2023 Mid-Year Cyber Claims Report

Understanding the cybercrime ecosystem to build cyber resilience

resilience

→ CyberResilience.com

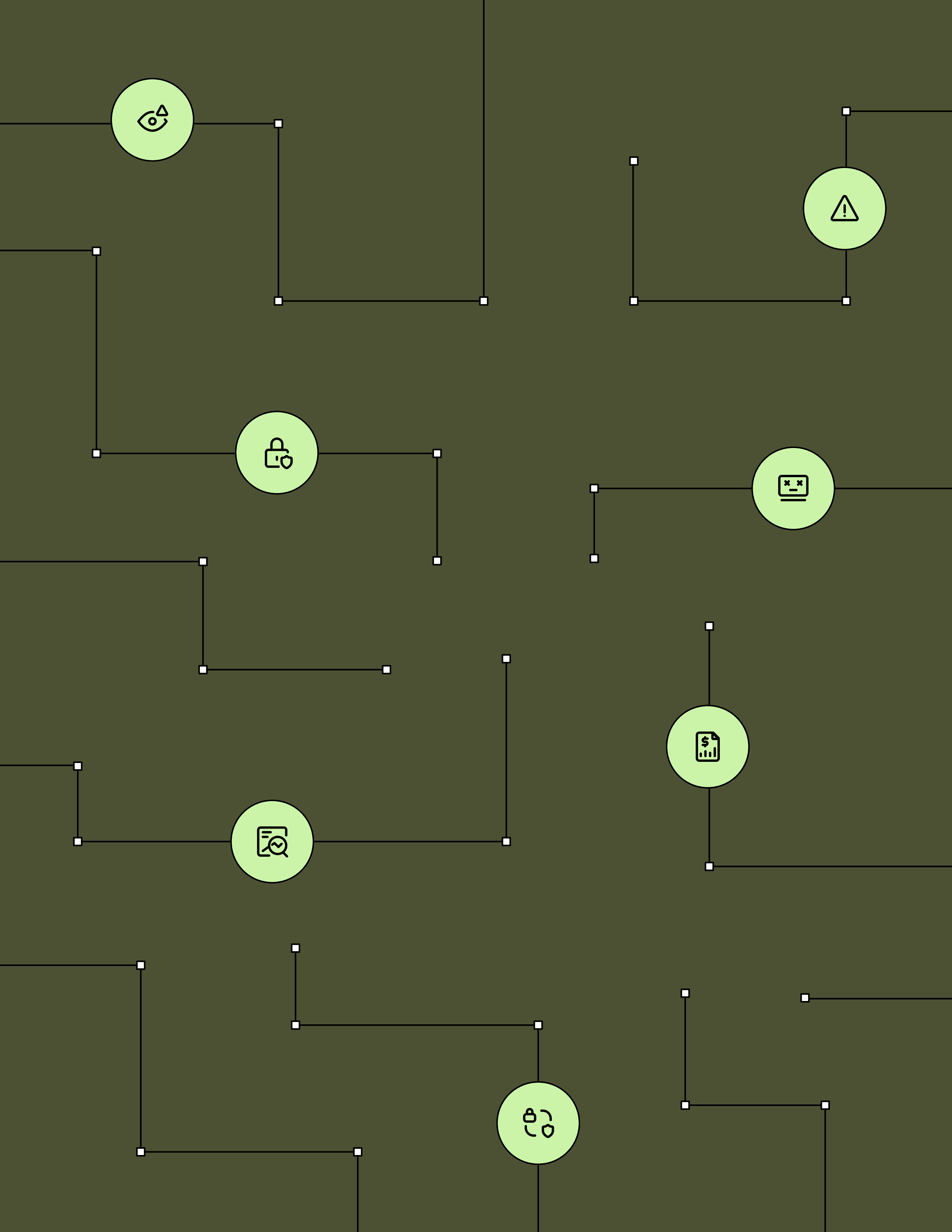


Table of Contents

YOUR RISK IS OUR RISK

Introduction

The first half of 2023 has once again seen an upheaval in the cybercrime industry. From Russian firms potentially licensing out advanced malware to **affiliate partners in the US and UK**,[1] to attacks against relatively unknown third-party SaaS suppliers scaling to **thousands of victim organizations at once**,[2] cybercrime actors are once again adeptly reacting to a shift in their market. As companies become more resistant to paying extortions, Resilience is seeing a move towards going after bigger fish and swimming upstream to hit vendors and bypass security controls. This has significant implications for those defending their organizations and trying to limit financial losses from these actors.

When we overlap Resilience's claims data with data from ransomware incident response partner **Coveware,**[3] blockchain analytics firm **Chainanalysis**,[4] security partner **Zscaler,**[5] and security firm **Sophos**,[6] it reveals five key findings that impact both network defenders and the cyber insurance industry at large.

KEY FINDING — 01

Enterprises are getting better at fighting ransomware extortions

Ransomware remains a leading cause-of-loss for our customers despite a continued decrease in clients electing to make an extortion payment. Ransomware notices comprised 16.2% of our total claims in 1H 2023, but only 15% of Resilience clients who experienced an extortion incident in this timeframe chose to pay to resolve an incident. This is less than half of the **2023 average rate of 39.5% observed by Coveware**[7] for the same period and is **down from 21.4% for Resilience Clients in 2022**.[8]

KEY FINDING — 02

Return of Big Game Hunting

Data from blockchain intelligence provider **Chainalysis**[9] shows that ransom costs continue to increase. This potentially indicates a return to "big-game hunting" tactics and an increase in the amount requested per ransom as criminal actors focus on bigger targets. Resilience tracks ransomware actors, revealing that ransomware-as-a-service actor **ALPHV/BlackCat**[10] made up 27.9% of all notices in Q1 of 2023. In Q2, **CL0P**[11] activity with Resilience surpassed them at 34.1% due to the MOVEit attacks.

KEY FINDING — 03

Third-Party Vendors Take Over as Lead Point-of-Failure

Bigger targets don’t necessarily have to mean bigger companies. The MOVEit attacks in May this year signaled ransomware actor tactics evolving towards targeting third-party vendors to scale their attacks. As of Q1 2023, our all-time claims data has consistently demonstrated that phishing attacks are our clients’ number one point-of-failure, at 23.4% of all claims. Post-MOVEit, vendor risk increased by 7% to become our clients’ most frequent point-of-failure at 28.9% of our all-time claims, while phishing remains at 23.1%.

KEY FINDING — 04

Cause-of-Loss Shifts from Ransomware to Encryption-less Extortion

Along with this more selective targeting of larger victims, threat actors are pivoting their approach to a new encryption-less extortion tactic, threatening to release sensitive data publicly. In Q1 of 2023, ransomware-related losses comprised 17.8% of claims notices at Resilience. After the MOVEit incident in Q2 of 2023, ransomware was replaced as the leading cause-of-loss. Resilience saw a 7% increase in vendor data breaches, jumping from 11.8% to 19.3% in Q2 of 2023, solidifying third-party vendor data breaches as the number one cause-of-loss.

KEY FINDING
— 05

Cyber Crime is Indiscriminate

While financial services have always been a target for cybercrime, healthcare-related companies make up the largest proportion of Resilience claims notices at 20.4% as of Q1 2023. However, in Q2 of 2023, manufacturing accounted for 39% of claims notices, dwarfing the traditional targets of finance and healthcare. We also saw a spike in incident notices from the education sector due to specific victims of the MOVEit attacks. Education clients made up 48% of Resilience's MOVEit victims, demonstrating how the downstream effects of losses at one or two vendors can lead to widespread incidents.

Monitoring Cyber Trends

We also dug into the MOVEit attacks of May 2023 and Resilience's response to the impact on our clients. This incident suggests that ransomware groups are now scaling attacks through vendors. It also highlights the significant costs of improperly managing third-party vendor risk. Based on our work with Resilience Solution clients, we found several ways to help build cyber resilience for any organization with a complex vendor risk environment.

This shift in Resilience claims data demonstrates how suddenly the threat landscape evolves as criminal actors create their own criminal market forces, **sometimes including regulating their affiliates**[12]. These forces directly affect the insurance market, as clients feel the impact through incidents, and insurers see the correlating rise in claims. Understanding the changes in cybercriminal business models can help organizations better prepare their security investments to limit financial damages & criminal profits.

THE THREAT LANDSCAPE EVOLVES AS CRIMINAL ACTORS CREATE THEIR OWN CRIMINAL MARKET FORCES, SOMETIMES INCLUDING REGULATING THEIR AFFILIATES.

2022
Claims
Report
In-house data demonstrates the successes of a Cyber Resilient mindset
resilience
→ CyberResilience.com

The Impact Of Cyber Resilience

As with the inaugural **Resilience 2022 Claims Report**,[13] we hope that sharing this data will help our clients and the security community better manage this dynamic challenge and build a more cyber resilient society.

REWRITING THE RULES OF RISK

Key Findings

Data from the Resilience Solution Engagements and Claims

As Resilience increases the number of clients continually engaged throughout their policy lifecycle, we can correlate data from claims notices with aggregated cyber hygiene data. This allows us to analyze how cyber incidents impact our clients and what resilience measures are having the most significant impact. For the first half of 2023, Resilience made the following pivotal observations based on analyses of our claims data, work with Resilience Solution clients, and public data from security firms, including **Chainalysis**,[14] **Coveware**,[15] **Zscaler**,[16] and **Sophos**.[17]

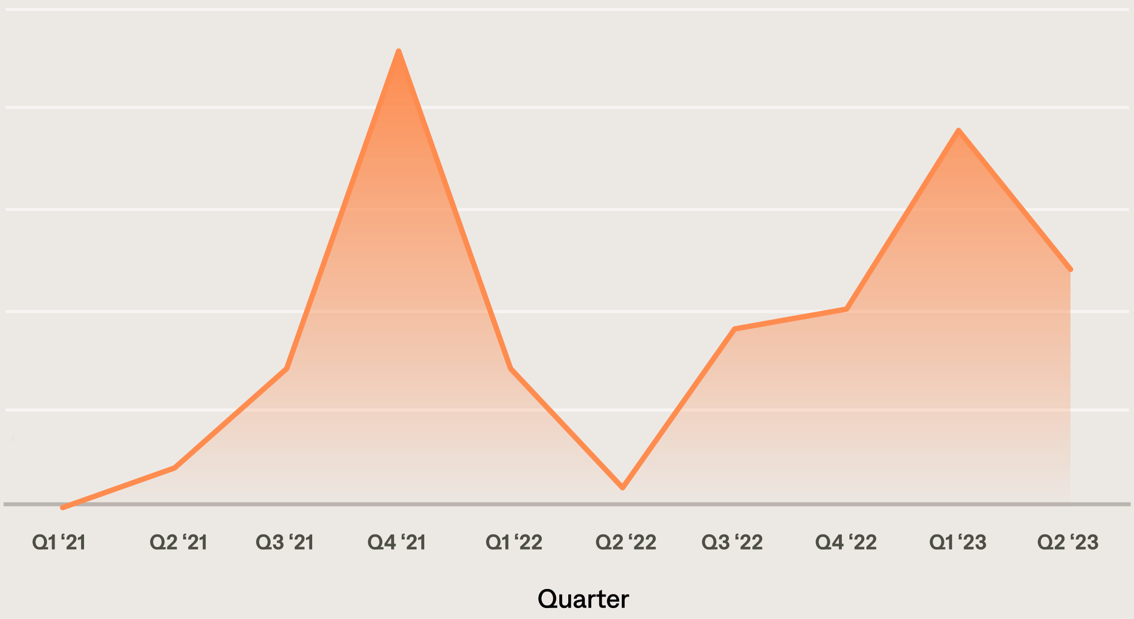
KEY FINDING — 01

Enterprises are getting better at fighting ransomware extortions

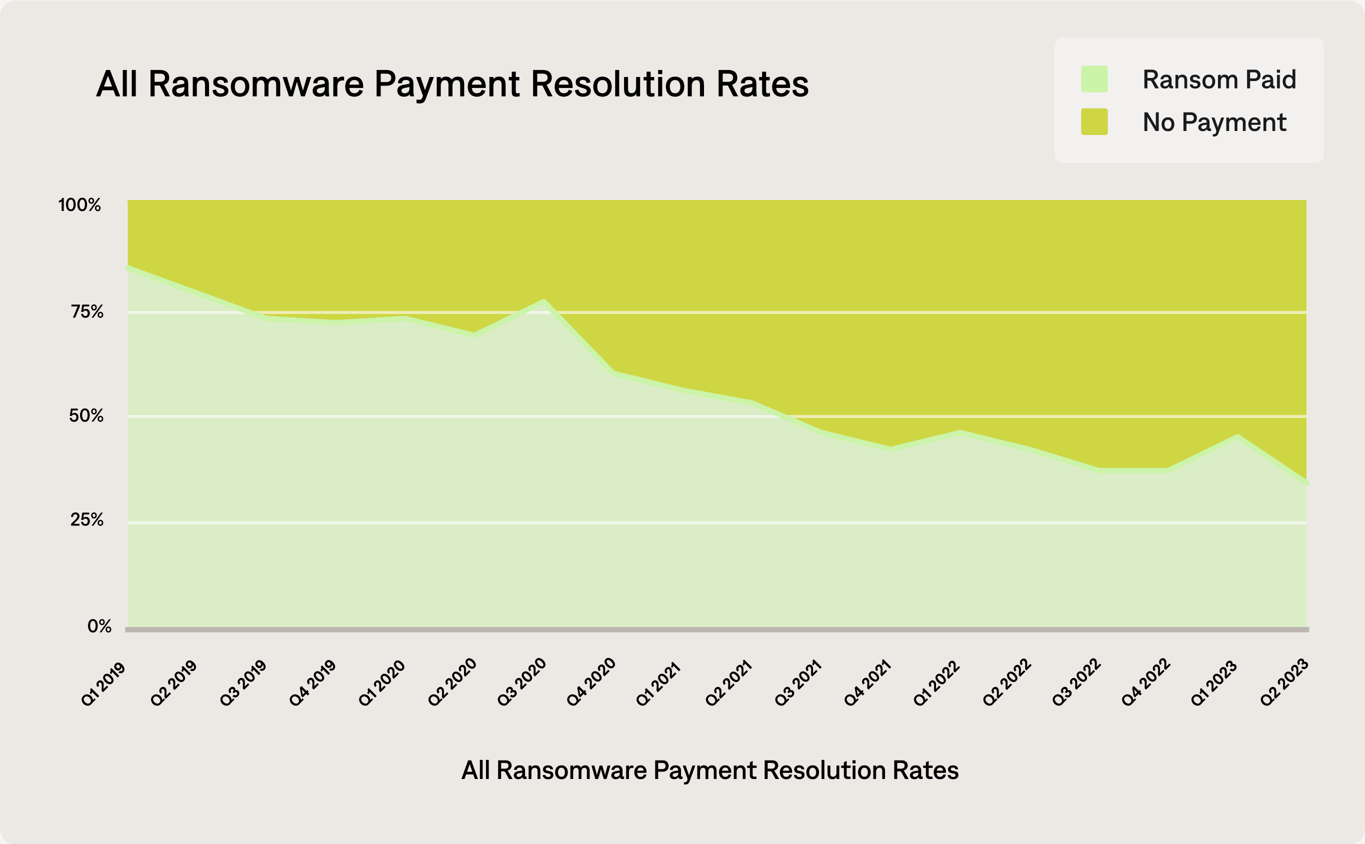
Resilience's internal claims portfolio reflects the trends observed by other security firms in the market, with ransomware remaining a top cause-of-loss overall. Resilience saw an 1100% increase in ransomware incident notifications from Q2 2022 to Q2 2023. The dip in 2022 correlated with the escalation of the hostilities in Ukraine and further highlights how the unique geopolitical situation potentially distracted or dissuaded cybercrime levels internationally. Additionally, while there was a 37% decrease in ransomware notices between Q1 2023 and Q2 2023, notices for 2023 have already reached 100% of 2022 levels and 84% of 2021 levels for Resilience. This sets 2023 as one of the most prolific years for ransomware on record.

2023 IS SET TO BE ONE OF THE MOST EXTENSIVE YEARS FOR RANSOMWARE ON RECORD

Ransomware-Related Notices by Quarter



A relative bright spot is data showing that, once again, fewer ransoms are being paid by Resilience's overall client base. Ransomware notices comprised 16.2% of our total claims in 1H 2023, but only 15% of the overall Resilience client base (both insurance only and Edge solution clients) who experienced an extortion incident in 1H 2023 elected to pay to resolve an incident. This is less than half of the 2023 average rate of **39.5% observed by Coveware**[18] for the same period and is **down from Resilience's overall client 2022 level of 21.4%**.[19]



*Coveware, Ransom Monetization Rates Fall to Record Low Despite Jump In Average Ransom Payments[20]

IN 68% OF ANALYZED CASES, THE BLUEPRINT'S RECOMMENDATIONS PROVED PIVOTAL IN IDENTIFYING THE CRITICAL POINT-OF-FAILURE LEADING TO LOSS, BASED ON A SAMPLE OF 38 ANONYMIZED RANSOMWARE CLAIMS.

To further understand why Resilience clients were more resilient to extortion attempts than the broader market, we partnered with the Institute for Security and Technology's Ransomware Task Force to analyze how our claims data matched up against their Blueprint for Ransomware Defense.[21]

The Blueprint was based on the Center for Internet Security's IG1 Safeguards to prioritize defenses against ransomware. With a sample of 38 anonymized ransomware claims, researchers could correlate that critical point-of-failure that led to a loss to the Blueprint's recommendations in 68% of the cases analyzed. While vendor risk led the way, software vulnerability, phishing, and privileged access were also core areas of security control that, if implemented properly, could have prevented a ransomware incident.

POINT OF FAILURE	RELEVANT BLUEPRINT SAFEGUARD	COUNT
Vendor	N/A	12
Software Vulnerability	7.3 7.4	8
Phishing	14.1 14.2 14.6	6
Privileged Access Management	5.4 6.1 6.2	6
Misconfigured/No MFA	6.3 6.4 6.5	3
System Misconfiguration	4.1 4.2 4.4 4.7	2
Backup Misconfiguration	11.2 11.3 11.4	1

*Institute for Security and Technology, Putting the Blueprint for Ransomware Defense to the Test[22]

As a member of the Ransomware Task Force, Resilience expands its ability to work with a broader community to understand and fight ransomware. Continuing to understand what security controls significantly reduce financial loss and, in turn, client incident costs is core to our model. This view not only defines our culture but drives our business model that your risk is our risk.

KEY FINDING — 02

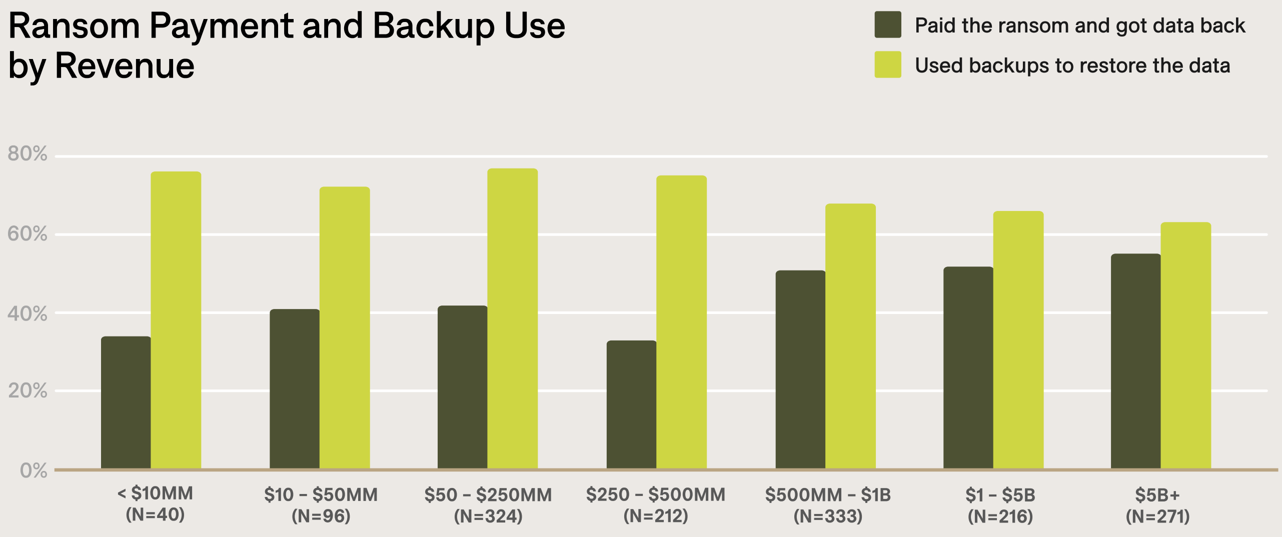
Ransomware actors are returning to big game hunting tactics

CRIMINALS SEEK LARGER PAYMENTS AND REFOCUS THEIR EFFORTS TOWARDS LARGER ENTERPRISES.

While **data from crypto analysis firm Chainalysis**[23] shows a stable attack rate of ransomware incidents for the beginning of 2023, there is a steep rise in the payment amount demanded per incident. As of mid-2023, victims have paid **$449.1 million**[24] to extortion groups. Should this pace continue, the total yearly figure could reach nearly **$900 million**.[25] This projection puts 2023 on pace to become the most financially damaging year for ransomware since 2021. The pivot to "**big game hunting**[26]" techniques means criminals seek larger payments and re-focus their efforts against larger enterprises.

According to a report by **Sophos**,[27] this tactic is proving successful as organizations with the highest revenue may be able to afford to pay larger extortion payments. The average cost of an extortion incident based on Sophos' survey has increased from **$812,380**[28] in 2022 to **$1,542,333**[29] in 2023. More organizations are paying higher amounts in 2023, with **40%**[30] of paying victims spending over $1 million this year compared to only **11%**[31] who paid more than $1 million in 2022.

Ransom Payment and Backup Use by Revenue



Ransom Payment and Backup Use by Revenue

*Sophos, The State of Ransomware 2023[32]

There is limited evidence to show why ransomware actors prioritize larger targets. However, when you combine the Chainalysis and Sophos data showing a rise in extortion payment volume and average cost with the decline in payment rate observed by Resilience and Coveware, changing criminal market dynamics may be driving these shifts in tactics. With the increased attention towards ransomware defense and pressure from law enforcement, a lower extortion success rate has probably forced criminals to target entities that provide a larger payout, such as the recent MGM and Caesars attacks.[33] Yet, as we have seen with MOVEit, investments in ransomware-specific controls can be bypassed and still lead to a data breach extortion from a third-party vendor.

ONLY 15% OF THE OVERALL RESILIENCE CLIENT BASE WHO EXPERIENCED AN EXTORTION INCIDENT IN 2023 ELECTED TO PAY TO RESOLVE THE INCIDENT.

KEY FINDING — 03

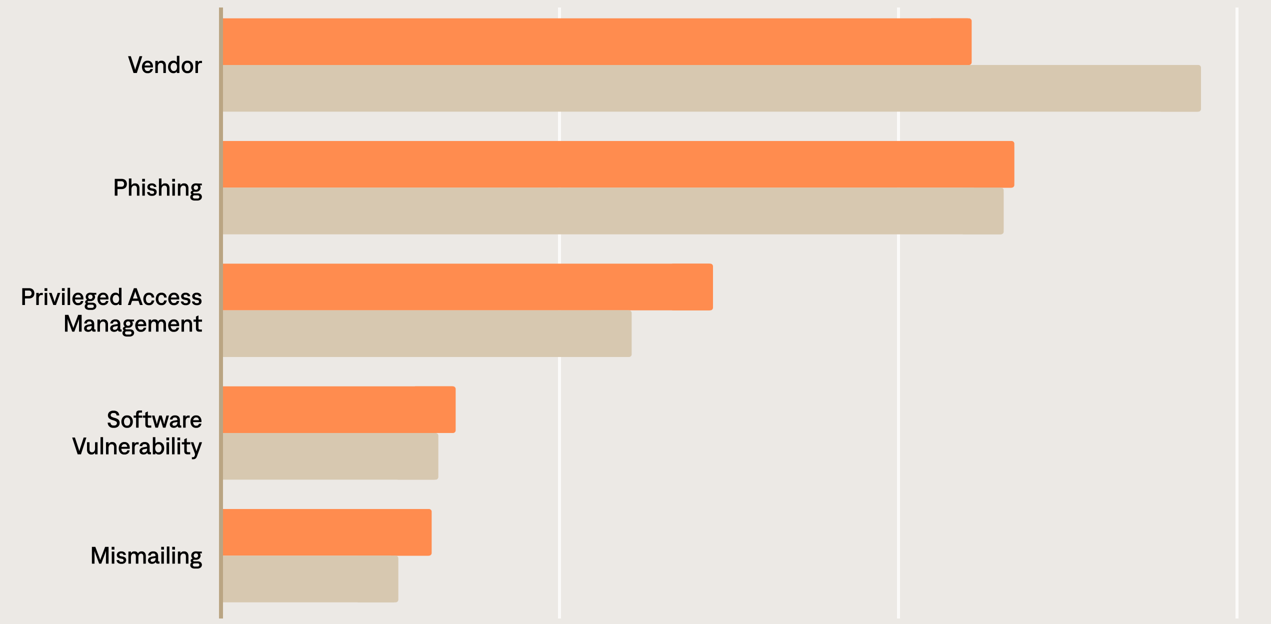
The risk from third-party vendors is now the leading incident point-of-failure

The MOVEit attacks represent an interesting shift in the threat landscape for ransomware. Resilience believes that leveraging the trusted access of third-party vendors to exfiltrate data, encrypt computer systems, and extort the vendor's customers signals a successful evolution in the ransomware actor toolkit. This aligns with ransomware actors moving towards "big game hunting" as payment rates decrease in volume. Supply chain attacks against trusted third-party vendors offer more expansive access to more victims and circumvent many known ransomware controls.

POST MOVEIT, THIRD-PARTY VENDOR RISK INCREASED BY 7% TO BECOME OUR MOST FREQUENT POINT-OF-FAILURE.

Our all-time claims data reflects this growing trend in attacks against vendors. Q1 2023 all-time claims data remained consistent in demonstrating that phishing attacks are our number one point-of-failure, responsible for 23.4% of claims notices. Given **phishing's role in initiating reconnaissance for most cyber attacks**,[34] it has featured prominently in claims data for most insureds. However, post-MOVEit, third-party vendor risk increased by 7% to become our most frequent point-of-failure at 28.9% of our all-time claims notices, while phishing remained consistent at 23.1%.

Top 5 Primary Point-of-Failure Notices between Q1 & Q2 2023



Resilience measures the "point-of-failure" for incident notices, tracking the initial security control failure that led to the cause-of-loss. In a vital feedback loop, this data not only helps Resilience underwriters improve in their assessment of risks but is also used to better inform our clients and the security community about how to prioritize investments in their cyber resilience.

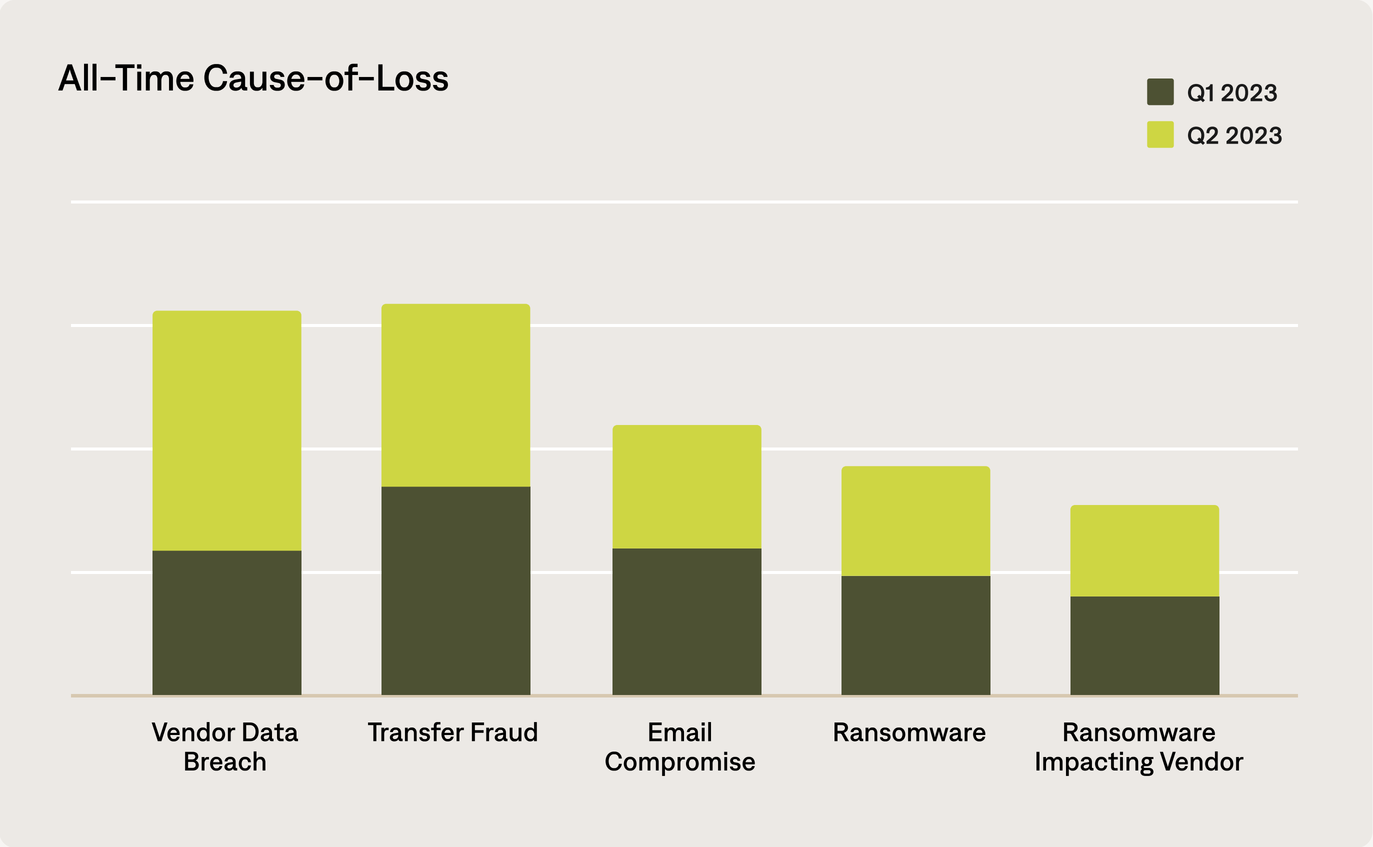
KEY FINDING — 04

Encryption-less extortion through vendor data breaches has caused more loss than ransomware encryption

ENCRYPTION-LESS EXTORTION ATTACKS HAVE INCREASED, WITH APPROXIMATELY 44 NEW RANSOMWARE FAMILIES USING THESE THREATS.

While ransomware criminals are turning to more significant ransom demands, they are also turning to more nefarious extortion tactics. A report by Resilience partner Zscaler[35] has noted that encryption-less extortion attacks have increased over the last year,[36] with approximately 44 ransomware families using double or multiple-extortion-based threats. Zscaler notes: **"...this tactic results in faster and larger profits for ransomware gangs by eliminating software development cycles and decryption support. These attacks are also harder to detect and receive less attention from the authorities because they do not lock key files and systems or cause the downtime associated with recovery."**

This strategy provokes payment by threatening the release of Private Identifiable Information of customers or even contacting secondary clients directly. A recent attack against the University of Manchester[37] showed bad actors contacting students directly and threatening to release information and research if the university did not pay. In another incident, private photos of cancer patients[38] appeared on the



Dark Web following the hospital's refusal to make an extortion payment. This trend is also present in Resilience's analysis of our all-time cause-of-loss dataset.

In Q1 of 2023, ransomware-related losses comprised 17.8% of claims notices. After the MOVEit incident in Q2 of 2023, Resilience saw a 7% increase in reports of vendor data breaches, jumping from 11.8% to 19.3% and solidifying third-party vendor data breach as the number one cause-of-loss. Upon closer examination, we find that the increase in vendor breach incidents is due to ransomware group CL0P's encryption-less extortion attacks against downstream clients of MOVEit.

Cause-of-Loss denotes the type of incident the insured has suffered (e.g., ransomware, insider threat, and accidental disclosure of personal data) and measures what part of an incident notice resulted in a financial loss for a Resilience client. This measurement is critical as cyber incidents' complexity complicates data collection.

> Vendor risk is one of the key topics we discuss with our insureds. Our team has drafted specific guidance to manage this risk, available to all our customers via our portal.
>
> Amanda Bevilacqua
>
> US Claims Operations Leader, **Resilience**

By understanding what part of an incident led to the most significant financial impact, we can help clients develop strategies for getting the highest return on investment from their security controls. This focus on limiting financial loss is core to our cyber resilience approach and has led to significant success with clients in fighting ransomware attacks.

KEY FINDING — 05

Cybercrime is indiscriminate, but some industries are more at risk

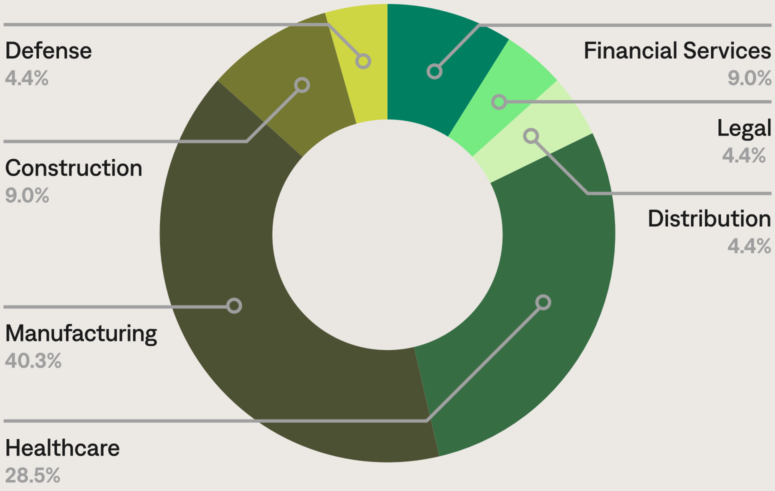
While financial services have always been a target for cybercrime, healthcare-related companies make up the most significant proportion of Resilience claims notices at 20.4% as of Q1 2023. This year has seen a **surge in cyber attacks against the healthcare industry**,[39] which typically has highly complex network environments and a low threshold for operational disruption. This combination has traditionally made them a significant target for ransomware criminals, **even during the global pandemic**.[40]

IN Q2 OF 2023, MANUFACTURING ACCOUNTED FOR 39% OF CLAIMS NOTICES

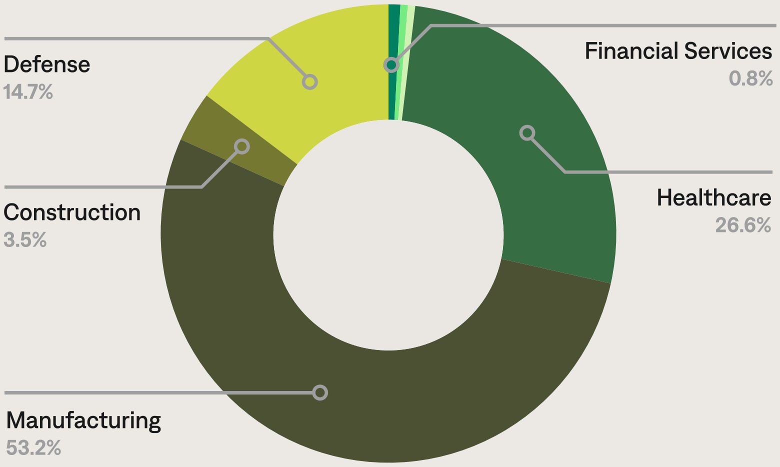
However, in Q2 of 2023, manufacturing accounted for 39% of claims notices, dwarfing the traditional targets of finance and healthcare. These findings are not indicative of the maturity of controls in the broader manufacturing industry. Rather, it's a byproduct of the often 24/7/365 operations of manufacturing businesses. This can make them more susceptible to incurring losses quicker when faced with an IT outage or cyberattack interrupting their business, as they may have limited capacity to disrupt operational production. As previously noted, many threat actors are aware of societal levers like this and are not afraid to pull on these to maximize financial gains.

Cause-of-Loss denotes the type of incident the insured has suffered (e.g., ransomware, insider threat, and accidental disclosure of personal data) and measures what part of an incident notice resulted in a financial loss for a Resilience client. This measurement is critical as cyber incidents' complexity complicates data collection.

Insured Industry: All Incurred Files



Incurred Amounts by Industry



Focusing on only the MOVEit portfolio, the education industry represents nearly half of Resilience's claims, at 48.1%. Financial services/banking follow at 30.8%, and healthcare at 9.6%.

48.1%	Education
30.8%	Financial Services/ Banking
9.6%	Healthcare

Though MOVEit was not a targeted attack in terms of industry, this data shows that Resilience's education clients were the most impacted. This can be attributed to **CL0P's targeting of the National Student Clearinghouse**[41] (which contains student data from thousands of colleges) and TIAA (a financial services provider for educators and academics), whose third-party vendor, PBI Research Services, was impacted by the MOVEit breach. The widespread impact to other organizations caused by CL0P's attacks on these entities further indicates the importance for companies to look beyond their own borders and consider the exposure presented by their supply chain when managing their cyber risk.

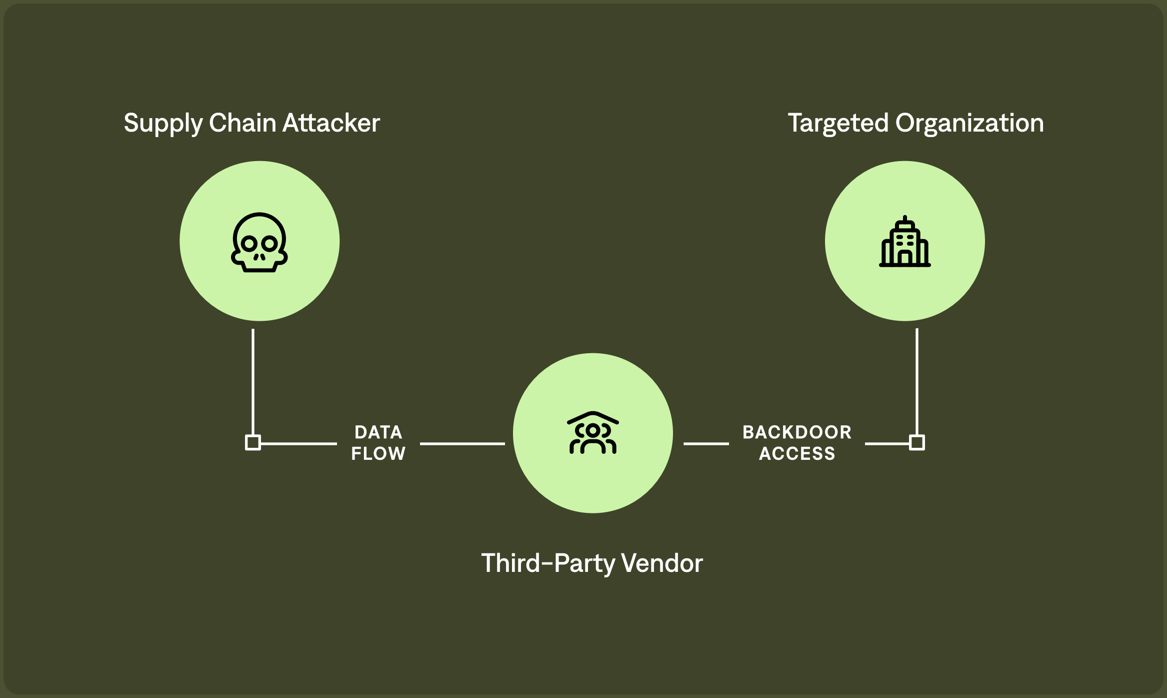
CASE STUDY

The MOVEit Attacks

Signals of a potential evolution in ransomware actor tactics

The shift towards “big-game-hunting” also coincided with a move by some threat actors to target supply chain vendors. Supply chain attacks help adversaries scale their operations by taking advantage of the trusted position of vendors to turn one breach into multiple incidents. This tactic is particularly effective in a post-pandemic world where companies have invested increasingly heavily in SaaS and cloud-based infrastructure to support remote work. The MOVEit breaches of June 2023 saw this supply chain-style attack matched with encryption-less ransomware tactics to impact millions of individuals and hundreds of organizations[42] worldwide.

The MOVEit breaches substantially impacted Q2 claims for Resilience's portfolio and hundreds of insurance companies globally. Due to the number of incident notifications from MOVEit-related cases, vendor risk has replaced phishing as our all-time key point-of-failure in Q2 2023 claims data.



Supply chain attacks are particularly damaging to both insurance providers and their client base as they are hard to identify and even harder to stop due to the incident taking place at a third-party. Because of this, while the MOVEit cases have caused widespread damage across various impacted direct victims, the full downstream scale of the incidents remains unknown.

MOVEit's Impact on Resilience

Resilience categorized the MOVEit incidents as direct or indirect to understand how client breaches occurred.

Direct hits were clients with the MOVEit software in their IT environment exposed through the initial breach.

Companies that did not integrate MOVEit but had vendors (or even vendors of vendors) impacted within their supply chain are considered indirect edits.

While CL0P, the ransomware gang behind the MOVEit attacks, stands to make **millions of dollars off the attacks,**[43] the volume of extortion payments made by victims has been lower for MOVEit incidents. It has also caused numerous incident responses, business interruption, data recovery costs, the risk of reputational damage, and potential legal and regulatory repercussions.

As of **July 18, 2023**, MOVEit claims were slightly more than 20% of Resilience's total claims portfolio.

1%	total claims were direct hits
99%	of notices were indirect hits
44%	were within our primary clientele
56%	were excess insurance accounts
None	of our clients impacted by MOVEit have had to pay a ransom to resolve the incident.

Vendor risk management is challenging, with no one-size-fits-all solution or instructions to defend your environment from your vendor's risk. However, there are best practices that organizations and their partners can take to limit the financial impact when a vendor breach takes place. Resilience has outlined its response to the incident to share some of these best practices with clients and partner firms.

MOVEit Timeline & Impact

In late May 2023, MOVEit was infiltrated by the Russian threat actor group CL0P (TA505). CL0P identified a previously unknown SQL injection vulnerability known as CVE-2023-34362.[44] This vulnerability within MOVEit Transfer led to escalated privileges and unauthorized access.

During the attack, MOVEit transfer web applications were infected with LEMURLOOT, a web shell that was leveraged to steal data from underlying MOVEit databases.

Shortly after organizations detected evidence of the attack, they patched the vulnerability. Despite this, MOVEit service users who had yet to install the patch on their networks remained at risk

MAY 31 2023

Progress publishes an advisory on a critical SQL injection vulnerability

JUNE 1 2023

Compromises begin to be noted; CISA publishes Security Advisory

JUNE 2–5 2023

Vulnerability ref assigned

Mandiant and Microsoft attribute to Clop Group or their affiliates, Lace Tempest

UK companies such as BA and BBC disclose breaches

Clop claim responsibility

JUNE 6–7 2023

Clop claim Clop group post a communication on their leak site demanding contact by June 14 to negotiate extortion payment in exchange for deletion of data

Resilience notifies customers they detect may be directly exposed to the vulnerability & publish a general advisory to the Platform

ROC engaged to leverage Resilience's combined expertise to support customers and assess exposure

JUNE 14 2023

Clop begin 'naming & shaming' organizations on their leaksite. A new deadline of June 21 is set for extortions to be negotiated before data is published.

Claims & Threat Intel monitor leaksite for Resilience insureds, proactive contracts to certain customers are undertaken

ONGOING

Claims Team continue to handle & track MOVEit exposure (volumes, industries, vendors)

Directly affected companies are in communication with Clop to nefotiate extoration payments

The incident ultimately impacted thousands of organizations and the data of more than **60 million people worldwide**.[45] Stolen information included personal identifying information such as dates of birth, social security numbers, contact information, banking and financial data, medical records, educational records, and more.

The CL0P ransomware group is expected to earn **$75-100 million in ransom funds**[46] through the exfiltration of this mass amount of data. According to Coveware's analysis, organizations are paying fewer ransoms. This cost was likely borne by a small group of victims who made larger payouts.

> MOVEit had at least 10x more direct victims than [both previous incidents involving Accellion and GoAnywhere, other file transfer software packages], so CL0P was able to focus on the largest and most likely to consider paying, even with well over 90% of victims not bothering to engage in a negotiation, let alone paying.[47]
>
> Bill Siegel
>
> Chief Executive Officer, **Coveware**

Resilience Responds

Resilience responded to the CL0P attacks by recommending that clients patch the MOVEit vulnerability **(CVE-2023-34362)**[48] as soon as possible and stop all HTTP and HTTPS traffic to the MOVEit Transfer environment. Security team members independently identified some clients as potential victims, utilizing similar research methods to how the CL0P group would identify targets. We then notified any clients who may have been directly exposed to the vulnerability and published a general advisory to our cyber risk platform.

Resilience continued to monitor publicly listed victims to notify clients of exposed data. This highlights our partnership approach to risk management.

Rather than waiting for an insured to file a claim, our Threat Intelligence team actively monitored the MOVEit actor's actions as they continued to post victim information. This partnership is core to a cyber resilience approach that focuses on limiting damages to all our clients so they can continue delivering value to theirs.

Andrew Bayers

Director of Threat Intelligence, **Resilience**

MOVEit
Client Use Case

Challenge

At the start of the MOVEit breaches, Resilience experts predicted widespread third-party impact but were still determining how this would impact our portfolio. As our clients began noticing their data leaked through MOVEit, our claims experts began working with them on notification and response strategies. Resilience's Threat Intelligence team continued to monitor the CL0P actor leak site for evidence of further client impact.

Problem

One client experienced an extortion demand of $15,000,000 after appearing on CL0P's MOVEit leak site. They called Resilience's 24/7 emergency hotline and contacted the Claims & Incident Management team, who confirmed that CL0P had exfiltrated thousands of files from the client's MOVEit platform. The client would need to review the files manually, notify any exposed clients, and engage incident response protocols to mitigate the event's impact.

Solution

The client determined they would not make an extortion payment and worked closely with their dedicated Resilience Incident Manager and Resilience Service Providers to proactively communicate with impacted individuals before CL0P published the data.

Resilience connected the client with a data mining specialist to assist with manually reviewing thousands of files. The client subsequently worked with public relations and crisis communication experts to deploy a robust communication program regarding their investigation status to outside parties and mitigate potential reputational harm.

Results

While a traditional insurance relationship focuses solely on the claims interaction, Resilience supplements its hands-on claims and incident management approach with a deeper partnership. Through our cybersecurity visibility and expertise, we were able to help this client determine the actual impact of the breach, notify their clients, and engage an incident response plan so that they did not make an extortion payment and reduced the impact of the incident.

What Organizations Should Know from the MOVEit Attacks

While MOVEit drastically impacted Resilience’s Q2 2023 claims data, it aligns with criminal motivations to adapt their tactics to shifting cybercrime market forces.

As efforts to share defensive tactics for ransomware increase in effectiveness, criminals are shifting to targeting third-party vendors with the same level of access to data as the victims themselves. While this lack of direct access limits their ability to encrypt their victim's data, it still allows for data extortion exposure. For CL0P, while this tactic appeared less successful at eliciting an extortion payment as a proportion of the number of compromises they achieved, the few times they were successful led to a massive payout.

> Ultimately, the majority of threat actors are financially motivated and will seek the most efficient and effective way to elicit a ransom payment, which may be driving why we are seeing more data extortions without encryption.

Mitch Gootnick

Director, Security Engagement & Claims, **Resilience**

Resilience has observed that a client’s ability to avoid making an extortion payment can be significantly strengthened by focusing on the following areas:

Thorough due diligence when selecting third-party vendors should be a core part of a cyber resilience program.

- ✓ Trusted third parties, such as SaaS vendors or business service providers, often regularly access sensitive company data. If an incident impacts them or their vendors, your organization’s data could be exposed “downstream” of the attack.
- ✓ Third-party vendors' access to critical data and infrastructure should be limited to business-critical needs. Security teams should also assess each vendor’s security practices, risk posture, and cybersecurity controls that are in place to protect themselves and any regulatory requirements of their customers, such as SOC-2, HIPAA, or GDPR. Third-party vendors should also provide proof of insurance to cover incident response or legal repercussions from a breach.

Continuous intelligence is needed before, after, and during an incident.

- ✓ While most security teams use threat intelligence for network protection, it is equally vital to ingest threat intelligence that can be leveraged during the chaos of an active incident.
- ✓ Threat actors may be employing tactics or malware against other organizations that are directly relevant to a holistic understanding of the decisions the organization is making during an incident.

Development and regular practice of a detailed and tailored Incident Response Plan (IRP) to thoroughly outline the steps required to recover from an incident.

- ✓ An IRP helps clients manage their regulatory compliance requirements, notification process, and data backup restoration, which can significantly drive high costs during an incident.
- ✓ A strong and tested IRP makes cyber incidents feel less unpredictable during a crisis. It helps reduce the human stress and business interruption impact that extortionists leverage to drive a ransom payment.

Prioritizing and contextualizing security control investment based on financial analysis of your organization's cyber value-at-risk.

- ✓ While most security teams use threat intelligence for network protection, it is equally vital to ingest threat intelligence that can be leveraged during the chaos of an active incident.
- ✓ Threat actors may be employing tactics or malware against other organizations that are directly relevant to a holistic understanding of the decisions the organization is making during an incident.

Connecting silos across risk management, cybersecurity, and financial leadership helps align strategic objectives that all focus on one goal.

- ✓ Traditionally, the security, risk management, and finance departments operate independently when addressing cyber risks. CISOs focus on technical threats and controls, Risk Managers purchase insurance, and CFOs look to minimize risk to the company’s balance sheet. However, successful organizations bridge the gaps between these silos to jointly plan investments against their cyber risk based on what will best serve the business.

- ✓ Joint planning between these three departments can help organizations understand how much risk they are buying down with their mitigation controls and risk transfer investments. Doing this in practice is a challenging feat. It requires strong communication and partnership between the three departments that should be actively encouraged by a company's executive leadership.

CONCLUSION

Understanding Data to Build Cyber Resilience

Cyber is a human-driven risk.

Unlike other lines of property and casualty insurance with risk models stretching back decades, cyber risk evolves as bad actors work to keep pace with mitigation strategies. The only way to combat a continuously changing threat is to constantly evolve risk mitigation.

Threat landscape is shifting.

As the threat landscape shifts, Resilience partners with our clients to help them understand the context and relevance to their organization and take steps to protect it. The impact of MOVEit demonstrates the importance of continuously monitoring your cybersecurity infrastructure, following threat alerts, addressing critical vulnerabilities, and maintaining a general awareness of your third-party vendors' risk posture.

We aim to provide **context**, **clarity**, **coverage**, **community**, and **counsel** to all our clients.

Most importantly, we help them **connect their internal silos of insurance, security, and finance to manage this risk holistically.**

The data consistently shows that organizations that can fight as a team and unite these mindsets fare dramatically better against modern, determined cybercriminals.

By offering data analysis to support a holistic review of cyber risk, we aim to align clients to a common goal:

↘ Building

Cyber Resilience

This material is provided for informational purposes only. Accordingly, this material should not be viewed as a substitute for guidance and recommendations of a trained professional. Additionally, Arceo Labs, Inc. d/b/a Resilience and its affiliates and subsidiaries (collectively, "Resilience") does not endorse any coverage, systems, processes, or protocols addressed herein. Any references to non-Resilience Web sites are provided solely for convenience, and Resilience disclaims any responsibility with respect to such Websites. To the extent that this material contains any examples, please note that they are for illustrative purposes only. Additionally, examples are not intended to establish any standard of care, to serve as legal advice appropriate for any factual situation, or to provide an acknowledgment that any factual situation is covered by Resilience products. This material is not intended as a solicitation of insurance coverage.

Glossary

Third-Party SaaS Provider

Vendor of a cloud based software platform that holds company data. Clients of SaaS vendors need to conduct a risk assessment of their service providers depending on the sensitivity, location, or regulatory requirements around the data they entrust the providers to process on their behalf.

Ransomware-As-A-Service

Ransomware actors are becoming increasingly efficient at launching attacks and managing extortions by dividing up the work stream among various parties. Often one actor (an access broker) will gain unauthorized access to a corporate network, then sell that access one a dark web marketplace to a second actor to use for extortion.

Phishing

One of the most common forms of attacking a network is to send an email with malware in an attachment or link and attempt to trick a target into opening it. Despite its common use, phishing is still a leading point of failure for cyber insurance claims.

Cause-Of-Loss

Resilience tracks what type of incident led to a claims notice, as well as the financial impact on the insured. This data helps identify trends in cybercrime tactics that can be useful when helping clients prioritize their defensive controls.

Supply Chain Attacks

Rather than approaching a well defended company's network directly, cybercriminals are beginning to attack "upstream" IT and SaaS service providers of their targets. As seen in the infamous Solarwinds attacks, it is hard to ensure that every vendor is following proper security controls and even the most well protected networks can be penetrated if a trusted vendor is compromised.

Transfer Fraud

One of the largest types of cyber crime involves defrauding companies to transfer funds to fake bank accounts. Often times leveraging sophisticated social engineering scams, attackers will wait for times when oversight is lax and often impersonate a trusted vendor to fool companies into wiring them funds. If caught quickly, often times law enforcement can assist in reversing these transfers.

Point-Of-Failure

Resilience tracks the technical security control that's believed to have led to claims incident reports. This information is helpful in understanding trends in cyber hygiene and how to model return on investment from security controls.

DDoS Attacks

A directed denial of service attack (DDoS) involves sending fraudulent internet traffic towards a specific website of server infrastructure. This malicious act can make a company's external IT infrastructure unavailable and cause a disruption to business or hurt their reputation with clients. Often criminals will extort a company to avoid or stop a DDoS attack. If caught quickly, however, their are many service providers that can reduce or filter the fraudulent traffic, limiting the impact of the attack.

Big Game Hunting

Big Game Hunting is a cybercriminals tactic that involves only attacking major organizations with large funds to pay an extortion. While these companies often have more substantial security programs, their larger revenue size means they can afford a larger extortion payment to resolve an incident. While paying a ransom may resolve an initial attack there is no guarantee attackers will not come back and attempt a second extortion once they know a victim. Is willing to pay.

Citations

1 Menn, J. (2023, September 29). MGM, Caesars Casino hacks point to an alliance of teens and ransomware gangs. The Washington Post. https://www.washingtonpost.com/technology/2023/09/22/mgm-hack-laid-to-star-fraud/

2 Schwartz, M. J., & Ross, R. (n.d.). Data breach toll tied to Clop group's moveit attack surges. Bank Information Security. https://www.bankinfosecurity.com/data-breach-toll-tied-to-clop-groups-moveit-attacks-surges-a-23153

3 Ransomware recovery first responders. Coveware. (n.d.). https://www.coveware.com/

4 The blockchain data platform. Chainalysis. (2023, October 11). https://www.chainalysis.com/

5 Home Page. Zscaler. (n.d.). https://www.zscaler.com/

6 Cybersecurity as a service delivered. SOPHOS. (2023, October 11). https://www.sophos.com/en-us

7 Siegel, B. (2023, July 21). Ransom monetization rates fall to record low despite jump in average ransom payments. Coveware. https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

8 2022 Resilience Claims Report. Resilience. (2023, May). https://unlock.cyberresilience.com/2022-claims-report

9 Team, C. (2023, July 12). 2023 crypto crime mid-year update: Crime down 65% overall. https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/

10 Mandiant. (n.d.). ALPHV ransomware affiliate targets vulnerable backup installations to gain initial access. https://www.mandiant.com/resources/blog/alphv-ransomware-backup

11 Ibid.

12 LockBit's New Regulations Sets Minimum For Ransom Demands. SOCradar. (2023, September 18) https://socradar.io/lockbits-new-regulations-sets-minimum-for-ransom-demands/

13 2022 Resilience Claims Report. Resilience. (2023, May). https://unlock.cyberresilience.com/2022-claims-report

14 The blockchain data platform. Chainalysis. (2023, October 11). https://www.chainalysis.com/

15 Ransomware recovery first responders. Coveware. (n.d.). https://www.coveware.com/

16 Home Page. Zscaler. (n.d.). https://www.zscaler.com/

17 Cybersecurity as a service delivered. SOPHOS. (2023, October 11). https://www.sophos.com/en-us

18 Siegel, B. (2023, July 21). Ransom monetization rates fall to record low despite jump in average ransom payments. Coveware. https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

19 2022 Resilience Claims Report. Resilience. (2023, May). https://unlock.cyberresilience.com/2022-claims-report

20 Siegel, B. (2023, July 21). Ransom monetization rates fall to record low despite jump in average ransom payments. Coveware. https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

21 Berg, L. (2023, August 28). Putting the blueprint for ransomware defense to the test. Institute for Security and Technology. https://securityandtechnology.org/blog/putting-the-blueprint-for-ransomware-defense-to-the-test/

22 Ibid.

23 Team, C. (2023, July 12). 2023 crypto crime mid-year update: Crime down 65% overall. https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/

24 Ibid.

25 Ibid.

26 Alder, S. (July 14, 2023). Return to big game hunting sees ransomware revenues soar. HIPAA Journal. https://www.hipaajournal.com/return-to-big-game-hunting-sees-ransomware-revenues-soar/

[27] Thomas, D. (2023, August 7). Report: Ransom payouts and recovery costs went way up in 2023. SC Media. https://www.scmagazine.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] State of Ransomware 2023. SOPHOS. (May 2023)https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

[33] 35. Kelleher, S. R. (2023, September 15). 2 casino ransomware attacks: Caesars paid, MGM did not. Forbes. https://www.forbes.com/sites/suzannerowankelleher/2023/09/14/2-casino-ransomware-attacks-caesars-mgm/?sh=146b1d02402d

[34] Phishing for information. Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1598/

[35] Zscaler 2023 ransomware report shows a nearly 40% increase. Zscaler. (n.d.-c). https://www.zscaler.com/press/zscaler-2023-ransomware-report-shows-nearly-40-increase-global-ransomware-attacks

[36] Kelly, R. (2023, June 29). Encryption-less ransomware: Warning issued over emerging attack method for threat actors. ITPro. https://www.itpro.com/security/ransomware/encryption-less-ransomware-warning-issued-over-emerging-attack-method-for-threat-actors

[37] lehighvalleylive.com, S. C. | F. (2023, March 14). Gang leaks Lehigh Valley Health Network Cancer Patient Photos as part of Data Hack. lehighvalleylive. https://www.lehighvalleylive.com/business/2023/03/gang-leaks-lehigh-valley-health-network-cancer-patient-photos-as-part-of-data-hack.html

[38] Kelly, R. (2023, June 29). Encryption-less ransomware: Warning issued over emerging attack method for threat actors. ITPro. https://www.itpro.com/security/ransomware/encryption-less-ransomware-warning-issued-over-emerging-attack-method-for-threat-actors

[39] Journal, K. N. W. S. (2023, September 8). Surge in hospital hacks endangers patients, cyber official says. The Wall Street Journal. https://www.wsj.com/articles/record-hacks-on-hospitals-endanger-patients-cyber-official-says-25a7ad3b

[40] Weiner, S. (2021, July 20). The growing threat of ransomware attacks on Hospitals. AAMC. https://www.aamc.org/news/growing-threat-ransomware-attacks-hospitals

[41] Schwartz, N. (2023, July 10). Which higher ed organizations have been affected by the MOVEIT data breach?. Higher Ed Dive. https://www.highereddive.com/news/higher-ed-organizations-moveit-hack-colleges-tiaa/685643/

[42] Abrams, L. (2023b, July 21). Clop gang to earn over $75 million from moveit extortion attacks. BleepingComputer. https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/

[43] Abrams, L. (2023b, July 21). Clop gang to earn over $75 million from moveit extortion attacks. BleepingComputer. https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/

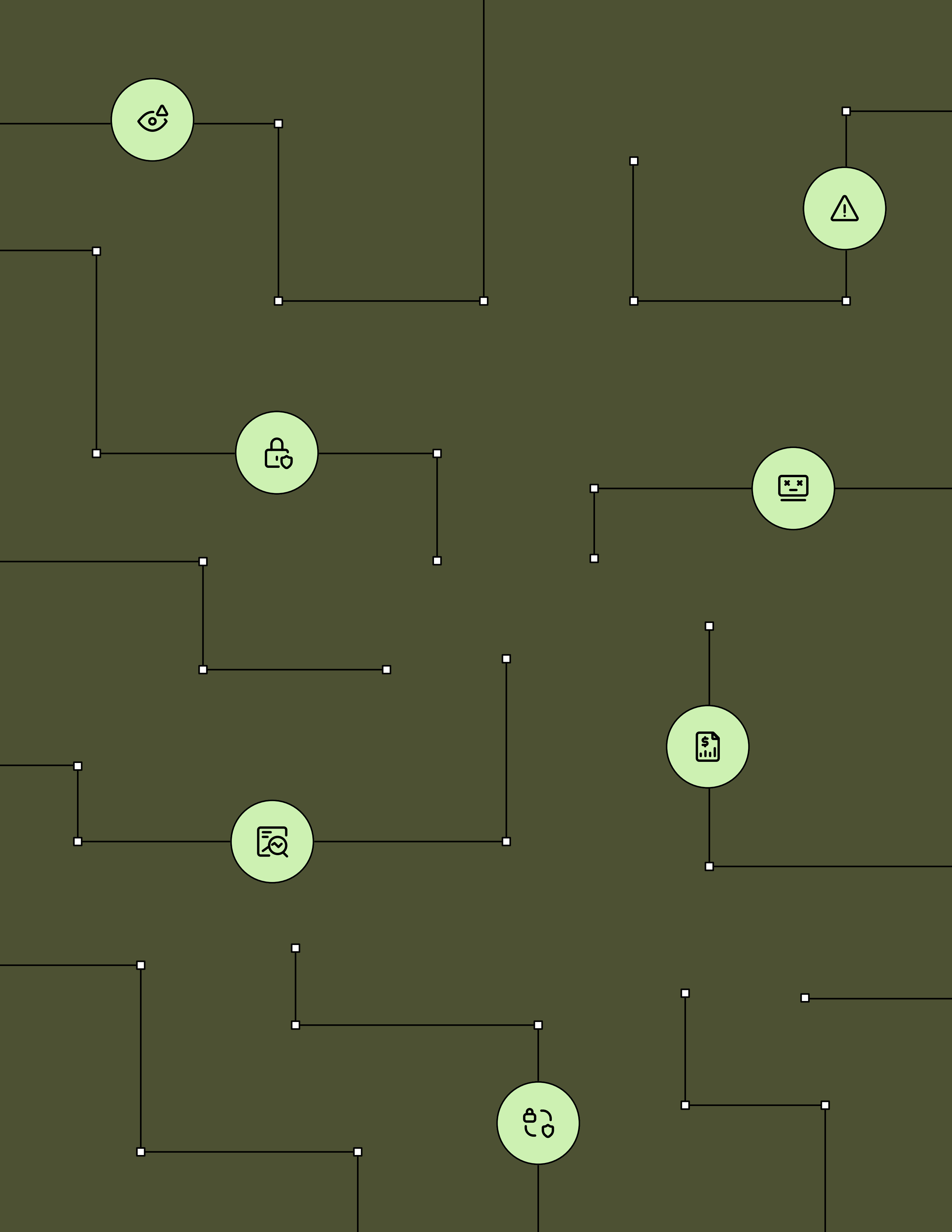
[44] National Vulnerability Database: CVE-2023-34362 Detail. United States Department of Commerce National Institute of Standards and Technology. https://nvd.nist.gov/vuln/detail/CVE-2023-34362

[45] Page, C. (2023, August 25). Moveit, the biggest hack of the year, by the numbers. TechCrunch. https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/

[46] Abrams, L. (2023b, July 21). Clop gang to earn over $75 million from moveit extortion attacks. BleepingComputer. https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/

[47] Abrams, L. (2023b, July 21). Clop gang to earn over $75 million from moveit extortion attacks. BleepingComputer. https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/

[48] National Vulnerability Database: CVE-2023-34362 Detail. United States Department of Commerce National Institute of Standards and Technology. https://nvd.nist.gov/vuln/detail/CVE-2023-34362



resilience

Your risk is our risk.