Akamai

State of the Internet
Volume 09 | Issue 04

Ransomware on the Move

Evolving Exploitation Techniques and the Active Pursuit of Zero-Days

Akamai

Table of contents

The dangerous shift to zero-day exploitation

In an evolving ransomware landscape in which adversaries seek to evolve past the ability of their victims to defend, ransomware groups are shifting their attack techniques away from phishing to put a greater emphasis on vulnerability abuse. Vulnerability abuse has grown considerably, both in scope and sophistication, as we extensively examined in our previous report, Slipping Through the Security Gaps. And ransomware groups have become more aggressive in their methods of both extortion and vulnerability exploitation, such as through in-house development of zero-day attacks and bug bounty programs. Ransomware groups are willing to pay for the opportunity for financial gain, whether it's to pay other hackers to find vulnerabilities in their ransomware software, or to acquire access to their intended targets via initial access brokers (IABs).

A deeper examination of the data reveals dangerous trends, echoing the explosion of high-profile attacks in 2022. Trends emerge in the growth of victims in various industries. Verticals with a rise in Internet of Things device connections, especially in manufacturing, have incurred a higher ransomware victim count. Yet, even verticals with a smaller victim count have been greatly affected, such as in healthcare, in which successful ransomware attacks could have severe consequences. Attackers are also shifting gears regarding tactics that can generate a more profitable pathway of value. They are finding more success as they move away from their initial extortion tactic — encryption — and focus their efforts more on data theft to gain an advantage over organizations relying on their backups. Attackers can also resort to multiple extortion tactics, including harassing the victim's customers or partners through emails or phone calls. Indeed, ransomware has evolved into a cybercriminal enterprise that goes beyond holding files or systems hostage.

We lay out the ransomware landscape in this State of the Internet (SOTI) report by exploring some of the most effective attack techniques and tools that ransomware groups are utilizing to achieve initial access through exfiltration. We also provide an extensive list of safeguarding techniques and recommendations. It is crucial that both industries and individuals protect themselves from the new wave of ransomware attacks, and this report will help provide insights for better defense and risk management of this growing concern.

> Ransomware groups have become more aggressive in their methods of both extortion and vulnerability exploitation.

Key insights of the report

- The ransomware threat landscape is seeing a concerning shift in tactics. The rampant abuse of zero-day and one-day vulnerabilities in the past six months led to a 143% increase in victims when comparing Q1 2022 with Q1 2023.
- Ransomware groups now increasingly target the exfiltration of files, which has become the primary source of extortion, as seen with the recent exploitation of GoAnywhere and MOVEit. This underscores the fact that file backup solutions, though effective against file encryption, are no longer a sufficient strategy.
- In some cases, the same victim was attacked twice by different ransomware groups. Akamai research finds victims of multiple ransomware groups are almost 6x more likely to experience a subsequent attack within the first three months of the initial attack. It's a race against time for organizations to close the gaps in their environment because of the likelihood of being attacked by another group.
- Ransomware groups, such as CL0P, are aggressively pursuing the attainment and development of zero-day vulnerabilities in-house. This has proven to be a successful strategy, with CL0P growing its number of victims by 9x from Q1 2022 to Q1 2023.
- LockBit dominates the ransomware scene with 39% of total victims (1,091 victims), more than quadruple the number of the second-highest ranked ransomware group. It has risen significantly in the absence of the previous front-runner, Conti, with its victim count increasing by 92% from Q4 2022 to Q1 2023.
- Attacks against specific verticals grew as well, with the number of manufacturing victims growing by 42% between Q4 2022 and Q4 2021, and the number of healthcare victims growing by 39% between Q4 2022 and Q4 2021.
- Two trends stand out from our analysis: First, a continuous activity from ransomware groups that may be dependent on variables like the group size and its resources; second, significant upticks in activities when critical zero-day vulnerabilities are exploited, such as CL0P's aggressive exploitation of highly targeted security flaws.
- Regulations enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) may make it illegal to pay ransom to certain parties or

individuals. Organizations that ignore the many impacts of ransomware attacks and data theft may face the difficult decision of violating OFAC regulations when giving in to ransom demands. This reinforces the need to have security controls and playbooks to thwart attempted attacks against your network.

LockBit dominates the ransomware landscape

Financially motivated threats like ransomware continue to wreak havoc on organizations despite the growing awareness of the ramifications of this threat. This is exemplified by the steady growth in victim companies between Q4 2021 and Q4 2022 (36%; Figure 1), and the giant leap of a 143% increase in the victim count year-over-year when comparing Q1 2022 with Q1 2023 due to the rampant abuse of zero-day vulnerabilities in recent months. The proliferation of ransomware victims is partially due to a confluence of factors, including the business operation behind the scenes, the as-a-service offerings in the dark web (for example, readily available access to corporate networks peddled via IABs), and the 2.5x growth in web attacks stemming from the ascending number of web application vulnerabilities like Log4Shell, ProxyLogon, and more recently, MOVEit, to name a few. The techniques the attackers are using are evolving and, as such, ransomware attacks can be challenging for victims to overcome because of their complex structure and their use of multiple attack vectors. In this section, we'll review the global trends and impacts ransomware has had over the 20 months from October 2021 to May 2023.

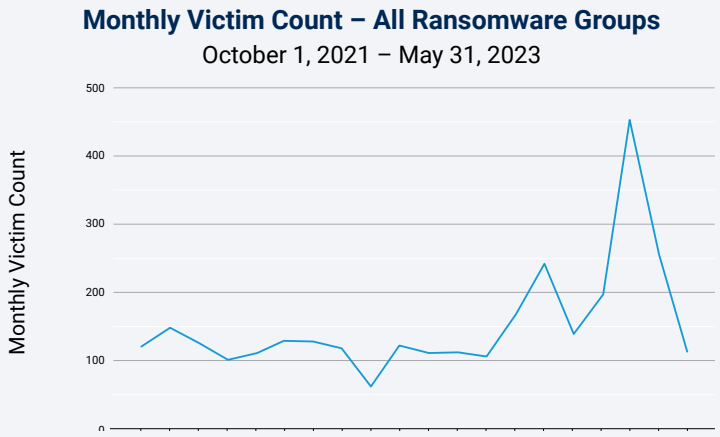


Fig. 1: The overall victim count from all ransomware groups grew by 143% from Q1 2022 to Q1 2023 due to the active exploitation of zero-day vulnerabilities

> Financially motivated threats like ransomware continue to wreak havoc on organizations.

We dove deeply into the data from published leak sites to see the dominant ransomware attackers (Figure 2). After Conti's disappearance, LockBit filled in the top spot, becoming one of the most prolific and active groups, with the highest number of victims based on the obtained information from published leak sites by attackers. Our data findings reveal that LockBit accounts for 39% (1,091 victims) of affected organizations, more than quadruple the number of victims of ALPHV ransomware, which ranks second. Because of LockBit's rampant activities and increased victimization, it generates a lot of attention from law enforcement and security defenders. All eyes are on LockBit — it's yet to be seen if it will follow in the footsteps of Conti, which ceased to operate but rebranded into smaller ransomware groups.

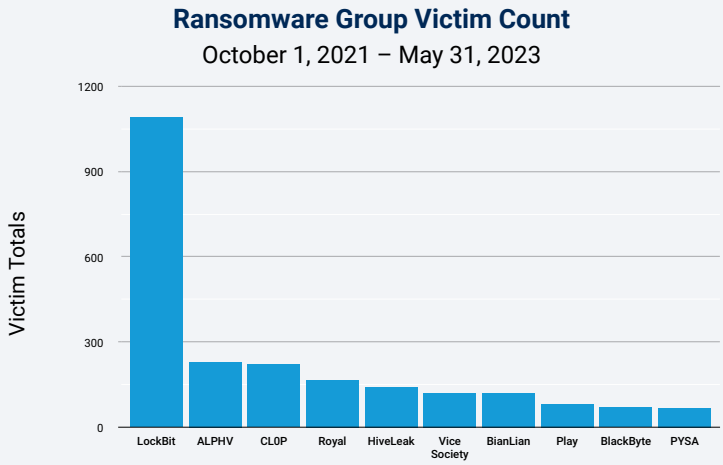


Fig. 2: The victim organizations of ransomware attacks are predominantly impacted by LockBit, followed by ALPHV, and CL0P

LockBit's continued success is due to its enhancements, including the introduction of novel techniques in its latest 3.0 version — like a bug bounty program (inviting all security researchers, ethical hackers, and unethical hackers to submit bug reports in their software for rewards ranging from US$1,000 to US$1 million; Figure 3) — and the use of Zcash cryptocurrency as a payment mode, which further amplifies this threat's prevalence. While the use of the bug bounty program is mostly defensive, it's unclear if this will also be used to source vulnerabilities and new avenues for LockBit to exploit victims.

Fig. 3: LockBit's bug bounty program entices hackers to submit flaws in their software (Source: Bleeping Computer)

Additionally, their affiliates, who deploy these attacks on targets, can earn as much as 75% of the ransom payment. To exert more pressure on their victims, the attackers behind LockBit have started reaching out to the victim's customers, informing them about the incident, and employing triple extortion tactics with the inclusion of Distributed Denial-of-Service (DDoS) attacks. To curb the prevalence of LockBit globally, the Cybersecurity and Infrastructure Security Agency (CISA), together with its international partners/counterparts, released a cybersecurity advisory, highlighting LockBit's techniques, which can aid security defenders in protecting their organizations.

Additionally, their affiliates, who deploy these attacks on targets, can earn as much as 75% of the ransom payment.

ALPHV, also known as BlackCat, has the second-highest number of victims next to LockBit. What sets this ransomware apart is its use of Rust programming language, enabling its ability to infect both Windows and Linux systems. Several vulnerabilities in Microsoft Exchange server (one of which, CVE-2021-34473, has a CVSS score of 10) were abused in order to infiltrate the intended targets. In one of the ALPHV attacks last year, the operators created a copy of their victim's website (using a typosquatted domain) as a new extortion technique; they published the stolen files in addition to leaking them on their website to mount pressure for their target to pay the ransom. Affiliates can earn up to 90% of the profit, making them even more enticing to other groups or new affiliates.

CL0P follows closely on the heels of ALPHV, with the third-highest number of victims. CL0P is a ransomware family known for abusing several zero-day vulnerabilities in managed file transfer platforms: a legacy file transfer appliance that reached its end of service in 2021 (used in attacks against oil companies);

GoAnywhere MFT security flaws in January 2023 (CVE-2023-0669); the PaperCut vulnerabilities in April 2023 (CVE-2023-27350 and CVE-2023-27351); and, more recently, a zero-day vulnerability in MOVEit Transfer (CVE-2023-34362; which led to data theft from a number of companies). More than 2,500 internet-facing servers that are running a vulnerable version of MOVEit are at risk of this security flaw. It is worth noting how CL0P has a relatively low victim count until its activity spikes whenever a new zero-day vulnerability is exploited as part of its operation. And unlike LockBit, which has a semblance of consistency or pattern, CL0P's attacks are seemingly tied to the next big zero-day vulnerability, which is hard to predict. We can speculate that the group tries to remain under the radar before striking, and our data shows this to be efficient as CL0P is one of the ransomware attacks that has successfully victimized organizations in the higher range category (more on this in our analysis by revenue section). It remains to be seen whether other ransomware groups will emulate CL0P's strategies.

> CL0P's attacks are seemingly tied to the next big zero-day vulnerability, which is hard to predict.

Although it's unclear when Royal ransomware emerged, what is known is that their operators could possibly be related to, or have ties to, the Conti Team One members, the group behind Conti ransomware. Royal ransomware may be a rebrand of Zeon ransomware, but unlike other ransomware operators, Royal does not have any affiliate programs and would typically purchase access to networks via IABs. The ransom demands could be between US$250,000 and US$2 million and can pose dangers by using remote desktop protocol (RDP) malware distributed through callback phishing as their point of entry.

Monthly trends unveil campaigns and victim baselines

Akamai research observed the ebb and flow of ransomware activities with significant spikes from prevalent strains in between (Figure 4). A snapshot of the overall victim total per quarter by all known ransomware groups signifies growth despite the fact that some groups may not be active or have disbanded or have stopped operations due to law enforcement efforts.

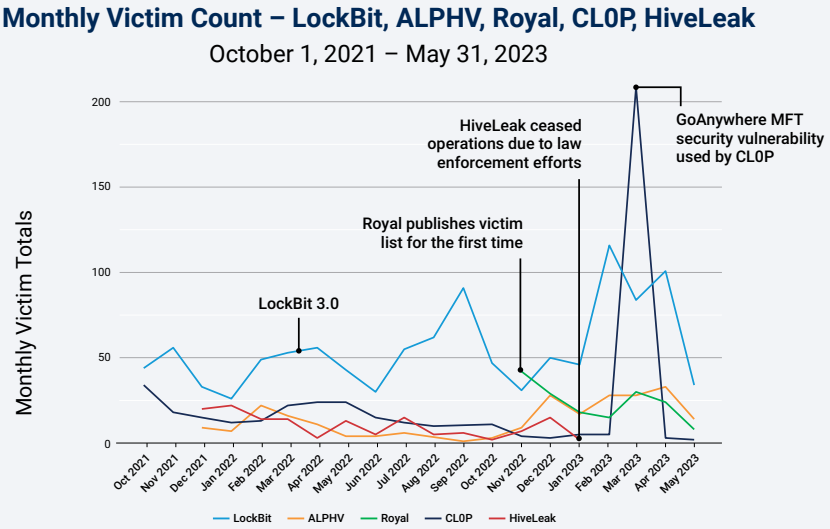
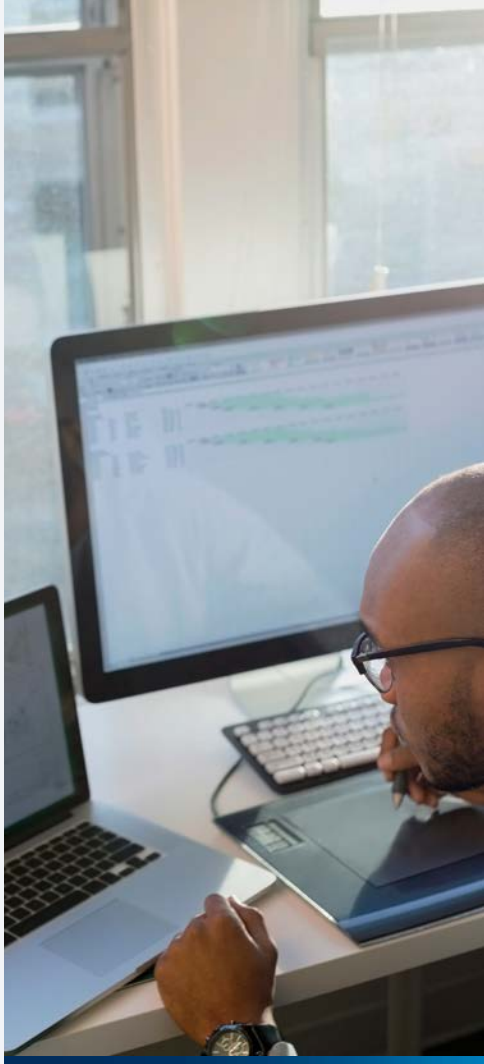


Fig. 4: A comparison of monthly ransomware victim count among top ransomware groups

While most ransomware threats have a baseline of activities whether in the high or low scale based on myriad factors like campaigns used, introduction of new tactics, and affiliate programs, among others, two trends stand out during our analysis of groups' activities. The first trend is a steady continuous activity from ransomware groups that may be dependent on variables like group size (the number of affiliates) and its resources. LockBit appears to have a consistent victim count of approximately 50 per month, while other ransomware groups had a lower count. ALPHV, which started with low activity, had several spurts in between 2021 and 2022.

The second trend indicates a massive upswing when certain groups abused critical zero-day vulnerabilities, as in our observation of CL0P's aggressive incorporation of highly targeted security flaws. From October 2021 to February 2023, CL0P's victim count sits lower than 35 per month — however, it is essential to highlight CL0P's unexpected ascent in March 2023, which may be related to the group's zero-day attack in Fortra's GoAnywhere software that impacted



> Akamai research observes the ebb and flow of ransomware activities with significant spikes.

several high-profile companies. In May 2023, CL0P abused a Structured Query Language injection (SQLi) vulnerability in MOVEit Transfer (CVE-2023-34362), and we're seeing another notable increase in activity.

On the other hand, HiveLeak (which is known for attacking several healthcare organizations in the United States, resulting in a reversion to paper charts and canceled urgent surgeries) was still one of the top ransomware groups in Q4 2022. It fell off the top 10 list in January 2023 because of the joint efforts of law enforcement in the United States and Germany, among others, to seize Hive's servers, preventing a potential whopping US$130 million ransom payout from their victims.

Quarterly analysis shows significant shifts in top ransomware

A closer comparison of Q4 2022 and Q1 2023 unveils not just possible patterns but also outliers in the ransomware trends. We observe that most ransomware threats have ramped up their activities at the beginning of the year, resulting in a notable growth in the number of victims; others have sustained their ranking in the top 4, as in the case of ALPHV and Royal. Q1 2023 is an anomaly since the number of victims are relatively higher than the baseline of other quarters observed in this report.

LockBit victims spiked by 92% in a span of a quarter (Q4 2022 to Q1 2023), highlighting the threat's consistent dominance. The significant jump of CL0P from number 10 to number 2 in Q1 2023 (Figure 5; a 1,642% increase) should be underscored, given this threat's use of multiple zero-day vulnerabilities in specific platforms — a new addition to their growing arsenal that can breach their intended target networks effectively. This puts organizations at an elevated risk of ransomware and necessitates bolstering their security measures or testing the efficacy of the security controls in place to mitigate the dangers posed by ransomware attacks. Additionally, timely patching is pivotal in closing the gaps in your perimeter.

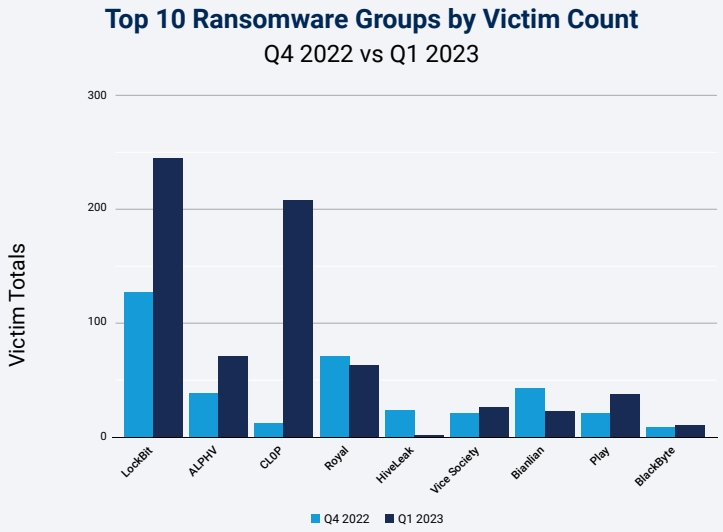


Fig. 5: CL0P's jump can be attributed to its perusal of a variety of zero-day vulnerabilities as a point of entry

The analysis of the number of victims per ransomware — despite being a subset of the total victim count as we can only observe those that were published in leak sites, and, therefore, represents only the victims that did not pay the ransom demands — offers a glimpse into their prevalence. The effects of ransomware attacks can go beyond financial losses, as we've seen in their impacts on critical infrastructure and other industries that are crucial to a country's economy. And one of the ways that many countries fight back against the elevated risk of ransomware attacks is through regulations that put organizations under scrutiny.

Organizations face higher risk of second attack within three months

The adage “lightning does not strike twice” does not necessarily apply to ransomware attacks. Akamai research finds that victims attacked by multiple ransomware groups are almost 6x more likely to experience a subsequent attack within the first three months than after more time has passed. This poses heightened dangers to organizations and brings to the fore the importance of preventing and mitigating initial ransomware attacks. While the victim company is distracted by remediating the initial attack, other ransomware groups that are likely scanning for potential targets and monitoring the activities of their competitors can also leverage this window of opportunity and hit the same company. Royal, for instance, attacked the same entity nearly four months after Hive first attacked it and the data breach had been publicly reported. CL0P’s initial infection of a company was capitalized on by two different groups, RansomHouse and Abyss, indicating that although one group may be responsible for the first attack, other attackers can take advantage and hit the same company. In some instances, the same group can target the same organization within 12 months or even longer; in this case, we can speculate that the target business did not entirely eliminate this threat in their network, whether it was a related backdoor or any tools. We saw this with LockBit, which victimized a real estate business once in 2021, then a second time in 2023.

It’s not so hard to imagine the crippling effects of consecutive ransomware attacks and the recovery time required to restore systems. Unfortunately, being attacked once and paying the ransom does not guarantee that your organization is safe, you can still be attacked again by the same group or, worse, by multiple groups. If the victim organizations have not yet closed gaps in their perimeter or remediated the vulnerabilities abused by attackers to breach their networks the first time, they can be used again. And it does not help if the victim chooses to comply with the ransom demands, as they may then be viewed as potential targets by the same group and others.

Can government policy turn the tide against ransomware?

There are three major types of extortion that are rampant today: data encryption, holding stolen data hostage, and DDoS. When deciding how to deal with responding to these attacks it is important to consider any regulatory or legal impacts. The first key area to consider is whether to pay the ransom. In 2022,

> The adage “Lightning does not strike twice” does not necessarily apply to ransomware attacks.

Florida joined North Carolina to become the second U.S. state to prohibit state and local government agencies from complying with or paying ransomware demands, and there are a number of states looking to enact similar laws. At the federal level, the 2023 national cyber strategy mentions ransomware 28 times and calls out CISA and the FBI as lead agencies in disrupting online criminal infrastructure and seizing cryptocurrency from ransomware campaigns.

Through the OFAC and the Financial Crimes Enforcement Network, the U.S. Department of the Treasury enforces regulations that make it illegal to pay a ransom to certain parties or individuals. The European Union (E.U.) has a similar stance on essential services, allowing the E.U. member states to impose fines for paying ransoms under the Network and Information Systems Directive. Additionally, once the revised Network and Information Security Directive is formally implemented, it will strengthen cybersecurity standards across many essential sectors, including healthcare, energy, digital services, electronic communications services, and postal/courier services, among others.

The second key area to consider is reporting. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 states that a covered entity that experiences a ransomware (covered cyber incident) shall report it to the agency within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred. It is critical to determine if any regulation and contractual agreements you have require reporting cyber incidents and include them in your crisis management plan.

> The U.S. Department of the Treasury enforces regulations that make it illegal to pay a ransom to certain parties or individuals.

Major shift in ransomware techniques yields greater success

Mitigating ransomware attacks requires a thorough understanding of the techniques and tools employed throughout the attack chain, from the initial access to the establishment of network persistence and subsequent encryption and data exfiltration. Tried-and-tested methodologies remain reliable; however, a shift in tactics and a growing complexity of attacks are being observed by the Akamai research team. The increasing number of web application vulnerabilities are being significantly abused to cast a wider net, and applications that hold sensitive information are being leveraged as another addition to extortion. Zero-day and one-day vulnerabilities are also becoming a staple in specific ransomware groups' cookbooks, with some security flaws exploited in proprietary or uncommon platforms or software.

This section highlights notable tactics from some of the top ransomware groups today. Security professionals can be three steps ahead of attackers by recognizing techniques commonly used in various stages of the attacks — such as initial access, command and control (C2), lateral movement, and exfiltration — aiding them in testing their security controls or through adversary simulations.

The state of the ransomware landscape today can be defined by the attackers' constant evolution of techniques to circumvent any defenses that can thwart their operation. In the past, the attack chain prominently revolved around phishing attacks as a vector or point of entry, encrypting files and calling it a day.

Mitigating ransomware attacks requires a thorough understanding of the techniques and tools employed throughout the attack chain.

Nowadays, breaching the system is just the beginning of a series of stages that do not necessarily end in encryption but in data exfiltration and, in some cases, DDoS attacks (Figure 6). Attackers try to maximize their damage while minimizing and modernizing their efforts, so they will employ many different extortion tactics to intimidate their victims into paying the ransom demands. And it may be that attackers are finding more success in data theft extortion instead of just in encrypting their intended target's files.

> Attackers try to maximize their damage while minimizing and modernizing their efforts.

Most modern ransomware attacks start with a network breach, either by exploiting a vulnerable internet-facing asset or by using social engineering tactics, followed by the execution of scanners to discover additional assets, credential dumping leading to privilege escalation in the domain, and, finally, the use of those credentials to steal sensitive information and spread ransomware across the entire network.

Our H1 2022 ransomware report detailed the baseline for attack techniques. This year we saw this evolution continue, with some unique trends that can shed a light on what we can expect in the coming months and years.

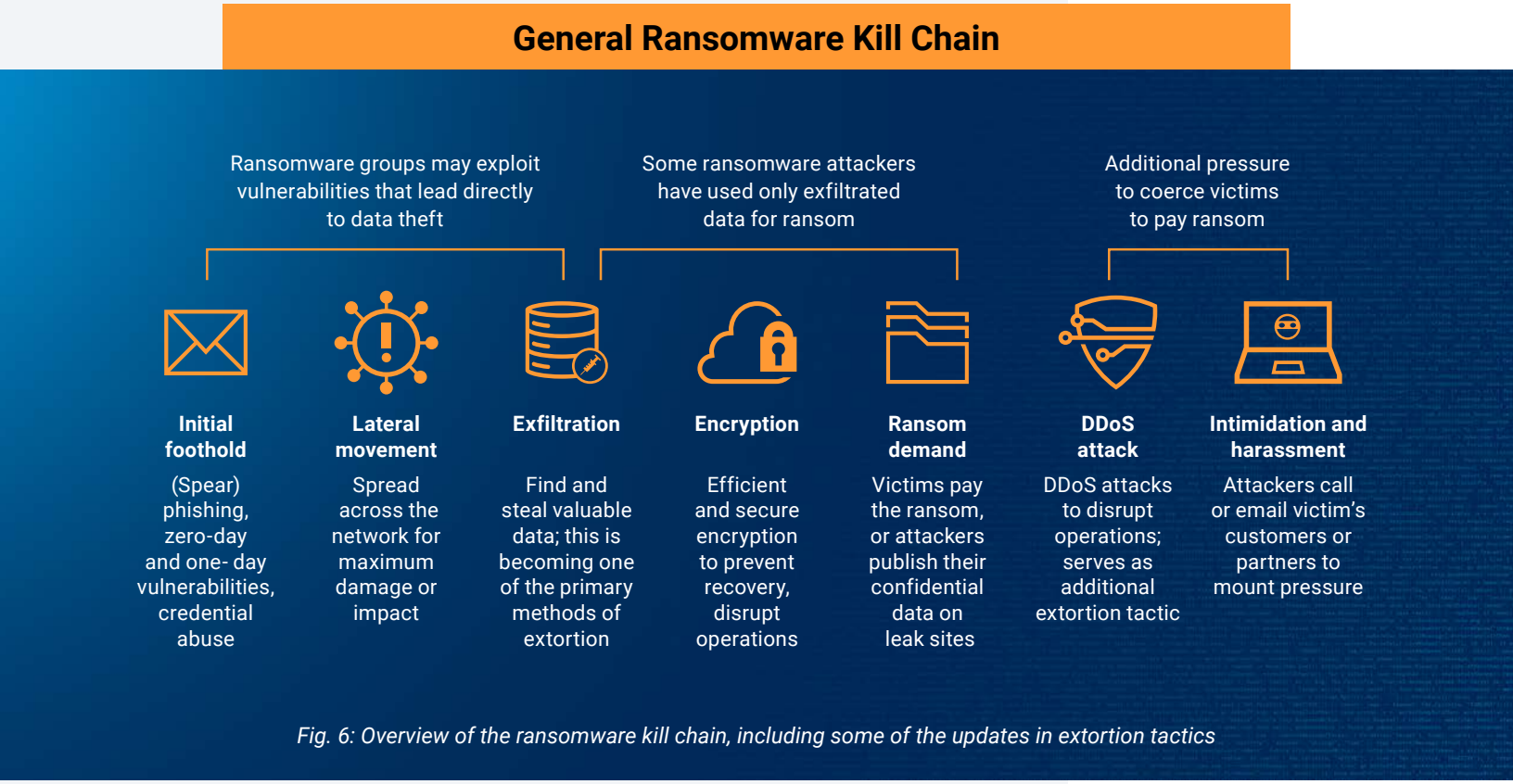


Fig. 6: Overview of the ransomware kill chain, including some of the updates in extortion tactics

Initial access methods

Phishing

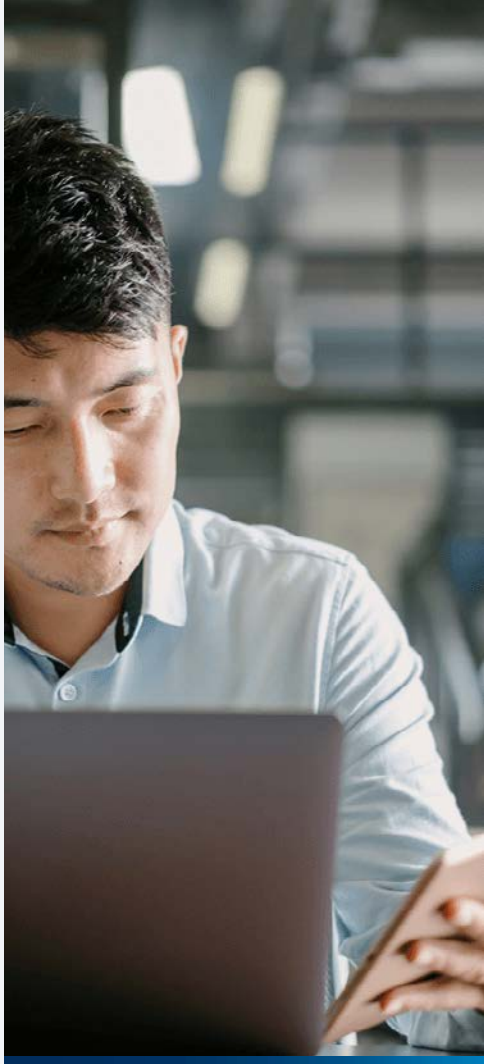
In 2023, attackers had to adapt their tactics when sending phishing emails. For years, attackers abused Microsoft Office attachments containing macros to run malicious code after users were lured into downloading them. This method was so common that it finally forced Microsoft to implement a policy change to block all macros from Office files downloaded from the internet.

This change has forced threat actors to ditch macros in favor of new methods to breach their targets. This year we saw a spike in the usage of various file formats to deliver malware, including ISO files, which have become a very common delivery option, allowing the bypass of some security mitigations. OneNote documents with embedded malicious files have also been seen spreading multiple malware families.

In addition, a LockBit affiliate has been reported using phishing emails that install the Amadey Bot malware to encrypt devices and take control, and CL0P actors have been sending large volumes of spear-phishing emails to employees to gain initial access into organizations. There has also been a callback social engineering phishing campaign on the rise that targets employees of various companies with what is being called a BazarCall attack. The BazarCall attack directs victims to a threat group's call center so that social engineering tactics may persuade victims to begin a remote screen-sharing session and remain on the call as attackers secretly establish a point of entry to victims' machines. We expect this trend of evolving phishing lures to continue; as detections continue to improve, attackers will sharpen their tactics.

Hunting for vulnerabilities: One-day and zero-day abuse

Zero-day and older vulnerabilities are the next big attack vector, with ransomware groups using software security flaws as an initial access point into networks at an increasing rate. Realizing the potential impact of code vulnerabilities and the fact that they are an easier pathway to infiltrate intended targets, attackers have remodeled their monetization tactics accordingly. In fact, the most common method attackers use to obtain initial access is the exploitation of internet-facing applications, often via the abuse of one-day vulnerabilities on unpatched systems. These groups have been very quick to adopt vulnerabilities that are



> The most common method attackers use to obtain initial access is the exploitation of internet-facing applications.

published, as well as to abuse zero-days. It's a race against time for organizations to patch and update their software or systems.

Older vulnerabilities such as Log4Shell (CVE-2021-44228) and ProxyLogon (CVE-2021-26855) are still being exploited in the wild to breach networks and deploy ransomware. Evidence of this has appeared as LockBit has been using Log4Shell to attack VMware instances. Also, some victims reported that BlackByte gained access through a known Microsoft Exchange Server vulnerability.

This year, we saw attackers moving away from traditional ransomware cases that target arbitrary servers and endpoints and toward abusing applications that hold sensitive data that can be leveraged against extorted companies. Notable examples include:

- The ESXiArgs ransomware campaign, which abused one-day vulnerabilities in VMWare ESXi servers to target virtual machines hosted on the server, encrypting them and thus making them unusable
- CL0P and Bl00dy ransomware, among others, which were observed exploiting the PaperCut MF/NG improper access control vulnerability that allowed authentication bypassing by remote unauthenticated attackers who executed arbitrary code on devices
- CL0P, which targeted a plethora of zero-day vulnerabilities in multiple managed file transfer (MFT) servers. The attack in March 2023 was quickly followed by an attack on MOVEit in May 2023. In both cases, vulnerabilities were used to steal sensitive files and extort the victims.

Although leveraging zero-day vulnerabilities is not particularly new, what is notable is how ransomware groups like CL0P, for instance, are actively seeking or researching vulnerabilities and abusing them on a large scale to compromise hundreds or even thousands of organizations. The huge spikes of CL0P victims in the weeks following the exploitation of zero-days demonstrates that such techniques can generate bigger payoffs, and this trend will likely continue in the near future. Similarly, LockBit's bug bounty program is an avenue for its operators to enhance their existing ransomware software.

> It's a race against time for organizations to patch and update their software or systems.

Stolen credentials

Valid stolen credentials may also allow for initial access to be achieved via an internet-facing application or exposed service. This has been observed as an attack vector for groups like Vice Society and ALPHV. Valid credentials may be purchased from dark web vendors or through phishing, brute force, or password guessing. After receiving valid credentials, an attacker may exploit external remote services, such as a VPN or RDP, to breach a network. In November 2022, attackers abused a vulnerability in Fortinet VPN servers to gain initial access, and then proceeded to spread ransomware to the entire network. LockBit affiliates ALPHV and Vice Society have been reportedly leveraging credential abuse for their attacks.

Drive-by compromise

There is also the potential for an attacker to gain initial access through a drive-by compromise. This is when system access is gained by adversaries via a user who is browsing a website that can be either malicious or legitimate yet compromised. This may be achieved by the exploitation of a user's web browser or via application access tokens granted to the attacker. Ransomware groups such as LockBit and REvil have been seen using this technique to gain initial access into a victim's system.

Partnerships with other cybercriminal groups: Initial access brokers

One of the most difficult steps in an attack is gaining initial access to the victim's network. IABs are malicious groups that specialize in exactly that. They use different tactics to breach networks and then proceed to sell access to the highest bidders. These groups use common methods, such as phishing and exploitation of one-day vulnerabilities, to gain a foothold in the network, then will gather information to verify the size and revenue of the breached company network and price access to it accordingly. Modern ransomware groups tend to outsource a lot of their tasks, including initial access to networks.

IABs continue to be a major vector for ransomware intrusions, with some IABs with strong ties to specific ransomware groups, as in the case of Qbot and Black Basta, while others sell access to various groups. Ransomware groups behind LockBit, DarkSide, Conti, and BlackByte, among others reportedly leveraged IABs

as part of their operations. According to our previous DNS report, Attack Superhighway: A Deep Dive on Malicious DNS Traffic, 26% of infected devices reached out to domains related to IABs (Figure 7) like Qakbot/Qbot (4% of infected devices) and Emotet (22% of infected devices).

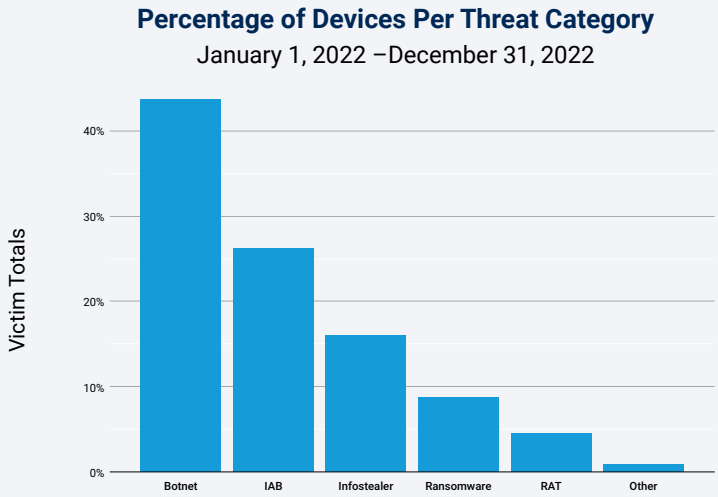


Fig. 7: Threat types present in enterprise environments based on analysis of malicious DNS traffic from Akamai's previous SOTI report, Attack Superhighway: A Deep Dive on Malicious DNS Traffic

How do IABs figure in the ransomware as a service (RaaS) business model and cybercrime landscape in general? Ransomware attackers need remote access and credentials not only to infiltrate their victims' networks, but also to move laterally, establish persistence, and gain access privileges, among other things. This symbiotic relationship between ransomware attackers and IABs could have exacerbated the rising number of ransomware attacks. And, as such, it is

important for defenders to be able to detect malware used by IABs, as the period from the initial infection to network-wide ransomware can be shockingly short.

Running with your data: How extortion tactics have evolved

Ransomware attackers are deviating from encryption, their primary method of extortion, and instead focusing their efforts solely on data theft, using leaked confidential data to extort their victims. They can threaten victims that they will release their confidential information online or sell it to the highest bidders on the dark web. This attack tactic further highlights the fact that backups are simply not enough to protect against ransomware — even if an organization can quickly recover from encryption, it can never recover from the loss of sensitive data. The attackers may also be finding more success and impact by stealing information rather than doing the tedious step of compromising the entire network. BianLian is an example variant that has resorted to data theft tactics without encryption, a decision that was likely made after a decryptor for the original ransomware payload was released. Organizations are strongly urged to adopt a Zero Trust security model with DDoS protection to safeguard their perimeter and limit the damages of ransomware in various stages of the kill chain.

In recent years, ransomware attackers have upped the ante with multi-extortion schemes, coercing their victims into giving in to the ransom demands. Most ransomware victims are grappling with a combination of extortion techniques, starting with the encryption of their data, barring the company from accessing it until a ransom payout. The second layer of extortion is stealing data and holding it hostage, which is now becoming the main tactic. And if the target organizations do not comply with the attacker's demands after such extortion tactics, they can take it further by launching DDoS attacks to overwhelm their site traffic and disrupt business operations, causing financial losses. ALPHV is one example of a group that launches DDoS attacks if the ransom demands are not met. DDoS attacks added to the mix can be arduous for security teams to effectively address when they are already dealing with a ransomware attack with exfiltration and encryption of their data. To make matters worse, adversaries may resort to intimidation or harassment by emailing the victims' customers, business partners, or even the media, relaying information that an organization has fallen victim to such attacks, resulting in a tarnished brand and reputation or loss of customer trust.

> Even if an organization can quickly recover from encryption, it can never recover from the loss of sensitive data.

Ransomware continues to target critical industries

Understanding who are the biggest ransomware attackers today and the tactics and techniques they use can aid defenders in bolstering their organization's security posture against ransomware attacks. However, it is crucial to know how industries are being targeted and which threats are specific to which industries and perimeters so pen test teams, red teams, and security professionals can simulate attack scenarios and understand how to close gaps in their environments.

Ransomware attacks remain rampant across industries and companies of varying sizes — attacks against organizations occur approximately every 19 seconds, totaling 1.7 million attacks each day — according to a report by Astra. Most of these attacks are outside the scope of our data collection, but the report states that they have cost an average of approximately US$1.85 million per incident over the last five years. Moreover, Cybersecurity Ventures predicts that ransomware will attack organizations every two seconds by 2031.

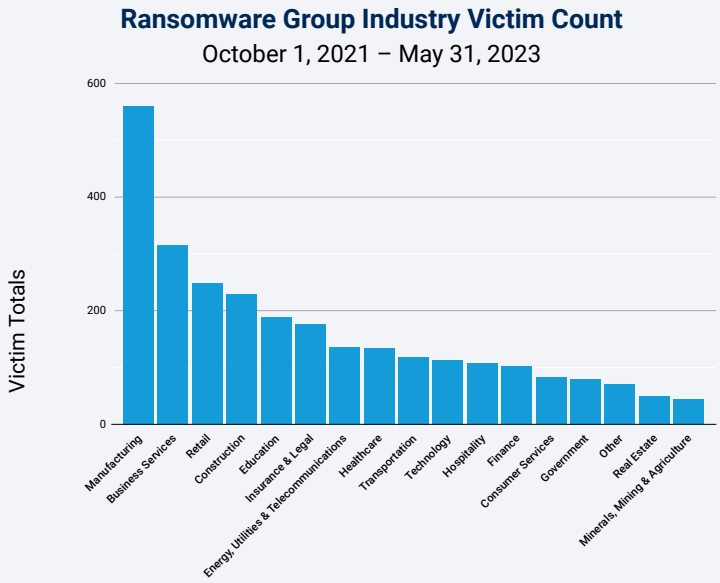


Fig. 8: Manufacturing remains the vertical with the highest number of victims of ransomware attacks

Manufacturing remains the top vertical (Figure 8), with the most victim organizations (20%) affected by ransomware attacks. Business services and retail follow at 11% and 9%, respectively. This result is echoed by last year's

global ransomware report, which shows manufacturing and business services as the top verticals victimized by Conti ransomware. Additionally, it is also consistent with the findings in our Attack Superhighway: A Deep Dive on Malicious DNS Traffic report, which showed that 30% of analyzed organizations with C2 traffic are in the manufacturing sector. Although it does not necessarily follow that manufacturing experiences more attacks than other industries, what is clear is that attackers are finding success in targeting this industry. It is also worth repeating that business services is the second highest in the list of ransomware victims, which underscores the potential for supply chain attacks. Case in point: A gasoline retailer suffered from a CL0P ransomware attack via their third-party service provider. A monthly comparison of ransomware victims among crucial industries also reflects an upward trend (Figure 9).

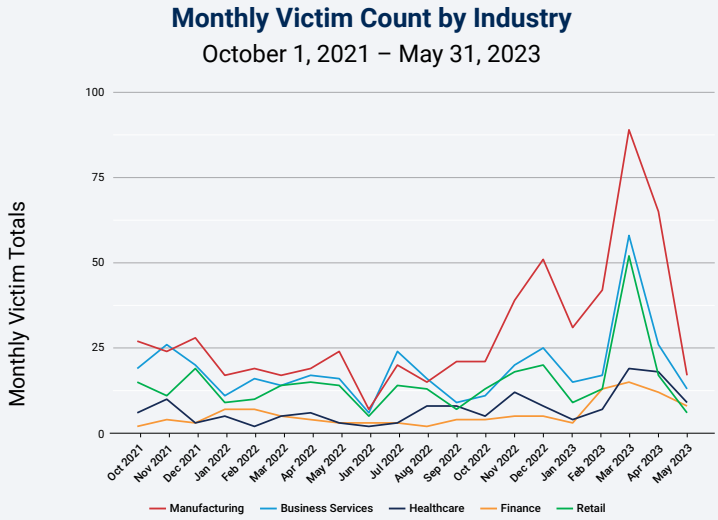


Fig. 9: A comparison of ransomware victims among crucial industries also reflect an upward trend

We looked at the following five industries to elucidate the top ransomware threats and to determine if there are convergences and divergences in attack trends: financial services, business services, manufacturing, commerce, and healthcare. LockBit reigned supreme, accounting for the majority of the victimized organizations across these aforementioned industries. In the manufacturing sector, LockBit was responsible for 41% of impacted organizations; in the financial services, it accounted for nearly 50% (although the number of victims is relatively smaller than in manufacturing). From its first emergence in 2019 as ABCD ransomware, LockBit underwent several improvements, with its 2.0 version having the fastest encryption mechanism as touted by its operators. HiveLeak was another ransomware prominent in these

> Business services is the second highest in the list of ransomware victims, which underscores the potential for supply chain attacks.

five industries, but their operations were halted last year when law enforcement breached Hive's networks. Let's look more closely at several industries to learn more about their challenges and what makes their environment ripe for exploitation for ransomware attacks.

Manufacturing

Manufacturers are often at a relatively high level of vulnerability to ransomware threats because of a prevalence of specialized and legacy operating systems and an increased attack surface due to a greater number of connected devices and equipment. The risk is exacerbated by the potential impact that can be inflicted on the company, their customers, and even society as a result of disrupted operations. When operations are halted, this results in shut down and/or damage to expensive capital equipment; loss of sales, market share, and even safety; and environmental damage to employees and the surrounding community. Moreover, successful attacks on manufacturers can create supply chain disruptions, causing delays in essential goods and services.

This increased risk comes from the plethora of legacy or old commercial software deployed across diverse manufacturing and supply chain sites, including on operational equipment, sensors, and other connected endpoints, from connected cars to chemical plants. This elevated risk is also observed in our data findings in which the number of impacted manufacturing companies spiked by 42% between Q4 2021 and Q4 2022. Over the long term, manufacturers will often possess valuable intellectual property, including proprietary designs, formulas, or trade secrets. Ransomware attacks can result in the theft or

42% ↑

spike in the number of impacted manufacturing companies between Q4 2021 and Q4 2022

exposure of this sensitive information, compromising competitiveness and potentially leading to legal consequences. Damage to a firm's reputation can also have lasting impacts.

Further complicating the picture for manufacturers is their typically complex, extended supply chains. These vendor and supplier relationships often come with automated data interfaces and a wide range of vendor personnel who use your sites and interact with equipment and control systems. This results in many more attack surfaces to be aware of and to defend.

Healthcare

Healthcare organizations, including hospitals, private clinics, pharmaceutical companies, and healthcare information technology, among others, face a significant set of security challenges: the usage of legacy systems on top of the continuous expansion of the Internet of Medical Things without corollary security strategies, as well as vulnerabilities within medical devices like MRI machines that provide an easy access point into healthcare networks. Additionally, the lack of cybersecurity staff, especially in smaller hospitals, poses another challenge for this vertical as it tries to secure its perimeter against cyberattacks.

According to the February 2023 Current and Emerging Healthcare Cyber Threat Landscape report from Health-ISAC, ransomware is a primary security concern for the healthcare industry. Apart from the aforementioned security challenges, healthcare data is also one of the most valuable assets on the dark web — more so than credit cards — which makes this industry an even more enticing target of

> The lack of cybersecurity staff, especially in smaller hospitals, poses another challenge.

cybercriminals. Between Q4 2021 and Q4 2022, the number of ransomware victims against this industry rose by 39%. BlackCat and LockBit specifically target healthcare companies and even go as far as customizing their tactics for specific victims.

Successful ransomware attacks could have especially dire consequences in healthcare since access to a patient's records is imperative in providing critical services and, in some cases, could mean life or death. Although certain ransomware groups openly declared that they would not target hospitals, our data shows that ransomware strains like LockBit and HiveLeak still target healthcare organizations.

Financial services

Ransomware has become ubiquitous among cybersecurity attacks in financial services. The Navigating Cyber 2023 report by the Financial Services Information Sharing and Analysis Center (FS-ISAC) reported that ransomware remains the biggest concern among financial institutions, and is rapidly becoming one of the top cybersecurity nightmares. Although the number of victims is relatively lower than in manufacturing or retail, we saw an increase of 50% in the totals of affected organizations within this vertical.

RaaS providers, who give affiliates access to their ransomware suite in exchange for a cut of the illegal profits, are likely to blame for this growth. Financial institutions are considered high-value targets because of the sensitive data they hold. As a result, the ransom demanded from these targets can be higher than from other targets. Financial services are the backbone of economic systems, so disruptions to their operations can have severe consequences, and even a short disruption can cause significant financial losses and reputational damage. Attackers exploit this position to demand substantial ransoms and use a variety of tactics, including exfiltrating data prior to encryption and extortion, using leak sites to shame and coerce victims into paying, and launching DDoS attacks against victims already struggling to cope with the ransomware attack. Intelligence-led threat hunting can be a proactive and effective defense mechanism.

Ransomware has become ubiquitous among cybersecurity attacks in financial services.

50% ↑

increase in totals of affected organizations within the financial services vertical

Commerce

The commerce vertical, which comprises retail businesses and hotel and travel companies, ranks second (if we combine retail and hospitality) in the number of ransomware victims per industry. This resonates with IDC's research that found ransomware attacks on retailers increased. This is also reflected in our data findings that indicated a 9% increase in victims within the retail sector. The surging risk of ransomware in this vertical stems from a combination of various factors: a growing complexity in the commerce environment, which makes it arduous to protect; a lower security maturity level; and the use of data-heavy applications, among others. For retailers in particular, a successful ransomware attack could mean that both store and online operations grind to a halt as critical systems or servers become inaccessible. Even sensitive customer personally identifiable information (PII) or credit card data could be exfiltrated and sold on the dark web — or even used as extortion by the attackers — leading to further damage to brand, reputation, and finances. It's not surprising that security leaders in the annual RH-ISAC CISO Benchmark report cited ransomware as the top risk facing their organizations in 2023. Retailers who suffered from ransomware attacks and decided to pay the ransom reportedly paid an average of US$160,000. In addition, the same IDC study also illustrated that there's more likelihood for retailers to suffer from extended business disruption during ransomware attacks.

Education

Educational institutions like universities and lower schools are increasingly becoming common targets of ransomware (the victim count increased by 128% when comparing Q4 2021 to Q4 2022), resulting in data theft and, in some cases, the closure of schools for days. This is particularly concerning because of the nature of the information this industry possesses, such as PII. One of the groups that targeted education was HiveLeak, which threatened to release highly sensitive student information, like psychological assessments and social security numbers. Another prominent ransomware that has disproportionately targeted education is Vice Society, which accounts for 39% of attacks, according to this report from Malwarebytes. Our data findings echoed this, with Vice Society (24%) as the top ransomware in education after LockBit. Ransomware attacks are becoming rampant not only in universities, but also in lower schools, possibly due to budget constraints, limited security resources,, and a lack of security awareness or training within the staff.

Analysis by revenue: Smaller organizations at high risk of ransomware

Every organization, regardless of company size or revenue, is at risk of ransomware attacks. Attackers have no preference among small and medium-sized businesses or larger enterprises. However, there is an assumption that larger enterprises with bigger revenue are more likely than other organizations to be targeted because they present a higher payoff. An analysis of victims by revenue illustrates an entirely different picture. More than 60% of analyzed victims (Figure 10) are in the smaller revenue bracket of up to US$50 million, demonstrating that attackers are also successful in launching attacks against smaller organizations. We can surmise that these lower revenue companies are more vulnerable to these attacks because their environment is easier to infiltrate, with limited security resources to combat the hazards of ransomware. At the same time, they have the capacity to pay the ransom to avoid business disruption and possible revenue loss.

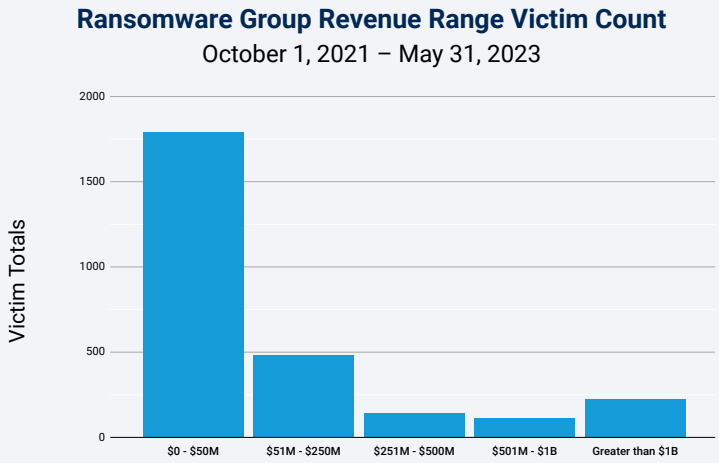
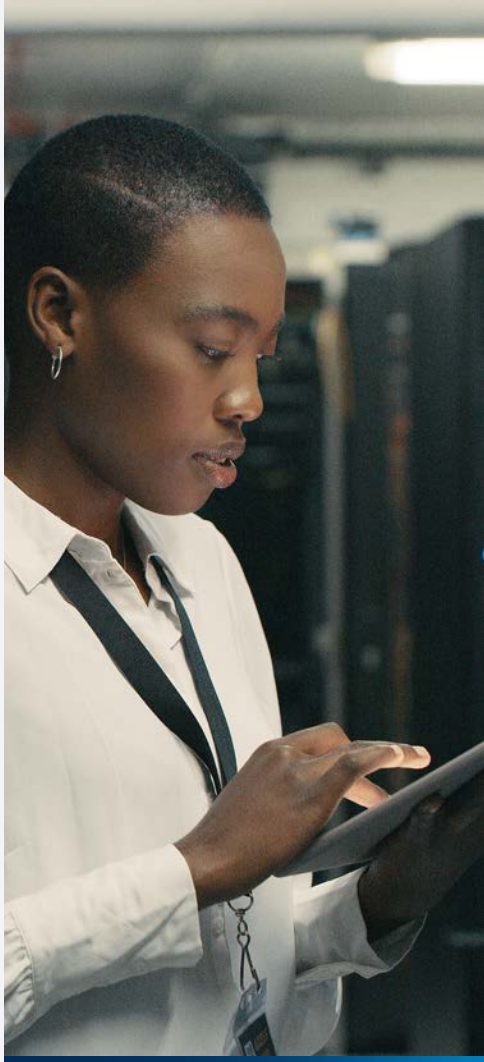


Fig. 10: The majority of ransomware victims are in organizations with reported revenue of up to US$50 million



More than 17% of reported victims are businesses with a revenue range of US$51 million to US$250 million. Additionally, larger enterprises with a reported revenue in the higher range of at least US$501 million and beyond are also susceptible to ransomware attacks, as observed in the percentage of victims (12%) in these brackets. Even though ransomware attacks impact a smaller percentage of larger enterprises, it is relevant to point out that high-value targets are also under attack and susceptible to the possible dangers of ransomware if they fail to protect their perimeter. A survey from Sophos indicates a correlation between the revenue of the targeted company and the amount of ransom paid to the attackers. The higher the revenue of the affected organization, the bigger the ransom payment. For example, the median ransom payment for organizations in the greater than US$1 billion bracket is US$1 million.

Our analysis also shows that most ransomware groups follow a similar trend regarding the number of victims and their corresponding revenue ranges. On average, for any given ransomware group, 67% of victims are in the lowest revenue range, with LockBit and PYSA having more concentration (nearly 75%) in this bracket. However, there are several groups that have a surprisingly high percentage of victims in the higher revenue ranges — HiveLeak has 21% of reported victims in the US$501 million and higher brackets, while CL0P has 29% and ALPHV has 15% of their affected organizations in that category.

Cybercrime magazine reports that global ransomware damage costs are predicted to exceed US$265 billion annually by 2031 — and increase to $42 billion annually next year, more than double what it was two years ago. With such a high velocity of annual cost increase, we can expect to see a drastic change in our victim totals over the next few years as the number of ransomware attacks continues to increase.

For more information on the ransomware trends in the Asia-Pacific and Japan (APJ) and Europe, Middle East, and Africa (EMEA) regions, please refer to the following snapshots of those regions.

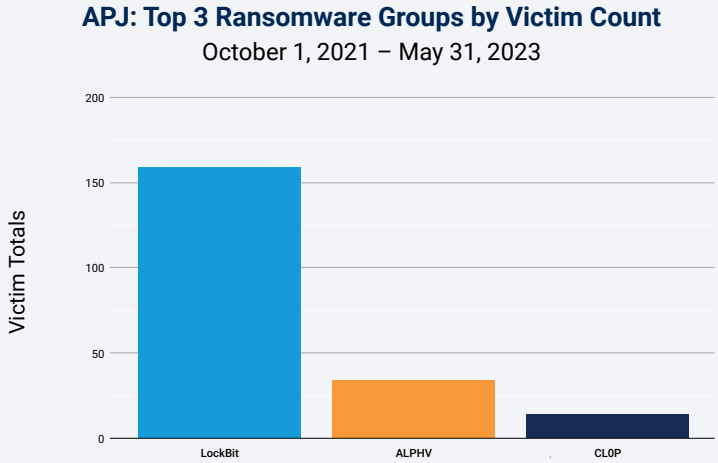
Ransomware:

APJ snapshot

The APJ Snapshot is a companion piece to our larger ransomware SOTI report, Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days (available in English only). Please refer to that report for detailed analyses of ransomware groups' attack trends, methodology, and techniques; a description of the stages of attacks and the corresponding solutions and recommendations to safeguard your organization; and our research methodologies.

LockBit dominates ransomware group activity

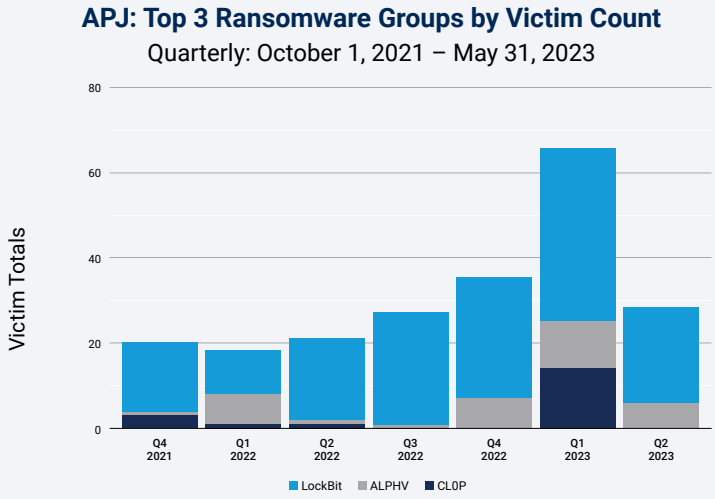
Despite a rising awareness of ransomware and an abundance of tools and best practices available to combat this threat, growth in victim companies in APJ increased by 50% between Q4 2021 and Q4 2022, with a giant leap of 204% in the victim count year-over-year when comparing Q1 2022 with Q1 2023. Consistent with data findings in our global report, between the period of October 1, 2021, and May 31, 2023, LockBit was responsible for the majority of attacks on victims, accounting for 51% of attacks in APJ, with ALPHV and CL0P rounding out the top three (APJ Figure 1).



APJ Fig. 1: The majority of the victim organizations of ransomware attacks in APJ were hit by LockBit, ALPHV, and CL0P

Quarterly analysis

Despite the prevalence of LockBit, CL0P ransomware was quite active from Q4 2021 through Q2 2022 and spiked in Q1 2023, elevating it to the position of third most active ransomware group in APJ and gaining ground on ALPHV (APJ Figure 2). CL0P's surge in activity can be attributed to its exploitation of a variety of zero-day vulnerabilities as a point of entry. A shift in attack techniques over the past six months, from phishing to the rampant abuse of vulnerabilities, is leading to the giant leap in victim counts. That said, only partial data was available for Q2 2023* at the time of this report, and as of May 31, 2023, CL0P registered no attacks, which could indicate Q1 2023 was an anomaly. However, it is important to note that in June 2023, as a result of the exploitation of the MOVEit vulnerability, CL0P claimed more victims, and a handful of companies in APJ are on that list.



APJ Fig. 2: A comparison of quarterly victim counts among the top three ransomware groups in APJ: LockBit, ALPHV, and CL0P

Critical industries at risk

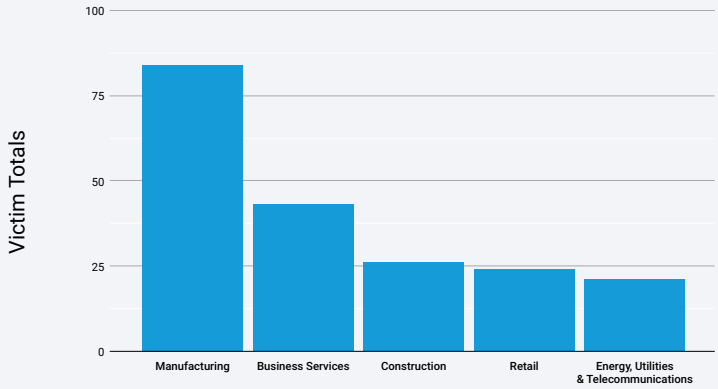
The top five critical industries at risk of ransomware in APJ are manufacturing, business services, construction, retail, and energy (APJ Figure 3). This follows the general worldwide trend, with the exception of the fifth position, which, on a global basis, is held by education. This is also largely consistent with last year's global ransomware report where manufacturing and business services also held the top two positions. During that time, they were victimized by Conti ransomware. After Conti's disappearance, LockBit filled the spot that Conti left.

**Q2 2023 is not a full quarter as the data has a May 31, 2023, cutoff.*

We also see overlap with the top affected industries in our previous DNS report, Attack Superhighway: A Deep Dive on Malicious DNS Traffic, reflecting a link between malicious command and control (C2) traffic and ransomware attacks.

APJ: Top 5 Industries by Ransomware Group Victim Count

October 1, 2021 – May 31, 2023



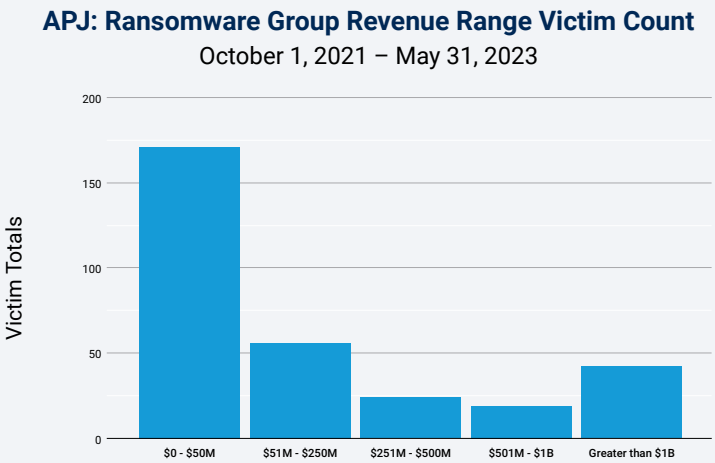
APJ Fig. 3: Manufacturing has the highest number of victim organizations in ransomware attacks in APJ

It is also important to note that LockBit does not discriminate: It is the most prevalent ransomware in each industry in APJ, accounting for 60% of attacks in manufacturing, 55.8% in business services, 57.7% in construction, and 45.8% in retail. Even in the energy sector, in which LockBit accounts for 28.6% of attacks, the remaining attacks are spread across several different ransomware groups, with no group accounting for more than 14.3%.

Ransomware groups focus on ROI

Every organization, regardless of company size or revenue, is at risk of ransomware attacks. However, mirroring the worldwide trend, the data shows that attackers are successful in launching attacks against smaller organizations in APJ (APJ Figure 4). According to a report by the Cyber Security Agency of Singapore, most of the reported ransomware victims in Singapore were small and medium-sized businesses in the manufacturing and retail sectors. We surmise that smaller companies have limited security resources to combat the hazards of ransomware, which makes them more vulnerable and easier to infiltrate, and they have the capacity to pay the ransom. However, the largest enterprises are also under attack, with research showing the higher the revenue of the affected organization, the bigger the ransom payment.

> Every organization, regardless of company size or revenue, is at risk of ransomware attacks.



APJ Fig. 4: The majority of ransomware victims in APJ are in organizations with reported revenue of up to US$50 million

APJ snapshot conclusion

Ransomware continues to wreak havoc on organizations. Globally and regionally, governments are forming a united front to address the threat and highlight techniques that can aid security defenders in protecting their organizations. A statement issued by the Foreign Ministers of Australia, India, and Japan, and the Secretary of State of the United States exemplifies the urgency to mitigate the impact of ransomware on national security and on all industry sectors and reinforces a commitment to building programs aimed at helping organizations enhance their cybersecurity capacity and build resilience. Earlier this year, the International Counter Ransomware Task Force, chaired by Australia, was established to drive greater collaboration among a coalition of 36 member states and the E.U. to counter the spread and impact of ransomware, including the sharing of cyberthreat intelligence. In October 2022, Singapore also formed its first inter-agency task force consisting of multiple government agencies to help defend businesses and critical infrastructure against ever-growing ransomware attacks.

As regulators put initiatives and policies in place to strengthen cybersecurity standards, it is important to understand the reporting requirements in your area so that you can include them in your playbook/crisis management plan, and be aware of the opportunities you have to mitigate risk by leveraging a multilayered defense.

For more information, please refer to the global ransomware SOTI report, Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days.

Ransomware:

EMEA snapshot

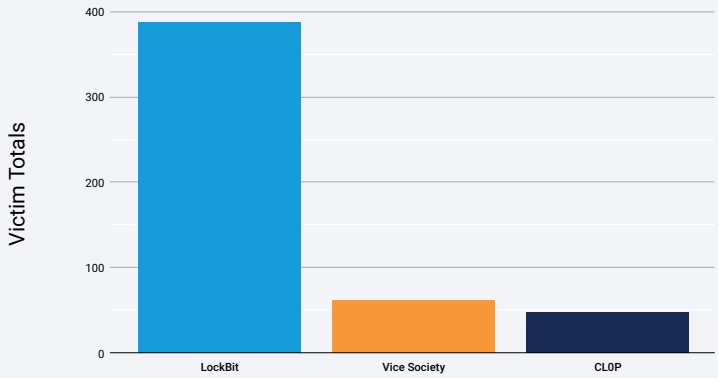
The EMEA Snapshot is a companion piece to our larger ransomware SOTI report, Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days (available in English only). Please refer to that report for detailed analyses of ransomware groups' attack trends, methodology, and techniques; a description of the stages of attacks and the corresponding solutions and recommendations to safeguard your organization; and our research methodologies.

LockBit dominates ransomware group activity

Despite a rising awareness of ransomware and an abundance of tools and best practices available to combat this threat, growth in victim companies in EMEA increased 18% between Q4 2021 and Q4 2022, with a leap of 77% in the victim count year-over-year when comparing Q1 2022 with Q1 2023. Consistent with data findings in our global report, between the period of October 1, 2021, and May 31, 2023, LockBit was responsible for the majority of attacks on victims, accounting for 45% of attacks in EMEA. However, in EMEA, Vice Society displaces ALPHV as the second most active group; CL0P is still third (EMEA Figure 1).

EMEA: Top 3 Ransomware Groups by Victim Count

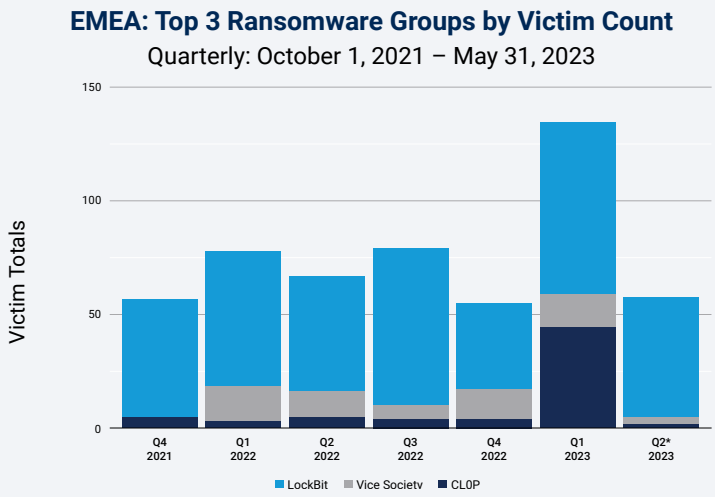
October 1, 2021 – May 31, 2023



EMEA Fig. 1: The majority of the victim organizations of ransomware attacks in EMEA were hit by LockBit, Vice Society, and CL0P

Quarterly analysis

When we look at victim counts by ransomware group (EMEA Figure 2), LockBit remains prevalent, and the consistent presence of Vice Society likely goes hand-in-hand with education being one of the top industries targeted by ransomware in EMEA (shown later in EMEA Figure 3) as Vice Society is a ransomware-as-a-service offering that disproportionately targets the education sector. However, consistent with global data trends, CL0P is rising in the EMEA ransomware landscape and its spike in Q1 2023 can be attributed to its exploitation of a variety of zero-day vulnerabilities as a point of entry. A shift in attack techniques over the past six months, from phishing to the rampant abuse of vulnerabilities, is leading to the leap in victim counts. That said, only partial data was available for Q2 2023* at the time of this report. As of May 31, 2023, CL0P activity returned to the level we saw in 2022. Although we cannot say definitively what the quarter will ultimately reveal, it is important to note that in June 2023 CL0P published the names of more victim companies in EMEA as a result of the exploitation of the MOVEit vulnerability, so the victim count will likely rise.



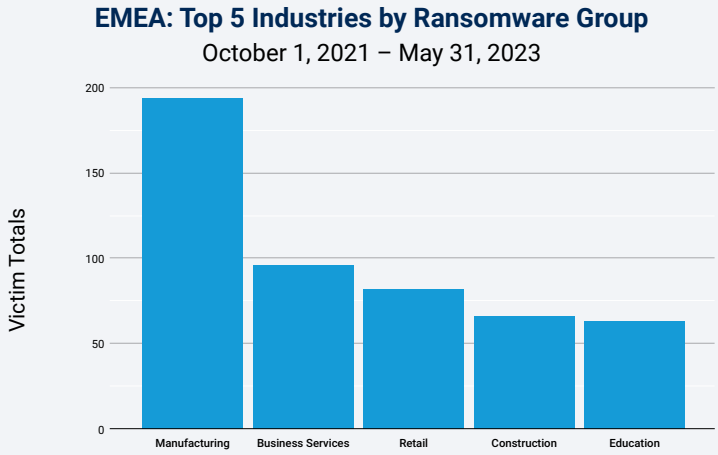
EMEA Fig. 2: A comparison of quarterly victim counts among the top three ransomware groups in EMEA: LockBit, Vice Society, and CL0P

Critical industries at risk

The top five critical industries at risk of a ransomware attack in EMEA are manufacturing, business services, retail, construction, and education (EMEA Figure 3). This corresponds to the same top five industries worldwide, and is also consistent with the 2022 global ransomware report, in which manufacturing and business services held the top two positions. During that time they were

**Q2 2023 is not a full quarter as the data has a May 31, 2023, cutoff.*

victimized by Conti ransomware. After Conti's disappearance, LockBit filled the spot that Conti left. We also see significant overlap with the top five affected industries in our previous DNS report, Attack Superhighway: A Deep Dive on Malicious DNS Traffic, reflecting a clear link between malicious command and control (C2) traffic and ransomware attacks.



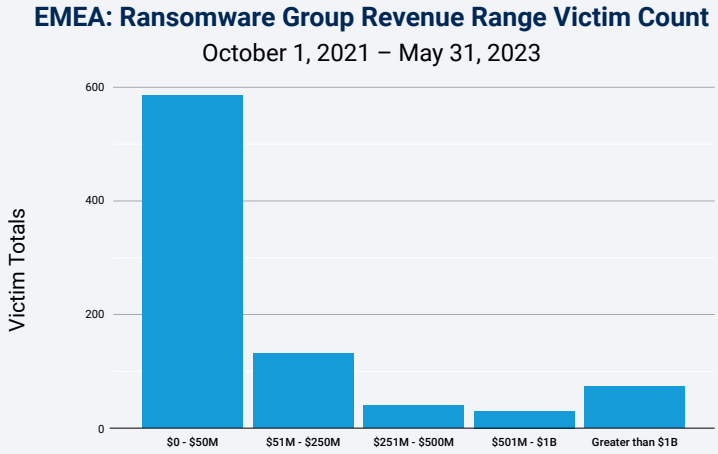
EMEA Fig. 3: Manufacturing is the vertical with the highest number of victim organizations in ransomware attacks in EMEA

It is also important to note that LockBit is the most prevalent ransomware in each of the four top industries in EMEA, accounting for 45.9% of attacks in manufacturing, 45.4% in business services, 45.1% in retail, and 53.6% in construction. Education is the exception: Vice Society is responsible for the most attacks (36.5%) and LockBit accounts for 22.2% of attacks.

> Every organization, regardless of company size or revenue, is at risk of ransomware attacks.

Ransomware groups focus on ROI

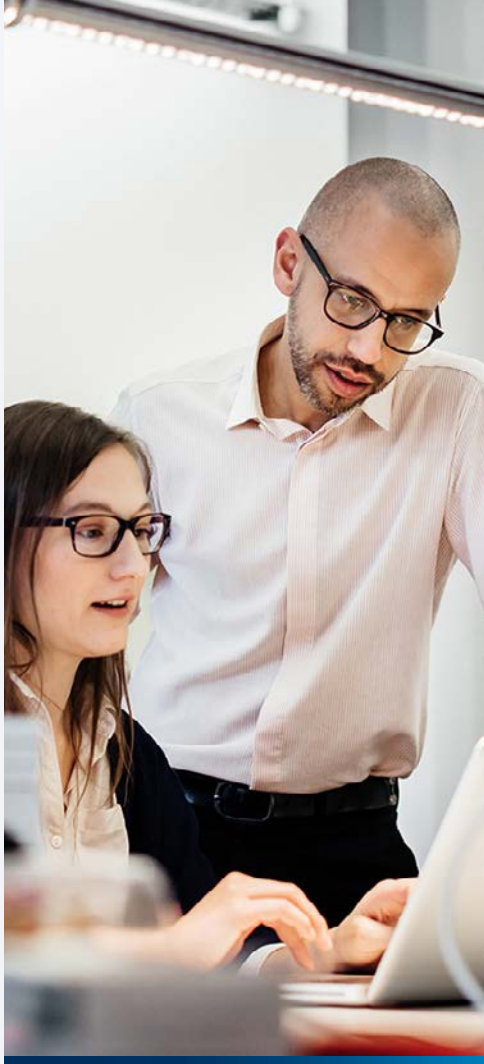
Every organization, regardless of company size or revenue, is at risk of ransomware attacks. However, mirroring the worldwide trend, the data shows that attackers are successful in launching attacks against smaller organizations in EMEA (EMEA Figure 4). We surmise that smaller companies have limited security resources to combat the hazards of ransomware, which makes them more vulnerable and easier to infiltrate, and they have the capacity to pay the ransom. However, the largest enterprises are also under attack, with research showing the higher the revenue of the affected organization, the bigger the ransom payment.



EMEA Fig. 4: The majority of ransomware victims in EMEA are in organizations with reported revenue of up to US$50 million

EMEA snapshot conclusion

Ransomware continues to wreak havoc on organizations. Globally and regionally, governments are forming a united front to address the threat and highlight techniques that can aid security defenders in protecting their organizations and building resilience. ENISA, the European Union Agency for Cybersecurity, issued a new Network and Information Systems Directive (NIS2) aimed at improving cybersecurity across the E.U. including new tasks such as the creation of a vulnerability registry. Outside the E.U., other countries are creating and enforcing their own controls, such as Saudi Arabia's National Cybersecurity Authority (NCA).



For more information, please refer to the global ransomware SOTI report, Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days.

As regulators put initiatives and policies in place to strengthen cybersecurity standards, it is important to understand the reporting requirements in your area so that you can include them in your playbook/crisis management plan, and be aware of the opportunities you have to mitigate risk by leveraging a multilayered defense.

Solutions and recommendations

In this report, we've discussed the various ransomware trends and how techniques in the different stages of attack are shifting. Since ransomware attacks are so multifaceted and include multiple stages and many tactics (Figure 11), recommendations will be divided into the various stages of the attack, and will span many different products and tactics.

To mitigate the ransomware threat effectively, organizations should:

- Adopt a multilayered approach to cybersecurity to address threats throughout the different stages of attack and across various threat environments. More information on specific solution types for the various stages of attack can be found in the next sections.
- Employ network mapping and segmentation to identify and isolate critical systems and limit network access to and from those systems. This limits the lateral movement of any malware should a breach occur.

- Keep all software, firmware, and operating systems up-to-date with the latest security patches. This helps mitigate known vulnerabilities that ransomware may exploit.
- Maintain regular offline backups of critical data and establish an effective disaster recovery plan. This ensures the ability to restore operations quickly and minimize the impact of a ransomware incident.
- Develop and regularly test an incident response plan that outlines the steps to be taken in case of a ransomware attack. This plan should include clear communications channels, roles, and responsibilities, and a process for engaging law enforcement and cybersecurity experts.
- Conduct regular cybersecurity awareness training to educate employees about phishing attacks, social engineering, and other common vectors used by ransomware threat actors. Employees should be encouraged to report suspicious activities promptly. This training should extend to policies and procedures for both working with vendors that are physically on-site and interacting with company systems remotely. All vendors and suppliers should also be required to undergo this training before accessing sites or systems.

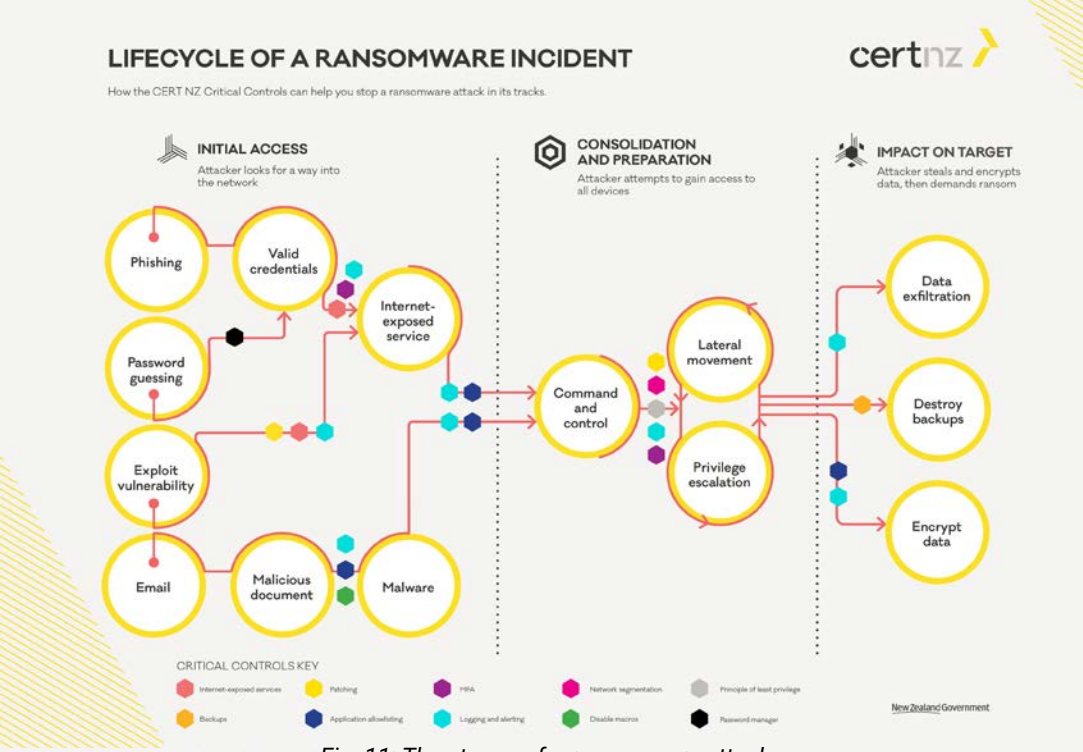


Fig. 11: The stages of a ransomware attack

Protection against initial access

Safeguard internet-facing servers

The exploitation of one-day and even zero-day vulnerabilities against internet-facing servers has become a popular vector for infection. One effective measure to protect against such threats is the implementation of web application and API protection (WAAP). A web application firewall (WAF), for example, acts as a protective shield, analyzing incoming web traffic and filtering out malicious requests that could potentially exploit vulnerabilities in web applications. By inspecting HTTP and HTTPS traffic, the WAF can detect and block common attack patterns and known exploit attempts. A WAF can offer features like virtual patching, which provides immediate protection against known vulnerabilities, even before a permanent fix is implemented. Additionally, WAF has proven to be quite an effective method to safeguard against previously unknown vulnerabilities, as in the MOVEit zero-day case discovered and exploited by the CL0P gang.

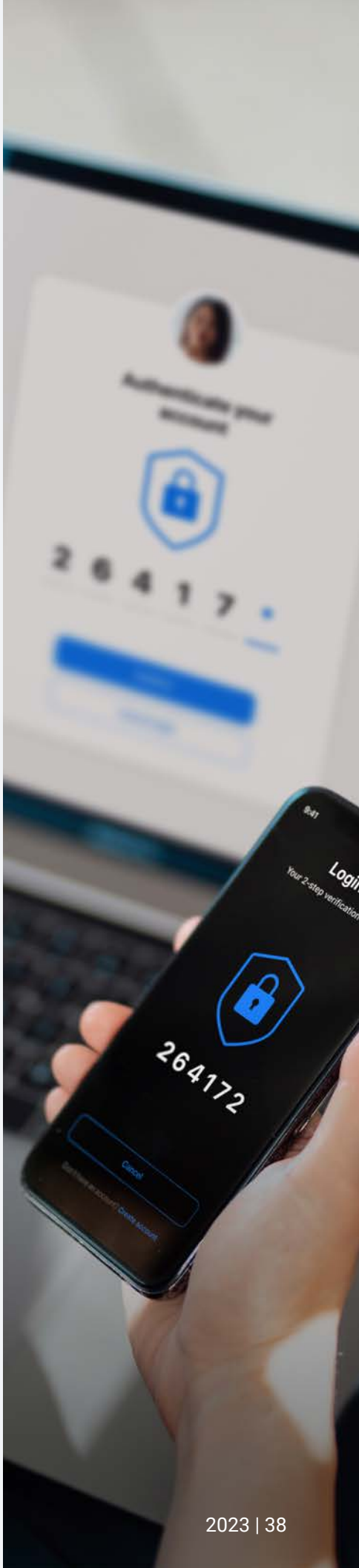
Defending endpoints from phishing

Use URL inspection capabilities to detect and block phishing attempts. Using this capability to protect your endpoints will enable you to scan each of the URLs your users click in real time, identifying any malicious or anomalous links and blocking them.

Additionally, endpoint detection and response tools can identify and send an alert on potential breaches or malicious activity resulting from a phishing email running malicious payloads.

Reduce VPN attack surface

Use Zero Trust Network Access (ZTNA) to enable a secure, application-specific VPN access and reduce external attack surface. ZTNA allows you to reduce risk significantly by allowing application-specific, role-based access to your network. ZTNA does not grant users full access to the entire network, like traditional VPNs, instead only allows limited access to specified applications. This way, even if attackers were to compromise the user's credentials and bypass the multi-factor authentication protection, they would not gain access to the entire network, only to a limited set of applications.



Use multi-factor authentication on critical services

Passwords can be compromised by attackers in a variety of ways, and strong passwords should no longer be considered an impenetrable defense. Attackers can use attacks such as brute force or credential stuffing to compromise passwords and breach your networks. This risk can be remediated by using a multi-factor authentication solution to protect your services.

Protection against C2

Block C2 servers

Use solutions that allow you to inspect outgoing internet traffic, such as a secure web gateway, in order to block known malware C2 servers. Solutions must be able to monitor all of your communications in real time and block communications to malicious domains, which would prevent the malware from running properly and accomplishing its goals.

Protection against discovery

Identify network scans

Use an intrusion detection system solution to help identify suspicious network scans (Figure 12). Attackers use various tools to identify their next target within your network; being able to detect this activity can allow you to stop the spread of the attack before it starts.

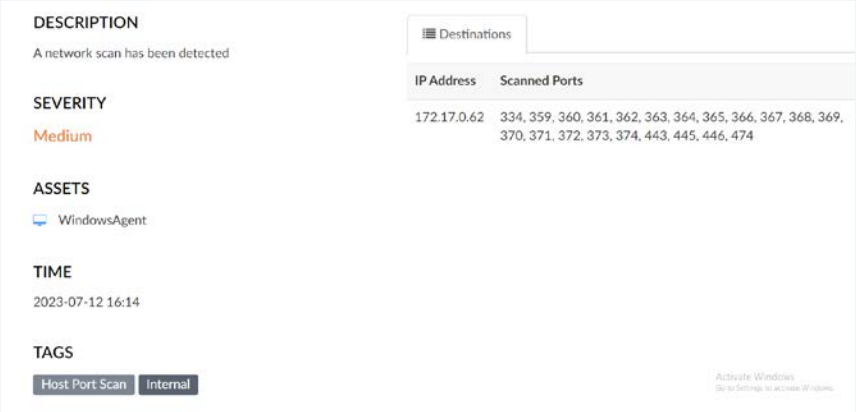


Fig. 12: Network scan incidents in Akamai Guardicore Segmentation

> Solutions must be able to monitor all of your DNS communications in real time and block communications to malicious domains.

Deception against discovery

Honeypots, if they can be created or provided by a solution, can help take advantage of attackers "probing in the dark." Luring attackers into honeypot servers, monitoring their activities, and alerting you once anomalies are detected can help detect and stop attackers' activities (Figure 13).

Fig. 13: A deception incident in Akamai Guardicore Segmentation

Protection against lateral movement

Restrict management ports

Software-based segmentation can be used to create a process-level policy to reduce the attack surface over sensitive ports. Preferably, use a solution that allows you to apply policy on the process level, enabling you to determine which processes should be communicating over sensitive management ports (Figure 14). In this way, you can limit the chance these ports would be used for malicious activity.

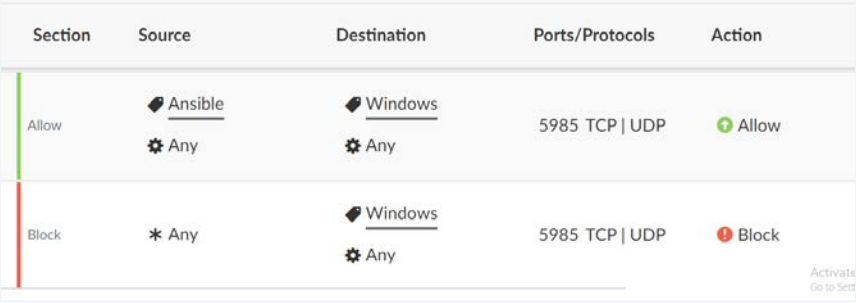


Fig. 14: Example of an Akamai Guardicore Segmentation policy to limit WinRM communications

Protection against exfiltration

Block exfiltration domains

Limit access to services that can be abused for data exfiltration by either using solutions that block known malicious URL and DNS traffic, or by using solutions or controls that allow blocking access to specific domains (Figure 15). By doing this, we can minimize the risk from attacker exfiltration tools by blocking their domains from all endpoints that do not require access to them, and only allowing access through approved applications such as browsers.

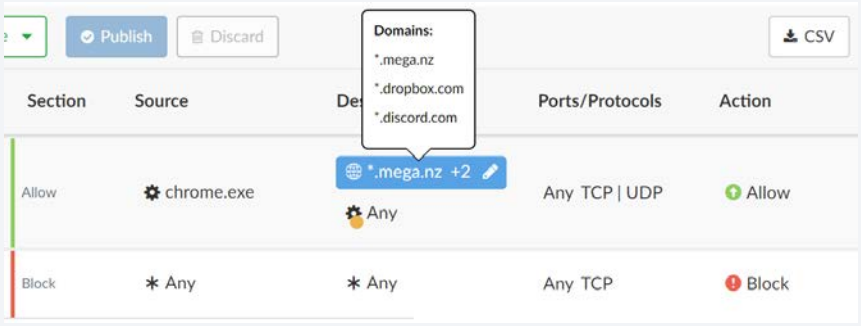


Fig. 15: Example of an Akamai Guardicore Segmentation policy to block exfiltration domains

Conclusion

This Akamai ransomware report highlights a rising trend among ransomware groups to shift their focus toward exploiting vulnerabilities in software to further extort the businesses. We expect that other MFT systems may be a high-value target this year for ransomware groups such as CL0P.

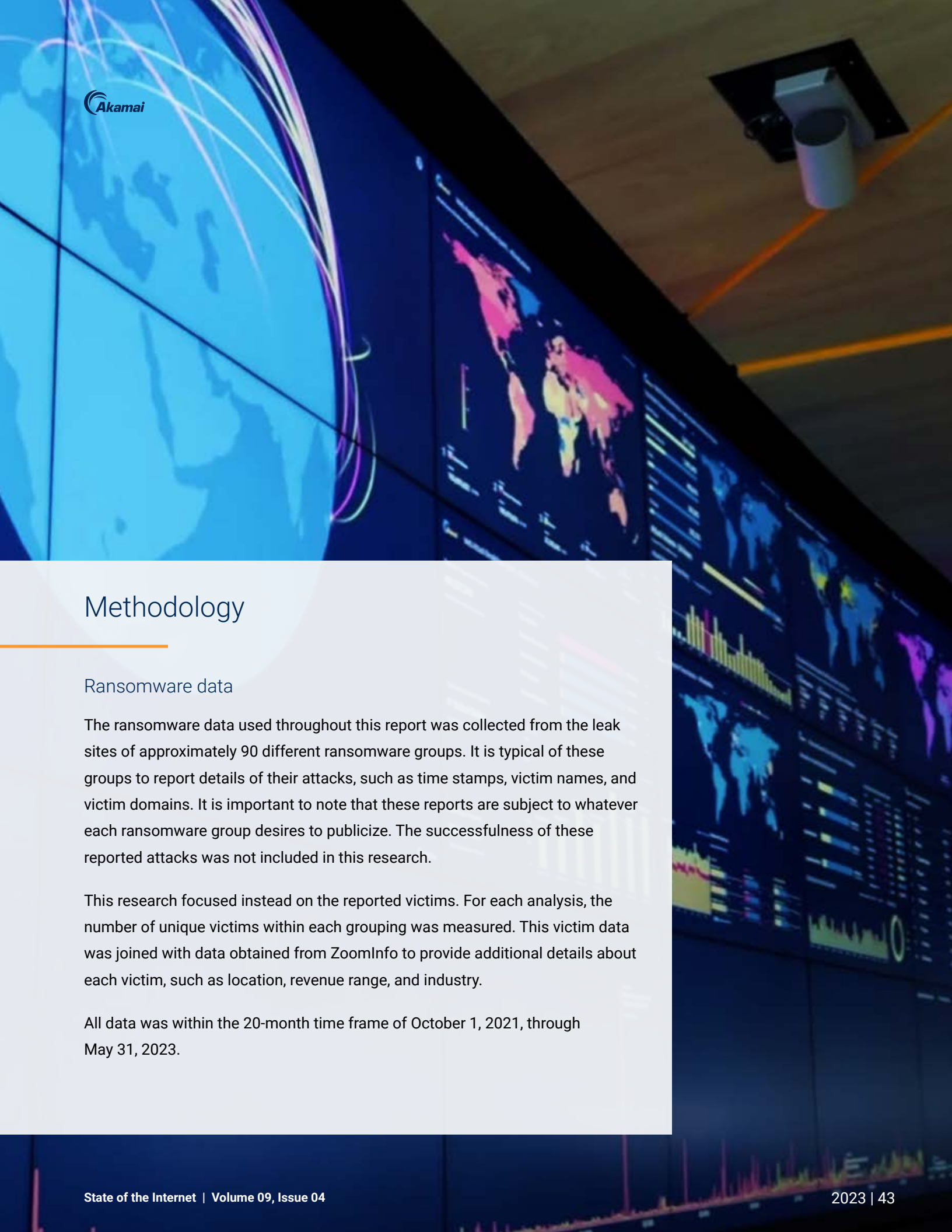
This shift represents a significant escalation in the tactics employed by these malicious actors, demonstrating their adaptability and determination to maximize the impact of their attacks. As organizations continue to bolster their cybersecurity defenses, it becomes imperative that file backup solutions no longer be used as a comprehensive solution to combat ransomware groups. To address the current challenges, organizations must prioritize proactive measures, such as network segmentation, vulnerability management, "virtual" and timely patching, and proactive monitoring of file transfer systems to mitigate the risk of falling victim to ransomware groups attacks.

Additionally, it is time to update the playbooks — there is more emphasis today on malware than social engineering, so technical controls are the front line of defense. Zero-day vulnerabilities and IABs require situational awareness and mitigation strategies to prevent both the spread of encryption and the exfiltration of data. Pen test teams and red teams should use groups like LockBit to model validation exercises. Organizations should review legislation with their legal teams to make sure the plan is complete and compliant, and leverage CISA and ISAC for best practices.

Finally, if you are hit: Realize that you do not have time to recover — the second wave can hit while you are mitigating the first incident. Be sure to have a team looking for the next attack.

Stay plugged into our latest research by checking out our security research hub.

> As organizations continue to bolster their cybersecurity defenses, it becomes imperative that file backup solutions no longer be used as a comprehensive solution to combat ransomware groups.



Methodology

Ransomware data

The ransomware data used throughout this report was collected from the leak sites of approximately 90 different ransomware groups. It is typical of these groups to report details of their attacks, such as time stamps, victim names, and victim domains. It is important to note that these reports are subject to whatever each ransomware group desires to publicize. The successfulness of these reported attacks was not included in this research.

This research focused instead on the reported victims. For each analysis, the number of unique victims within each grouping was measured. This victim data was joined with data obtained from ZoomInfo to provide additional details about each victim, such as location, revenue range, and industry.

All data was within the 20-month time frame of October 1, 2021, through May 31, 2023.

Credits

Editorial and writing

Eliad Kimhy
Lance Rhodes
Charlotte Pelliccia
Badette Tribbey

Review and subject matter contribution

Moshe Cohen
Ori David
Shiran Guez
Ophir Harpaz
Reuben Koh
Richard Meeus
Steve Winterfeld
Maxim Zavodchik

Data analysis

Chelsea Tuttle

Marketing and publishing

Kimberly Gomez
Georgina Morales Hampe
Shivangi Sahu

More State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/ Security reports. **akamai.com/soti**

More Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports,and cybersecurity research. **akamai.com/security-research**

Akamai data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. **akamai.com/sotidata**

More on Akamai solutions

To learn more about Akamai's solutions for ransomware, visit our **Security Solutions** page.