ThreatLabz Report

Zscaler ThreatLabz 2023 Ransomware Report

Contents

Executive summary

Ransomware attacks are on the rise, and businesses of all sizes are at risk. The Zscaler ThreatLabz 2023 Ransomware Report provides an overview of the ransomware threat landscape, including the latest trends, techniques, and defense strategies.

The report found that ransomware attacks increased by over 37% in 2023 (tracked between April 2022 and April 2023) compared to the previous year, with the average enterprise ransom payment exceeding $100,000, with a $5.3 million average demand. The most common targets were businesses in the manufacturing, services, and construction sectors.

Ransomware attacks are becoming increasingly sophisticated, with attackers using a variety of techniques to exploit vulnerabilities in organizations' systems and networks. These techniques include phishing, social engineering, and exploiting known vulnerabilities.

Additionally, in the past year, ransomware actors increased profits by leveraging:

- **Ransomware as a service:** Affiliate networks helped distribute ransomware widely, enabling skilled network breachers to share profits with advanced ransomware groups.
- **Encryptionless ransom attacks:** In a concerning development this year, rather than encrypting victim files, attackers focused on exfiltrating sensitive data as leverage for extortion. This presents new challenges for victims and security professionals because traditional methods of file recovery and decryption may not apply. Understanding the techniques leading up to these encryptionless attacks is crucial for developing robust mitigation strategies and effectively countering whatever comes next.

The Zscaler ThreatLabz 2023 Ransomware Report offers businesses the information they need to better understand and protect themselves against evolving ransomware attacks. Following the recommendations in this report can help businesses reduce their risk of being targeted by ransomware and minimize the impact of an attack if one does occur.

[1] Verizon Data Breach Report 2022: average ransomware payment $170,404 in 2022

[2] McAfee Labs 2022 Threat Report: average ransomware payment was $112,446 in 2022

[3] IBM X-Force Threat Intelligence Index 2022: average ransomware payment was $312,493 in 2022

[4] Coveware Ransomware Report 2022: average ransomware demand for enterprises was $5.3 million in 2022

Key findings

The battle against ransomware attacks has intensified during the April 2022 through April 2023 period, as proven by the key findings in this year's report:

In the Zscaler cloud, ransomware attacks witnessed a staggering 37.75% increase, signaling a growing threat to organizations worldwide. Worse, the payloads observed in the Zscaler sandbox surged **57.50%**. With ransomware extortion attacks based on the number of infected victims soaring by **36.68%** in the same period, it's clear that businesses must be prepared to combat this ever-evolving menace.

The United States stands as the primary target for ransomware campaigns and is impacted more than any other country.

The threat landscape continues to evolve, with the emergence of encryptionless ransom attacks gaining traction. This insidious approach presents a new challenge as attackers bypass encryption to directly target and compromise vital systems and data.

The manufacturing, services, and construction sectors have been the targets of ransomware attacks more often. Known for their critical infrastructure and valuable intellectual property, these industries have become prime targets for cybercriminals seeking financial gain and disruption.

Businesses must adopt a comprehensive zero trust security strategy to combat the rising tide of increasingly sophisticated ransomware attacks. This approach entails implementing robust measures such as zero trust network access (ZTNA) architecture, granular segmentation, browser isolation, advanced sandboxing, data loss prevention, deception technology, and cloud access security broker (CASB) solutions. By adopting these proactive defenses, organizations can fortify their security posture and effectively protect against ransomware attacks.

Report methodology

The research methodology for this report is a comprehensive process that uses multiple data sources to identify and track ransomware trends. The report team collected data from a variety of sources, including:

Zscaler's global security cloud, which processes over 300 trillion daily signals and blocks 8 billion threats per day, with over 250,000 daily security updates. The team analyzed this data—which includes information about the source IP addresses, destination IP addresses, and file types associated with ransomware attacks—to identify ransomware activity.

External intelligence sources. The team also collected data from external intelligence sources, such as threat intelligence feeds, open source research, and law enforcement reports, which provided additional information about ransomware attackers, their targets, and their methods.

ThreatLabz research team's own analysis of ransomware samples and attack data. The team also reviews the regular publications released by ThreatLabz, which analyze ransomware samples and attack data for identifying new ransomware families, tracking the evolution of existing ransomware families, and developing new methods of preventing and responding to ransomware attacks.

The team used this data to identify key trends in the ransomware threat landscape, including:

- The most active ransomware families
- The industries and geographies most targeted by ransomware
- The most common attack vectors used by ransomware attackers
- The most effective methods for defending against ransomware

This report is a valuable resource for organizations seeking to understand the ransomware threat landscape and take steps to protect themselves from attack. It provides valuable insights into the latest ransomware trends as well as best practices for prevention and response.

2022—2023 Ransomware attack statistics

The proliferation of ransomware continues to pose a significant threat to organizations, individuals, and critical infrastructure worldwide. Cybercriminals constantly adapt and refine their tactics, leveraging leaked source code, advanced encryption schemes, and emerging programming languages to maximize their illicit gains. This section of the report aims to shed light on the latest trends and developments in the ransomware landscape, providing insights for cybersecurity professionals seeking to improve their defenses against these attacks.

These key highlights will be explored in the sub-sections to follow:

- Encryptionless ransom attacks (or ransom attacks without file encryption) increased in 2022 and the beginning of 2023.
- Threat actors used leaked ransomware source code such as Babuk and Conti, as well as leaked builders such as LockBit, to launch attacks.
- Ransomware attackers are shifting away from languages like C/C++ to Golang and Rust to optimize encryption speed and cross-platform compatibility.
- Ransomware criminals are using more advanced polymorphic obfuscation to hinder analysis and evade static antivirus signatures.
- Ransomware developers have shifted away from RSA-based encryption toward elliptic curve-based algorithms, including Curve25519, NIST B-233, and NIST P-521.

Overall increase in ransomware attacks

The rise in ransomware attacks poses significant risks to businesses of all sizes and industries, as these attacks often lead to severe financial losses, operational disruptions, reputational damage, and the compromise of sensitive information.

The latest ThreatLabz analysis of ransomware attacks over the period from April 2022 through April 2023 reveals another concerning trend. Based on blocked attempts observed across the Zscaler cloud, there was a 37.75% increase in ransomware attacks during this time frame.

This surge in attacks is a clear warning that organizations must remain proactive, adaptive, and committed to cybersecurity. By prioritizing robust defense measures, fostering a culture of security awareness, and embracing collaboration, organizations can strengthen their resilience against ransomware threats and minimize potential impacts.

Industry verticals affected by ransomware

In the past few years, the manufacturing industry has consistently been the primary target of ransomware attacks, and this trend continues. Data from April 2022 through April 2023 reveals that manufacturing remains the most targeted industry vertical, accounting for 14.8% of total ransomware attacks. This finding highlights the ongoing vulnerabilities and attractiveness of manufacturing companies to threat actors.

Following closely behind manufacturing is the services sector, which experienced a significant 11.66% share of ransomware

attacks. The education industry also faced a considerable threat as the target of 7.64% of attacks. A ransomware group known as Vice Society has consistently targeted the educational sector.

The healthcare sector, despite its critical nature, has not been spared, with 6.09% of ransomware incidents targeting healthcare organizations. Similarly, the retail and wholesale sector, which handles substantial amounts of customer data, faced 5.96% of ransomware attacks. Lastly, the construction industry, known for its reliance on technology and interconnected systems, experienced a notable 5.74% share of the total attacks.

Figure 1 shows the number of attacks by industry based on victim companies hosted on data leak sites from April 2022 through April 2023.

It should be noted that this information pertains to the number of attacks based on victim companies hosted on data leak sites, which offers insight into the prevalence of attacks but may not encompass the full scope of all ransomware incidents. Many attacks go unreported or are resolved privately via a ransom payment without public disclosure. Therefore, these figures should be viewed as indicative of broader trends in ransomware targeting rather than an exhaustive representation of the entire threat landscape. Collaboration between industry stakeholders, government agencies, and cybersecurity professionals remains a crucial strategy for sharing threat intelligence and collectively combating ransomware gangs.

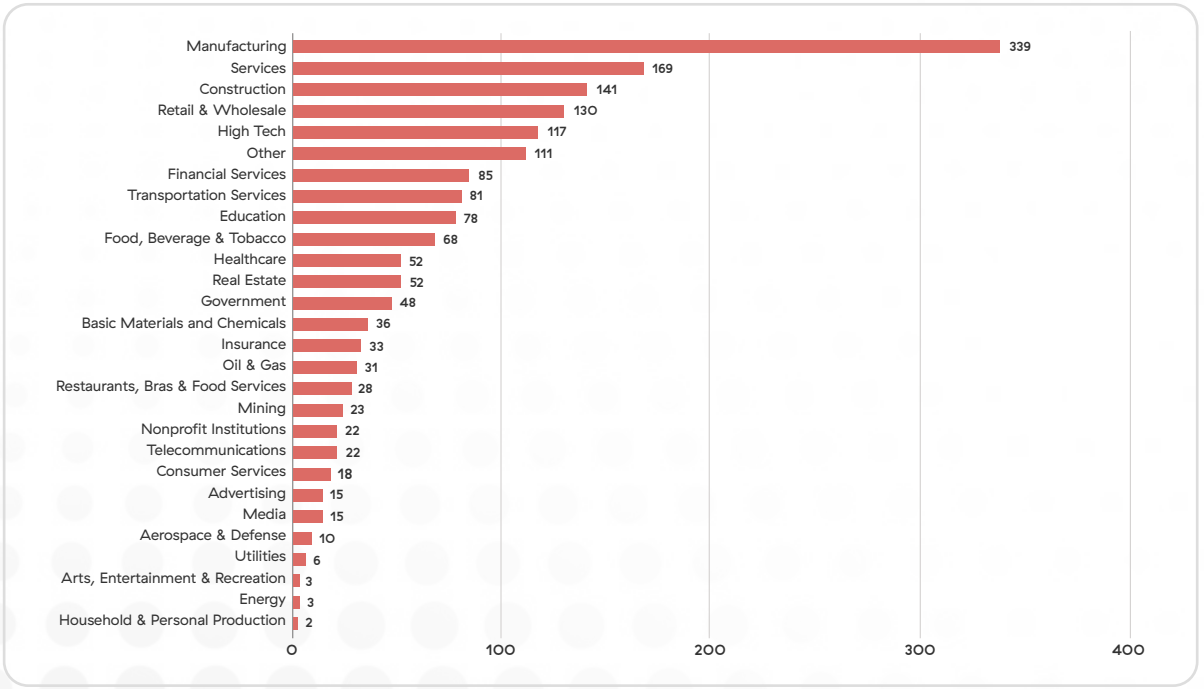


Figure 1: Ransomware attacks by industry based on data leak sites

Ransomware attack trends

This year saw a staggering 550% surge in double extortion attacks on household and personal products, in addition to a significant 433.33% increase in attacks on the arts, entertainment, and recreation industry. It's important to note that these sectors started from a relatively low baseline of attacks in the previous year's report, making their growth appear more substantial.

As shown in figure 2, several other industries observed triple-digit year-over-year percentage growth in double extortion attacks, highlighting the escalating threat landscape.

These findings emphasize the pervasive and evolving nature of ransomware attacks targeting a wide range of industries. Even sectors with historically low attack rates can experience sudden surges in ransomware incidents. The exponential growth in attacks reflects the increasing sophistication and relentless pursuit of profit by ransomware groups.

While the provided data focuses on the percentage change in extortion attacks by ransomware groups, it's important to remember that it represents a specific aspect of the overall threat landscape. Many attacks may go unreported or undetected, making it challenging to capture the full scope of the problem.

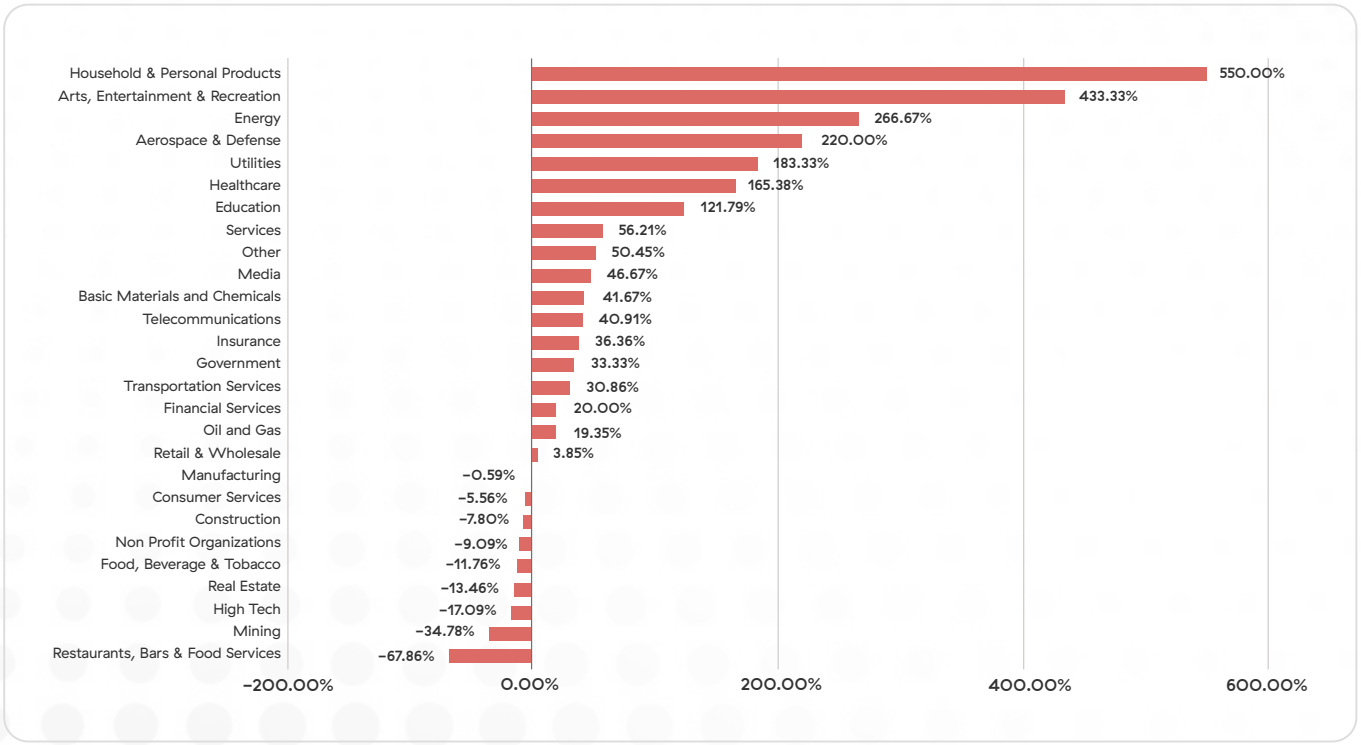


Figure 2: Year over year comparison of extortion attacks by industry, showcasing percentage of change

Ransomware victims by country

Ransomware groups target organizations from different industries and countries. The United States is the most affected country, with 40.34% of overall victims impacted by double extortion attacks, followed by Canada (6.75%), the United Kingdom (6.44%), Germany (4.92%), and France (3.89%). Figure 3 shows a heatmap of countries affected by ransom extortion attacks in the past year.

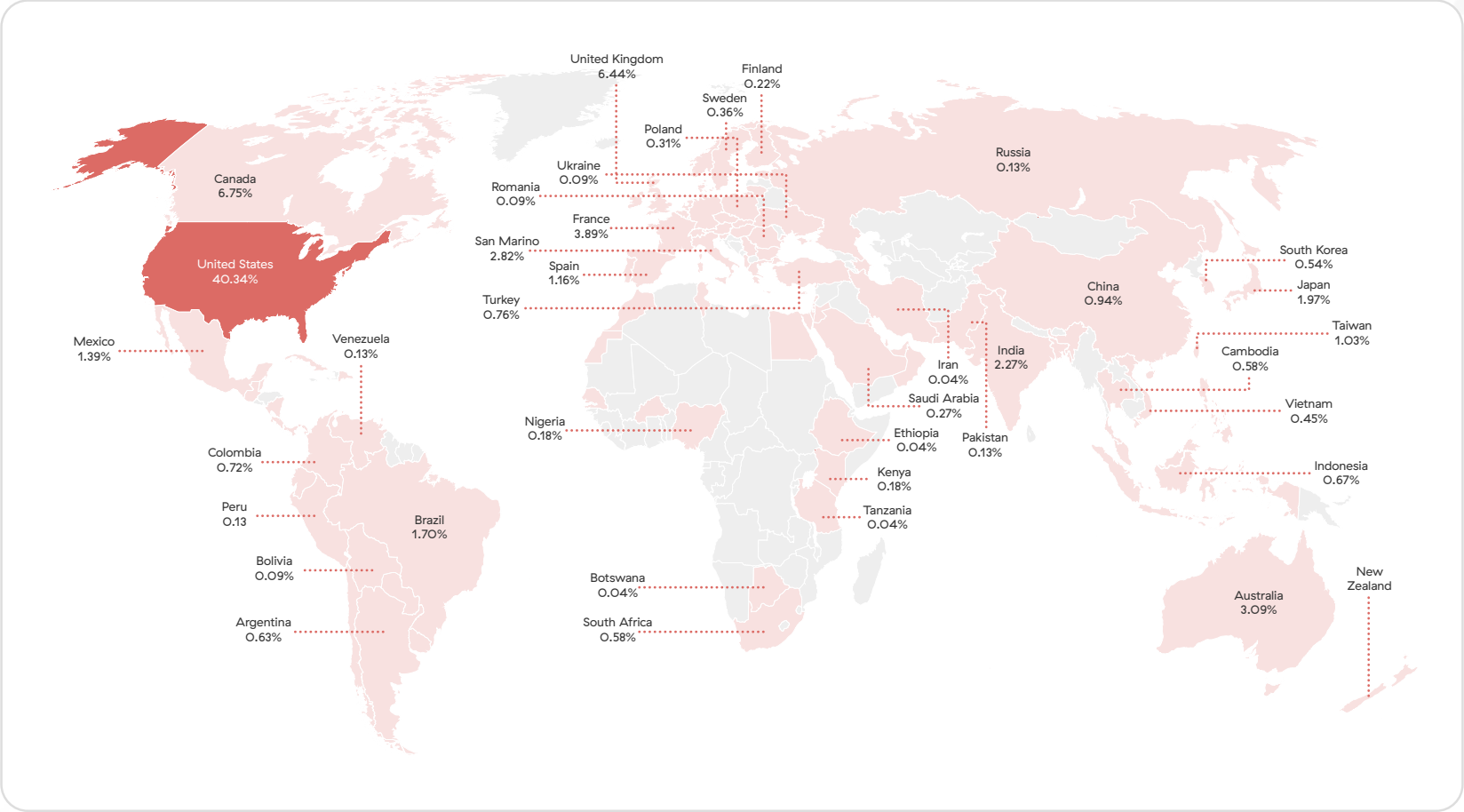
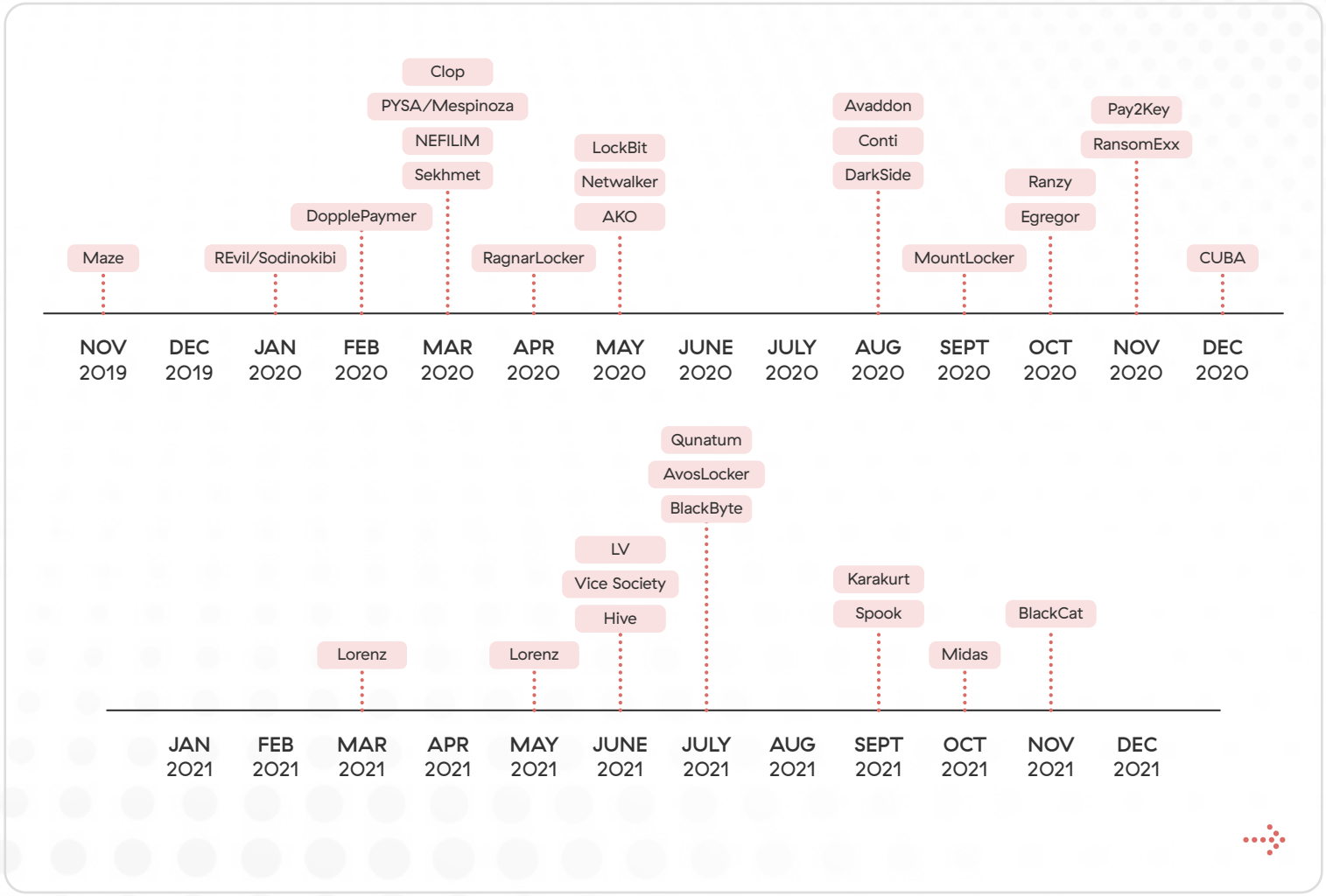


Figure 3: Breakdown of ransomware victims by country

Top ransomware families

LockBit, ALPHV/BlackCat, and BlackBasta were the most prevalent ransomware extortion groups over the last year based on the number of victims listed on their leak sites. Figure 4 shows the most active ransomware families for the past several years, including when they first emerged and began publishing data on leak sites.



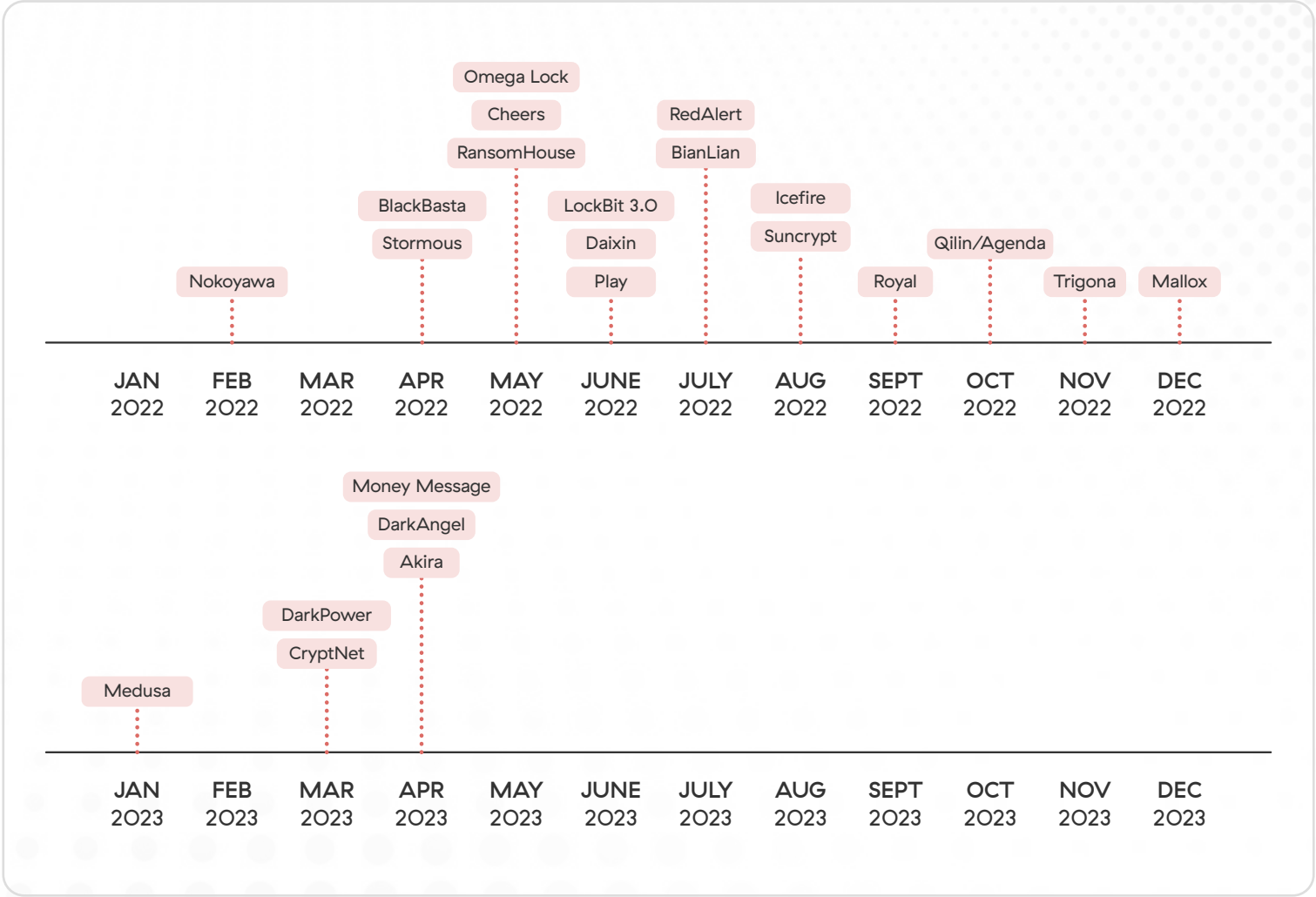


Figure 4: Timeline of ransomware families publishing victims data

Figure 5 shows the number of data leak victims per ransomware group over the last year.

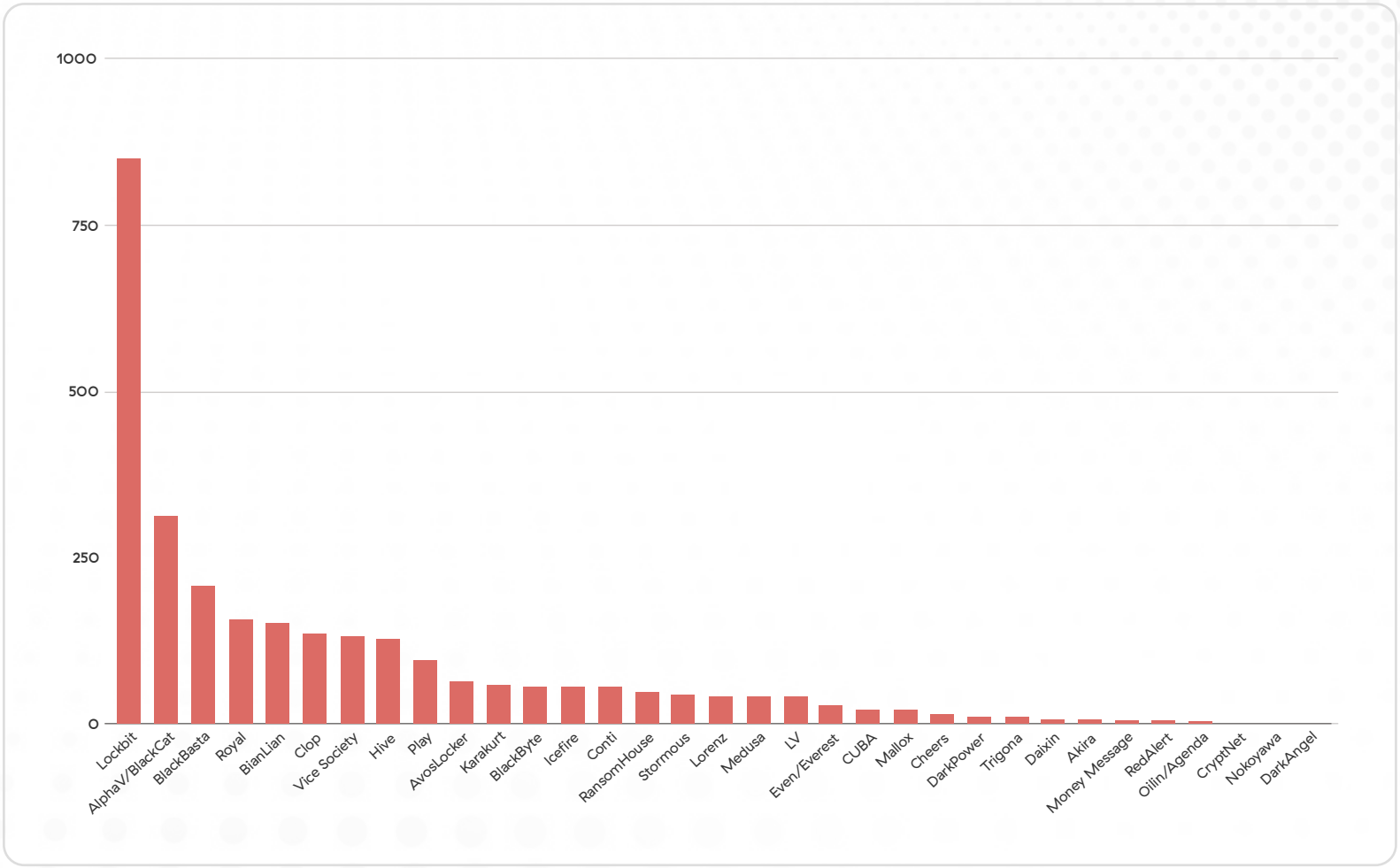


Figure 5: Ransomware attacks by family, April 2022—April 2023

2023—2024 predictions

1. **Encryptionless ransom attacks:** Traditional ransomware encrypts a victim's files and demands a ransom for their release. However, more and more cybercriminals are shifting toward encryptionless ransom attacks, which focus on stealing and threatening to expose sensitive data instead of encrypting it. This approach adds a new layer of complexity and challenges for cybersecurity professionals.

2. **AI-powered ransomware attacks:** Ransomware groups are expected to increasingly leverage artificial intelligence (AI) capabilities—including chatbots, AI-developed malware code, machine learning algorithms, automated processes, and more—which will enable them to develop more sophisticated and efficient techniques, making it harder for traditional cybersecurity measures to detect and prevent such attacks. AI is also likely to lower the bar for developing ransomware by less sophisticated threat actors.

3. **Increased targeting of the cyber-insured:** Cybercriminals have been focusing more on targeting organizations with cyber insurance coverage, a profitable trend likely to continue to increase in the next year. Attackers know that insured victims are more likely to pay ransoms since they can rely on the insurance to cover the costs. This targeting strategy aims to maximize the chances of successful ransom payments.

4. **Increased targeting of public entities:** Another trend that ramped up in 2023 and is expected to continue is ransomware attacks targeting cities, states, municipalities, law enforcement, K-12 schools, and other educational institutions and public entities. These entities often have a very low security posture to protect critical data and systems, making them attractive targets for cybercriminals seeking easy payouts or valuable, easily sold information. These types of attacks often significantly disrupt important public services and expose large caches of sensitive information, including PII, financial data, private records, and much more.

5. **New ransomware-as-a-service (RaaS) offerings:** RaaS is a business model in which cybercriminals commission affiliates to compromise organizations and deploy their ransomware. The vast majority of ransomware groups employ RaaS, and it has proven effective over the years, leading to increases in the number of attacks each year.

6. **Initial access brokers:** There has been an increase in the number of threat groups that will breach an organization, and then sell access to a ransomware group (or affiliates of a ransomware group). This enables threat actors with penetration testing skills to profit from their work without having the expertise required to conduct a full-scale ransomware and/or encryptionless extortion attack.

7. **Attacks on cloud services:** With the growing adoption of cloud computing and storage, ransomware attackers are likely to develop new types of ransomware and campaigns optimized for targeting cloud services and workflows. Compromising cloud environments can result in widespread damage, business disruption, and theft of sensitive data, impacting multiple users or organizations simultaneously. This possibility highlights the need for robust security measures and proactive defenses in cloud-based environments.

8. **Attacks against additional operating systems and platforms:** Ransomware groups will continue to expand their arsenals to attack mission-critical servers that run on non-Windows-based platforms. Threat actors have increasingly built ransomware to encrypt files on Linux and ESXi servers, which often host databases, file servers, and web servers. Some threat groups have also shown interest in developing ransomware for macOS.

Ransomware prevention guidance

As ransomware attacks continue to grow in frequency, sophistication, and impact, stakeholders must stay informed about threat actors' evolving tactics and techniques as detailed in this report. By staying ahead of the curve and implementing proactive cybersecurity measures, organizations and individuals can better protect themselves against the ever-present ransomware threat.

When it comes to defending against ransomware attacks, it is critical to embrace a layered approach that can disrupt the attack at each stage—from reconnaissance and initial compromise to lateral movement, data theft, and payload execution. By following these best practices compiled by our experts, you can help protect your organization from future ransomware attacks:

1. **Back up all data regularly and securely**. This must also include offline backups.
2. **Keep software updated**. Security patches should be applied as soon as they are available.
3. **Remove applications from the public internet** to prevent ransomware actors from exploiting vulnerabilities in public-facing applications. This will make it much more difficult for attackers to gain access to the apps. Use a zero trust architecture to secure internal applications, making them invisible to attackers (see figure 7).
4. **Implement least-privileged access policies** to restrict user access to only the resources they need to do their jobs. This helps prevent attackers from gaining access to sensitive data or systems, even if they compromise a user account.
5. **Enable multifactor authentication (MFA)** to add an extra layer of security to user accounts. MFA requires users to enter a secondary mode of verification in addition to their password, which can help to prevent attackers from gaining access to user accounts if they have obtained compromised credentials.
6. **Enforce a consistent security policy** to help ensure that all users are following the same security procedures, which can help prevent initial compromise. This should include things like strong passwords, MFA, and regular security updates. With a distributed workforce, it is even more important to implement a security service edge (SSE) architecture that can enforce a consistent security policy so that your users are protected no matter where they are.
7. **Train employees** to identify and avoid ransomware attacks. Regularly conducted security awareness training helps employees identify and avoid ransomware attacks.
8. **Have a response plan** to act quickly and effectively in the event of a ransomware attack. This should include steps for things like data recovery, incident response, and communication with customers and employees. Make sure you have a physical, printed copy and phone tree located in an accessible location in case all system access or building access is compromised.
9. **Inspect encrypted traffic**. More than 95% of attacks use encrypted channels, which often are not inspected, making it easy for even moderately sophisticated attackers to bypass security controls. Organizations must inspect all traffic, encrypted or not, to prevent attackers from compromising their systems.
10. **Use a zero trust network access (ZTNA) architecture**. Implement granular user-to-application and application-to-application segmentation, brokering access using dynamic least-privileged access controls to eliminate lateral movement. This allows you to minimize the data that can be encrypted or stolen.
    a. **Implement Zscaler Private Access™ (ZPA™)** to effortlessly provide industry-leading ZTNA for your users. ZPA uses context-based access control to restrict user access to apps and data regardless of location, which helps prevent lateral threat movement and limit ransomware's blast radius.

11. **Use browser isolation** to prevent ransomware from executing on user devices. Browser isolation creates a sandboxed environment for each user, so that if ransomware is executed, it cannot affect the user's device or the rest of the network.
    a. **Implement Zscaler Browser Isolation** to create a secure browsing environment by isolating web content and executing it in the cloud. Any potentially malicious code or ransomware in isolation cannot reach the user's device, providing an additional layer of protection against web-based attacks.

12. **Use an advanced sandbox** to automatically detect unknown threat payloads. Signature-based detection is not enough to protect against the latest ransomware variants. An advanced inline sandbox can detect unknown payloads and prevent them from executing before they reach your users.
    a. **Implement Zscaler Sandbox** to detect and block unknown ransomware variants. This inline sandbox uses AI-powered behavioral analysis, ML, and threat intelligence to identify and quarantine suspicious files. By analyzing the behavior of these files in a controlled environment, the sandbox can determine if they pose a threat and prevent them from being delivered to users.

13. **Use inline data loss prevention (DLP)** to prevent the exfiltration and loss or exposure of sensitive data.
    a. **Implement Zscaler DLP** to prevent the exfiltration of sensitive data, such as credit card numbers, Social Security numbers, and intellectual property. Inspect everything without latency, taking the guesswork out of data classification. This can help to protect against double extortion attacks, where attackers encrypt data and then threaten to publish it if a ransom is not paid.

14. **Use deception technology** to lure attackers into traps and prevent them from gaining access to your systems. Deception tools create fake assets and data that look like valuable targets, which can help waste the attacker's time and resources as well as prevent them from finding and exploiting real vulnerabilities.
    a. **Implement Zscaler Deception™** to proactively defend against ransomware attacks by creating a network of decoy systems, files, and credentials that lure attackers. Alerts are triggered when an attacker interacts with these decoys, allowing security teams to quickly identify and respond to potential threats.

15. **Use a cloud access security broker (CASB)** to control and monitor cloud application usage. A CASB helps prevent users from downloading malicious files from cloud applications, and it can also help prevent data from being exfiltrated to the cloud.
    a. **Implement Zscaler CASB** to gain visibility and control over cloud application usage. By enabling you to monitor and enforce security policies for cloud services, it can prevent the upload or download of sensitive data, detect risky user behavior, and provide insights into the security posture of cloud applications.

16. **Follow Zscaler ThreatLabz research feeds** to gain regular insights on the latest ransomware threats and developments, including published indicators of compromise (IOCs) and MITRE ATT&CK mappings. This information can be used to train your team, improve your security posture, and help prevent ransomware attacks. ThreatLabz also maintains GitHub repositories with IOCs, tools (including proof-of-concept ransomware decryption tools), and an archive of ransomware notes from all major ransomware groups.

Follow ThreatLabz on Twitter @ThreatLabz and our security research blog.

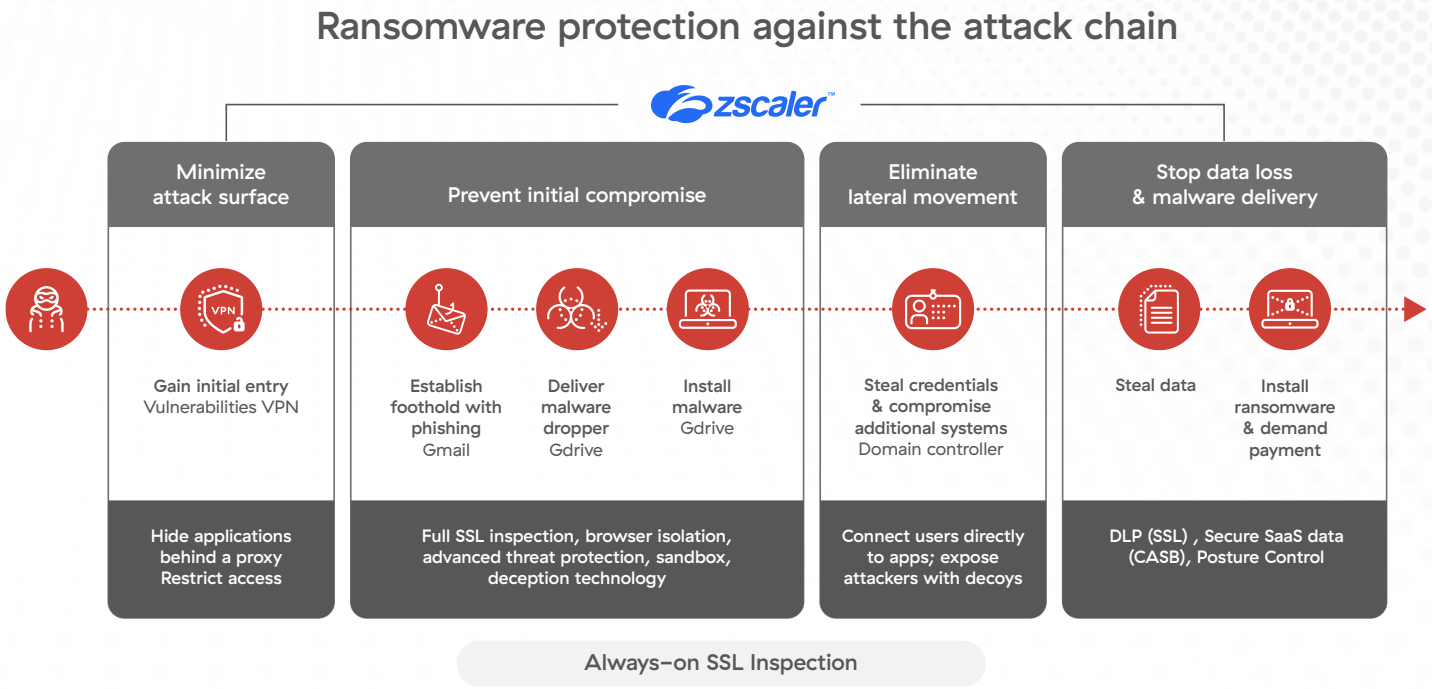


Figure 6: Mapping zero trust architecture across the ransomware attack chain

By implementing these best practices and advanced security measures, you can significantly enhance your organization's defense against ransomware attacks. The combination of ZTNA, browser isolation, advanced sandboxing, data loss prevention, deception technology, and CASB provides a comprehensive and layered approach to protect against different stages of a ransomware attack, from initial infection to data exfiltration.

Related Zscaler Products

Zscaler Private Access™ safeguards applications by limiting lateral movement with least-privileged access, user-to-app segmentation, and full inline inspection of private app traffic.

Zscaler Internet Access™ helps identify and stop malicious activity by routing and inspecting all internet traffic through the Zscaler Zero Trust Exchange™.

Advanced Threat Protection blocks all known command-and-control (C2) domains.

Advanced Firewall extends C2 protection to all ports and protocols, including emerging C2 destinations.

Browser Isolation creates a safe gap between users and malicious web categories, rendering content as a stream of picture-perfect images to eliminate data leakage and the delivery of active threats.

Zscaler Sandbox prevents unknown malware delivered in second stage payloads.

Zscaler Deception™ detects and contains attackers attempting to move laterally or escalate privileges by luring them with decoy servers, applications, directories, and user accounts.

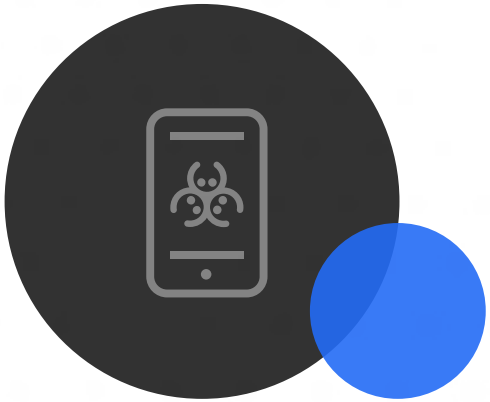
Key ransomware trends

Ransomware as a service (RaaS)

The dark web has become a popular place for threat groups to sell their wares to would-be criminals. We've detailed the impact of these marketplaces for other attack types, such as the growth of phishing as a service in the ThreatLabz 2023 Phishing Report.

RaaS is a popular model wherein threat groups sell their tools and services on the dark web. It involves two parties: operators who recruit affiliates and provide them with ransomware, tools, access to data leak sites, negotiation assistance, and other support in exchange for 70—80% of the profits; and affiliates who execute the attacks. This model benefits both parties, enabling affiliates to conduct effective attacks without developing the tools themselves while operators expand their operations and profits.

RaaS has led to an increase in both the number and impact of attacks. The volume of ransomware attacks has risen because more affiliates can easily execute attacks. Ransom amounts have also increased due to the double extortion tactic, in which threat actors steal data and threaten to publish it unless the ransom is paid, resulting in higher payments.



Encryptionless extortion

Encryptionless extortion is one of the most notable changes over the last year. Some threat actors have shifted away from file encryption to stealing large amounts of data from organizations and demanding a ransom payment to avoid public release. ThreatLabz has observed multiple victims that had more than 10 TB of data stolen as well as one victim that lost more than 24 TB of data.

The trend started with groups including Babuk and SnapMC in 2021, and other groups have followed suit over the last year, including Karakurt, Donut, RansomHouse, and BianLian. The latter group dropped file encryption in 2023 and resorted to encryptionless attacks after a free decryption tool was released. Ransomware threat actors are moving toward encryptionless extortion attacks for several reasons:

- **Reduce business disruption:** Encryptionless attacks are designed to be less disruptive, which can be costly for victims. Less disruption may enable victims to pay higher ransoms since their businesses can continue to drive sales, and thus profits, despite the attack.
- **Reduce reputational harm:** Businesses that are not disrupted are less likely to publicly disclose a breach, protecting their reputation from irreparable harm. The cost of paying a ransom can dwarf the potential damages from loss in sales, litigation, and trust. Thus, it can be a "win-win" if the organization pays a ransom to prevent disclosure of potentially damaging information and avoid a major business disruption.

- **Reduce scrutiny from law enforcement and security researchers:** Nondisruptive attacks can fly under the radar of law enforcement and security researchers. Ransomware actors have learned from the Colonial Pipeline hack and REvil supply chain attack targeting Kaseya, which drew significant attention that ultimately led to each group's demise.
- **Launch hard-to-detect attacks:** Many organizations have security solutions for endpoints, but an encryptionless extortion attack can be conducted using legitimate tools and native Windows applications (a.k.a., living-off-the-land), making them harder to detect and prevent. Many organizations invest too little in network monitoring and DLP, which can detect these types of attacks.

Major vulnerabilities used in ransomware attacks

Awareness of major vulnerabilities exploited in ransomware attacks is vital for organizations seeking to strengthen their defenses against evolving threats. By prioritizing vulnerability mitigation, promptly applying patches, and following cybersecurity guidelines, organizations can significantly reduce the risk of falling victim to ransomware attacks. This section provides a comprehensive summary of the key vulnerabilities leveraged in recent ransomware attacks, emphasizing the need for proactive prevention and effective incident response.

ProxyNotShell vulnerabilities in Microsoft Exchange

The ProxyNotShell vulnerabilities are a set of two security flaws in Microsoft Exchange Server versions 2013, 2016, and 2019. These vulnerabilities allow attackers to execute arbitrary code on a vulnerable server, which can then be used to install ransomware or other malware.

Ransomware attackers have been using the ProxyNotShell vulnerabilities in attacks since at least September 2022 and again in December 2022. The Play ransomware group successfully gained initial access through both ProxyNotShell vulnerabilities. In these attacks, the attackers first exploited the CVE-2022-41040 to gain access to the Remote PowerShell service on the vulnerable server. Once they had access to the Remote PowerShell service, they exploited the remote code execution (RCE) vulnerability CVE-2022-41082 to execute arbitrary code on the server.

The ProxyNotShell vulnerabilities are a serious security risk, and organizations should take steps to mitigate them. Microsoft promptly addressed these vulnerabilities in November 2022, releasing security updates to address the vulnerabilities, and organizations should apply these updates as soon as possible. In addition, organizations should consider disabling the Autodiscover endpoint in Exchange Server, as this can help to prevent attackers from exploiting the vulnerabilities.

PaperCut vulnerability

The PaperCut vulnerability is a critical remote code execution vulnerability in the PaperCut NG/MF print management software. The vulnerabilities, CVE-2023-27350 and CVE-2023-27351, were first disclosed in March 2023 and have been exploited by ransomware attackers including Clop, LockBit, and BlOOdy.

The vulnerability allows attackers to execute arbitrary code on vulnerable systems without authentication. This can be used to install ransomware, steal data, or disrupt operations. Specifically, CVE-2023-27350 allows an unauthenticated attacker to get remote code execution on a PaperCut Application Server. CVE-2023-27351 allows an unauthenticated attacker to fetch information about a user stored within PaperCut NG/MF.

PaperCut has released a patch for the vulnerability on versions 20.1.7, 21.2.11, 22.0.9, and later, which should be applied as soon as possible along with the following mitigation measures:

- **Disable remote access to PaperCut servers:** This can be done by changing the server's listening port from 8080 to a nonstandard port.
- **Use strong passwords and multifactor authentication for PaperCut accounts:** This can help to prevent attackers from gaining unauthorized access to the at-risk servers.
- **Monitor PaperCut servers for suspicious activity:** This can be done by using a security information and event management (SIEM) tool or by manually reviewing the log files.

By taking these steps, organizations can help to protect themselves from the PaperCut vulnerability and other ransomware attacks.

IBM Aspera Faspex file sharing software vulnerability

The IBM Aspera Faspex file-sharing software vulnerability, CVE-2022-47986, is a critical remote code execution vulnerability that affects IBM Aspera Faspex versions 4.4.2 and earlier. The vulnerability was disclosed in January 2023 and has been exploited by ransomware attackers in the wild including by the IceFire ransomware group.

The vulnerability, caused by YAML, is a deserialization flaw that allows attackers to execute arbitrary code using an obsolete API call on vulnerable systems without authentication. This can be used to install ransomware, steal data, or disrupt operations.

IBM has released a patch for the vulnerability, and organizations should apply it as soon as possible. In addition, organizations should consider the following mitigation measures:

- **Disable remote access to Aspera Faspex servers:** This can be done by changing the server's listening port from 8080 to a nonstandard port.
- **Use strong passwords and multifactor authentication for Aspera Faspex accounts:** This can help to prevent attackers from gaining unauthorized access to the at-risk servers.
- **Monitor Aspera Faspex servers for suspicious activity:** This can be done by using a security information and event management (SIEM) tool or by manually reviewing the log files.

By taking these steps, organizations can help to protect themselves from the IBM Aspera Faspex vulnerability and other ransomware attacks.

Privilege escalation vulnerabilities

Ransomware threat groups often exploit various privilege escalation vulnerabilities as part of their attacks. One such vulnerability is CVE-2022-24521, which affects the Windows Common Log File System. This vulnerability, which was patched in April 2022, enables the attacker to elevate their privileges once they successfully exploit the vulnerability. Notable ransomware groups like Cuba, RedAlert, and Yanluowang have been known to exploit CVE-2022-24521 in their attacks.

Another vulnerability that has been leveraged for privilege escalation is known as PrintNightmare and is tracked as CVE-2021-34527. It was patched in July 2021 but has been exploited by affiliates of the BlackBasta group. By exploiting this vulnerability, they gain the ability to perform privileged operations after gaining initial access to the network.

Furthermore, the Nokoyawa ransomware group has been observed exploiting the vulnerability CVE-2023-28252. This vulnerability, which affects the Windows Common Log File System, was patched in April 2023. Similar to CVE-2022-24521, this vulnerability allows attackers to escalate their privileges within the compromised system.

These privilege escalation vulnerabilities serve as valuable tools for ransomware threat groups, enabling them to gain higher levels of access and control within targeted networks. It highlights the importance of promptly patching and updating systems to mitigate the risk posed by such vulnerabilities.

The role of CISA and vulnerability prioritization

The Cybersecurity & Infrastructure Security Agency (CISA) maintains a complete list of vulnerabilities, including those which are actively being exploited by ransomware groups. Organizations are strongly advised to follow this list and prioritize addressing the vulnerabilities mentioned therein. Proactive vulnerability management is a key element in bolstering overall cybersecurity posture.

Law enforcement takedowns

The most notable law enforcement action over the past year was an FBI–led operation that disrupted Hive ransomware on January 26, 2023. Hive ransomware was used to target more than 1,500 victims in over 80 countries around the world. The FBI was able to penetrate Hive's servers in July 2022 and capture the group's encryption keys, which were turned over to the victim organizations. This prevented $130 million dollars in ransom payments to the Hive group. Unfortunately, there were no arrests tied to these seizures, and the group may have already resurfaced under the brand name U–Bomb. Figure 7 shows a comparison between the former Hive ransom chat portal and the striking resemblance with the new U–Bomb portal.

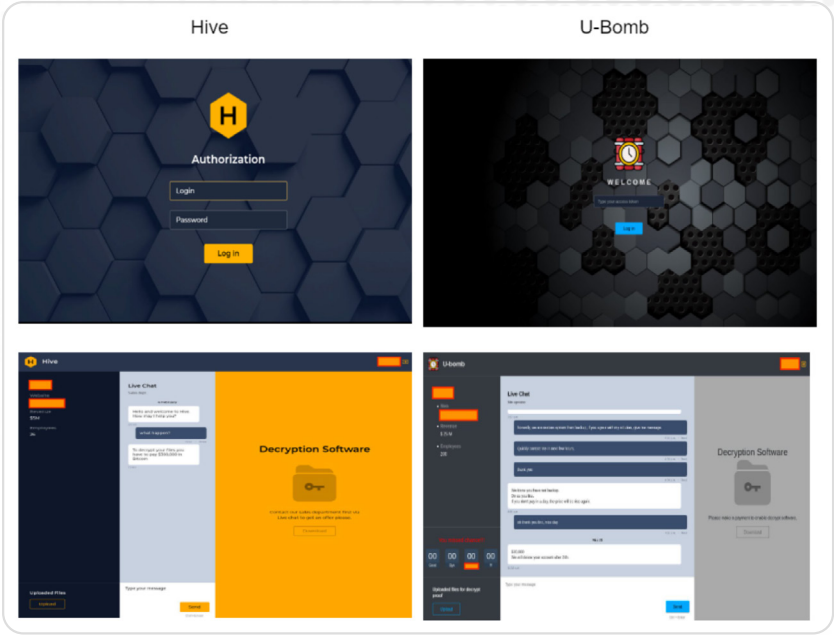


Figure 7: Comparison of the Hive (left) and U–Bomb (right) ransom chat portals

Evolution of cross–platform ransomware development

A significant trend that emerged in 2022 and continues to gain momentum in 2023 is the adoption of new programming languages by ransomware attackers. Traditionally, C and C++ were the go–to languages for developing ransomware strains. However, threat actors have now shifted their focus to more contemporary programming languages like Golang and Rust, which offer robust cross–platform code compilation capabilities. This transition enables attackers to target multiple operating systems, including Windows and Linux, and multiple architectures such as x86, x64, and ARM, using a single codebase. Moreover, it provides several advantages, such as improved performance, enhanced memory safety, and increased resistance against reverse engineering, making detection and analysis more challenging.

The BlackCat group, a prominent ransomware operator, transitioned to using the Rust programming language in late 2021. Following suit, the Hive ransomware group also shifted from Golang to Rust in 2022. The latest iteration of RansomExx, known as RansomwareExx2, emerged in November 2022 and employed Rust as its programming language. Similarly, Nokoyawa 2.0 began utilizing Rust for development starting in September 2022. In December 2022, the Agenda/Qilin ransomware code was ported from Golang to Rust. Another ransomware variant, Luna, also embraced the Rust programming language for its development efforts.

Rust, as a programming language, offers several advantages for ransomware development:

- **Fast encryption speed:** Rust facilitates efficient encryption processes, enabling swift execution of ransomware operations.
- **Resistance to reverse engineering:** Rust's design and tooling make it relatively challenging to reverse engineer, adding an additional layer of protection to the ransomware codebase.
- **Granular control over low-level resources:** Rust provides developers with deep control over low-level system resources, allowing them to optimize and manipulate code behavior as desired.
- **User-friendly syntax:** Rust offers a syntax that is considered more intuitive and readable, contributing to improved development efficiency.
- **Abundance of third-party libraries:** The Rust ecosystem boasts a wide range of third-party libraries, including encryption libraries, which simplifies the implementation of advanced functionalities in ransomware.

Table 2 shows a comparison of ransomware families that utilize Golang or Rust in their latest versions.

The shift toward Golang and Rust as preferred languages for ransomware development reflects the evolving landscape of cyberthreats. As attackers continue to refine their techniques, it becomes crucial for cybersecurity professionals and organizations to stay vigilant and employ robust security measures to mitigate the risks posed by these cross-platform ransomware attacks.

Ransomware Family	C/C++	Golang	Rust
Hive		✓	✓
BlackCat/ALPHV			✓
BlackByte	✓	✓	
RansomExx	✓		✓
BianLian		✓	
Snatch		✓	
Nokoyawa	✓		✓
Agenda/Quilin		✓	✓
Luna			✓

Table 2: Overview of programming languages used by ransomware families

Fallout from Conti disbanding

In May 2022, the Conti ransomware group disbanded after a vigilante researcher hacked the group's infrastructure following the invasion of Ukraine. The researcher posted sensitive information including the group's source code and internal chat logs. This was a major development in the ransomware landscape, as Conti was one of the most active and sophisticated ransomware groups in operation. The disbanding of Conti has led to the creation of new ransomware groups that sought to fill the void left by Conti.

In addition, the Conti source code has since been used by numerous threat groups to launch attacks with ransomware brands named ScareCrow, Meow, Putin, and most recently Akira. The LockBit threat group has also used the leaked Conti ransomware source code for attacks, and refer to that specific variant as LockBit Green.

There are several ransomware groups that are likely members of the former Conti group including BlackBasta. Shortly after the demise of Conti, ThreatLabz observed BlackBasta using a ransomware negotiation script that was nearly identical to Conti as shown in figure 8.

ThreatLabz has also observed similarities in the tactics, techniques, and procedures (TTPs) with the Royal ransomware group, Diavol, and Karakurt.

New ransomware families

In this section, we delve into the emergence of new ransomware families that use double extortion attacks and the shift observed in the ransomware landscape. Recent data indicates a notable increase in the creation of new ransomware families compared to the emergence of new groups in previous years. This trend highlights the dynamic nature of the ransomware ecosystem, with threat actors constantly evolving to take advantage of potential financial gains.

In 2021, ThreatLabz observed the launch of 19 new ransomware families that used double or multi-extortion tactics. This means that in addition to encrypting the victim's data, the ransomware operators also stole a copy of the data and threatened to publish it online if the ransom was not paid. This year, another 25 new ransomware families, shown in table 3, have adopted this tactic. This list includes families that use encryptionless data extortion attacks, which means that they do not encrypt the victim's data at all. Instead, they simply steal the data and threaten to publish it online.

The use of double or multi-extortion tactics is a growing trend in ransomware attacks. This is because it increases the chances that the victim will pay the ransom. If the victim only has to pay to get their data back, they may be able to resist the temptation to pay. However, if the victim knows that their data will be published online if they do not pay, they are more likely to pay the ransom to avoid embarrassment and damage to their reputation.

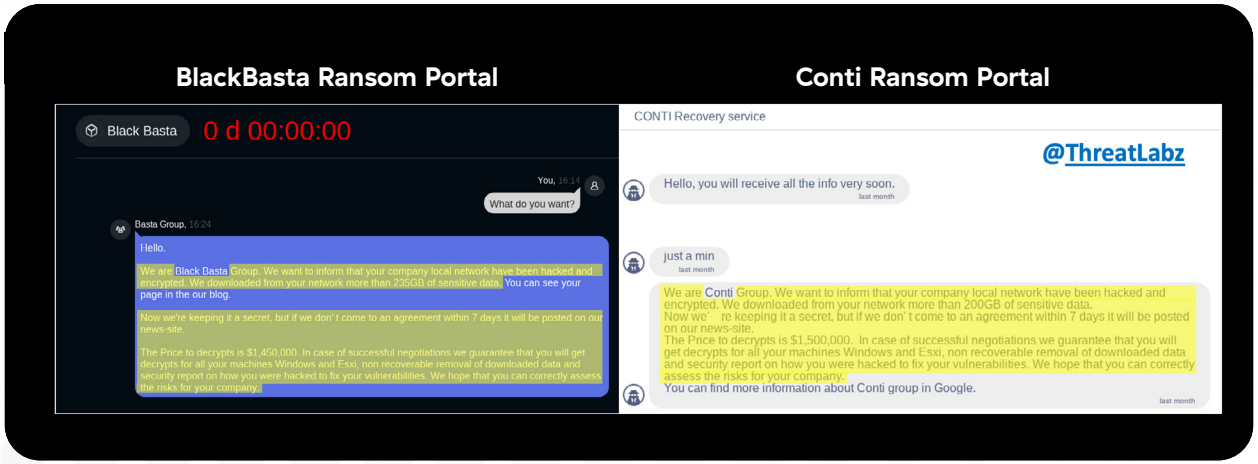


Figure 8: Similarities (highlighted) between BlackBasta and Conti ransom communications

The use of encryptionless data extortion attacks is a new and worrying trend because it involves one less step in the attack chain for detection, and it forces victims to pay the ransom if they do not want their sensitive business data exposed.

OLD February 2021 through March 2022

Lorenz	LV	Spook
Grief	BlackByte	Karakurt
Hive	AvosLocker	Midas
Vice Society	Quantum	ALPHV/BlackCat
LockBit 2.0	Rook	
Nokoyawa	Prometheus	
Yanluowang	AtomSilo	
Xinglocker		

NEW April 2022 through April 2023

Stormous	Omega Locks	RedAlert
BlackBasta	LockBit 3.0	BianLian
RansomHouse	Daixin	IceFire
Cheer	Play	SunCrypt
Royal	Medusa	Dark Angels
Qilin/Agenda	DarkPower	Akira
Trigona	CryptNet	Monti
Mallox	Money Message	CrossLock

Table 3: 24 new ransomware families

Leaked source code

The following section explores the exploitation of leaked source code and builders by ransomware threat actors. The leaked source code of Conti and Babuk ransomware and the leaked LockBit builder contributed to the increase in ransomware activity over the past year. There were two versions of the Conti source code that were leaked and labeled as version 2 and version 3. The former version was used by many of the less sophisticated threat actors because version 3 added ChaCha encryption to the ransom note, which requires modifications to the code or a builder that can properly encrypt the ransom note and patch the compiled ransomware executable. Figure 9 shows an example of the leaked Conti version 3 source code compiled using Microsoft Visual Studio.

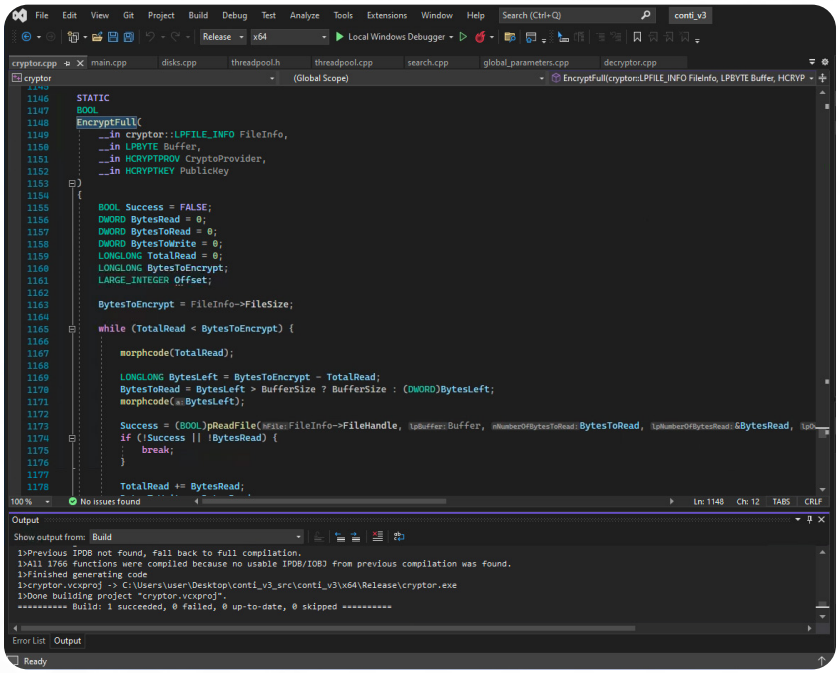


Figure 9: Leaked Conti version 3 source code compiled in Microsoft Visual Studio

Over the past year, the Conti source code has been used by groups such as ScareCrow, Akira, Meow, Putin, and LockBit Green.

The Babuk ransomware source code was also leaked by a developer in September 2021, and over the past year has been used by ransomware groups including DATAF, BabLock, and Dark Angels.

In September 2022, a builder for the LockBit ransomware was leaked. This leak made it trivial for any threat actor to customize LockBit ransomware to their own specifications, including the encryption keys, files and directories to target, and ransom note. Figure 10 shows an example of the files produced by the leaked LockBit builder.

There have been a number of threat groups that have used the leaked LockBit builder over the past year to create their own ransomware attacks, including SchoolBoys and BlOOdy.

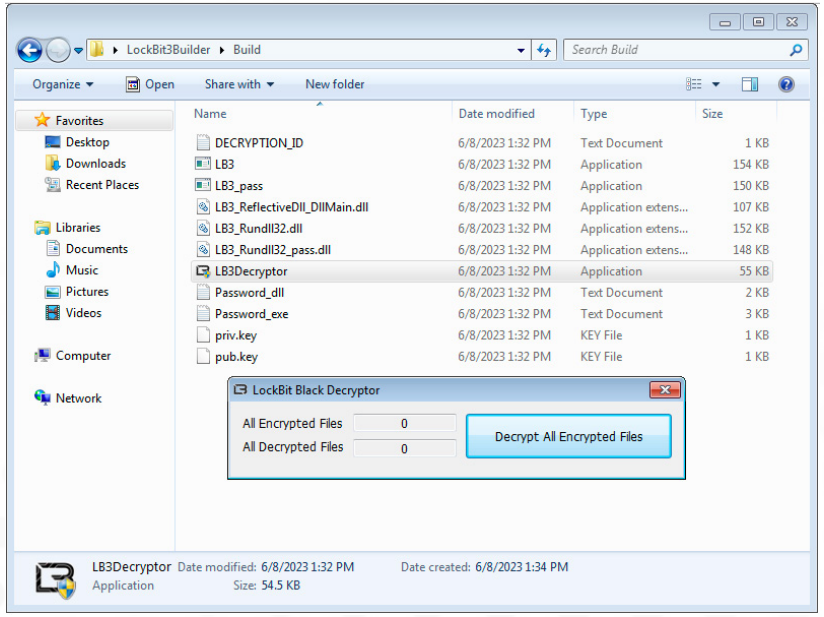


Figure 10: Ransomware files generated from the leaked LockBit builder

Increasing use of elliptic curve cryptography for encryption

In the landscape of ransomware, a notable development has been the adoption of advanced encryption techniques, specifically centered around elliptic curve–based encryption algorithms. Elliptic curve cryptography (ECC) is a form of public key cryptography based on elliptic curve theory, offering an alternative to the RSA algorithm with several advantages. ECC enables faster encryption and decryption processes while demanding fewer CPU and memory resources. Despite shorter key lengths, ECC provides the same level of security as RSA.

To augment the complexity of decryption and intensify the pressure on victims, attackers have incorporated ECC schemes with elliptic curves including **Curve25519, NIST B–233, NIST P–521,** and **NIST K–571**. For example, a new ransomware family identified by ThreatLabz in March 2023, known as Money Message, leveraged NIST K–571 to generate a per file ChaCha20 key using the Elliptic Curve Diffie–Hellman (ECDH) algorithm. In November 2022, the latest version of the BlackBasta ransomware introduced ECC utilizing the NIST P–521 (secp521r1) elliptic curve and XChaCha20 as replacement encryption algorithms. The Crypto++ library facilitates these encryption schemes within BlackBasta 2.0.

Initially developed in the C programming language, the Nokoyawa ransomware utilized ECC with NIST B–233 (sect233r1) and Salsa20 for file encryption. However, in September 2022, Nokoyawa underwent a transition and was rewritten in the Rust programming language, implementing ECC with Curve25519 and Salsa20 for file encryption. Similarly, the BlackByte ransomware was originally created in C#, but later it was reimagined in the Go programming language. Recent iterations of BlackByte incorporate Curve25519

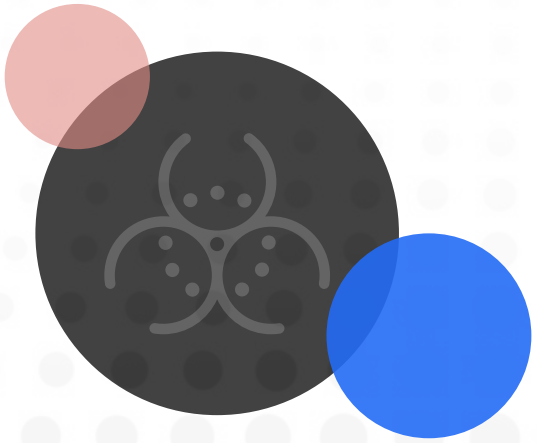
Elliptic curve cryptography for asymmetric encryption and ChaCha20 for symmetric file encryption.

Table 4 provides a list of some of the ransomware families that have utilized ECC-based encryption over the past year.

The adoption of elliptic curve-based encryption in ransomware operations signifies a shift towards more efficient encryption methods, emphasizing the need for heightened cybersecurity measures to counter these evolving threats.

Ransomware	ECC based algorithm	Systemmetric algorithm
Money Message	NIST K-571 (aka sect571k1)	ChaCha20
BlackBasta 2.0	NIST P-521 (aka secp521r1)	XChaCha20
Nokoyawa 1.0 & 1.1	NIST B-233 (aka sect233r1)	Salsa20
Nokoyawa 2.0 & 2.1	Curve25519	Salsa20
REvil variants (e.g., RansomCartel)	Curve25519	Salsa20
BlackByte	Curve25519	ChaCha20
Babuk variants	Curve25519	HC-128

Table 4: Overview of encryption algorithms used by ransomware families



Advanced polymorphic code obfuscation

Ransomware developers employ various techniques of obfuscation to enhance the complexity of their software and impede analysis. Some ransomware families rely on a few fundamental obfuscation methods, while others employ a wide array of techniques. The extent of obfuscation employed by a particular ransomware family depends on the skill level of the developers and the available resources at their disposal.

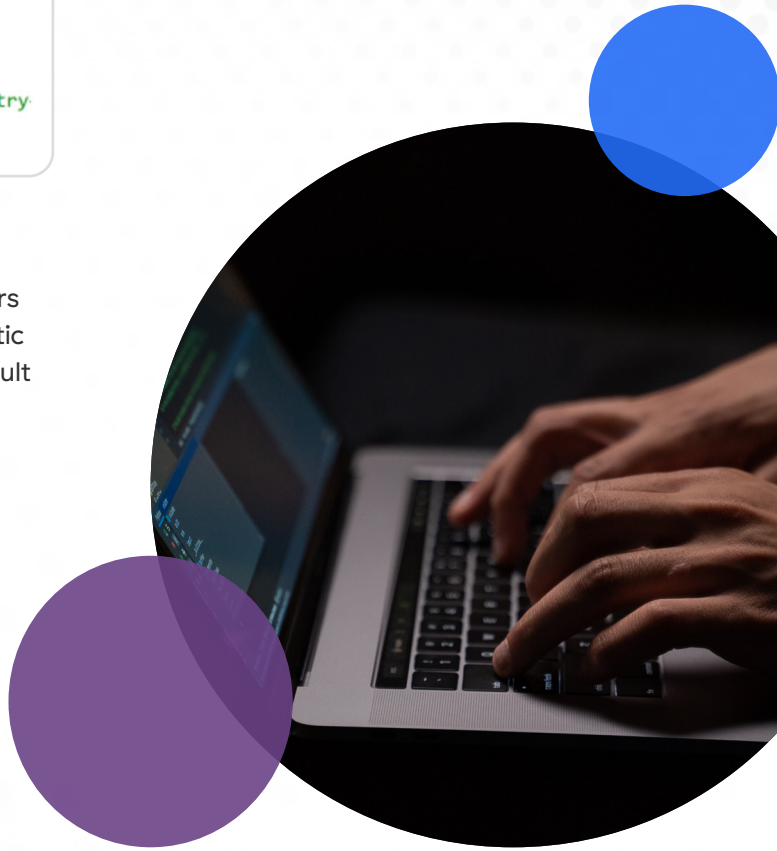
In general, most ransomware developers have increasingly incorporated obfuscation to hinder analysis and bypass static binary signatures. Prominent groups such as BlackByte, BlackCat/ALPHV, and BlackBasta have actively employed these tactics. Presently, many ransomware families utilize ADVobfuscator, an open source obfuscation library, to implement polymorphic string encryption. The library alters the encryption pattern of strings in the ransomware's code during compilation time through the use of macros in the source code. When the ransomware code is compiled, the compiler will replace the macros with code that will build obfuscated strings on the stack and choose random mathematical operations such as subtraction, addition, and exclusive-or (XOR) to decrypt each string. Therefore, every time the code is compiled, the method to decrypt the strings will differ and the sample will have a unique checksum, which may evade security software that blocks specific file hash values.

An example of the string obfuscation implemented by BlackBasta is shown below in figure 11.

```
.text:1000ABD9 33 C0                                xor     eax, eax
.text:1000ABDB B2 5B                                mov     dl, 5Bh ; '['
.text:1000ABDD C7 45 A6 34 00 35 00                 mov     [ebp+var_5A], 350034h
.text:1000ABE4 C7 45 AA 3E 00 7B 00                 mov     [ebp+var_56], 7B003Eh
.text:1000ABEB 33 C9                                xor     ecx, ecx
.text:1000ABED C7 45 AE 2F 00 32 00                 mov     [ebp+var_52], 32002Fh
.text:1000ABF4 C7 45 B2 36 00 3E 00                 mov     [ebp+var_4E], 3E0036h
.text:1000ABFB C7 45 B6 61 00 7B 00                 mov     [ebp+var_4A], 7B0061h
.text:1000AC02 C7 45 BA 7E 00 75 00                 mov     [ebp+var_46], 75007Eh
.text:1000AC09 C7 45 BE 6F 00 3D 00                 mov     [ebp+var_42], 3D006Fh
.text:1000AC10 C7 45 C2 7B 00 28 00                 mov     [ebp+var_3E], 28007Bh
.text:1000AC17 C7 45 C6 3E 00 38 00                 mov     [ebp+var_3A], 38003Eh
.text:1000AC1E C7 45 CA 34 00 35 00                 mov     [ebp+var_36], 350034h
.text:1000AC25 C7 45 CE 3F 00 28 00                 mov     [ebp+var_32], 28003Fh
.text:1000AC2C 66 89 45 D2                          mov     [ebp+var_2E], ax
.text:1000AC30
.text:1000AC30                              loc_1000AC30:                           ; CODE XREF: VisibleEntry
.text:1000AC30 66 0F BE C2                          movsx   ax, dl
.text:1000AC34 66 31 44 4D A4                       xor     word ptr [ebp+ecx*2+Format+2], ax
```

Figure 11: Example BlackBasta string obfuscation

The use of obfuscation by ransomware developers is a growing trend. As ransomware developers become more sophisticated, they are using more and more obfuscation techniques to evade static binary signatures and make their ransomware more difficult to analyze. This makes it more difficult for organizations to defend themselves against ransomware attacks.



Top 5 ransomware families to watch in 2023

Ransomware continues to pose a significant threat of financial losses, data breaches, and operational disruption to organizations and individuals worldwide. Understanding prevalent ransomware families' characteristics and tactics is crucial for developing effective defense strategies.

This section provides an overview of the five prevalent ransomware families and extortion groups, including their infection chains, data leak sites, and industries targeted. The MITRE ATT&CK tactics and techniques associated with each family are provided in the Appendix.

We will examine the LockBit, BlackCat, Clop, BlackBasta, and Karakurt ransomware families in detail. Analyzing the attack patterns of these ransomware families can help organizations enhance their preparedness strategies and implement proactive security measures to significantly mitigate the risks of falling victim to these campaigns.

#1 LockBit ransomware

LockBit ransomware first emerged in September 2019 and quickly became one of the most active and notorious threat groups ThreatLabz followed. The past year saw some significant developments, with two new versions of the ransomware.

In June 2022, the group released LockBit 3.0 (a.k.a. LockBit Black, because it shares code with the defunct BlackMatter ransomware). In September 2022, the LockBit 3.0 builder was leaked. After the leak, several other ransomware groups including SchoolBoys and the BlOOdy ransomware gang used the builder to create and launch their own ransomware campaigns. In January 2023, the group created LockBit Green, which is based on the leaked Conti source code. In April 2023, the group appeared to have developed ransomware for macOS, although the code was still rather primitive.

Over the past year, LockBit started leaking chat logs from victims that refused to pay ransoms. One such set of logs, involving the Royal Mail Group in the UK, revealed the ransom demand was set at US$80 million based on 0.5% of the postal service's revenue (see figure 12). This is one of the largest ransom demands ThreatLabz has ever observed.

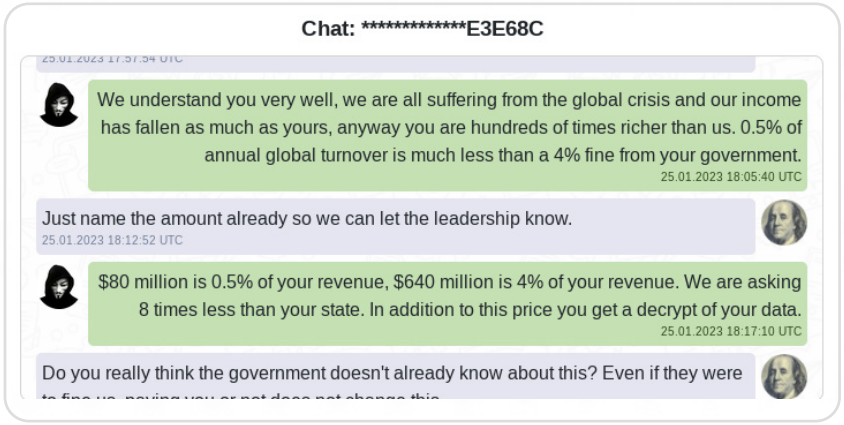


Figure 12: Leaked chat logs from the Royal Mail Group with a US$80M ransom

Over the past year, LockBit also introduced a bug bounty program, encouraging researchers to report bugs for $1,000 to $1 million bounties (see figure 13).

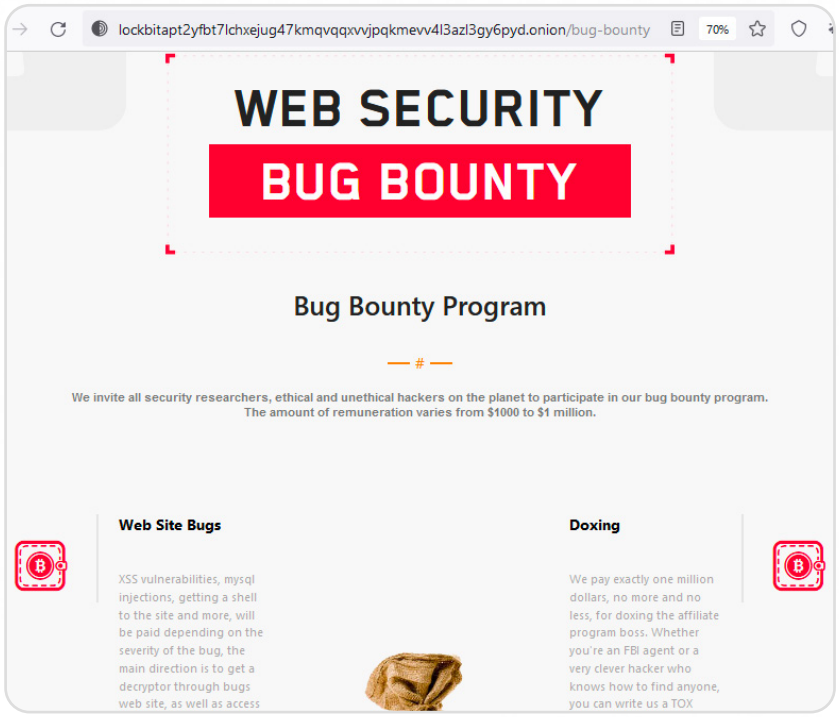


Figure 13: Screenshot of LockBit bug bounty program

LockBit leverages a large affiliate network to conduct breaches, exfiltrate data, and deploy its ransomware. Some of these affiliates break into organizations through spam emails that contain malicious attachments or links. Others have leveraged brute force password attacks targeting Remote Desktop Protocol (RDP) or VPN credentials, purchased compromised stolen credentials through initial access brokers, performed drive-by downloads, and exploited public-facing applications.

LockBit infection chain

The following is a detailed account of an attack conducted by a LockBit affiliate. The initial compromise in this attack began with the victim unknowingly accessing a compromised website, triggering a drive-by download of SocGholish malware, disguised as a software update. Once executed, SocGholish downloaded a Cobalt Strike beacon (a popular post-exploitation tool) and utilized PowerShell to gather system and domain information.

To evade detection and ensure a smooth, unhindered encryption process, the threat actor deployed a batch script that terminated various processes and services associated with antivirus software, databases, backups, and other programs that could potentially impede the encryption of files.

Further, the attacker used tools such as Seatbelt and BloodHound to gather additional system information. Seatbelt is a reconnaissance tool used to extract data about user accounts, local groups, security policies, and more. BloodHound assists in identifying and exploiting Active Directory vulnerabilities.

With this information and an established foothold, the threat actor employed PsExec for lateral movement, enabling them to traverse across the victim's network and gain access to other systems. This lateral movement technique facilitated the spread of the attack within the compromised network.

To exfiltrate the victim's data, the attacker employed MegaSync, a file synchronization tool that allowed for the transfer of stolen information to an external location under the attacker's control.

Finally, in the last stage of the attack, the attackers deployed and executed the LockBit ransomware. This malicious software encrypted the victim's files, rendering them inaccessible until a ransom was paid.

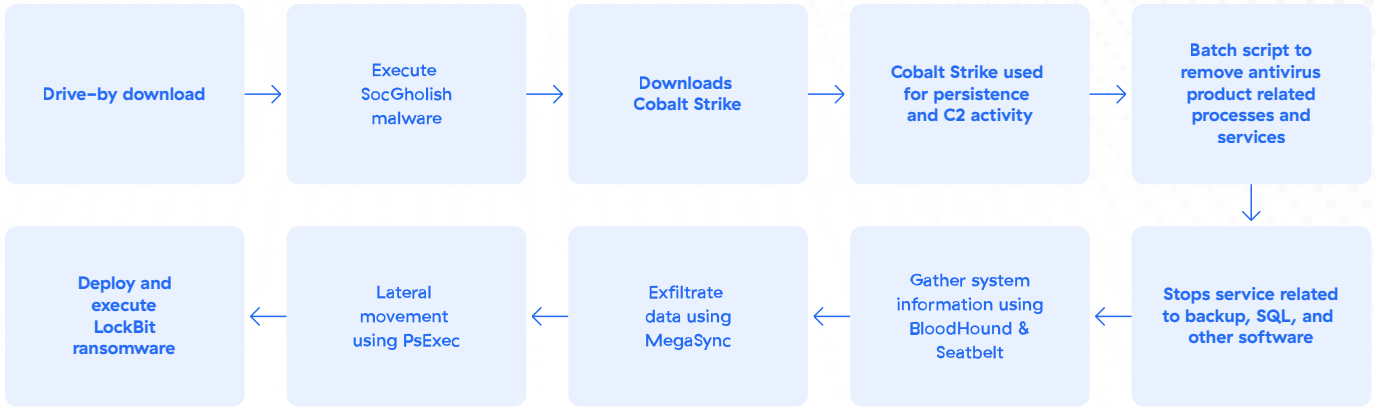


Figure 14: LockBit infection chain, including data exfiltration and file encryption

Figure 14 illustrates the full step-by-step attack sequence this LockBit affiliate followed to carry out the attack.

If the ransom demanded by LockBit is not paid, the group publishes the stolen data. Figure 15 shows a screenshot of the LockBit data leak site. This platform where stolen data is exposed and made publicly accessible serves as a stark reminder of the consequences to organizations that fail to meet LockBit's demands.

LockBit infections by industry

LockBit has consistently targeted various industries, with the manufacturing sector being the primary target over the past year, accounting for approximately 15.35% of LockBit's total attacks. This sector includes a broad range of businesses involved in the production of goods across fields such as automotive, electronics, textiles, and more. The focus on this industry suggests that LockBit aims to exploit vulnerabilities in critical supply chains, disrupt operations, and potentially gain access to valuable intellectual property.

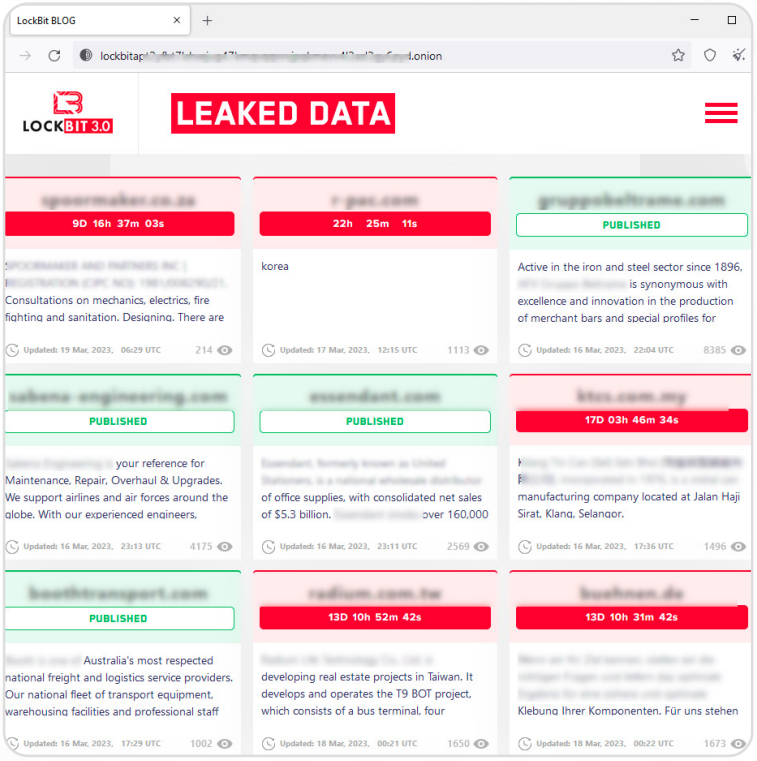


Figure 15: A screenshot of the LockBit 3.0 data leak site

Significant attacks by LockBit on the services industry accounted for approximately 12.71% of the attacks. This industry encompasses a wide array of professional, technical, and support service providers, making it an attractive target for LockBit to exploit sensitive client data, financial information, and intellectual property.

LockBit also directed approximately 7.43% of its attacks at the construction sector, which includes construction companies, contractors, and related businesses involved in building infrastructure and structures. Targeting of this industry suggests LockBit may aim to disrupt ongoing projects, compromise project plans, or gain access to valuable project data.

Additionally, the retail and wholesale sector faced a substantial 6.77% of LockBit's attacks. This sector encompasses businesses involved in the sale of goods to consumers or through wholesale distribution. LockBit's targeting of this sector may stem from a desire to compromise customer data, financial information, or disrupt business operations.

Figure 16 shows the industries most affected by LockBit as a percentage of total attacks. Organizations in these industries should prioritize cybersecurity, implement robust security measures, and educate their employees about potential threats to mitigate the risks posed by LockBit and other ransomware groups.

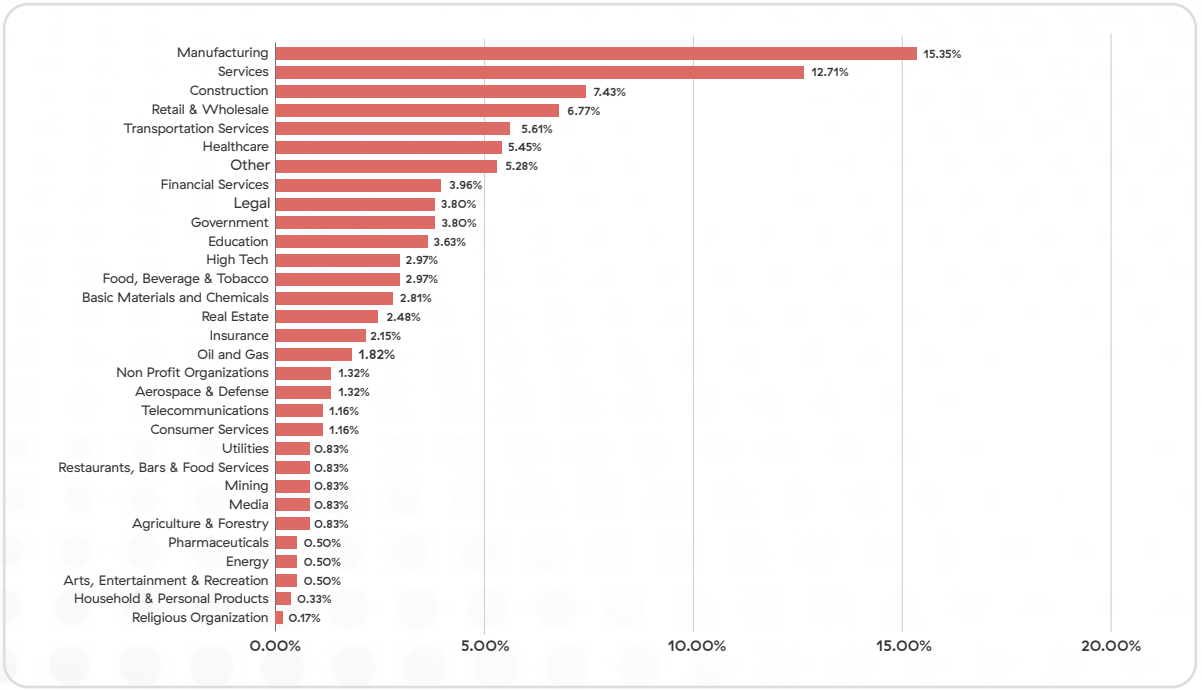


Figure 16: Industry verticals targeted by double extortion attacks using LockBit

LockBit infections by country

While LockBit has left a significant impact on organizations around the globe, those in the US were most affected, with approximately 28.9% of LockBit victim organizations located in the US. This underscores the group's concerted efforts to exploit vulnerabilities in American systems and networks.

France emerged as the second-most impacted country, home to approximately 8.1% of LockBit victim organizations. This demonstrates the LockBit group's intention to target organizations in this European nation, potentially aiming to gain access to valuable data or disrupt critical sectors.

Approximately 4.7% of LockBit victim organizations were located in Canada, while the UK and Germany followed closely, each accounting for 3.9% of affected organizations. This highlights LockBit's global reach and impact as the group infiltrates organizations across different continents.

Figure 17 shows the countries most affected by LockBit as a percentage of total attacks, showcasing the wide-ranging consequences of this ransomware group's activities. These statistics emphasize the urgent need for robust cybersecurity measures and proactive defense strategies in heavily targeted countries. Organizations and governments must prioritize cybersecurity efforts to effectively combat the threats posed by these malicious actors as well as protect critical infrastructure and sensitive data.

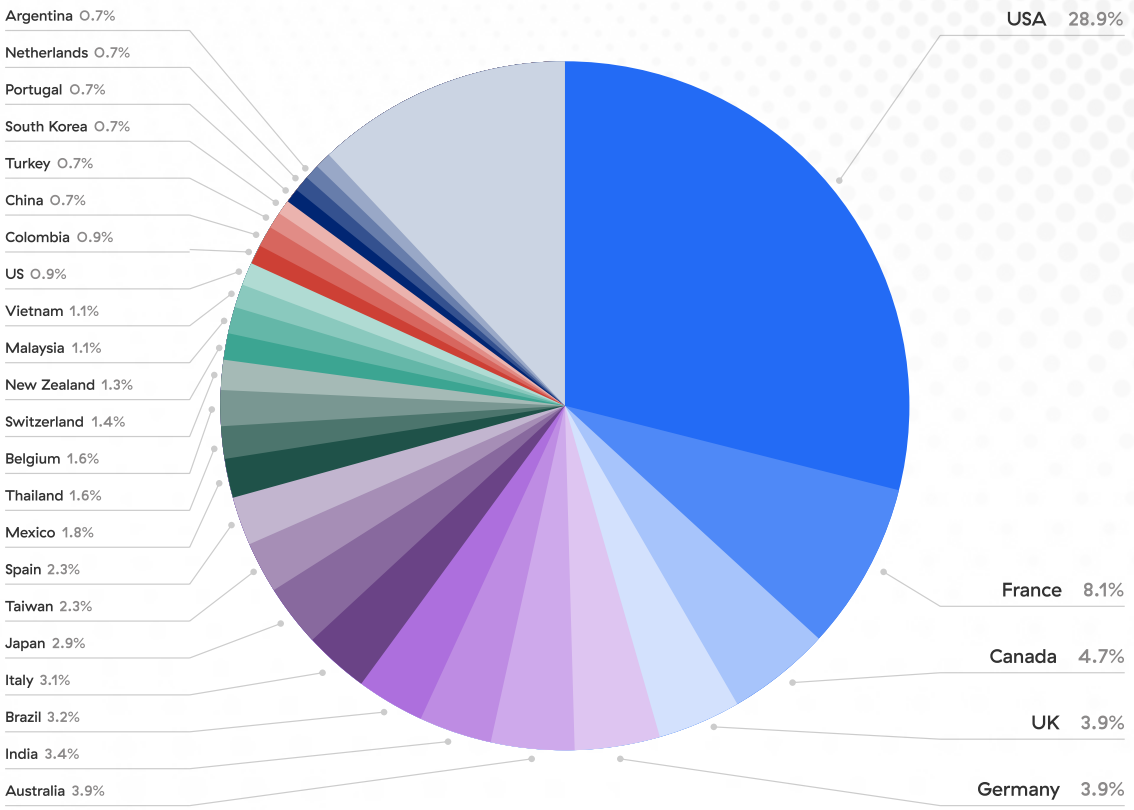


Figure 17: Countries targeted by double extortion attacks using LockBit

#2 BlackCat/ALPHV ransomware

The BlackCat group is a sophisticated RaaS operation, active since November 2021, known for using a variety of methods to infiltrate victim networks, including exploiting known vulnerabilities, phishing attacks, and social engineering. Once inside a network, BlackCat operators typically use a combination of tools and techniques to move laterally, escalate privileges, and exfiltrate data. The group then deploys its ransomware payload, which encrypts the victim's files.

BlackCat is implemented in the Rust programming language, which is efficient for file encryption and cross-platform compatibility. Files are encrypted using a per-file AES key encrypted using a per-victim RSA public key. Because BlackCat leverages an affiliate network to conduct breaches, exfiltrate data, and deploy the ransomware, the flow of attacks varies widely between affiliates. When victims pay a ransom for file decryption, they receive BlackCat decryption tools for 11 different platforms, as shown in figure 18.

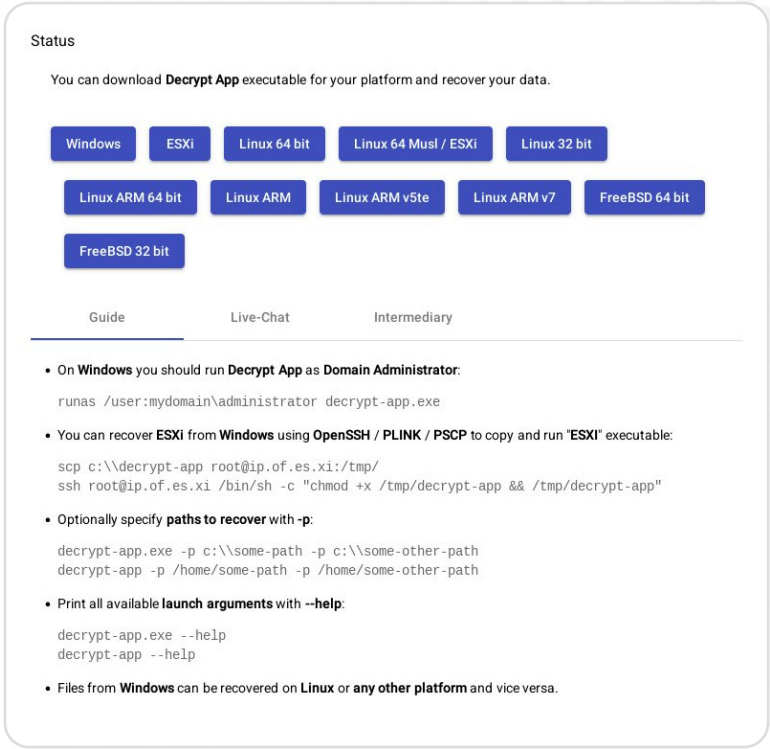


Figure 18: BlackCat/ALPHV decryption tools spanning 11 different platforms

BlackCat/ALPHV infection chain

The following example demonstrates an attack carried out by a BlackCat affiliate. The initial attack took advantage of vulnerabilities in Microsoft Exchange, namely CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065, which enabled the execution of remote code on the targeted server.

In the sample analyzed for this use case, the BlackCat affiliate exploited four vulnerabilities in Microsoft Exchange to gain initial access to the victim's network. Once inside, the attackers used a variety of tools and techniques to gather information about the victim's environment, including cmd.exe, net.exe, ADRecon, and AdFind. The attackers then extracted credentials from the

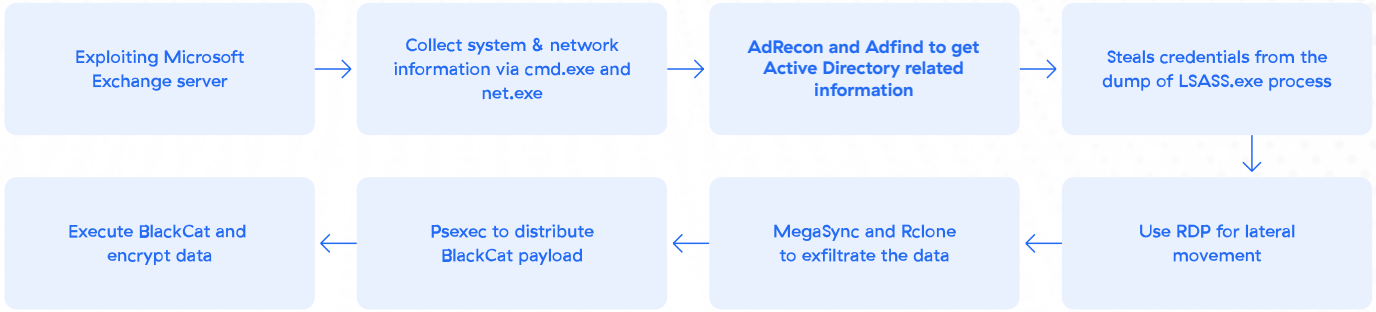


Figure 19: BlackCat/ALPHV infection chain

lsass.exe process, which allowed them to move laterally using RDP. Once they had access to the victim's critical systems, the attackers used MegaSync and Rclone to exfiltrate data. Finally, the attackers used PsExec to remotely execute the BlackCat ransomware payload, which encrypted the victim's data. This process is illustrated in figure 19.

In addition to the steps shown in figure 19, BlackCat affiliates have been observed to include multi-extortion tactics, including distributed denial-of-service (DDoS) attacks. These tactics involve launching attacks on either the victim's website or network to pressure them into negotiating with the operators and compelling them to pay higher ransom amounts. In cases where a victim refuses to comply with the ransom demands and associated threats, BlackCat posts data stolen during the breach on its data leak site, as depicted in figure 20.

This attack demonstrates the sophistication and creativity of the BlackCat ransomware group, which constantly evolves its tactics and techniques to evade detection and maximize profits.

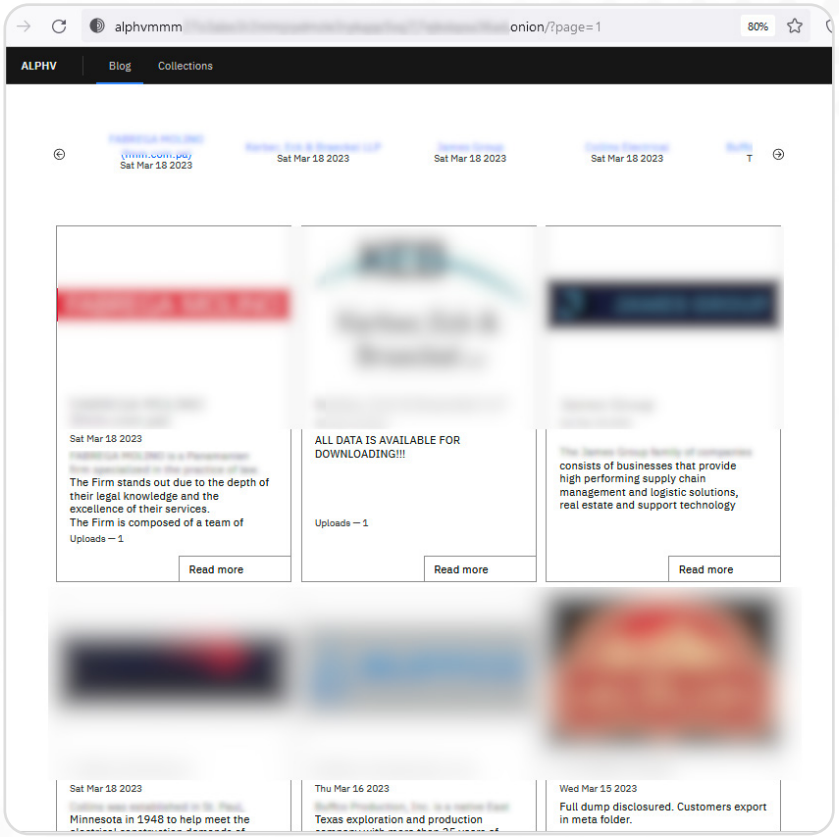


Figure 20: A screenshot of the BlackCat/ALPHV data leak site featuring non-paying victims' data

BlackCat/ALPHV infections by industry

Over the past year, BlackCat has focused its attacks on various industries, primarily the services industry, accounting for approximately 13.78% of the group's total attacks. This sector encompasses a wide range of businesses involved in providing professional, technical, and support services.

BlackCat also directed a significant portion—approximately 12.99%—of its attacks toward the manufacturing sector. This industry includes companies engaged in the production of goods, spanning diverse sectors such as automotive, electronics, textiles, and more.

The legal industry, comprising law firms and legal services providers, was also a notable target for BlackCat, accounting for approximately 8.27% of the attacks. The attackers likely saw value in compromising sensitive legal information, client data, or intellectual property associated with law firms and their clients.

Furthermore, BlackCat showed considerable interest in targeting the financial services sector, which accounted for approximately 5.51% of the attacks. This sector encompasses banks, financial institutions, insurance companies, and other entities involved in financial transactions and services. The attackers may have sought to gain access to valuable financial data and personal information or discover other exploitable vulnerabilities in banking systems to use for scams and other forms of attack.

Figure 21 highlights the varying degrees of attention BlackCat has given to different industries. It is important for organizations operating in these sectors to be aware of the heightened risk and take appropriate measures to enhance their cybersecurity posture.

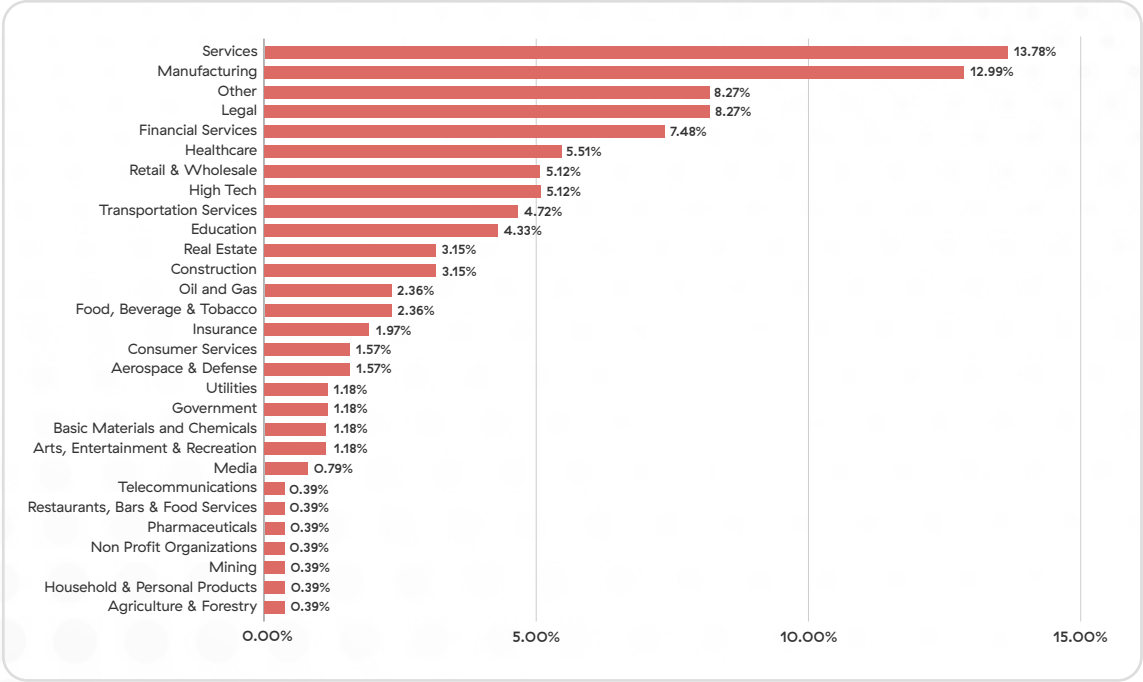


Figure 21: Industry verticals targeted by double extortion attacks using BlackCat

BlackCat/ALPHV infections by country

The BlackCat ransomware group has had a significant impact on organizations worldwide, with the US being the most heavily targeted country. Approximately 32.8% of infected organizations fell victim to BlackCat attacks within the US, reflecting the group's focus on exploiting vulnerabilities within American systems and networks.

Canada also felt a significant impact as home to approximately 8% of infected organizations targeted by BlackCat. The UK also faced considerable attacks, accounting for approximately 6% of the affected organizations. These numbers highlight the global reach of the BlackCat group and its ability to breach security measures in multiple regions.

Australia ranked next among the most affected countries, with approximately 5.2% of BlackCat attack victims. The group's targeting of Australia indicates their intent to exploit vulnerabilities within organizations across different continents.

Germany, with approximately 4.8% of affected organizations, rounds out the list of the countries most impacted by BlackCat. This demonstrates the group's proficiency in infiltrating and compromising systems within highly developed and technologically advanced nations.

Figure 22 shows the countries most affected by BlackCat as a percentage of total attacks, showcasing the significant impact the group had on organizations globally. These statistics emphasize the need for robust cybersecurity measures and heightened vigilance in countries heavily targeted by BlackCat as well as the need for organizations and governments in these regions to prioritize zero trust defense strategies that can stand up to the advanced tactics used by this group.

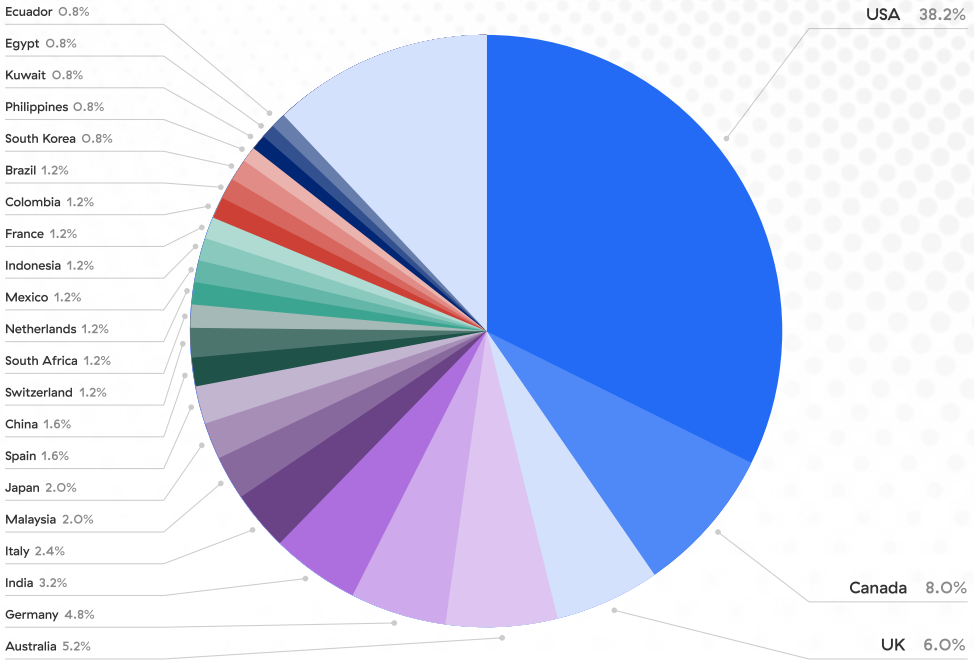


Figure 22: Countries targeted by double extortion attacks using BlackCat BlackCatpaying victims' data

#3 Clop ransomware

Clop, first spotted in February 2019, started using double extortion tactics in March 2020. The Clop group focuses its efforts mostly on large organizations and is known to demand more than US$10 million from large organizations.

ThreatLabz has observed Clop attacks leveraging spam as well as exploiting the SolarWinds Serv-U CVE-2021-35211 vulnerability, which enables remote code execution with elevated privileges for initial access. Members of the Clop group have also exploited vulnerabilities in the Accellion File Transfer Appliance (FTA) tracked as CVE-2021-27101, CVE-2021- 27102, CVE-2021-27103, and CVE-2021-27104. In an

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

Figure 23: Clop data leak post related to the MOVEit Transfer application attack

attack last year, the group exploited the CVE-2022-31199 vulnerability in Netwrix Auditor to infiltrate a victim's network.

In early June 2023, the Clop group exploited CVE-2023-34362, a zero-day vulnerability in the MOVEit Transfer application. Shortly thereafter, Clop posted a message on its data leak site (see figure 23) encouraging victims to contact them to start ransom negotiations.

Clop infection chain

The following is a detailed example of an attack conducted by Clop. The threat actor compromised the victim network by exploiting the CVE-2022-31199 vulnerability in Netwrix Auditor, and then dropped TrueBot malware, which downloaded Cobalt Strike and Grace malware. The attacker used Cobalt Strike for command-and-control communication to establish a foothold in the network, and then used the nltest and sqlcmd tools to collect network information, the ADRecon tool to enumerate hosts from Active Directory, and RDP for lateral movement. The Teleport tool was used for data exfiltration. Finally, the group deployed and executed the Clop ransomware payload to encrypt the victim organization's files. This attack chain is shown in figure 24.

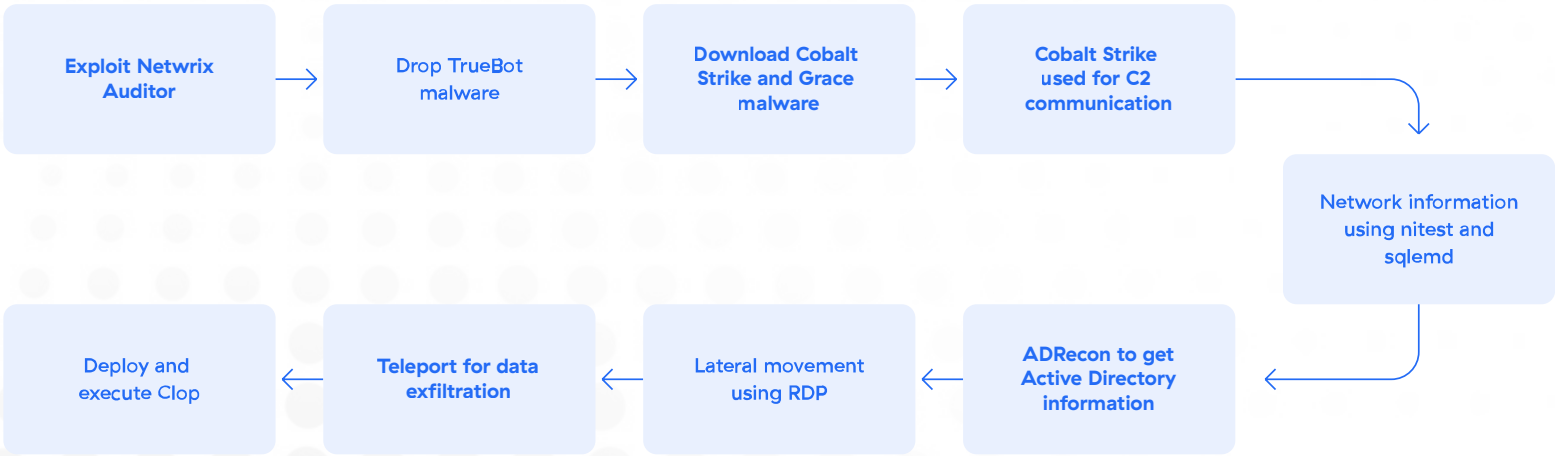


Figure 24: Clop attack chain

If a victim refuses to comply with Clop's ransom demands, the attackers publish the stolen data on their designated leak site. This serves as a potent deterrent and powerful means of coercing organizations into meeting the ransom demands Clop sets forth.

Figure 25 shows Clop's leak site. Public disclosure of sensitive data poses significant risks to a victim organization, including reputational damage and loss of customer trust, potential legal implications, and possible fines from regulatory administrations.

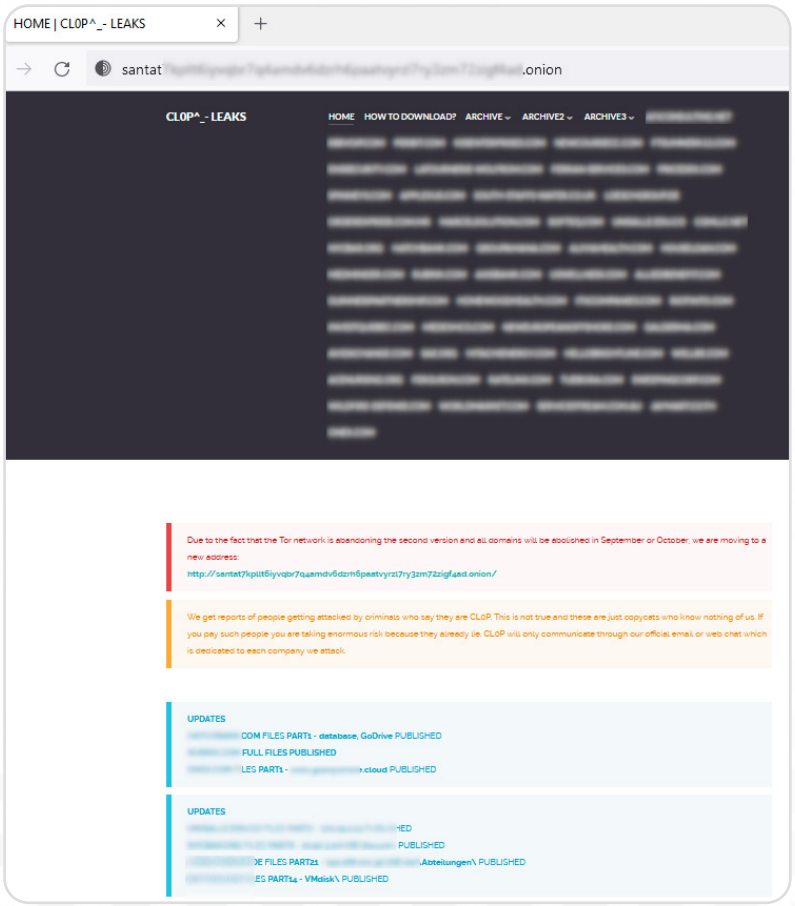


Figure 25: A screenshot of the Clop data leak site

By exposing the stolen data on their leak site, Clop aims to increase the pressure on victims to submit to their demands. This tactic underscores the importance of robust cybersecurity measures and proactive defense strategies to prevent falling victim to ransomware attacks and the subsequent exposure of sensitive information.

Clop infections by industry

In the past year, the technology industry has emerged as the primary focus of ransomware attacks orchestrated by the Clop group. Accounting for a significant portion of their total attacks, technology stood at the forefront, representing approximately 12% of all targeted sectors.

Following closely behind the technology sector, services encountered a considerable share of Clop's attention, accounting for approximately 11.20% of the group's total attacks. This demonstrates that Clop's reach extends beyond just one industry, highlighting their ability to target a wide range of sectors.

The healthcare industry also found itself in the crosshairs of Clop's attacks, accounting for about 10.40% of the total. This sector, known for handling sensitive patient information and critical infrastructure, became a prime target due to its vulnerability to ransomware attacks.

In addition to technology, services, and healthcare, the manufacturing industry faced its fair share of assaults by Clop, representing approximately 8.0% of their targeted attacks. This signifies that Clop's malicious operations spread across sectors, leaving no industry untouched.

Figure 26 showcases the distribution of Clop's attacks across various industries, emphasizing the need for robust cybersecurity measures

among these sectors to mitigate the risks posed by cybercriminal groups like Clop.

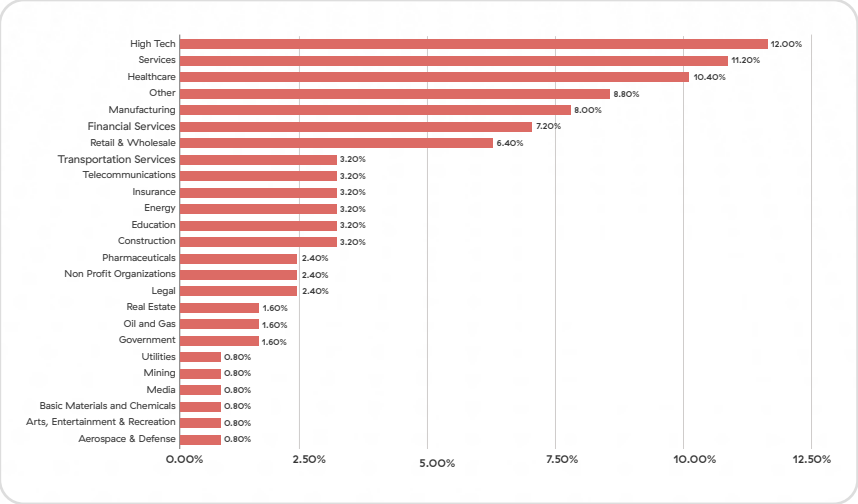


Figure 26: Industry verticals targeted by double extortion attacks using Clop

Clop infections by country

The US emerged as the hardest-hit country in attacks orchestrated by the Clop group, with nearly half of the breached organizations—48.4%—based in the US. This highlights the scale and severity of the cyberthreat faced by US businesses and institutions.

Following closely behind the US, Germany endured a significant share of Clop's attacks, with approximately 7.0% of the total. The UK and Canada shared a similar level of impact, each experiencing 6.3% of Clop's attacks. Australia also faced a substantial threat from Clop, with attacks on Australian organizations making up 4.7% of the total.

Figure 27 shows the countries most severely affected by the Clop group, underscoring the global reach of the group's operations and highlighting the imperative for international collaboration and enhanced cybersecurity measures to combat this persistent threat.

The disproportionately high number of breaches in the US suggests that a combination of factors, including its large population of businesses, government entities, and infrastructure, make it an attractive target for cybercriminals. Additionally, the nation's position as a global technology leader and the concentration of valuable data in its borders contribute to its vulnerability.

These statistics serve as a reminder of the urgent need for organizations and governments worldwide to invest in proactive measures to safeguard their critical systems and sensitive information. The battle against cyberthreats like Clop requires continuous vigilance, collaboration, and the adoption of robust defense strategies.

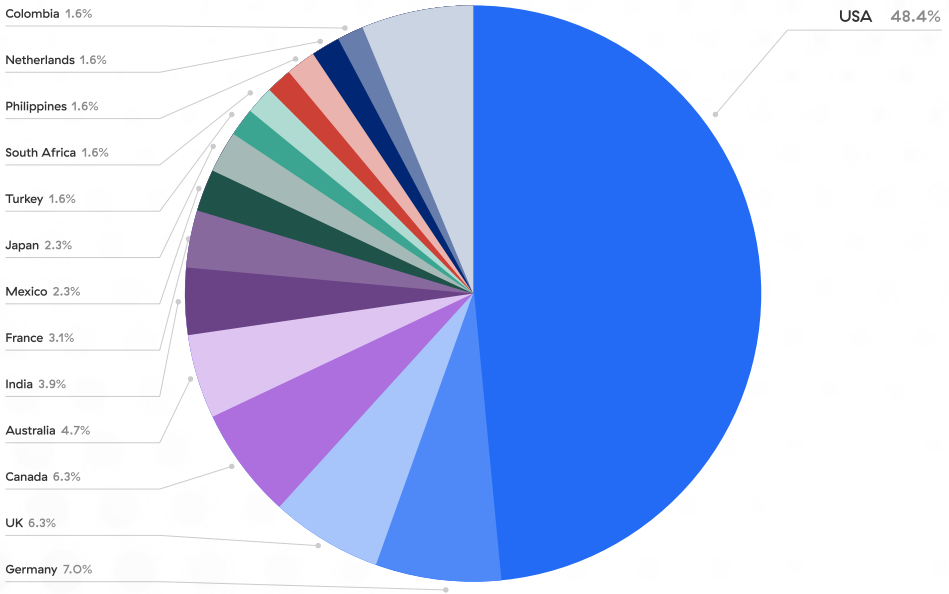


Figure 27: Countries targeted by double extortion attacks using Clop

#4 BlackBasta ransomware

First identified in April 2022, BlackBasta is likely a successor to the Conti ransomware and has since been one of the most active ransomware groups. BlackBasta affiliates use multiple mechanisms to achieve initial access, including malicious spam emails that deliver Qakbot with a campaign tag containing a prefix bb followed by an integer value. Recently, ThreatLabz observed a new backdoor known as Pikabot that used distribution methods similar to those of Qakbot. Interestingly, these Pikabot samples also contained bb campaign tags, indicating that they may have ultimately led to a BlackBasta ransomware attack.

BlackBasta infection chain

The following example of a BlackBasta affiliate's attack demonstrates the group's sophisticated tactics. The attack began with the assailant sending a spam email designed to trick the recipient into opening an attached Microsoft Excel (XLS) file and executing a malicious macro. Upon execution, the macro code initiated the download of the Qakbot trojan, which served as the initial payload. Once inside the compromised system, Qakbot facilitated the delivery of a Cobalt Strike beacon, establishing a persistent presence in the network.

To further exploit the compromised environment, the attacker utilized the powerful Mimikatz tool to extract credentials from the system. With these credentials in hand, the attacker employed the PsExec tool for lateral movement, enabling them to traverse the network and gain access to additional systems.

To evade detection and hinder defensive measures, the attacker leveraged PowerShell commands to disable anti-malware applications, making it more challenging for security software to detect and mitigate the ongoing threat. Moreover, the attacker employed Group Policy Objects (GPOs) to disable Windows Defender and Windows Security Center, further compromising the system's security posture.

Having established a firm foothold and compromised multiple systems, the attacker proceeded to exfiltrate critical data using the versatile Rclone tool. This stage involved the extraction and transfer of sensitive information from the compromised network to an external location under the attacker's control.

Lastly, in the final stage of the attack chain, the attacker deployed BlackBasta ransomware to encrypt files on the compromised

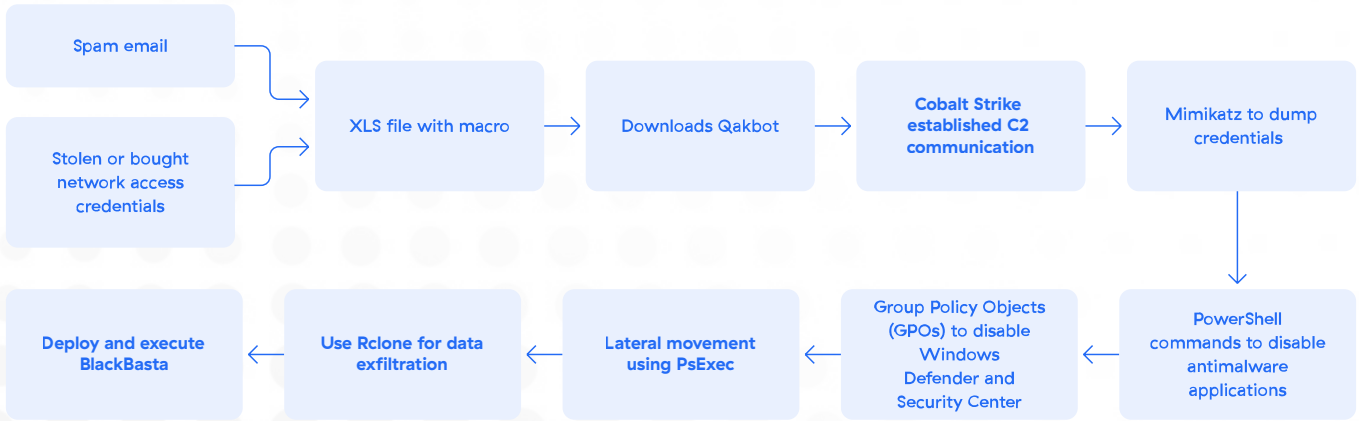


Figure 28: BlackBasta infection chain

systems, rendering them inaccessible and unusable to the victim.

Figure 28 depicts the intricacies of this attack chain's various stages and techniques.

If the demanded ransom goes unpaid, BlackBasta escalates to publicly disclosing the stolen data on their leak site, as depicted in figure 29. This tactic aims to compel impacted organizations to comply with extortion demands lest they suffer reputational damage, financial repercussions, and potential legal consequences.

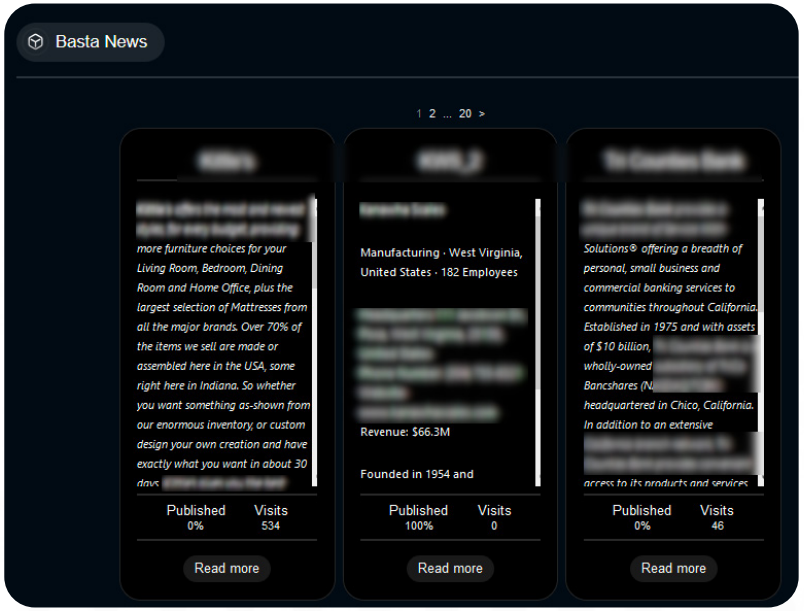


Figure 29: Screenshot of the BlackBasta data leak site

BlackBasta infections by industry

BlackBasta primarily focused its attacks on the manufacturing industry, which accounted for a significant 26.06% of their total attacks. The services industry was targeted the second most, facing 13.33% of the group's attacks. The construction sector also saw notable attention from BlackBasta, suffering 9.09% of the total attacks. Transportation services were the targets of a lesser, but still significant 5.45% of the attacks. Figure 30 shows an overview of BlackBasta's targeting preferences across various industries.

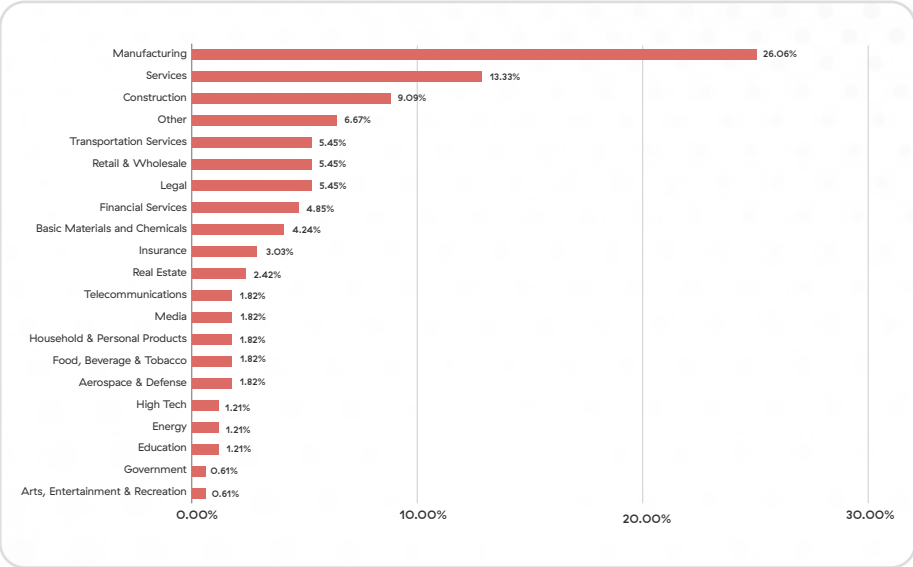


Figure 30: Industry verticals targeted by BlackBasta

BlackBasta infections by country

The US bore the brunt of BlackBasta's attacks, with 56.6% of total attacks targeting US organizations. Germany stood at a distant second with 13.3%, while Canada endured a substantial 9.2% of the total attacks. The UK and Switzerland each experienced a noticeable impact with 3.1% of the attacks. Figure 31 depicts the countries most affected by BlackBasta attacks, illustrating the severity of the situation in different parts of the world.

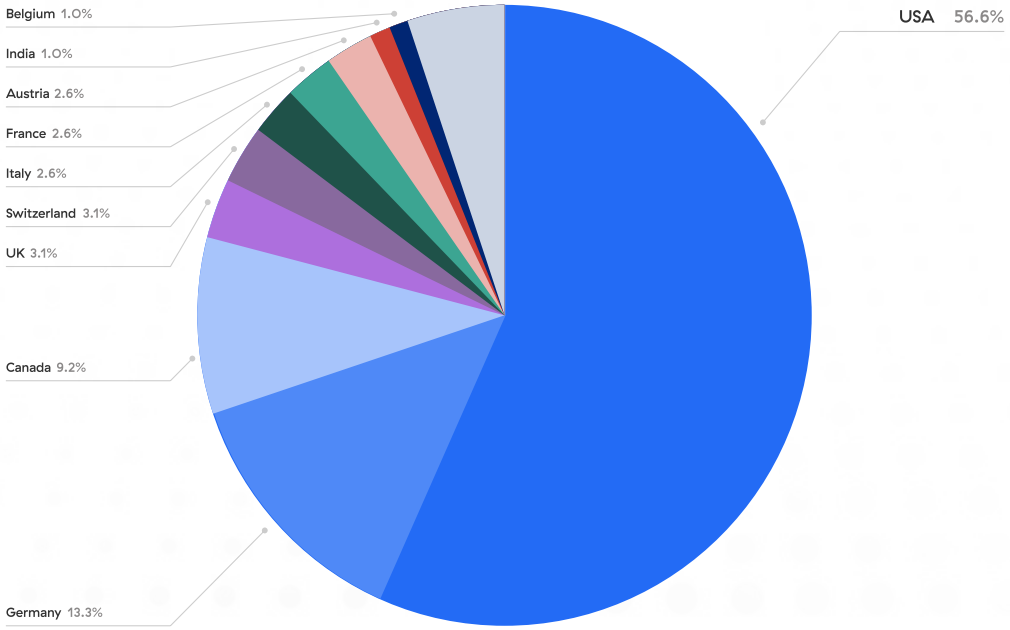


Figure 31: Countries targeted by double extortion attacks using BlackBasta

#5 Karakurt extortion group

The Karakurt extortion group has observably close ties with both the former Conti ransomware group and Diavol. In June 2021, Karakurt introduced a data leak site, marking the inception of their operations. The first observed attack by this group was initiated in September 2021, with the leakage of victim data starting in November of the same year.

Karakurt's distinctive encryptionless ransom attacks set the group apart. Unlike traditional ransomware attacks that encrypt files and demand payment for decryption, Karakurt adopts a different approach: instead of encrypting data, they extract sensitive information from their victims and use it as leverage for extortion. Following their attack, Karakurt delivers a ransom note via email to the victim organization's employees, providing essential details on how to contact the attackers and initiate ransom negotiations.

To amplify the pressure on the victim, Karakurt also reaches out to the victim's business partners and clients with emails and phone calls, sharing information about the attack and divulging specific details about the compromised data, coercing the external parties to advocate for negotiation and a ransom payout. By leveraging external pressure and potential reputational damage, Karakurt seeks to maximize their chances of receiving a substantial payment.

The Karakurt group's tactics demonstrate the ongoing evolution of cybercriminal operations, emphasizing the need for organizations to bolster their cyber defenses, implement robust incident response plans, and educate employees on best practices to mitigate the risks these types of extortion–based attacks pose.

Karakurt infection chain

This example attack orchestrated by Karakurt involves a series of malicious actions carried out to compromise a targeted network. The initial breach uses stolen credentials, specifically exploiting vulnerabilities in Remote desktop protocol (RDP) or Virtual private network (VPN) services. Karakurt uses the stolen credentials to gain unauthorized access to the victim's network, setting the stage for further infiltration.

To establish a persistent presence in the victim's network and exert control over its systems, Karakurt employs a tool called Cobalt Strike. This sophisticated tool serves as a versatile platform for executing various post-exploitation activities, including lateral movement and command execution, making it a favored choice for advanced threat actors.

In some instances, Karakurt also employs the remote desktop software AnyDesk to gain remote access to systems within the victim's network. This allows the threat actor to extend control and maneuver within the compromised environment, potentially targeting additional systems or extracting sensitive information.

To facilitate network reconnaissance and identification of potential targets, Karakurt employs Angry IP Scanner. This tool enables them to scan the network, identify vulnerable hosts, and gather information on potential entry points for further exploitation.

Once inside the network, Karakurt utilizes a powerful credential-dumping tool called Mimikatz to extract and harvest credentials stored in the victim's systems, including passwords and authentication tokens. Armed with these stolen credentials, Karakurt can escalate privileges and move laterally across the network, expanding their control and compromising additional systems.

For lateral movement and exploration of a victim's network, Karakurt often relies on a combination of Cobalt Strike and RDP. These tools enable them to traverse the network, moving between systems and compromising new targets, expanding their reach and control.

For exfiltrating sensitive data from the compromised network, Karakurt employs file transfer tools such as Rclone and FileZilla, which enable the threat actor to discreetly transfer stolen data from the victim's systems to external servers under their control, further enabling their malicious activities.

Figure 32 shows an example Karakurt attack chain, showcasing the various stages and tools involved in their sophisticated intrusion techniques.

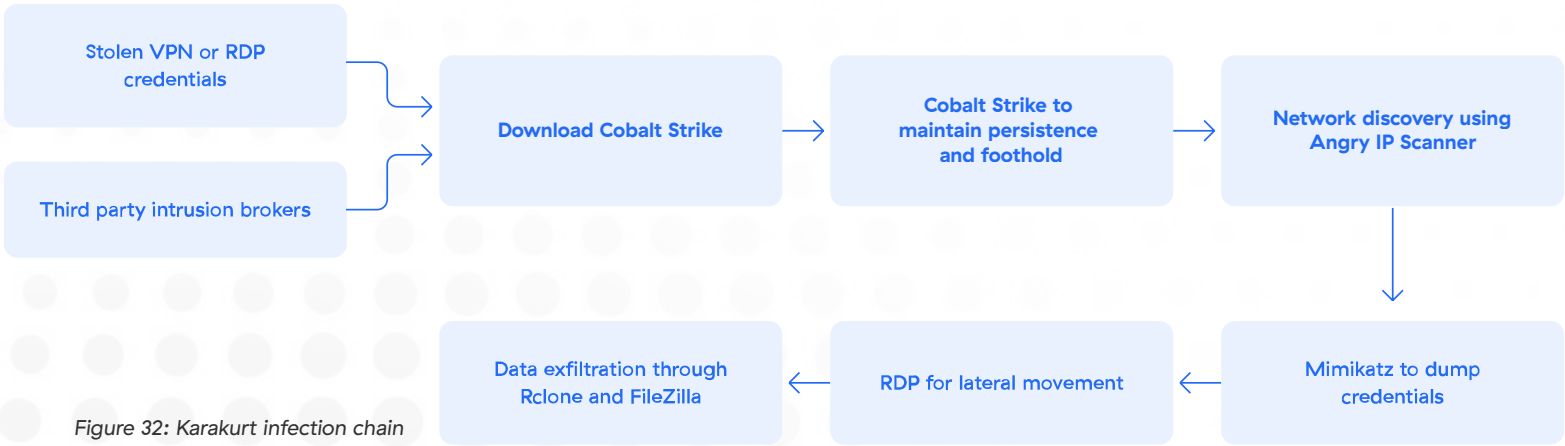


Figure 32: Karakurt infection chain

Figure 33: A screenshot of the web page advertising data leak auctions by Karakurt group

If a victim refuses to comply with Karakurt's ransom demands, the group publicly discloses the stolen data on its designated leak site (see figure 33). This poses immense risks for victim organizations, including reputational damage, possible regulatory fines, and legal ramifications.

By making the stolen data available on their leak site, Karakurt aims to magnify the consequences for victims who refuse to comply. The threat of public exposure pushes organizations to reconsider their stance and ultimately succumb to the ransom demands in an attempt to protect their reputation and prevent further damage.

To intensify the pressure further: the Karakurt group threatens to both publish and auction off the leaked data, if necessary. In their relentless pursuit of financial gain, Karakurt uses a separate auction site (see figure 34) dedicated to selling the stolen data.

The promise of publishing leaked data if ransoms are unpaid threatens reputational harm on victim organizations. In parallel, the auction site is a means to monetize the stolen data, providing an alternative avenue for Karakurt to profit from their criminal activities. By offering the compromised information to the highest

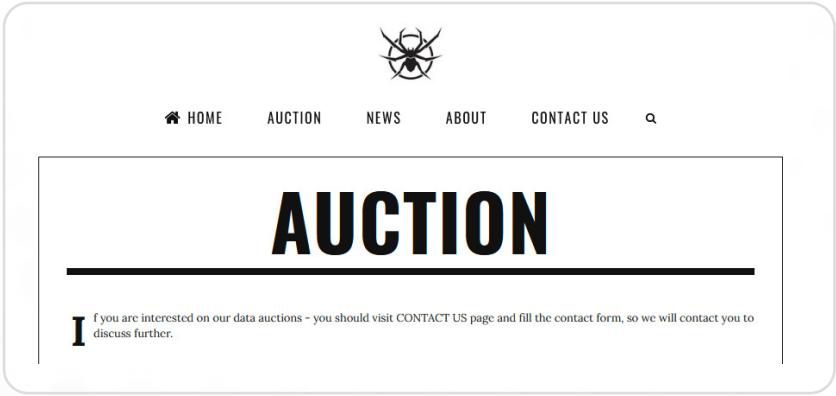


Figure 34: A screenshot of the Karakurt data auction site

bidder, they exploit the value certain entities may place on obtaining such data, whether for illicit purposes or competitive advantage.

The use of a dedicated auction site demonstrates the sophistication and adaptability of the Karakurt group. It underscores their intention to extract maximum financial gain from their victims, leveraging the stolen data as a valuable commodity in the underground market.

This dual threat underscores the critical need for prompt, decisive action by organizations at risk.

Karakurt infections by industry

Karakurt has demonstrated a notable focus on specific industries, especially the healthcare sector, which was the target of approximately 19.61% of all Karakurt incidents. This sector manages valuable patient data, making it an attractive target for cybercriminals seeking to exploit sensitive information for profit through encryptionless attacks and escalation auctions to other criminal enterprises on the dark web.

Following closely behind healthcare, the services industry faced around 17.65% of the total attacks. Encompassing a wide range of organizations in finance, hospitality, and professional services, this sector became a prime target due to its diverse customer base, interconnected networks, and access to valuable personal and business information.

The manufacturing and education industries were subject to considerable attacks, each accounting for approximately 7.84% of Karakurt incidents. Manufacturing organizations, known for their reliance on critical infrastructure and intellectual property, were enticing targets for extortion. Similarly, educational institutions, which house extensive student and faculty data, were not spared from the threat actor's focus.

Figure 35 shows the distribution of Karakurt's attacks across industries, underscoring the need for organizations in the healthcare, services, manufacturing, and education sectors, in particular, to prioritize cybersecurity and adopt robust defense strategies to safeguard their systems, protect sensitive information, and mitigate the risks posed by Karakurt and similar threat actors.

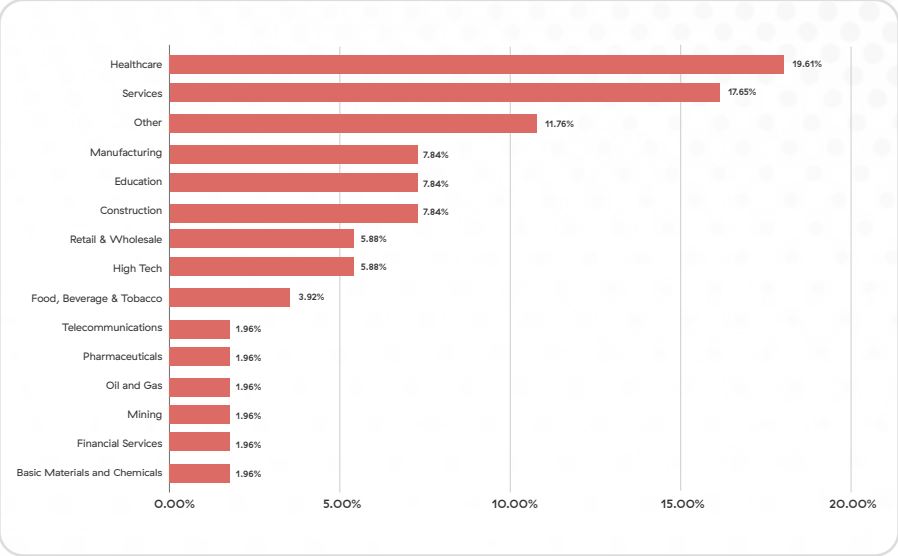


Figure 35: Industry verticals targeted by Karakurt

Karakurt infections by country

Karakurt has left a significant impact on organizations across different countries. The US emerged as most affected, with approximately 50% of Karakurt victim organizations in its borders. This statistic highlights the continued vulnerability and attractiveness of American entities as prime targets for threat actors malicious activities.

Trailing the US, Canadian organizations accounted for approximately 15.5% of the victims. The UK, known for its robust business and technological infrastructure, faced a significant impact as well, with around 8.6% of Karakurt's victim organizations based there.

Turkey and Germany were also substantial targets, home to approximately 5.2% and 3.4% of Karakurt's victims, respectively. This demonstrates the Karakurt group's wide reach, transcending international boundaries to exploit vulnerabilities in organizations worldwide.

Figure 36 depicts the distribution of Karakurt's attacks by country. The prevalence of attacks in these regions underscores the urgent need for enhanced cybersecurity measures, information sharing, and international collaboration to mitigate the risks posed by Karakurt and similar threat actors.

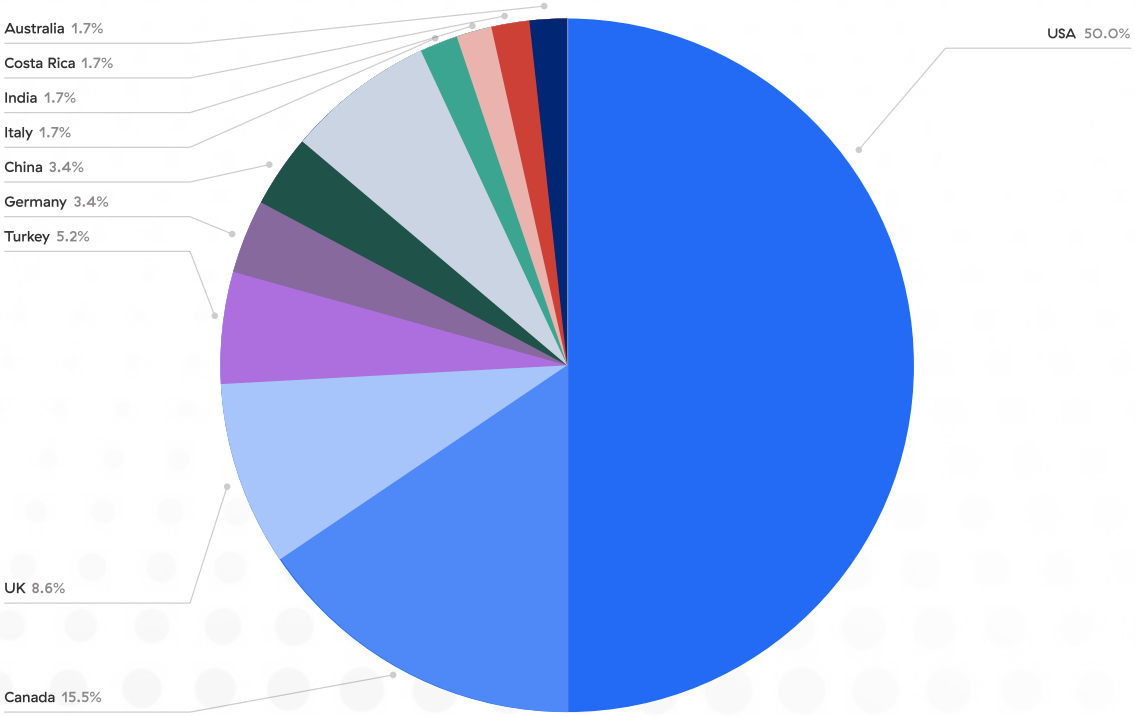


Figure 36: Countries targeted by encryptionless ransom attacks by Karakurt

Conclusion

In light of escalating ransomware threats, it is crucial for organizations to prioritize robust cybersecurity strategies and maintain constant vigilance.

Zscaler, a leading provider of zero trust defense solutions, offers a comprehensive suite of measures designed to effectively combat these evolving risks through cutting-edge technologies, such as behavioral analysis, machine learning, and AI, to identify and mitigate threats before they can inflict any harm.

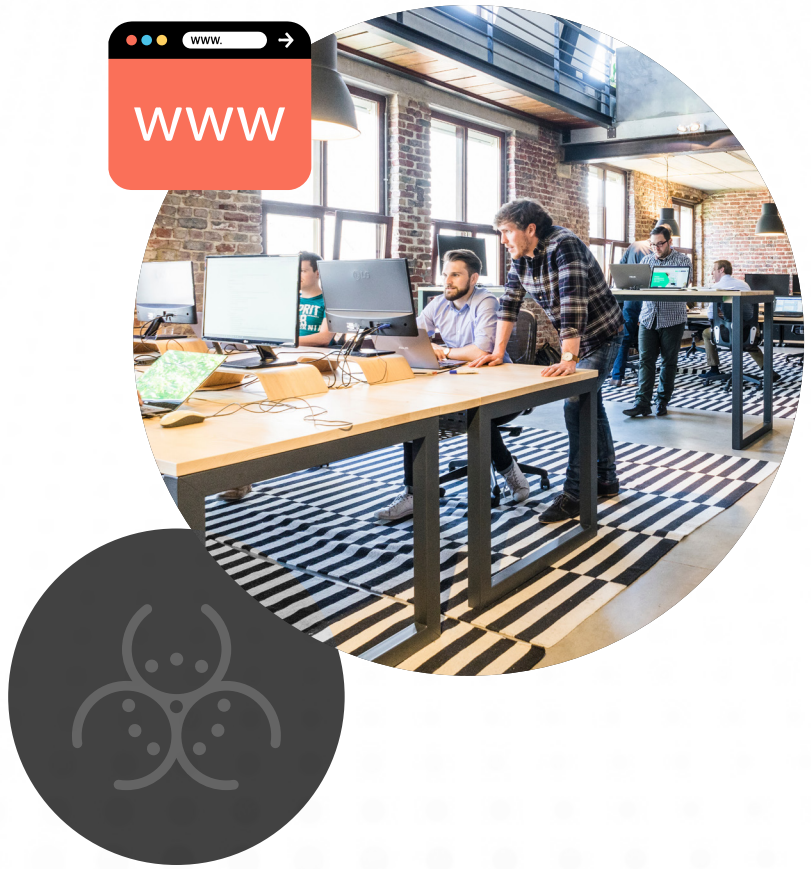
- **Network segmentation** is a fundamental aspect of zero trust architecture. By segmenting the network into smaller, isolated zones, organizations can minimize the lateral movement of ransomware within their systems. This approach ensures that even if one segment is compromised, the rest of the network remains secure, limiting the potential impact of an attack.
- **Zscaler Posture Control** enables organizations to enforce strict security policies across their network and endpoints. By ensuring that all devices meet predefined security requirements, organizations can significantly reduce the attack surface for ransomware threats. This proactive measure helps prevent unauthorized access and strengthens the overall resilience of the organization's defenses.
- **Network monitoring** plays a critical role in detecting and mitigating ransomware threats. Through TLS/SSL introspection, Zscaler examines encrypted traffic to uncover hidden malicious activities. This comprehensive visibility enables proactive identification of ransomware, helping prevent attacks before they can cause harm.
- **Zscaler Data Loss Prevention (DLP)** adds another dimension to ransomware defense. By monitoring sensitive data and implementing policies to prevent unauthorized access or transmission, Zscaler helps keep critical information out of threat actors' hands. This mitigates the potential impact of ransomware attacks and reduces the likelihood of data exfiltration.
- **Zscaler Sandbox** analyzes suspicious files and executables in a controlled virtual environment, helping to identify and block malicious code before it can infiltrate an organization's network. This proactive approach helps organizations stay ahead of emerging ransomware variants and zero-day attacks.
- **Zscaler Browser Isolation** executes web sessions in isolated containers away from the user devices, preventing malicious code from reaching the endpoint and compromising the system. By rendering web content remotely, Zscaler effectively eliminates the risk of drive-by downloads and zero-day exploits that may be used by ransomware operators. This ensures that employees can safely browse the internet without exposing their devices or networks to ransomware.
- **Zscaler Deception** employs decoy systems, files, and credentials deployed strategically across the network to lure threat actors into setting off alarms. This enables Zscaler to identify and track attackers' behavior, gain insight into their tactics and motives, and gather threat intelligence to help organizations strengthen their defenses, anticipate potential ransomware attacks, and respond effectively to mitigate their impact.

Zscaler emphasizes the importance of regular software updates and patches to address known vulnerabilities. Promptly applying these updates can significantly reduce the risk of exploitation by threat actors, who often target outdated software. The Zscaler platform ensures seamless integration with various applications and systems, allowing organizations to streamline the process of updating their software infrastructure.

In addition to proactive defense measures, Zscaler advocates for the maintenance of secure and up-to-date backups of critical data—a crucial safeguard against some types of ransomware attacks that also helps with recovery from all types of attacks. In the unfortunate event of a successful attack, having reliable offline backups empowers organizations to swiftly restore systems and data rather than relying on the decryption process, which can be lengthy and riddled with issues and software bugs.

Zscaler promotes collaborative information sharing among organizations, security vendors, and law enforcement agencies. Pooling our collective threat intelligence will help us identify emerging ransomware trends, develop effective countermeasures, and orchestrate a coordinated response to ransomware incidents. The Zscaler platform facilitates secure data exchange and collaboration to foster a unified front against ransomware attacks.

Organizations must prioritize robust cybersecurity strategies and remain vigilant in the face of evolving ransomware threats. To effectively combat these risks, adopting a multifaceted zero trust approach, such as Zscaler's, is paramount. By leveraging Zscaler's advanced security solutions, regularly updating software, maintaining secure backups, and fostering collaboration, organizations can bolster their defenses and mitigate the impact of ransomware attacks.



Appendix

Ransomware MITRE ATT&CK Tables

LockBit

Initial Access	Execution	Persistence	Privilege Escalatation	Defense Evasion	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Spear phising link	Command & scripting interpreter	Boot or logon autostart execution	Abuse elevation control mechanism: bypass user account control	Deobfuscate/ decode files or information	System network configuration discovery	Lateral tool transfer	Archive collected data	Application layer protocol: web protocols	Exfiltration over web service	Data encrypted for impact
Spear phising attachment	User execution	—	—	Impair defenses: disable or modify tools	Remote system discovery	Remote services: remote desktop protocol	Data from local system	—	Exfiltration over web service: exfiltration to cloud storage	Inhibit system recovery
Valid accounts	System services	—	—	Indicator removal on host: clear Windows event logs	File and directory discovery	—	—	—	—	—
Exploit public-facing application	—	—	—	Domain policy modification: group policy modification	Security software discovery	—	—	—	—	—
Drive-by compromise	—	—	—	—	Domain trust discovery	—	—	—	—	—

Table 5: LockBit mapping to the MITRE ATT&CK framework

BlackCat/ALPHV

Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Valid accounts	Command & scripting interpreter	Boot or logon autostart execution: registry run keys/ startup folder	Impair defenses: disable or modify tools		System network configuration discovery	Remote services: remote desktop protocol	Archive collected data	Exfiltration over web service: exfiltration to cloud storage	Data encrypted for impact
Exploit public-facing application	User execution	—	Deobfuscate/ decode files or information	OS credential dumping: LSASS memory	Remote system discovery	Lateral tool transfer	Data from local system		Inhibit system recovery
—	—	—	Domain policy modification: group policy modification	—	File and directory discovery	—	—	—	—
—	—	—	—	—	Security software discovery	—	—	—	—

Table 6: BlackCat/ALPHV mapped to the MITRE ATT&CK framework

Clop

Initial Access	Execution	Persistence	Privelege Escalation	Defense Evasion	Discovery	Lateral Movement	Command & Control	Exfiltration	Impact
Valid accounts	Command & scripting interpreter	Boot or logon autostart execution	Access token manipulation	Masquerading: invalid code signature	System network configuration discovery	Remote services: remote desktop protocol	Application layer protocol: web protocols	Exfiltration over C2 channel	Data encrypted for impact
Spear phishing attachment	User execution	—	Bypass user account control	Impair defenses: disable or modify tools	Remote system discovery	Lateral tool transfer	Data from local system	—	Inhibit system recovery
Exploit public-facing application	—	—	Exploitation for privilege escalation	Deobfuscate/ decode files or information	File and directory discovery	—	—	—	—
Supply chain compromise	—	—	—	Process injection: DLL injection	Query registry	—	—	—	—
—	—	—	—	—	Security software discovery	—	—	—	—

Table 7: Clop MITRE ATT&CK table

BlackBasta

Initial Access	Execution	Persistence	Privelege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration	Impact
Valid accounts	Command & scripting interpreter	Boot or logon autostart execution	Exploitation for privilege escalation	Masquerading: invalid code signature	OS credential dumping	System network configuration discovery	Remote services: remote desktop protocol	Exfiltration over web service	Data encrypted for impact
Phishing	User execution	—	—	Impair defenses: disable or modify tools	—	Remote system discovery	Lateral tool transfer	—	Inhibit system recovery
Exploit public-facing application	—	—	—	Deobfuscate/ decode files or information	—	File and directory discovery	—	—	Service stop
—	—	—	—	Process injection: DLL injection	—	Query registry	—	—	—
—	—	—	—	—	—	Security software discovery	—	—	—

Table 8: BlackBasta mapping to the MITRE ATT&CK framework

Karakurt

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
Valid accounts	Command and scripting interpreter	Valid accounts	Valid accounts	Deobfuscate/decode files or information	System network configuration discovery	Remote services: remote desktop protocol	Archive collected data	Application layer protocol: web protocols	Exfiltration over web service
—	System services: service execution	—	—	—	Remote system discovery	—	Data from local system	—	—
—	—	—	—	—	File and directory discovery	—		—	—

Table 9: Karakurt mapped to the MITRE ATT&CK framework

The evolution of ransomware

Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment before they can be decrypted. The first known ransomware attack occurred in 1989, when a biologist named Joseph Popp sent infected floppy disks to attendees of the World Health Organization's international AIDS conference. The disks contained a program that encrypted the victim's files and demanded a ransom of $189 in return for the decryption key.

Ransomware has evolved significantly over the years, becoming one of the most prominent and damaging types of cyberthreats. Here's an overview of the evolution of ransomware:

- **Early history:** An early iteration of ransomware known as "screen lockers" falsely claimed to encrypt files. A significant turning point came with the emergence of the Gameover Zeus botnet, which began deploying a ransomware variant named CryptoLocker to target systems that were not profitable through wire/ACH fraud. This marked a significant shift in the evolution of ransomware as it moved from mere screen-locking tactics to genuine encryption-based attacks.
- **Ransomware worms:** Ransomware started using worm-like capabilities to spread rapidly in networks and across connected systems. This allowed it to propagate autonomously, infecting multiple devices and systems without requiring direct user interaction. Notorious worms like NotPetya and WannaCry have demonstrated the potential for widespread damage and financial losses.
- **Ransomware negotiation and payment process:** To facilitate ransom negotiations and payment, cybercriminals have established professional customer support systems. They often provide decryption tools or unlock codes upon receiving payment. Use of cryptocurrency in payment has made it easier for criminals to maintain their anonymity.
- **Advanced encryption and evasion techniques:** As cybersecurity measures improved, ransomware developers began employing more sophisticated encryption algorithms and techniques to evade detection. This included the use of asymmetric encryption, where separate keys are used for encryption and decryption, making it more challenging to crack the encryption without the private key.
- **Targeted ransomware:** Instead of indiscriminate attacks, cybercriminals started targeting specific organizations, particularly those that controlled valuable data or critical infrastructure. Threat actors conduct extensive reconnaissance to identify vulnerabilities and design tailored attacks.
- **Ransomware as a service (RaaS):** Ransomware evolved into a lucrative business model with the rise of RaaS platforms, which allow cybercriminals to purchase or lease ransomware variants and infrastructure from developers, streamlining the distribution process. This led to a significant increase in the number of attacks as more individuals with limited technical skill could carry out ransomware campaigns.
- **Double extortion:** To increase their chances of receiving payment, cybercriminals began to not only encrypt victims' data, but also exfiltrate sensitive information before the encryption stage. The actors gain leverage to demand higher payouts by threatening to expose or sell the stolen data if the ransom is not paid.
- **Multiple extortion:** In 2020, ransomware attackers began to add more attack layers beyond double extortion to increase business disruption and the pressure on victims. These

tactics range from launching DDoS attacks to contacting key stakeholders, partners, and customers with threatening messages.

- **Targeting critical infrastructure:** Recent years have seen an alarming increase in ransomware attacks targeting critical infrastructure, including healthcare systems, government agencies, and utilities. These attacks have the potential to cause severe disruptions, endanger lives, and result in substantial economic damage. The Colonial Pipeline attack in 2021 is a notable example.
- **Supply chain attacks:** The REvil ransomware incident was a notable supply chain attack in which thousands of downstream customers were compromised through a vulnerability in Kaseya. Attackers focus on exploiting the weakest link in the chain, leveraging their access to data or systems. Some attacks are opportunistic, executed swiftly and targeting valuable assets, as seen with Lapsu$. In other instances, these attacks can evolve into sophisticated, multi-stage ransomware campaigns that may impact the primary target as well as its partners and customers.
- **Encryptionless attacks:** As more organizations have implemented or improved offline backups and data recovery strategies, encryptionless attacks have become more prevalent since they emerged last year. Attackers primarily target industries that handle highly sensitive PII, particularly those with privileged relationships with clients, such as the legal and healthcare sectors. Many victims choose to pay the ransom regardless of encryption, as their main concern is preventing leakage of sensitive data. By avoiding encryption, attackers enable quicker and more efficient data recovery, providing a more favorable experience for the victims seeking to restore their systems and often resulting in a faster payout.

Ransomware is always evolving as cybercriminals continuously adapt and refine their tactics and techniques. To protect against this ever-changing threat, it is crucial for individuals, organizations, and governments to remain vigilant and implement the latest, most robust cybersecurity measures.

Multiple extortion ransomware attack

Today's ransomware attacks typically include these stages:

1. **Initial compromise:** Attackers use a variety of intrusion vectors to gain access to systems, including phishing emails, exploiting vulnerabilities in remote administrator or VPN tools, and using brute force or stolen credentials to access RDP connections. Supply chain attacks are yet another method to infiltrate an organization.
2. **Lateral movement:** After gaining initial access, threat actors gather infrastructure information and move laterally across network systems, escalating privileges and establishing persistence mechanisms as needed, cataloging key data to steal or encrypt, and depositing ransomware payloads for later execution.
3. **Data exfiltration:** In the case of a double extortion attack, attackers steal sensitive data to use as a secondary extortion tactic. This lets them demand higher ransoms by reducing victims' leverage: even if they can recover the encrypted data from backups, they still must face the threat of the cybercriminals leaking the stolen data.
4. **Ransomware execution:** Attackers deploy and execute the ransomware, encrypting targeted files on systems connected to the network. Ransomware typically terminates processes related to security software and databases to maximize the number of files it can encrypt. Shadow copy backups are also usually deleted from the system to hinder file recovery. Some ransomware families also reboot compromised systems in Safe Mode to bypass security endpoint software prior to file encryption. After file encryption, victims receive instructions for paying the ransom and decrypting their files.
5. **Negotiation:** If the victim does not negotiate, some hacking groups will wage a DDoS attack against the victim's network or website, disrupting their business operations to gain additional leverage.

Figure 37 shows the typical attack chain of a multi-extortion ransomware attack.

Multiple extortion ransomware attack sequence

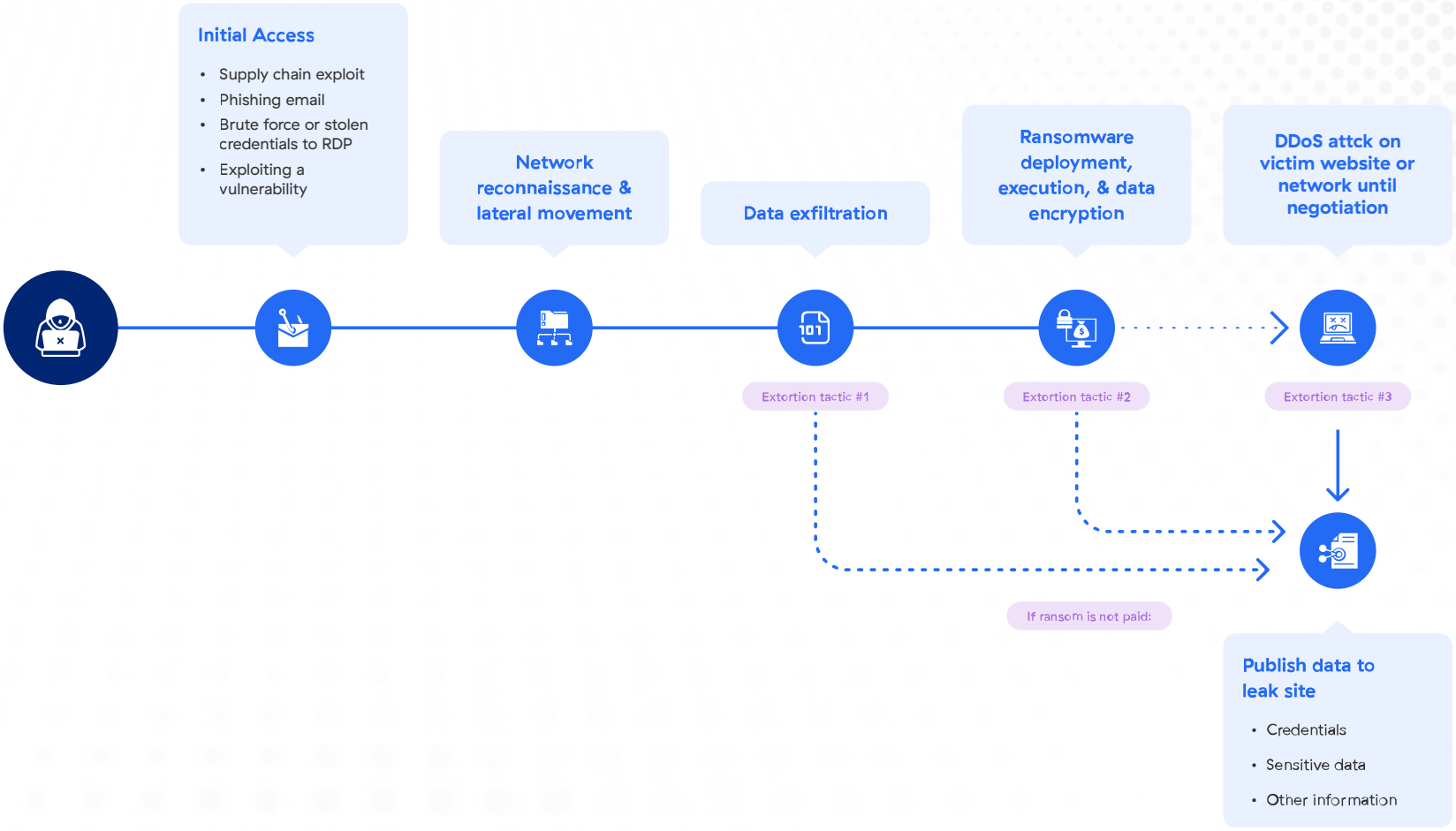


Figure 37: Infection chain of a ransomware attack

Encryptionless extortion group attack sequence

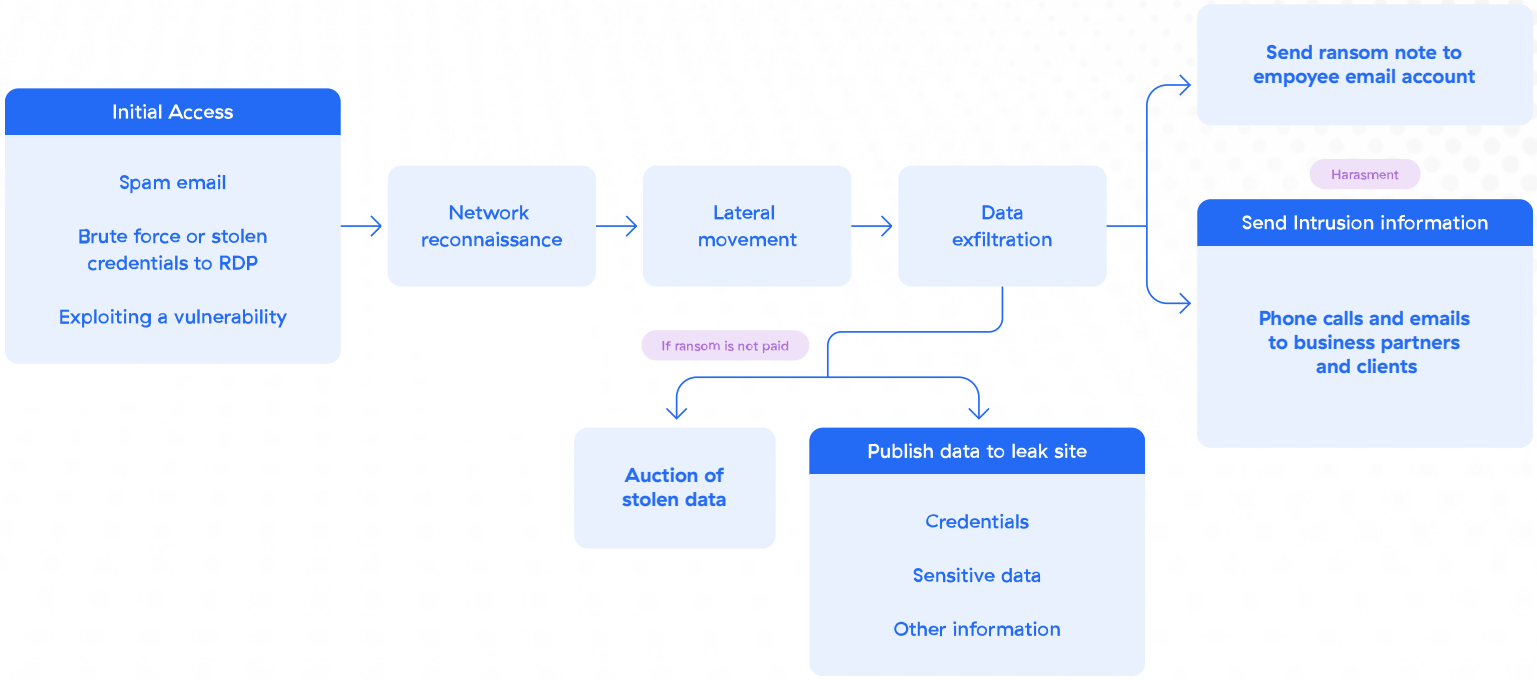


Figure 38: Attack sequence of data extortion group

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

Stay updated on ThreatLabz research by subscribing to our Trust Issues newsletter today.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com.