Unless otherwise noted, all data within this report is based on Arete incident response cases.

H1 2023 Highlights From Arete's Incident Response Cases

Using frontline data from incident response engagements, Arete identified and analyzed notable trends and shifts that highlight the evolving state of the cyber threat landscape.

Top Variants Observed

In the first half of 2023 (H1 2023), we saw LockBit rise to the top spot, accounting for 30.3% of Arete's observed ransomware cases. New variants appeared on the scene, including Akira and Luna Moth. Despite the emergence of new variants over the past two years, Arete data indicates that dominant and well-established actors still maintain their top positions.

TOP RANSOMWARE VARIANTS OBSERVED

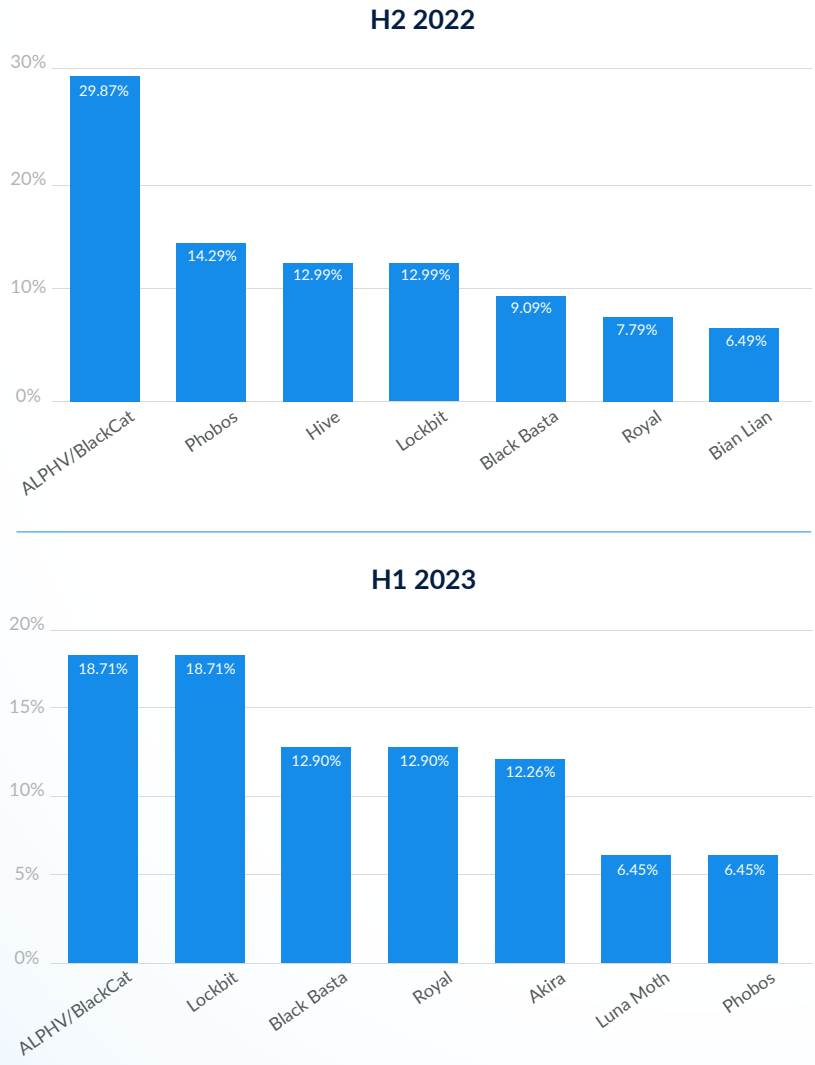


Figure 1: Top Ransomware Variants Observed in H2 2022 and H1 2023

Figure 2 shows the top ransomware variants observed over the past 4 quarters and is color-coded according to each variant's current state of activity.

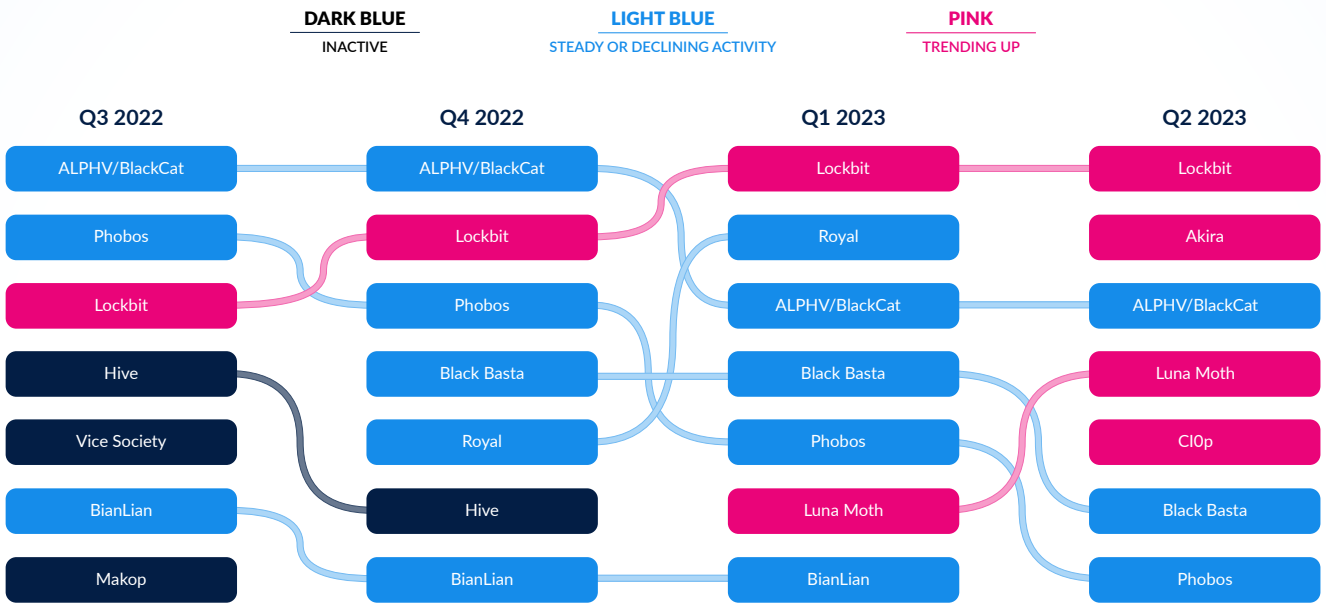


Figure 2: Top Ransomware Variants Observed from Q3 2022 to Q2 2023

LockBit and ALPHV/BlackCat retained spots in the top three over the past four quarters, showcasing their continued dominance. Lockbit has made continuous development efforts throughout its tenure, including improvement to its ransomware builder, releasing new builders to their affiliates, and working to target other operating systems. Lockbit can now target Linux systems, and a developmental Lockbit macOS encryptor was spotted in the wild. Arete has observed updated versions of LockBit, including LockBit Green and LockBit Black.

BlackCat utilizes a unique method requiring command line arguments to encrypt files on victim systems. To aid in propagation, the group uses stolen admin credentials together with the embedded PsExec utility, eliminating the need to propagate the ransomware manually. This, together with additional techniques and benefits to affiliates, could contribute to its ongoing status as one of the top three most prevalent threat actor groups.

Another variant observed over the past three quarters is Royal ransomware, which, like BlackCat, requires command line arguments to run correctly in a victim system. Royal has been active since September 2021 and was first observed in an Arete engagement during Q4 2022. In Q1 2023, we observed a spike in cases, but the frequency subsequently dropped in Q2.

In Q2 2023, we observed the emergence of Akira, a new ransomware group that quickly became the number two most observed variant. In June 2023, a cybersecurity firm released a free Akira decryptor requiring unencrypted and encrypted file pairs to decrypt correctly. We expect to see Akira release an updated version of their ransomware, eliminating the flaw that allowed the creation of the free decryptor. However, like some other ransomware operations, they may decide to move to an extortion-only model at some point.

See page 10 for tactics, techniques, and procedures (TTPs), and detailed insights on the top five variants observed.

TOP 5 INDUSTRIES IMPACTED BY RANSOMWARE

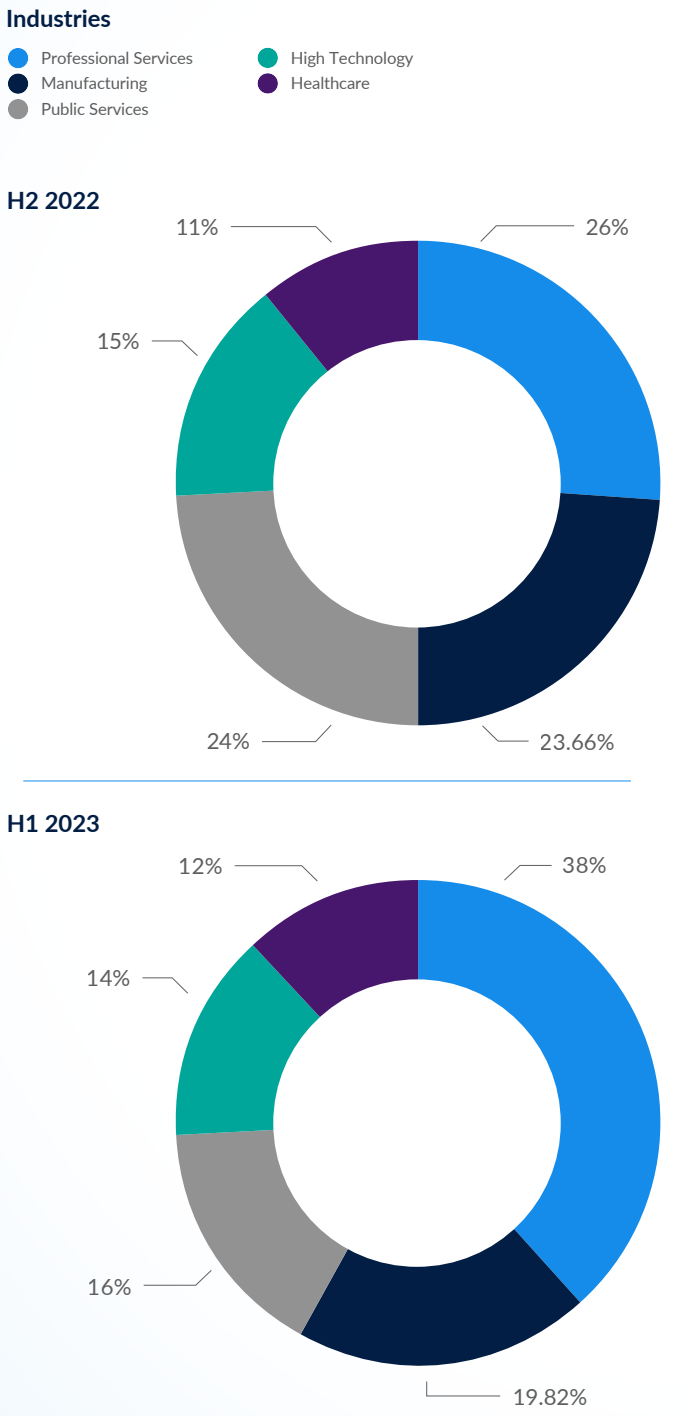


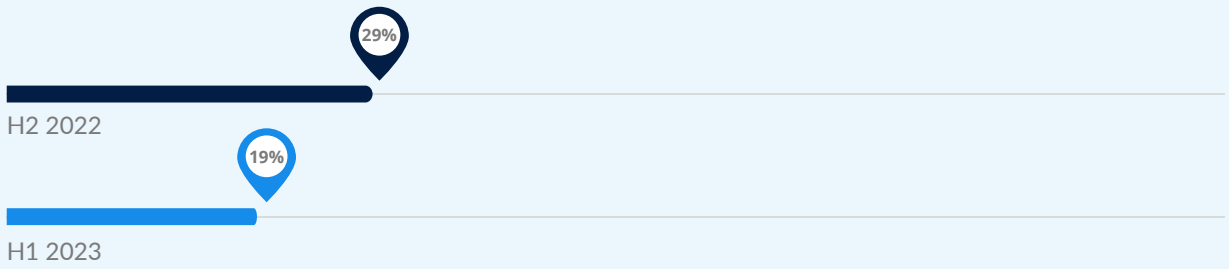
Figure 3: Top 5 Industries Impacted by Ransomware in H2 2022 and H1 2023

In the first half of 2023, Arete saw a distinct rise in targeting against the professional services sector, an almost 12% increase from the second half of 2022. This is primarily due to the rise in activity from the extortion group Luna Moth, which disproportionately targeted law firms. Luna Moth's activity subsequently declined in the second half of Q2, and we expect to see a decrease in the targeting of the professional services sector in Q3 due to Luna Moth's drop in activity.

Interestingly, from the various industries we track in our data, the top five industries impacted by ransomware stayed the same from the second half of 2022 to the first half of 2023. These industries have each retained a spot in the top five since 2019. Organizations in these industries often house valuable data, including customer information, intellectual property, financial records, and operational secrets that threat actors can exploit for monetary gain or competitive advantage. These industries also consist of critical operational facilities like manufacturing plants, hospitals, and transportation networks that may make them more willing to pay ransoms to restore operations and avoid disruption. These industries will likely remain in the top five as threat actors continue to follow the money and leverage their successful experience in attacking these organizations.

Ransom Demands and Payments

Percentage of time a ransom is paid



Median Ransom Demand

While the overall ransom demands from cybercriminals continue to trend upwards, Arete's data shows that a ransom was paid in just 19% of cases in the first half of 2023. This may be due in part to the industry-wide increase in exfiltration-only attacks.

Arete has also enhanced our ability to restore clients to normal operations without ransom payments. Arete's restoration engineers build tailored restoration and remediation plans for our clients. These tailored plans allow Arete to assess the impact of a ransomware event properly, determine the validity of the organization's backups, identify recoverable data via means other than backups, and create a timeline for restoration. This data-driven analysis helps create the best path forward and often eliminates the need to pay a ransom. The facilitation of a ransom payment is always a last resort for Arete, and we are proud to have avoided the need for our clients to pay a ransom in over 80% of our cases this year.

The facilitation of a ransom payment is always a last resort for Arete, and we are proud to have avoided the need for our clients to pay a ransom in over 80% of our cases this year.

Initial Access Vectors

TOP METHODS OF INTRUSION

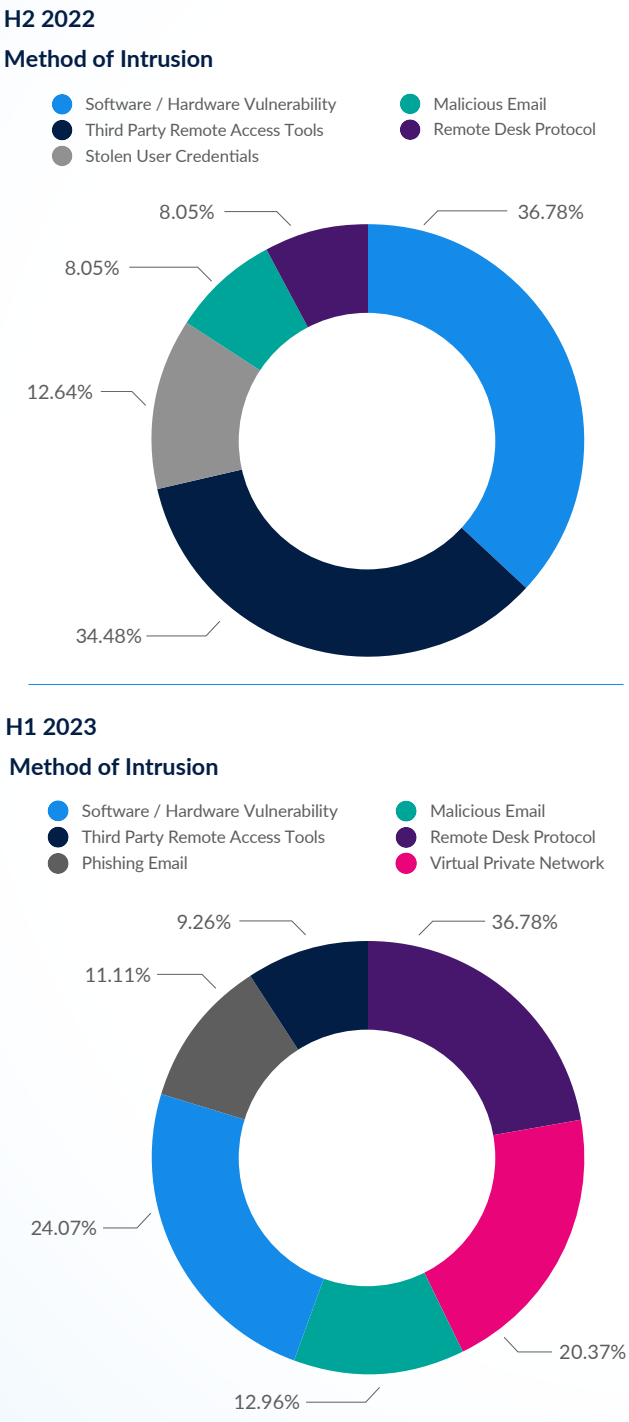


Figure 4: Initial Access Vectors Observed in H2 2022 and H1 2023

The first half of 2023 saw a shift in dominant initial access vectors. Notably, third-party access tools accounted for 34.5% of initial access in the second half of 2022 and just 9.3% in H1 2023. Remote Desktop Protocol (RDP) held the top spot in H1 2023, observed in 24.5% of cases, up from just 8.1% in H2 2022.

A primary contributor to these shifts is threat actors' increased use of initial access brokers. Initial access brokers always pursue the latest vulnerabilities, tactics, and tools. As their role in the cyber ecosystem continues to expand, we will likely see frequent shifts in which vectors are used most often.

For detailed information about these initial access vectors, see the appendix.

POST-EXPLOIT TOOLSETS OBSERVED IN INCIDENT RESPONSE AND MANAGED DETECTION AND RESPONSE INVESTIGATIONS

The following list represents the post-exploit toolsets our analysts observed in incident response and managed detection and response engagements in H1 2023. Documentation and analysis of malware help us understand cyberattacks' nature, scope, and impact during an investigation. This insight can give network defenders a more accurate picture of the threat landscape and help them understand how to reduce the risk of a significant incident by ensuring their endpoint and network appliances properly detect and block these threats.

Agent Tesla	Gozi	RedLine
AZORult	Hancitor	SocGholish
Babadeda	IcedID	Smoke Loader
BlueFox	Jupyter	SystemBC
Brute Ratel	Metasploit	Vidar
Cobalt Strike	Mimikatz	WSH RAT
CoinHive	Neshta	XMRig
Emotet	NETSupport RAT	Xtreme RAT
Expiro	PoisonIvy	Xworm
FlawedAmmyy RAT	Qbot	Zloader
FloodFix	Quasar RAT	

For information about each of these toolsets, please see the appendix.

Threat Actor Insights

Tactics, techniques, and procedures (TTPs) and analysis on the top 5 threat actor ransomware groups observed during the first half of 2023.

LockBit

LockBit has remained at the forefront of the cybercrime sector over the last several years due to its constant development efforts and continued iterations of its ransomware encryptor. The group commonly utilizes a double-extortion technique and, in some cases, even triple extortion, in which they launch DDoS attacks on the victim's network. Additionally, they leverage a data leak site (DLS) for posting victim data. Operationally, LockBit members recruit experienced affiliates tasked with gaining initial access to victim networks in exchange for a percentage of the paid ransom. The LockBit 3.0 ransomware is continuously evolving, and in April 2023, samples designed to encrypt on Apple's macOS arm64 architecture were discovered on Virus Total, which raised concerns about the evolving risk of ransomware on macOS systems. Lockbit 3.0 is already capable of encrypting on Windows, Linux, and VMware ESXi virtual machines and aims to expand the group of potential targets to include organizations migrating to virtual environments.

Lockbit 3.0 is already capable of encrypting on Windows, Linux, and VMware ESXi virtual machines and aims to expand the group of potential targets to include organizations migrating to virtual environments.

Notable Tactics, Techniques, and Procedures (TTPs)

- LockBit affiliates use various tools during intrusions to achieve network reconnaissance, remote access, credential dumping, and exfiltration. Affiliates also use batch scripts, PowerShell, Metasploit, and Cobalt Strike to gain initial access and move laterally through a victim's network to identify and target high-value assets for encryption.
- In LockBit 3.0, ransom notes titles were changed from 'Restore-My-Files.txt' to '[id].README.txt'.
- LockBit 3.0 has leveraged the iControl CVE-2021-22986 and Fortinet CVE-2018-13379 vulnerabilities, enabling remote code execution on a system or file downloads containing sensitive information, including usernames or passwords, without authentication.
- In a recent case, Arete identified LockBit utilizing double encryption for the first time.
- In several recent LockBit cases, Arete identified multiple ransomware notes in client environments, raising concerns over the plausibility of decryption. Despite these concerns, the threat actor was able to successfully decrypt the files in cases with multiple ransom notes identified.
- In a recent case, Arete observed a change with the decryption tool provided by the threat actor, which required the tool to be deployed utilizing the command line. In previous cases, the decryption tool was easily deployed by running the tool as an administrator. This seems to be an isolated incident, and we have not seen any further changes in the threat actor's decryption tool.

Black Basta

Black Basta emerged in late 2021 and often utilizes a double extortion technique. Black Basta is a cybercriminal organization that offers Ransomware-as-a-Service (RaaS) to other hackers, meaning that anyone can use Black Basta's software and infrastructure to launch ransomware attacks and share the profits with Black Basta's operators.

Black Basta is a cybercriminal organization that offers Ransomware-as-a-Service to other hackers, meaning that anyone can use Black Basta's software and infrastructure to launch ransomware attacks and share the profits with Black Basta's operators.

According to a threat assessment by Arete's Threat Fusion Center, Black Basta uses various methods to attack its victims, including:

- Sending phishing emails that contain malicious attachments or links that download and run Black Basta's software
- Using stolen passwords or hacking tools to access the victim's network remotely
- Dropping an image file named dlaksjdoiwg,jpg that replaces the desktop wallpaper
- Using encryption techniques to lock the victim's data and hide their activities
- Installing the GHOSTRAT remote access trojan to execute the payload

ALPHV/ Blackcat

ALPHV/Blackcat emerged in late 2021, targeting organizations across various sectors and regions. ALPHV/Blackcat differs from other variants because it has unique features and techniques that make it more challenging to detect and stop. It is known to distribute various payloads, including Cobalt Strike, Trickbot, and Qakbot. The group has demonstrated continuous innovation, regularly incorporating new discovery techniques, defense evasion, and various post-compromise activities.

ALPHV/Blackcat differs from other variants because it has unique features and techniques that make it more challenging to detect and stop.

Notable Tactics, Techniques, and Procedures (TTPs)

- Tools used by BlackCat, according to Arete's incident response engagement datasets, include CobaltStrike, Mimikatz, Megasync, LaZagne, and WebBrowserPassView.
- Based on command line switches seen in Windows and Linux variants, Arete notes that BlackCat builds victim-specific samples.
- ALPHV/Blackcat uses various entry points to infect the victim's network, including phishing emails, compromised credentials, and remote desktop protocol (RDP) brute force attacks.
- It also utilizes other malware infections as stepping stones to launch its ransomware payload.
- To increase potential reach and impact, ALPHV/ Blackcat targets both Windows and Linux devices, as well as network-attached storage (NAS) devices, which are often used to store backups and sensitive data.

Royal

Royal ransomware has been active in the cybercrime ecosystem since September 2021. Rather than operating as a RaaS, which has recently dominated the threat landscape, Royal is believed to loosely operate as a closed group. When the group emerged, it utilized other variants' data encryptors before developing its proprietary encryptor. While the group does not appear to target a single sector or organizational size disproportionately, they do not shy away from encrypting large organizations with ransomware.

While Royal does not appear to target a single sector or organizational size disproportionately, they do not shy away from encrypting large organizations with ransomware.

According to a threat assessment by Arete's Threat Fusion Center, Royal uses various methods to attack its victims, including:

- Sending phishing emails that contain malicious attachments or links that download and run Royal ransomware's software
- Using stolen passwords or hacking tools to access the victim's network remotely
- Using malicious advertisements that redirect the victim to a website that downloads and runs Royal ransomware's software
- Deploying CobaltStrike to maintain persistence on a system
- Exfiltrating credentials, laterally spreading across the system's domain, and encrypting devices

Akira

The first ransomware attack by Akira occurred in early April 2023, and the group quickly amassed victims throughout the first half of 2023. Akira encrypts and exfiltrates data to a remote server and extorts victims by threatening to post sensitive information on their data leak site (DLS). The ransomware appends a ".akira" extension to encrypted files and uses a password-protected TOR site for communication and negotiations with its victims.

Akira encrypts and exfiltrates data to a remote server and extorts victims by threatening to post sensitive information on their data leak site.

Notable Tactics, Techniques, and Procedures (TTPs)

- According to Arete's incident response engagement data, Akira targets education, professional services, retail, hospitality, healthcare, and manufacturing organizations.
- To date, Akira has primarily targeted entities in Canada and the United States.
- Arete has observed Akira often using the same verbiage during negotiations. The threat actor sends a list of the five deliverables they will provide after payment, including decryption assistance and evidence of data removal, along with an option to pay for all five of the deliverables listed or just some of them. After payments are made, Arete has observed Akira sending the same "security report" regardless of the victim.
- The decryptor Akira provides is known to be unreliable and problematic, randomly skipping files or decrypting a file without removing the .akira extension. In late June 2023, researchers at Avast developed a decryptor for Akira and released it as a public download. Arete assesses that Akira will likely adjust its encryption schema to mitigate future victims' ability to use this public tool.

Trends in top variants, ransom demands and payments, and TTPs shift over time in response to various external factors, including socioeconomic events, the actions of affiliates, new vulnerabilities and opportunities, and evolving business models. In the next section, we explore critical happenings from the first half of 2023 and the effect they continue to have on the threat landscape.

Opening the Floodgates: Lower Barrier of Entry into Cybercrime

With an influx of new tools, shifting business models, and leaked resources at their disposal, emerging cybercriminals have an unprecedented opportunity to establish new operations. Arete has observed the increased effect of this shift in the first half of 2023.

Cybercrime-as-a-Service

The well-known Ransomware-as-a-Service (RaaS) model has dominated the cybercrime industry over the last few years and into H1 2023, and Cybercrime-as-a-Service has grown in parallel. Cybercrime-as-a-Service has lowered the barrier of entry into cybercrime by giving threat actors access to various resources that allow them to work their way through the attack lifecycle effectively.

The threat actors behind ransomware operations can:

- Engage with initial access brokers to purchase access to victim organizations.
- Leverage exploit code purchased from vulnerability marketplaces.
- Purchase access to remote access trojans (RATs).
- Purchase access to post-exploitation command & control (C2) frameworks.
- Opt or buy into an existing ransomware affiliate program.

Cybercrime-as-a-Service has led to a distinct increase in initial access brokers and credential shops and has increased the ability of even inexperienced actors to exploit victim organizations effectively.

Leaked Source Code

Over the last several years, there have been a few proprietary ransomware encryptor leaks, which have significantly increased accessibility and put powerful encryptors into the hands of emerging cyber criminals, making it easier than ever to stand up new ransomware operations.

Babuk Source Code Leak

In September 2021, a Babuk affiliate leaked the group's C++ source code, giving emerging actors an effective tool for targeting Linux operating systems and paving the way for VMware ESXi attacks. While originally slow to be adopted, in the first half of 2023, a slew of emerging threat actors used the source code to target Linux environments. These threat actors include:

- TRM Locker
- Rook
- Dataf Locker
- RA Group
- Lock4

Conti Leak

In February 2022, a Conti affiliate disgruntled by the group's stance on the Russia-Ukraine war leaked the ransomware operation's information, including negotiations, hierarchy, and source code. Following these leaks, the group inevitably ceased operations, and the individuals behind Conti ransomware joined other ransomware groups or stood up their own operations. The leaked source code has been used to enable various ransomware operations, including:

- Putin Team ransomware
- Scarecrow ransomware
- BlueSky ransomware

LockBit Builder Leak

Following the leaked Conti source code, an angry LockBit developer leaked the group's builder in September 2022. The leak allowed aspiring cyber-criminals to easily download the builder, alter the ransom note to their liking, and encrypt victim environments, as long as they gained initial access. The builder's ease of access and granularity enabled many unknown actors to target victims in the wild without sophisticated capabilities. However, one large ransomware group, dubbed Bl00dy ransomware, continues using the builder throughout their campaigns.

The addition of these leaked tools into the cyber-crime ecosystem empowered emerging actors to create their own ransomware operations rather than becoming an affiliate for an existing group. This influx of new actors has increased difficulty in attribution following a security incident. Arete has developed an extensive repository of threat actor TTPs, and detection mechanisms, including Yara and SentinelOne countermeasures, to detect and attribute threat actor activity. However, actors cannot wholly rely on leaked source code to enable their operations, as it is the final stage of the attack lifecycle.

Arete has developed an extensive repository of threat actor TTPs, and detection mechanisms, including Yara and SentinelOne countermeasures, to detect and attribute threat actor activity.

The AI Revolution and Cybercrime

ChatGPT Changes the Game

ChatGPT, the revolutionary product from OpenAI, encompasses a large dataset of human conversations and can generate and address human-like responses. Since its launch in January 2023, it has garnered massive global attention and grown significantly. A free version is available for all users, but OpenAI also launched a paid version with unrestricted availability.

Although ChatGPT has filters intended to prevent the tool from generating harmful content, users have discovered workarounds and methods to bypass these filters and leverage the tool to enable cybercrime operations. Because of its immense capabilities, ChatGPT has become a preferred tool for script kiddies and attackers. It can assist in identifying vulnerabilities, reverse-engineering shellcode, and even generating code for malware. Multiple threads in underground forums have addressed the utilization of ChatGPT for fraudulent activities. In a hacking forum called 'Breached,' Arete has observed discussions among threat actors regarding the use of ChatGPT in creating and sharing malware code.

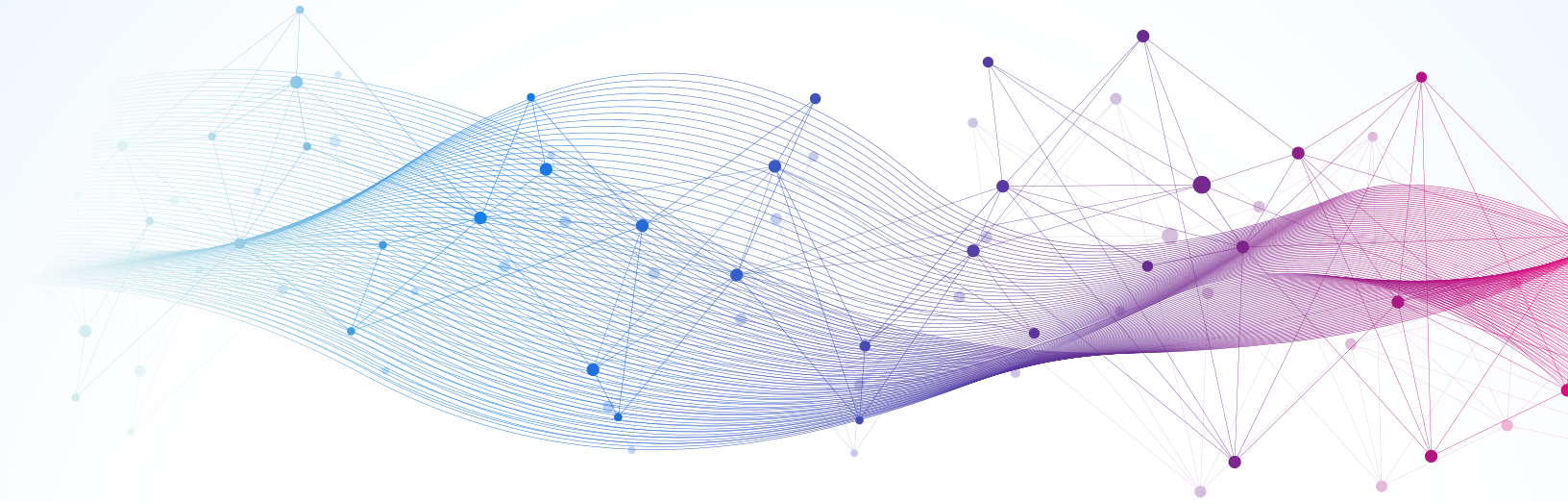
Because of its immense capabilities, ChatGPT has become a preferred tool for script kiddies and attackers.

WormGPT Enables Cybercriminal Operations

Discovered by cybersecurity firm SlashNext on July 13, 2023, WormGPT is a blackhat version of ChatGPT. It is designed to generate malicious content, including phishing emails, malware code, fake news, and social media posts. WormGPT is based on the GPT-J language model, developed in 2021 by EleutherAI, an open-source AI research group. Depending on the user's input and preferences, the tool generates texts in different languages, formats, and styles and creates code snippets for various programming languages, including Python, Java, C#, PHP, and HTML.

WormGPT is described on dark web forums as a "sophisticated AI model" and a "best GPT alternative for blackhat" designed especially for cybercrime. WormGPT has no ethical boundaries or safety mechanisms to prevent it from responding to harmful or illegal requests and is allegedly trained with data sources, including malware-related information. Still, the specific datasets remain known only to WormGPT's author. This tool poses a severe threat to online security and privacy, as it can create convincing texts that can trick users into revealing sensitive information, downloading malicious software, or falling for scams. This new and emerging threat requires more research and analysis to understand its full capabilities and potential impacts.

Cyber criminals can leverage AI tools to create phishing scams, social engineering attacks, and spamming. In the near term, it is likely that new versions of AI software will continue to be developed, leading to increasing functionality for threat actors. This, coupled with threat actors continuing to expand their knowledge of manipulating the software, will lead to threat actors increasingly utilizing AI in their day-to-day operations.



Ease of Rebranding Lessens the Role of Reputation

Historically, threat actors have leaned heavily on their reputations to intimidate their victims. And while actors like LockBit and ALPHV/BlackCat continue to be mainstays, the ease of rebranding has caused new and lesser-known actors to place less emphasis on their reputation. Groups can easily create new ransom notes and encrypted file extensions using ransomware builders, build new communication infrastructure, and create new logos for their branding. This rebranding trend could lead to false claims, unreliable proof-of-deletion, or re-extortion.

Rebranding trends could lead to false claims, unreliable proof-of-deletion, or re-extortion.

The Flawed Affiliate Model?

As Ransomware-as-a-Service (RaaS) operations continue to be plagued by dissatisfied or sloppy affiliates, we will likely see a shift in the RaaS-dominated cybercrime ecosystem. Initially, RaaS groups will likely emphasize vetting affiliates before onboarding. Large ransomware operations could use their resources to effectively create a vetting and onboarding process comparable to that of top-tier human resources departments. Additionally, threat actors will likely consider using new tools to develop their own ransomware operation rather than becoming an affiliate of an existing RaaS. Even inexperienced actors could use tools, including artificial intelligence, initial access brokers, commodity RATs, and leaked ransomware source code, to create their own ransomware operation without significant development capabilities.

The Migration to Exfiltration-Only Operations

While ransomware has been the dominant tactic recently, some threat actors are changing tactics to focus on data extortion instead of encryption. Data extortion is a technique that involves stealing the victim's data and threatening to publish it online if the ransom is not paid. Notably, the prolific group Luna Moth made a resurgence in Q1 of 2023 and focused heavily on exfiltration before silently disappearing again in the second half of Q2. Exfiltration-only operations have several attractive benefits, including a decreased footprint within the network, not having to maintain or alter an encryptor, and eliminating the potential of disgruntled affiliates releasing their encryptor and causing negative publicity.

Luna Moth Extortion Group

Active since March 2022, Luna Moth launched phishing campaigns impersonating popular online learning platforms Zoho MasterClass and Duolingo. The phishing emails claim that the recipients have been charged for a subscription and offer a PDF attachment with a phone number to call for more information. If the recipients open the attachment and call the number, they are greeted by a human operator who pretends to be a customer service representative and convinces them to install a remote administration tool (RAT) on their device. This RAT gives the attacker complete control over the device and allows them to access and exfiltrate any data available.

Luna Moth does not use any sophisticated or custom-made tools but rather leverages commercially available RATs, including Atera, Splashtop, Syncro, and AnyDesk, as well as publicly available tools SoftPerfect Network Scanner, SharpShares, and Rclone. These tools are stored on compromised machines under false names to avoid detection. The group also uses VPN services and TOR to hide their identity and location.

Once Luna Moth steals the data, they contact victims via email or phone and demand a ransom, usually ranging from $100,000 to $1 million, depending on the amount and sensitivity of the data. They threaten to publish the data on their website or sell it to other criminals if the ransom is not paid within a specific timeframe. The group also provides proof of the data breach by sending samples of the stolen files or screenshots of their website.

> **Luna Moth's attacks are simple but effective, exploiting human psychology and trust rather than technical vulnerabilities.**

Luna Moth's attacks are simple but effective, exploiting human psychology and trust rather than technical vulnerabilities. The group targets small and medium-sized businesses that may not have adequate security measures or backups in place and may be more likely to pay a ransom to avoid reputational damage or legal consequences. The group also operates opportunistically, stealing any data they can access, regardless of its value or relevance.

Luna Moth's novel extortion campaign demonstrates that cyberattacks do not require ransomware to be successful.

MOVEit Vulnerability Exploited by Cl0p Ransomware

A serious ransomware threat is looming over critical infrastructure, as cybercriminals linked to notorious Russian ransomware group Cl0p are exploiting a security flaw in MOVEit Transfer, a tool used by hospitals, health systems, corporations, and government agencies to share large files over the internet. Cl0p, also known as TA505, has been using a structured query language (SQL) attack vector to infect internet-facing MOVEit Transfer web applications with malware and then steal data from underlying databases.

The MOVEit vulnerability was disclosed by U.S.-based company Progress Software, the developer of MOVEit Transfer, on June 5, 2023. The exploitation of the vulnerability has affected several organizations worldwide, including British Airways, the BBC, Boots, Ofcom, Transport for London, Ernst & Young, and several U.S. federal agencies. Cl0p has released the names of several victims and some of their stolen data on its website since June 13, 2023, in an attempt to pressure these organizations to pay ransom demands.

This attack is known as a supply-chain attack, as it targets widely used software that serves as a gateway to many other organizations. The MOVEit attack is a remote code execution attack in which attackers can exploit and upload a webshell to exfiltrate data from vulnerable servers. This vulnerability is one of the latest examples of ransomware groups becoming more sophisticated and aggressive in their tactics, targeting critical infrastructure and sensitive data.

There was no data encryption during these attacks. Instead, Cl0p was able to exfiltrate large amounts of data from victim organizations effectively. Following the mass exfiltration of data, Cl0p extorted the victims of the MOVEit attack via direct emails and postings on their DLS. This series of cyberattacks is an example of the trending shift to exfiltration-only operations.

The MOVEit vulnerability is one of the latest examples of ransomware groups becoming more sophisticated and aggressive in their tactics, targeting critical infrastructure and sensitive data.

Focus on Increasing Attack Surface

As ransomware groups continue to expand their capabilities, they are also expanding outwards to be able to target multiple operating systems, thus increasing their potential attack surface. Arete has observed a distinct rise in groups targeting Linux operating systems, primarily through the VMware ESXi vulnerabilities and attempts at creating ransomware to target macOS.

The Future of Ransomware Against macOS

Ransomware attacks have been a significant threat to Windows and Linux users for years, but macOS users have largely avoided this threat thanks to Apple's security features and lower market share. However, in 2023, a new ransomware threat on macOS was discovered, indicating that the threat landscape may be changing for Apple users.

The ransomware showcasing the ability to target macOS environments was later attributed to the notorious LockBit ransomware group. In April 2023, security researchers found samples of LockBit encryptors for macOS on VirusTotal, a malware analysis repository. The samples were uploaded in November and December 2022 but went unnoticed until MalwareHunterTeam spotted them.

The LockBit encryptors for macOS were designed to target both newer Macs running Apple processors (arm64 architecture) and older Macs running PowerPC chips. However, the researchers found that the encryptors were not very effective, as they were unsigned, did not account for Apple's security restrictions (TCC/SIP), and had bugs that caused them to crash. The encryptors also did not have any network communication or ransom note functionality.

The researchers concluded that the LockBit encryptors for macOS were more of an experiment than a viable threat. Still, LockBit could improve and iterate on these tools in the future. The fact that LockBit was developing a macOS version of its ransomware could signal a trend toward more Mac-targeted ransomware, especially as more businesses and institutions adopt Macs.

LockBit was not the only ransomware group to show interest in macOS in 2023. In May 2023, ransomware group Akira was found to have published data from a macOS victim on its website. Akira uses a combination of phishing emails, remote access tools, and PowerShell scripts to compromise and encrypt devices.

These incidents suggest that macOS users should not be complacent about the risk of ransomware attacks. While macOS has some built-in security features that make it harder for ransomware to run, such as Gatekeeper, FileVault, and XProtect, these features are not foolproof and can be bypassed by determined attackers. Moreover, macOS users may be more vulnerable to phishing emails and social engineering tactics, as they may have a false sense of security and lower awareness of cyber threats.

Ransomware attacks are a severe threat to any device user, regardless of the operating system. MacOS users should not assume they are immune from this threat but rather take proactive measures, like those on page 26, to secure their data and devices from ransomware attackers.

Ransomware attacks are a severe threat to any device user, regardless of the operating system.

Targeting of VMware ESXi Servers

Over the past two years, cybercriminals have targeted VMware ESXi servers due to a software vulnerability known as CVE-2021-21974, with over 3,200 servers compromised globally.

A ransomware variant dubbed ESXiArgs appeared to be the first to leverage the vulnerability to run exploit code remotely. ESXiArgs was initially identified as encrypting files with the .vmxf, .vmx, .vmdk, .vmsd, and .nvram extensions on compromised ESXi servers and creating a .args file, but recently the group started encrypting more extensive amounts of data.

Arete observed the latest version of Royal Ransomware specifically targeting VMware ESXi virtual machines. Additionally, LockBit released a new iteration of their ransomware builder, allowing threat actors to target Linux environments actively. This new variant, LockBit Green, allows ransomware-as-a-service (RaaS) affiliates to encrypt VMware ESXi hypervisors.

Threat actors are likely targeting the ESXi machines because, after the deployment of the payload, they can encrypt multiple hosts via a single command.

Arete observed the latest version of Royal Ransomware specifically targeting VMware ESXi virtual machines.

The Continued Impact of the Russia-Ukraine War on Cybercrime

The ongoing conflict between Russia and Ukraine in the Donbas and Luhansk regions, which started with the 2014 annexation of Crimea, escalated into a full-scale war on February 24, 2022. After seven months of war and heavy losses of regular troops, Vladimir Putin announced "partial mobilization" targeting prior-service males under the age of 55, which led to over 2 million males fleeing Russia to avoid being drafted. Since cybercriminals that operated out of Russia and Ukraine had plenty of funds available for relocation, the mass exodus likely explains the slowdown we observed in ransomware-related attacks in 2022.

Ironically, along with increasing risks of mobilization, Russian hackers are now facing uncertainty about the country's "safe haven" status that they enjoyed so far. War-related expenses and the economic impact of imposed sanctions prompted the Russian government to propose a new law that enables the confiscation of proceeds from cybercriminal operations.

The mass exodus of cybercriminals from Ukraine and Russia also provided a unique opportunity for international law enforcement agencies to track and arrest cybercriminals in countries that have extradition treaties with the United States. Since the beginning of the war in Ukraine, several high-profile arrests have been announced publicly, including suspected JabberZeus top manager Vyacheslav "tank" Penchukov and a suspected "Evil Corp" second-in-command Igor Turashev.

As a result of increased law enforcement action, we have seen an influx of cybercriminal groups deciding to break up into smaller independent teams or re-brand in the first half of 2023. Every month, some groups disappear (or announce "retirement), and "new" groups enter the market, which has increased the challenge of accurate attribution.

With rising multi-dimensional pressure on cyber-criminal groups, we'll likely continue to observe the shift from large Ransomware-as-a-Service (RaaS) and private groups toward compartmentalized cellular structure operations, which enable smaller teams to operate independently while making the enterprise more resilient to identification and infiltration. The cellular structure can make it harder for these groups to coordinate large-scale actions, and there's a greater risk of cells being infiltrated or turning against each other. Nevertheless, it has proven to be effective for many cybercriminal organizations. In the long run, this structural change may also slow down the speed of innovation since smaller cells will be less likely to have sufficient resources to make significant investments in research and development.

As a result of increased law enforcement action, we have seen an influx of cybercriminal groups deciding to break up into smaller independent teams or re-brand in the first half of 2023.

Law Enforcement Actions Against Cybercriminals

In an effort to counter ransomware and other malicious cyber activity, global law enforcement entities have banded together to dismantle cybercriminals by targeting their infrastructure, implementing sanctions, and conducting counter-surveillance activities.

High Profile Ransomware Attacks

2021
REvil attacks against the world's largest meat processor, JBS, and software company Kaseya, impacted over 1,500 businesses worldwide.

2021
Darkside attack against Colonial Pipeline significantly impacted fuel supply that is said to have increased prices in the U.S. by $3 for the first time in seven years.

2021
Hive attack against the Memorial Health System, a hospital network in Ohio and West Virginia, forced hospitals to turn away patients as Covid-19 surged.

2023
Vice Society attack against Los Angeles Uniffed School District, the second-largest school district in the United States.

The increase in high-profile ransomware events led Congress to form CISA's Joint Ransomware Taskforce (JRTF). In November 2022, the White House sponsored the second International Counter Ransomware Initiative Summit.

Hive Website Seized

Hive, a notorious ransomware gang that targeted dozens of organizations worldwide, including hospitals, schools, and businesses, faced a significant blow from law enforcement agencies. In coordination with international partners, the FBI seized the website Hive used to communicate with its victims and publish stolen data. More than 30 global private sector and U.S. government agencies contributed to the success of this operation.

The website, hosted on the dark web, displayed a message from the FBI in January 2023 announcing it had been seized as part of an ongoing investigation. The message also warned that anyone who accessed the website may have been exposed to malware and advised them to scan their devices for infections.

The FBI stated that it took action against Hive after identifying its infrastructure and obtaining a court order. The agency also said it is working with foreign law enforcement agencies to identify and apprehend the individuals behind Hive.

One of Hive's most notable attacks was against Memorial Health System, a hospital network in Ohio and West Virginia, in August 2021. According to Attorney General Merrick Garland, the attack forced the hospital to turn away patients as Covid-19 surged. Other victims of Hive include Canadian energy company Inter Pipeline, software provider Kaseya, and Iowa-based agricultural cooperative New Cooperative.

The seizure of Hive's website is part of a broader effort by the U.S. government and its allies to combat the growing threat of ransomware, which has caused significant disruption and damage to critical infrastructure and public services.

FBI Cracks Down on Genesis Marketplace

In collaboration with law enforcement agencies from 18 countries, the FBI cracked down on Genesis Marketplace, one of the largest illicit marketplaces for stolen credentials and related sensitive information. The operation, which took place on April 27, 2023, resulted in the arrest of 119 suspects and the seizure of over $1.5 million in cryptocurrency and cash.

Genesis Marketplace was a dark web platform specializing in selling digital fingerprints, which are data collections that identify a user's device and online behavior. The data included browser cookies, IP addresses, user-agent details, device IDs, operating system information, and login credentials for various online services.

Genesis Marketplace had over 350,000 digital fingerprints listed for sale, ranging from $5 to $200. The platform also had over 250,000 login credentials for various online services, including email, banking, social media, gaming, and e-commerce. The platform claimed to have over 55,000 active users and generated over $100 million in revenue since its inception in 2017. The market offered its customers a browser extension that allowed them to impersonate the victims whose digital fingerprints they purchased. The customers could then access the victims' accounts without triggering security alerts or verification processes. Genesis Marketplace also provided its customers with tools to create their own digital fingerprints and sell them on the platform.

The FBI said it initiated the investigation into Genesis Marketplace in 2019 after receiving a tip from a confidential source who provided access to its backend server and database, which contained evidence of the platform's operations and transactions. The FBI was able to identify and locate the suspects involved by tracing their online activities and transactions. They obtained search warrants for several locations and seized various devices and documents related to Genesis Marketplace.

The FBI coordinated with law enforcement agencies from Australia, Belgium, Canada, Colombia, Denmark, France, Germany, Italy, Japan, Netherlands, Poland, Romania, Spain, Sweden, Switzerland, Ukraine, the United Kingdom, and Uruguay to execute the operation.

The FBI stated that the operation was a significant step in disrupting and dismantling Genesis Marketplace and its infrastructure. The agency also said it is committed to protecting consumers and businesses from cybercrime and holding cybercriminals accountable.

Due to the U.S. Department of the Treasury sanctioning Genesis Marketplace for its part in stealing and selling device credentials and related sensitive information, it has been added to Arete's Sanctioned and Restricted Malware/Entities List.

The FBI coordinated with law enforcement agencies globally to disrupt and dismantle Genesis Marketplace and its infrastructure.

How the U.S. Government Took Down a Russian Cyber Espionage Network

On May 9, 2023, the U.S. government executed a successful operation to disrupt and disable a covert cyber espionage network operated by Russia's Federal Security Service (FSB). The FSB used the network, dubbed Snake, to collect sensitive intelligence from high-priority targets worldwide, including government networks, research facilities, and journalists.

Snake is considered the most sophisticated cyber espionage tool in the FSB's arsenal, employing stealthy host components and encrypted network communications. Snake also uses a peer-to-peer (P2P) network of infected computers to relay operational traffic to and from the FSB's ultimate targets, making it harder to detect and trace.

The operation, codenamed MEDUSA, was a joint effort by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). The agencies leveraged their unique authorities and capabilities to identify, analyze, and disrupt Snake's infrastructure and operations.

The operation involved several steps:

- The CISA issued a Cybersecurity Advisory (CSA) to provide network defenders with technical information and mitigation recommendations on Snake.
- The FBI obtained court orders to seize domains and servers used by Snake as part of its P2P network.
- The NSA provided intelligence and technical expertise on Snake's activities and targets.
- The FBI created and deployed a tool called PERSEUS, designed to disable Snake's malware on compromised computers in the U.S.
- The CISA coordinated with international partners to share information and assistance on Snake.

The operation resulted in the disruption of Snake's P2P network, the removal of Snake's malware from hundreds of computers in the U.S., and the exposure of Snake's targets and techniques. The agencies also warned that Snake may still pose a threat and urged network defenders to remain vigilant and apply the recommended mitigations.

The operation demonstrates the U.S. government's commitment and ability to counter malicious cyber activity from foreign adversaries. It also showcases the importance of collaboration and information sharing among federal agencies and international partners. The agencies stated they will continue to monitor and respond to any attempts by the FSB or other actors to reconstitute Snake or launch new cyber operations against the U.S. or its allies. Global law enforcement agencies coming together to combat cybercrime showcases their continued efforts to disrupt cybercrime around the world.

Global law enforcement agencies coming together to combat cybercrime showcases their continued efforts to disrupt cybercrime around the world.

What to Expect

In the second half of 2023, Arete expects large ransomware operations like ALPHV/BlackCat and LockBit to continue to evolve their operations to leverage new vulnerabilities, expand their attack surface, and explore the benefits of data exfiltration. We also expect to see groups create more extensive vetting processes in response to the data and source code leaks that have plagued several large ransomware operations recently. These efforts will likely allow these ransomware groups to remain at the forefront of the cybercrime sector while continuing to conduct their operations at a higher degree of sophistication.

The barrier of entry into cybercrime is lower than ever, and along with these mainstay actors, Arete also expects to see an influx of new or re-branded groups as they move away from the affiliate model towards a more cellular structure. Emerging threat actors will likely leverage artificial intelligence, initial access brokers, commodity RATs, and leaked ransomware source code to build their own operations without needing support from large affiliate programs.

The continued downstream impact of the Russia-Ukraine War has caused a shift in the cybercrime ecosystem that Arete expects to continue throughout the rest of 2023. In response to disgruntled affiliates and increased law enforcement action, cybercriminals seek to deflect risk and disguise their tactics to become increasingly elusive.

Arete also expects global governments and law enforcement agencies to continue their successful efforts in targeting cybercriminals. As threat actors benefit from an influx of new tools and technologies, so do threat hunters and network defenders. Organizations are increasingly prioritizing cybersecurity as a risk management issue and becoming more resilient against cyber threats, and Arete is committed to helping organizations mitigate and respond to cyber incidents.

To increase cyber resiliency and secure data and systems, Arete recommends that organizations consider implementing the following proactive measures:

- Regularly update security software and patch against vulnerabilities.
- Limit user privileges to the least access required to complete job requirements.
- Conduct end-user training to educate employees on common social engineering techniques.
- Implement an XDR (Extended Detection and Response) tool like SentinelOne to detect ransomware and other malware threats.
- Utilize an attack surface management toolset to enumerate externally facing infrastructure and identify associated vulnerabilities.
- Conduct annual penetration testing to identify security gaps and weaknesses.
- Remain informed about the latest ransomware trends and techniques.
- Define an Incident Response Plan to streamline recovery from ransomware attacks.

Resources

Disclaimer: Unless otherwise noted, all data within this report is based on Arete incident response cases.

- https://securityscorecard.com/research/deep-dive-into-ALPHV-blackcat-ransomware/
- https://www.malwarebytes.com/blog/news/2022/09/lockbit-builder-leaked-by-disgruntled-developer
- https://intel471.com/blog/lockbit-3-0-builder-code-leak-points-to-another-disgruntled-criminal-employee
- https://www.sentinelone.com/anthology/akira/
- https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/
- https://blog.cyble.com/2023/06/28/akira-ransomware-extends-reach-to-linux-platform/
- https://www.cisecurity.org/insights/blog/the-conti-leaks-a-case-of-cybercrimes-commercialization
- https://cybernews.com/news/putin-team-ransomware-emerges-from-leaked-contis-source-code/
- https://ieeexplore.ieee.org/document/9153425
- https://unit42.paloaltonetworks.com/bluesky-ransomware/
- https://techmonitor.ai/technology/cybersecurity/babuk-source-code-ransomware-malware
- https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
- https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/
- https://www.sentinelone.com/blog/LockBit-for-mac-how-real-is-the-risk-of-macos-ransomware/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-039a
- https://krebsonsecurity.com/2023/04/fbi-seizes-bot-shop-genesis-market-amid-arrests-targeting-operators-suppliers/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a
- https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/
- https://www.cisa.gov/joint-ransomware-task-force
- https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/
- https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/

Cyber Emergency Helpline 866 210 0955
Phone 646 907 9767

New Engagements
arete911@areteir.com

General Inquiries
marketing@areteir.com

www.areteir.com