

RELIAQUEST[®] 

Annual **Cyber-Threat** Report

2025

Executive Summary: 2024 At A Glance

Incident Metrics and Breach Details

3 Minutes

Lowest Mean Time to Contain (MTTC)
Using Automated Response Playbooks

48 Minutes

Average Time from Initial Access to
Lateral Movement, or "Breakout Time"

**Two-
Thirds**

Of Critical Hands-on-
Keyboard Incidents
Involved Legitimate
Software

Inadequate Logging

Top Cause of Breaches

85%

Of Incidents Involved
Compromised Service Accounts

Initial Access Techniques

Phishing

Top Initial Access Technique
for the 2nd Year Running

30%

Of Phishing Messages
Involved Credential Harvesters

1 in 4

Active Intrusions Started
with Exploitation of
Public-Facing Applications

45%

Of Hands-on-Keyboard Intrusions Began with
Abuse of External Remote Services Like VPNs

100%

Of Deployed MFA Controls Bypassed via
Session Hijacking in Successful Business
Email Compromise (BEC) Attacks

Malware and Threat Actors

SocGhosh

Top Malware Thanks to New Python Tactics

AsyncRAT

Rises From 4th to 2nd Place Among Top Malware Threats

Microsoft Teams

Abused for Social Engineering by Black Basta

United States

Region with the Most Targeted Victims

**Manufacturing &
Professional Services**

Sectors with the Most Targeted Victims

478,000

Lumma Listings on
Criminal Marketplaces

5,253

Organizations Named
on Ransomware
Data-Leak Sites

4 hr 29 min

Fastest Exfiltration
Time

80%

Of Breaches Featured
Exfiltration vs 20%
with Encryption

3 Recommendations Organizations Can't Afford to Ignore



Incorporate AI and Automation into Security Operations

Attackers are adopting AI and automation to supercharge common attacks. That means it's no longer optional for organizations to use AI and automation to their own advantage.

When integrated into a security operations platform, these technologies can help contain threats rapidly, drive down response times, and allow security teams to focus on tackling more complex challenges.

Agentic AI, which can autonomously handle alerts end-to-end, shows particular promise for SecOps.



Barricade Common Entry Points: Phishing, Drive-By Compromise, Public-Facing Assets, and External Remote Services

Phishing and drive-by compromise were the top initial access methods, while public-facing assets and internet-facing external remote services fueled active intrusions.

Mitigate these risks by securing remote services (e.g., with client-based certificates) and monitoring public-facing assets.

Patching promptly is key; attackers are moving faster than ever, fueled by an abundance of available credentials.



Eliminate Blind Spots: Deny Attackers Any Opportunity

Most "hands-on-keyboard" breaches resulted from insufficient logging and unmanaged devices. Manage your attack surface and eliminate blind spots by deploying an endpoint security solution across all assets.

Enable detailed logging for all devices, including endpoints and servers, to capture user activity, system changes, and network traffic.

Review log retention periods for hot and cold storage and establish clear procedures for retrieving cold storage logs during investigations.

Table of Contents

Introduction: 2024 in Review—Fast Threats Demand Faster Responses	1
Inadequate Logging Responsible for Most Breaches in 2024	2
Breaking In: The Trends Shaping Initial Access Tactics	3
Old Habits Die Hard: Attackers’ Most Frequent Initial Access Techniques	4
Phishing Trends: The Tactics Honing Cybercrime’s Most Reliable Weapon.....	5
Session Hijacking Bypassed MFA in Every Successful BEC Incident in 2024.....	8
Social Engineering: How Attackers Weaponize Microsoft Teams.....	10
GreyMatter Automations for Combatting Email Attacks	12
Critical Entry Points: VPN and Voice Phishing Among Most-Successful Techniques	13
Abuse of External Remote Services Led to 45% of Hands-on-Keyboards Intrusions	14
23% of Active Intrusions Initiated via Exploitation of Public-Facing Applications	16
Voice Phishing Behind 14% of Breaches.....	18
Access via Cloud Accounts and Trusted Relationships Achieved in 9% of Intrusions	20
GreyMatter Automations for Combatting Unauthorized Access.....	22

SocGholish Secures Top Spot Again in 2024 Malware List	23
SocGholish Persists in First Place with Python	24
ScreenConnect Abuse Propels AsyncRAT to Second Place.....	26
Copy, Paste, Compromised: Lumma Rises to Third Place with Innovative Tactics	28
GreyMatter Automations for Combatting Malware	30
48 Minutes to Breakout: Unmasking Post-Compromise Trends	31
An Attacker’s Route to Control	32
Why RDP Became the Tool of Choice for Lateral Movement	32
Valid Accounts, Invalid Intent: Easy Access to Privilege Escalation.....	34
The Adversary’s Toolkit: Post-Exploitation Essentials.....	36
GreyMatter Automations for Combatting Legitimate Tool Abuse.....	38
Ransomware Decoded: Exfiltration Is the New Encryption	39
Exfiltration Outpaces Encryption in Modern Breaches.....	39
Ransomware in 2024: Increased 11.9%, Hit New Highs.....	41
GreyMatter Detections and Automations for Combatting Ransomware.....	45
Next Steps: A CISO’s Checklist	46

Introduction: 2024 in Review—Fast Threats Demand Faster Responses

In 2024, speed became more important than ever in defending against cyber threats.

48 Minutes

Attackers are moving at unprecedented speeds—last year, upon gaining initial access, they achieved lateral movement in an average of 48 minutes and managed to exfiltrate data in as little as 4 hours.

Attackers are also getting better at adapting to and evading the latest security controls, making the adoption of AI and automation imperative for organizations. Using AI and automation to tackle initial access attempts not only strengthens defenses but also empowers analysts to focus on what matters most: **detecting and investigating the stealthiest and most impactful intrusions.**

Though attackers are moving faster, they're still using tried-and-tested methods like phishing to achieve initial access. They cast a wide net, indiscriminately targeting organizations with minimal effort and often causing significant damage. The year's high count of disclosed vulnerabilities provided cybercriminals with entry points, while software suppliers remained a top target as a way to infiltrate organizational networks.

Ransomware and extortion remained critical threats compared to 2023, but the dynamics have shifted. Affiliates splintered into smaller groups, while leaked ransomware source code on cybercriminal forums sparked a wave of new attackers on the scene, with many focused entirely on data exfiltration. The result is a more fragmented, but no less dangerous, ransomware ecosystem.

In a world of accelerated attacks, automation is the ultimate ally for defenders. ReliaQuest customers using Automated Response Playbooks in 2024 saw a dramatic improvement in response times, with the fastest mean time to contain (MTTC) cyber threats as low as 3 minutes. In comparison, customers yet to implement Automated Response Playbooks reported an average MTTC of 6.3 hours.

Additionally, in August 2024, ReliaQuest launched its first-of-its-kind AI agent for security operations, further speeding up containment of threats with better accuracy and consistency. By seamlessly handling routine Tier 1 and Tier 2 tasks and executing response actions securely, the GreyMatter AI Agent eliminates errors and delivers unparalleled efficiency in accelerating remediation times, allowing security teams to upskill by focusing on more critical tasks.

By automating 100% of the investigation process—including data aggregation, analysis, and response—the **GreyMatter AI Agent has reduced the average MTTC for ReliaQuest customers to less than 5 minutes.**

At ReliaQuest, we remain committed to helping organizations strengthen their security posture and take control of their defenses.

Our Annual Cyber-Threat Report presents an in-depth analysis of the most critical cyber threats observed from January 1 to December 31, 2024. Find out the emerging tactics, techniques, and procedures (TTPs) employed by adversaries and benchmark your security defenses against our findings to identify key areas for improvement.

Security leaders can use these findings to refine their cybersecurity strategies, address coverage gaps, and enhance employee awareness of evolving threats.

Inadequate Logging Responsible for Most Breaches in 2024

Our analysis of 2024 customer breaches revealed **five critical security control failures** at the core of these incidents. Neglecting or underestimating these foundational security practices leaves organizations exposed—regardless of how sophisticated or varied an attacker’s methods may be. Addressing these weaknesses within networks is essential to avoid becoming the next target.



Before advancing to sophisticated response strategies, fortifying foundational defenses is critical. Ensure comprehensive endpoint security coverage—prioritizing critical assets—and implement robust logging to maintain full visibility across the network.

To counter the risks of social engineering and stolen credentials, enforce strong identity controls like device-based certificate authentication. Bolster these efforts with regular penetration testing, including social engineering scenarios, to uncover and address procedural gaps—particularly in help-desk operations. Though basic, these steps form the bedrock of a resilient security posture.

Breaking In: The Trends Shaping Initial Access Tactics

Initial access is the critical first step of every cyber attack.

It's the moment attackers breach any configured defenses to gain a foothold in a network and set their plans into motion.

In this section of the report, we analyze key findings from GreyMatter customer alerts to reveal how attackers attempted to gain network access and which techniques proved most effective.

First...

We'll examine phishing and business email compromise (BEC) attacks, which are increasingly bolstered by advanced tactics like bypassing MFA and abusing Microsoft Teams for social engineering.

Then...

We'll dissect the initial access techniques with the highest success rates, including targeting external remote services (boosted by a 250% surge in initial access brokers [IABs] offering VPN access), compromising cloud accounts, and conducting voice phishing attacks.

Finally...

We'll review the top malware shaping today's threat landscape, with "SocGhosh" leading the charge.

Read On To

find out the tactics adversaries are using to compromise systems, learn how to defend against these threats, and discover how ReliaQuest empowers enterprises to stop incidents before they escalate into full-scale breaches.

Old Habits Die Hard: Attackers' Most Frequent Initial Access Techniques

The consistency in top-ranked initial access techniques from 2023 to 2024 highlights their effectiveness and reflects attackers' strategy of indiscriminately targeting a wide pool of victims.

Phishing and drive-by compromise remain go-to methods, powered by the scalability and affordability of phishing-as-a-service (PaaS) and malware-as-a-service (MaaS) offerings.

These services allow attackers to flood inboxes with phishing campaigns or lure victims to malicious websites through manipulated search engine results.

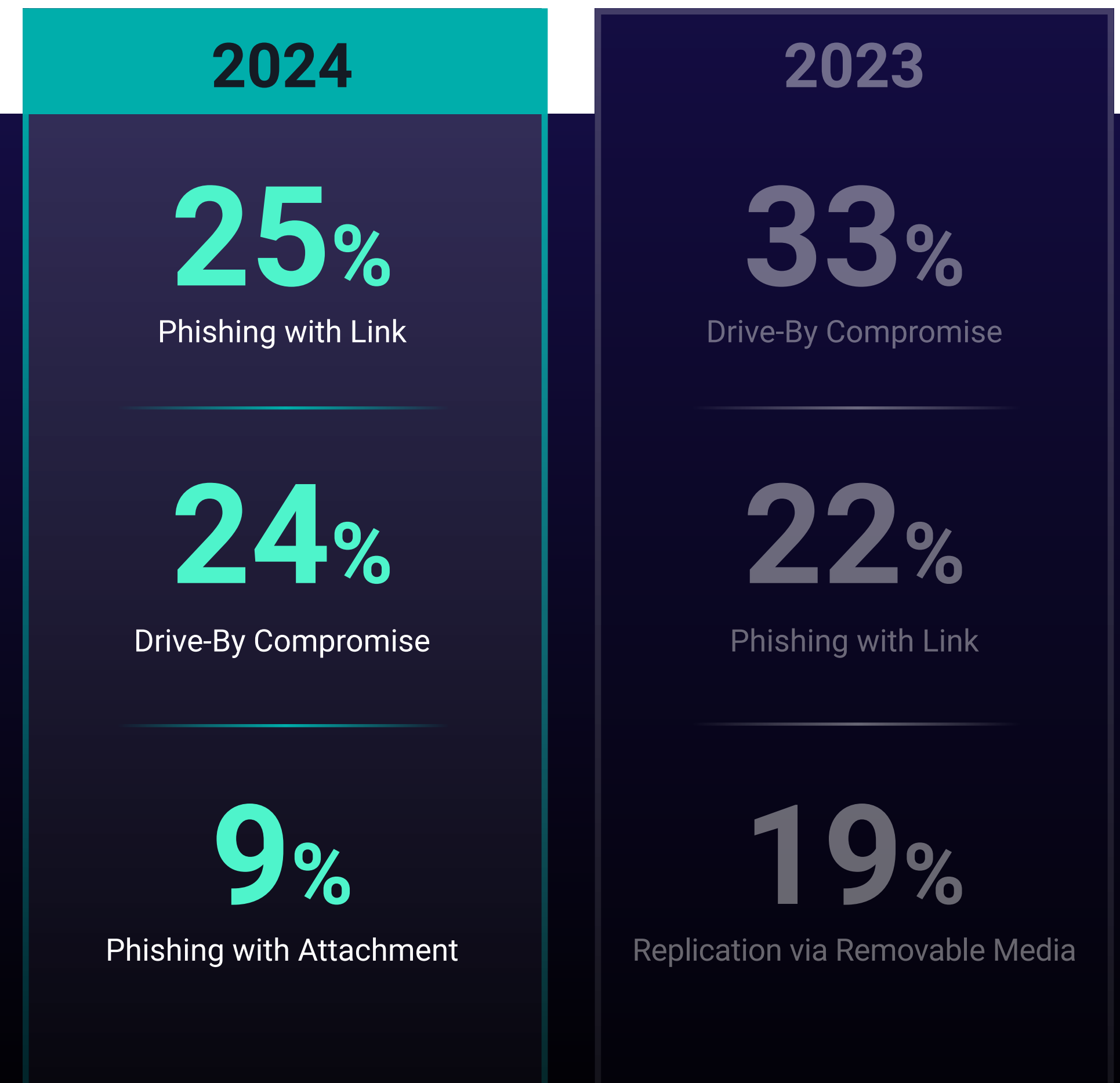
While most initial access attempts are blocked early, when successful, these broad-spectrum attacks can pave the way for more advanced threats, highlighting the importance of understanding their mechanics.

Through our analysis of phishing emails reported to the GreyMatter Phishing Analyzer, we uncovered:

- ✓ The most prevalent types of malicious email sent
- ✓ The trigger words used to boost email open rates
- ✓ The tactics designed to trick recipients into clicking malicious links


We'll also look at one of the top concerns for CISOs—BEC—by demonstrating how attackers leverage simple phishing techniques to bypass MFA and execute these high-impact attacks.

Finally, we'll explore adversaries' weaponization of a trusted communication platform to worm their way into networks.



Phishing Trends: The Tactics Honing Cybercrime's Most Reliable Weapon

To expose the tactics behind the number-one cyber threat facing enterprises today, we turned to the [GreyMatter Phishing Analyzer](#):



A tool designed to automate the triage of employee-reported phishing emails, enabling faster identification and remediation of malicious activity.

This data is collected from phishing emails that evaded detection by email security gateways and provides insight into adversaries' phishing techniques.

Data from the GreyMatter Phishing Analyzer revealed that nearly 30% of phishing messages that made it past traditional email security tools involved credential harvesters, often disguised as fake Microsoft login portals.

We also identified any financial-themed keywords attackers used to create a sense of urgency and the trusted platforms they abused to make phishing campaigns appear more legitimate.

Knowing what to look for in phishing emails not only helps predict attacker strategies but also sharpens employee training, turning your workforce into a powerful first line of defense against phishing attacks.



Nearly 30% of Reported Phishing Emails Contained Credential Harvesters

Credential Harvesters

Dominated as the most reported category of malicious emails, with fake Microsoft login portals being the most common type. These emails lure victims to fraudulent websites designed to steal credentials, often to lay the groundwork for larger attacks like BEC.

Enhanced by AI, credential harvesting emails now feature much more polished language, fewer errors, and highly convincing designs, making them an increasingly effective and scalable weapon for cybercriminals.

Scam Emails

Crafted to solicit money or extract confidential employee information, scam emails were also widespread in 2024.

Reconnaissance Emails

Another common type of email sent was single-word or blank emails—known as reconnaissance emails—which are used to verify whether an account is active (i.e., no bounce-backs are received) or to gauge the likelihood that the inbox owner might respond.

Malware-Laden Emails

Attackers also sent a significant volume of malware-laden emails containing attachments or URLs to deploy malicious files upon download.

URGENT:

Keywords That Hook

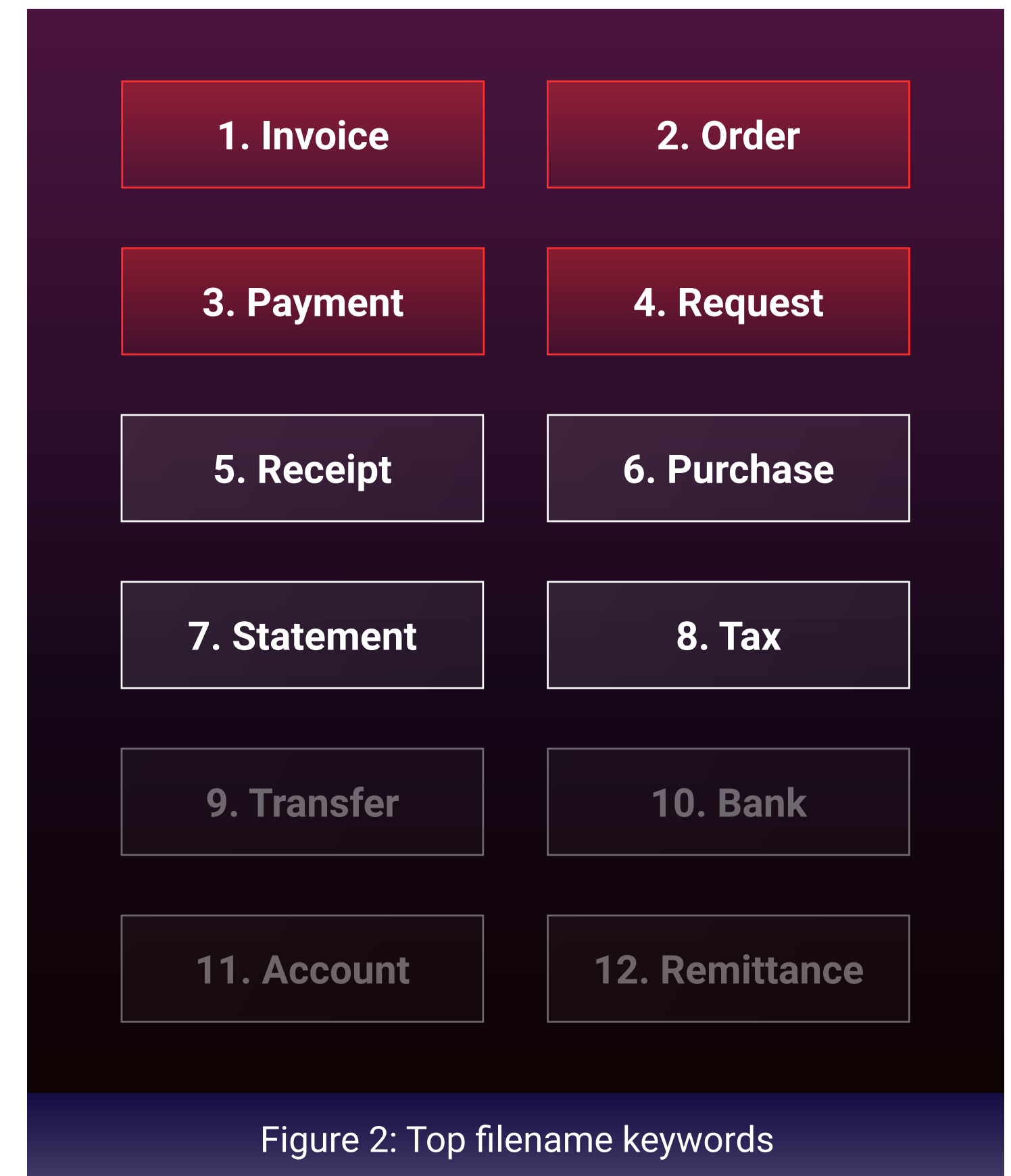
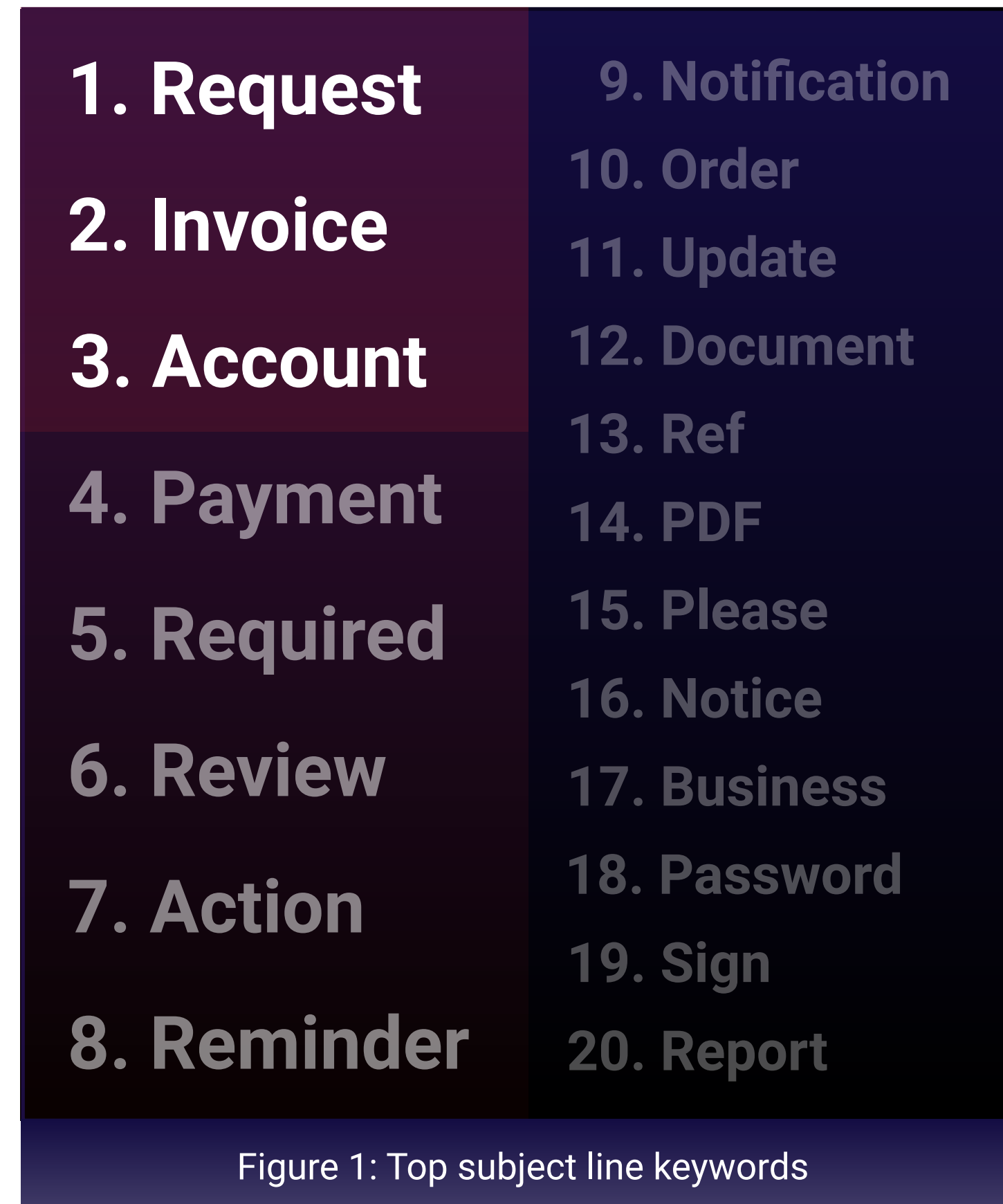
Attackers use deceptively urgent language to manipulate victims into engaging with phishing emails.

They understand that a sense of urgency often overrides caution, causing recipients to act hastily without evaluating risks.

Financial keywords like “payment,” “invoice,” and “statement” dominated phishing email subject lines and filenames last year.

This tactic is particularly effective because phishing emails that mimic financial statements blend seamlessly into routine tasks, like processing invoices or reviewing account statements, catching users off guard.

Training end users to **pause, verify suspicious emails, and think critically** before taking action is key to disrupting attackers’ strategies and reducing the success of phishing attempts.

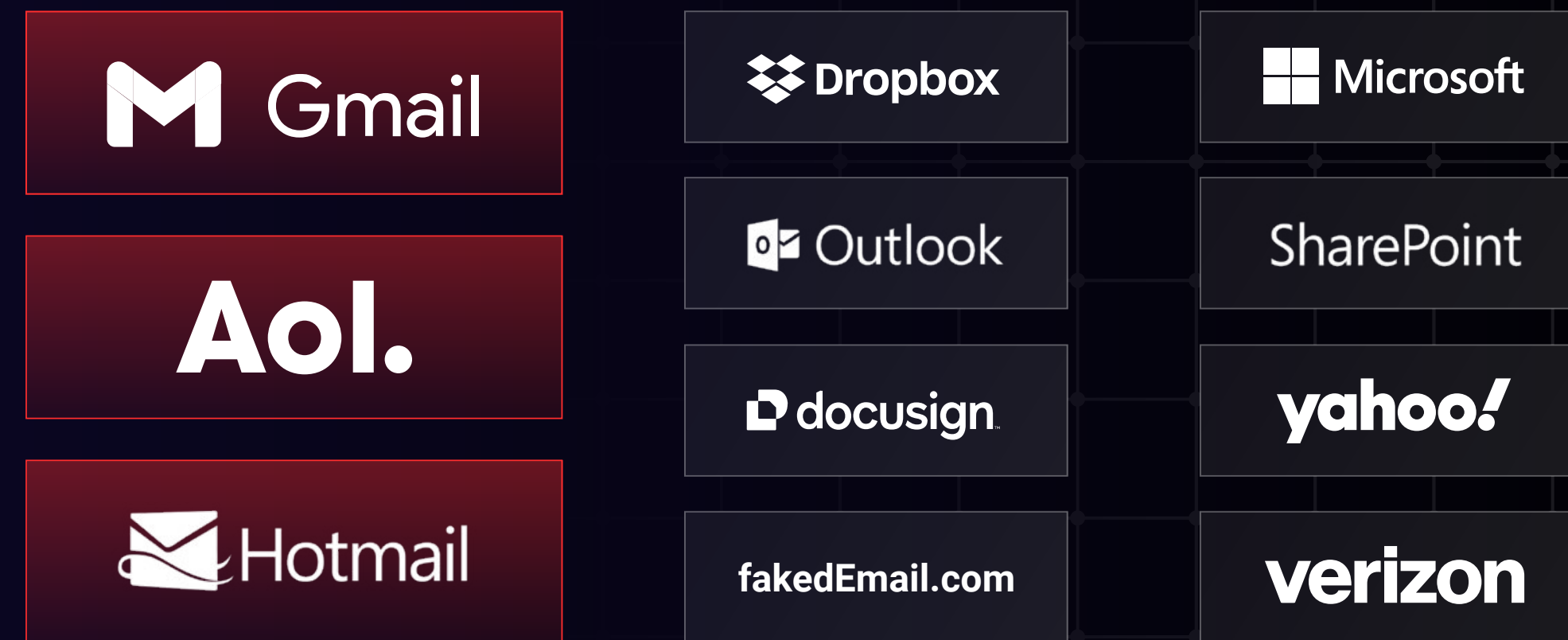


Attackers' Favorite Email Providers and File-Sharing Platforms

Free email providers like Gmail and file-sharing platforms like Dropbox and Docusign were among the top tools used in phishing campaigns last year.

These platforms are highly trusted and widely used in business, making it easy for attackers to exploit the trust users place in them.

Phishing emails leveraging these tools appear more genuine and are therefore harder to spot.



Free email services allow attackers to remain anonymous by enabling them to quickly create new accounts and replace blocked ones, while file-sharing platforms are perfect for hosting malicious files or hiding phishing links.

To counter these tactics, businesses must fine-tune their email security tools to catch suspicious activity that hides behind a veil of legitimacy. Employees must also carefully scrutinize links or emails from trusted platforms, as attackers rely on this very trust to bypass defenses and infiltrate organizations.

Take Action

Against Phishing

- ✓ Rather than just blocking specific file types, configure email security tools to inspect the contents of HTML files for malicious links, scripts, or QR codes.
- ✓ Configure email security tools to flag unusual activity from trusted platforms like free email providers and file-sharing services.
- ✓ Use banners to highlight attention-grabbing terms like "payment," "invoice," and "statement" to educate employees on common phishing tactics.

Session Hijacking Bypassed MFA in Every Successful BEC Incident in 2024

BEC is one of the most dangerous methods attackers use to achieve their financial objectives.

These attacks often start with a phishing email—frequently sent from a compromised partner—containing a link to an attacker-controlled website. This site acts as an adversary-in-the-middle (AiTM), intercepting MFA requests and session tokens from the legitimate login portal.

With the stolen session tokens, the attacker can authenticate to the service without needing credentials or access to the MFA-enrolled device, effectively bypassing both.

To stay under the radar while executing their strategies, attackers often use commercial VPNs to mask their activities:

- Express VPN
- Surfshark VPN
- Nord VPN
- SurfEasy VPN
- Hide My Ass VPN
- Private Internet Access VPN

The combination of a high success rate and devastating impact makes BEC a top security concern for organizations.

By analyzing real-world compromises of corporate employee email accounts, we've identified the key tactics attackers rely on, what makes them so successful, and, most importantly, the steps defenders must take to stop them.

[Here are our key takeaways](#) ↓

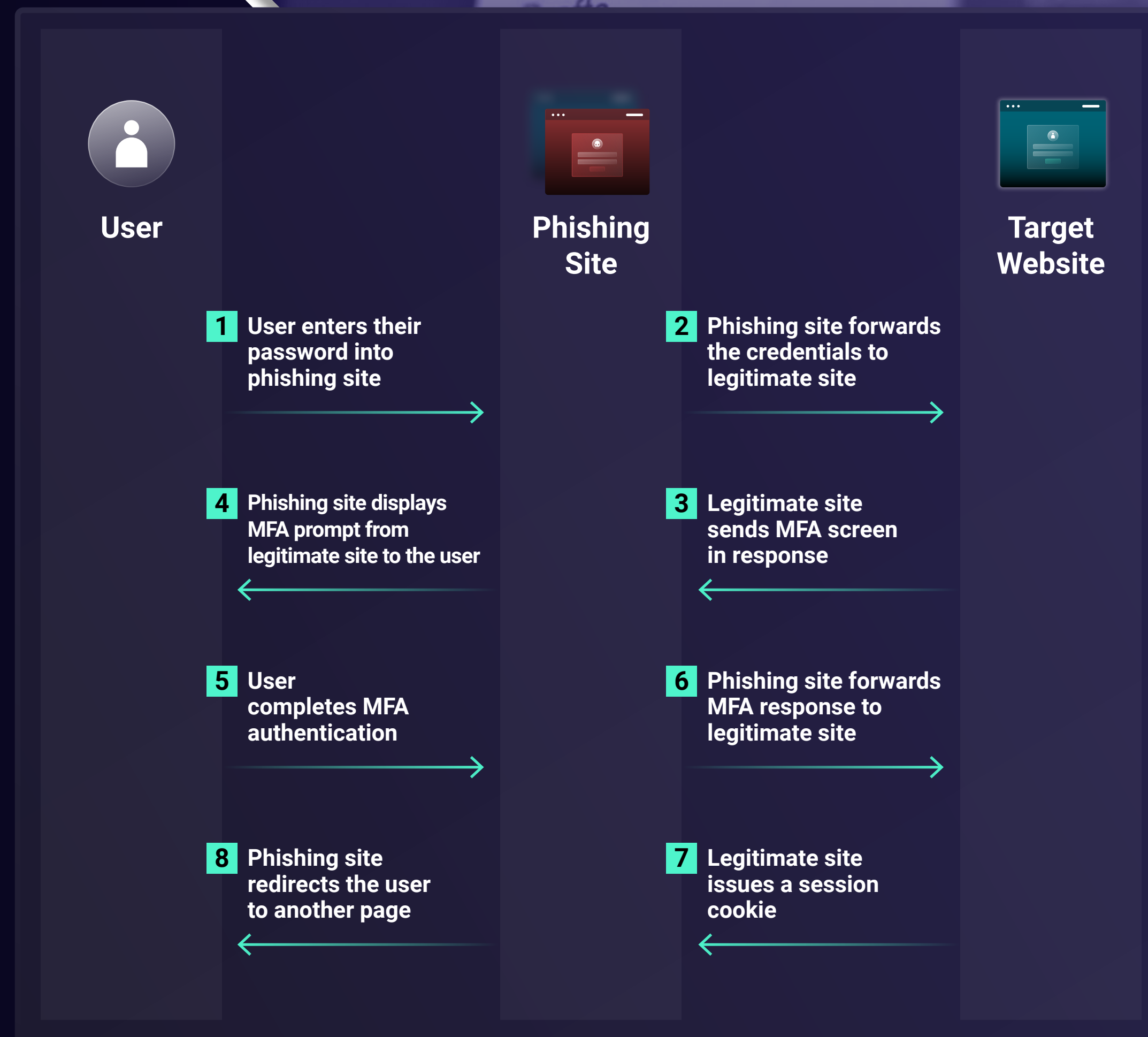


Figure 4: How AiTM phishing bypasses MFA and steals session tokens



MFA Isn't Foolproof: In every incident where MFA was configured, attackers managed to bypass it by stealing session tokens through AiTM phishing. Session token interception is now a standard feature in modern phishing toolkits, reducing the level of technical expertise required to bypass MFA.



Trust Is a Weapon: 9 out of 10 phishing emails came from hacked accounts at trusted partner organizations, exploiting established relationships to successfully deceive targets.



Attackers Hide Their Tracks: After hijacking a session, attackers used VPNs to conceal their location, allowing them to bypass location-based detections and evade regional access-control policies.



Compromised Accounts Spread the Attack Internally: In 80% of cases, compromised accounts were used to send phishing emails to other employees within the same organization.

Business Email Camouflage

In February 2024, we identified a compromised email account belonging to a customer in the information sector. The account had been compromised after a user inadvertently provided their credentials in response to a phishing email impersonating a legitimate IT consulting company.

We promptly informed the customer's security team, who contacted the user to verify the activity. However, the threat actor, posing as the user, misled the security team by claiming the activity was legitimate.

We immediately followed up with the customer to confirm that the account had been compromised and that the security team had unknowingly been communicating with the threat actor. The attacker's access was swiftly revoked, and the credentials for the compromised account were changed.

Take Action

Against BEC

- ✓ Train users to recognize common phishing keywords, understand procedures for reporting suspicious emails, and be aware that even trusted partner email accounts can be compromised and used for phishing attacks. Incorporate internal phishing scenarios into security awareness training to help employees effectively identify and respond to these threats.
- ✓ Block anomalous top-level domains (TLDs), such as ".ru," ".xyz," and ".ly," as these TLDs are commonly used to host credential harvesters.
- ✓ Implement conditional access policies to block authentication from noncompliant devices. Deploy phishing-resistant MFA, such as Fast Identity Online (FIDO), for administrators or other high-risk accounts. Additionally, shorten session timeouts for Microsoft 365 to minimize the window of opportunity for attackers to exploit stolen session tokens and maintain access.

Social Engineering: How Attackers Weaponize Microsoft Teams

Black Basta Exploits Microsoft Teams for Initial Access

Throughout 2024, ReliaQuest observed the ransomware group “[Black Basta](#)” employing a new social engineering tactic that leverages Microsoft Teams for initial access.

By compromising legitimate Microsoft Entra ID tenants or creating fraudulent ones, the group impersonates IT support or help-desk staff to deceive targeted users into engaging with malicious Teams messages.

Black Basta typically begins the attack by spamming users with hundreds of phishing emails. Shortly after, the attackers follow up with either a phone call or a Teams chat message (see Figure 5).

These messages often originate from external accounts with display names like “Help Desk” or “Support Team,” intentionally crafted to appear both legitimate and urgent to increase the likelihood of user interaction.



Once attackers establish contact, they manipulate victims into downloading remote monitoring and management (RMM) tools, such as Quick Assist or AnyDesk, under the guise of providing support sessions. These tools grant attackers the ability to install and execute malicious files, facilitating initial access to the organization’s network.



In some cases, attackers have also been observed persuading users to download malicious files themselves—such as scripts or executables—via QR codes, further expanding their arsenal of social engineering techniques.

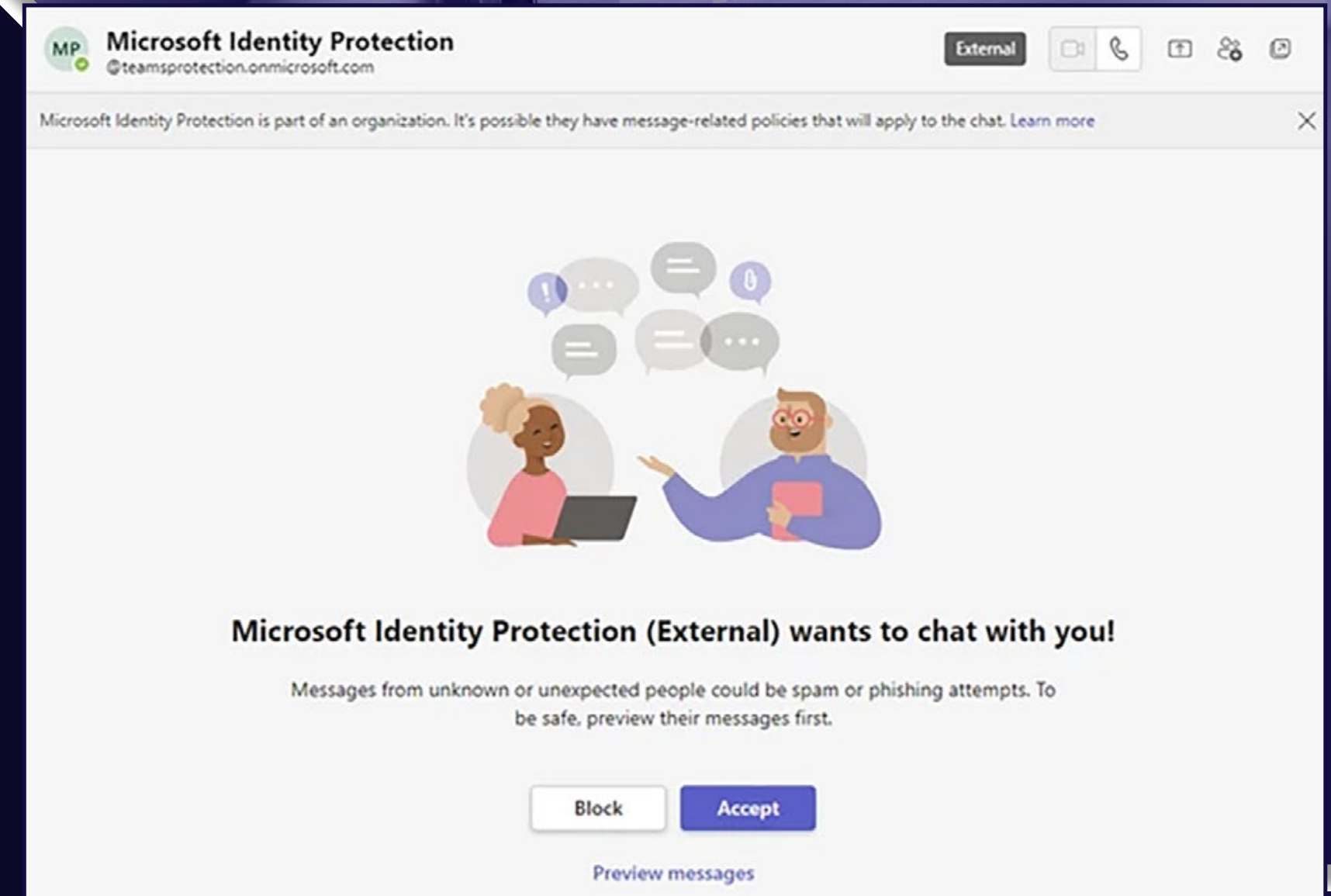


Figure 5: Sample external Microsoft Teams message request (source: microsoft[.]com)

Manipulating Trust: Social Engineering Through Familiar Platforms

As this is a relatively new technique, most organizations have yet to take appropriate defensive measures. Unlike phishing, which is commonly mitigated with security controls and user training, this approach targets less-secured communication channels where users are more likely to engage with malicious activity.

We predict with high confidence that this technique will gain popularity among cybercriminals, largely due to the ease of creating new Microsoft Entra ID tenants, making these accounts disposable and easily replaced if blocked. This tactic highlights why social engineering remains one of the most effective forms of initial access.

By exploiting human trust in familiar platforms, threat actors significantly increase their chances of success compared to traditional phishing techniques.

As Black Basta and other threat groups continue to innovate, organizations must prioritize addressing these vulnerabilities. Implementing strict controls on external Teams communication, monitoring for anomalous activity—such as messages originating from unexpected locations or using suspicious naming conventions—and providing robust user training are critical.

Without these preventative measures in place, these increasingly sophisticated social engineering campaigns are likely to be successful.

Take Action

Against Microsoft Teams Social Engineering

- ✔ Limit Microsoft Teams messaging to approved external tenants only to block malicious actors from impersonating legitimate organizations.
- ✔ Train employees to identify fake support messages, avoid unverified downloads, and recognize QR code scams on platforms like Teams and Slack.
- ✔ Deploy advanced email filtering solutions, such as email security gateways, spam filtering, and advanced threat protection for email, to detect and block mass spam campaigns before they reach user inboxes.

GreyMatter Automations for Combatting **Email Attacks**

To counter the evolving tactics behind phishing, BEC, and social engineering attacks, ReliaQuest offers its customers a proactive defense strategy through its **Automated Response Playbooks**.

These Playbooks automatically contain and respond to threats, significantly improving MTTC and minimizing potential damage.

Additionally, GreyMatter offers out-of-the-box and custom threat hunting packages that are built to identify specific attacker techniques and behaviors.

By leveraging the end-to-end automation capabilities of GreyMatter, organizations can detect, respond to, and neutralize threats in minutes.

Recommended Automated Response Playbooks



Block Domain: Prevents access to a specific malicious domain, which disrupts phishing campaigns, malware delivery, and command-and-control (C2) communications.



Block Email Domain: Blocks emails originating from malicious domains, reducing phishing attempts and preventing attackers from using compromised or fake domains to target users.

Recommended Threat Hunting Packages



Phishing—Microsoft Teams: Identifies malicious messages from external domains in Microsoft Teams to detect and block phishing attempts that deliver credential-harvesting links or malicious files through Teams. By monitoring these messages, customers can stop attackers from using tools like “TeamsPhisher” before users interact with harmful links, reducing the risk of compromised accounts or data breaches.



Phishing—Spearphishing Attachments: Detects spearphishing attachments with uncommon but business-relevant file extensions. This threat hunting package leverages telemetry from email gateways and endpoints to identify malicious emails that mimic legitimate communications. This allows customers to quickly spot and block these threats, minimizing attackers’ foothold in the network and reducing the risk of compromise.



Hygiene—MFA Modifications: Monitors unauthorized actions, such as threat actors registering new MFA devices or tricking users into resetting their MFA. By auditing MFA changes, customers can ensure MFA is implemented correctly, confirm that changes follow proper procedures, and quickly identify suspicious activity.

Critical Entry Points: VPN and Voice Phishing Among Most-Successful Techniques

In 2024, GreyMatter continued to serve as a critical line of defense, swiftly detecting and containing the vast majority of initial access attempts observed. Among all the attempts analyzed in the previous section, only a tiny fraction—just 0.02%—managed to bypass its defenses.

While these successful techniques represent only a very small proportion, they demand close attention, as they allowed threat actors to engage in hands-on-keyboard activity, taking real-time control of compromised systems.

In this section, we focus on the critical 0.02% of successful attempts, examining how attackers used social engineering tactics in addition to exploiting external services, public-facing applications, cloud infrastructure, and trusted relationships.

We've also included real-world examples to illustrate the damage these techniques can inflict and outlined clear steps to mitigate these risks.

By prioritizing defenses against these methods, organizations can significantly reduce the risk of attacks escalating into lateral movement, privilege escalation, or data exfiltration.



Figure 6: Successful initial access methods in 2024

Abuse of External Remote Services Led to 45% of Hands-on-Keyboard Intrusions

Last year, threat actors were most successful in gaining network access via external remote services like VPN portals, Remote Desktop Protocol (RDP), and virtual desktop infrastructure (VDI).

These trusted services act as gateways to an organization's internal network, allowing attackers to slip past traditional perimeter defenses and gain direct access to sensitive systems and data.

Once inside, adversaries exploit the trust inherent in these services to operate under the radar, carrying out data theft, lateral movement, or ransomware attacks—all while evading detection. In some cases, they also plant backdoors for future intrusions.

External remote services rely on valid account credentials for authentication, but attackers can easily overcome this hurdle by:

Brute-Forcing
Passwords

Mining Data
Breaches

Purchasing Credentials
from Online Marketplaces

IABs are the middlemen in this ecosystem, selling stolen credentials—often obtained through information-stealing malware (infostealers)—to various threat actors, including [ransomware affiliates](#), so they can launch devastating attacks with ease.

Once exposed, data may be leaked or sold online, leaving organizations to face severe reputational and regulatory consequences.

The rise in attacks targeting external services has fueled a growing demand for accesses, and IABs are meeting this demand at premium prices:

- IAB listings offering access via VPNs surged by 250% between 2023 and 2024.
- The average “buy now” price for these listings climbed 46%, increasing from \$2,370 to \$3,455.



Figure 7: IAB listings in 2024 by sector

While all industries are targeted for initial access, certain sectors are more heavily sought after than others.



Manufacturing, for example, is a prime target due to its reliance on legacy systems, extensive use of remote access, and prioritization of operational continuity over credential hygiene best practices. If IABs can easily infiltrate a network in a particular industry, they are more likely to target other organizations in the same sector, assuming they have the same weaknesses in security practices.

Take Action

Against VPN Attacks

- ✔ Implement device-based certificate authentication for VPNs to verify devices before they connect.
- ✔ Combine this with MFA for an added layer of security against unauthorized access.
- ✔ Enforce conditional access policies for VPN authentication, such as location and device compliance.

23% of Active Intrusions Initiated via Exploitation of Public-Facing Applications

2023

2024

Between 2023 and 2024, adversaries targeting public-facing applications **increased by 3%**, a trend highly likely fueled by the 2,000-plus critical vulnerabilities identified last year.¹

These critical vulnerabilities—which are remotely exploitable, require no privileges or user interaction, and are characterized by low complexity—are an attractive opportunity for attackers.

With minimal effort, a single exploit can breach multiple organizations, delivering significant returns on investment for cybercriminals.

Although fewer critical vulnerabilities were identified in 2024 compared to the 4,000-plus seen in 2023, a surge in proof-of-concept (PoC) exploits likely leveled the playing field, giving lower-skilled attackers more opportunities to strike. PoC exploits are easily deployable bits of code designed to demonstrate vulnerabilities, making it easier to test or exploit security weaknesses.

In 2024, PoC exploits were released for all three of the most-exploited vulnerabilities, turning opportunistic attacks into focused campaigns. With these ready-made tools in hand, attackers—regardless of skill level—had a clear and easy path to exploitation.

Most Exploited Vulnerabilities of 2024

- CVE-2024-1708 affecting ConnectWise ScreenConnect
- CVE-2024-50623 impacting Cleo Harmony, VLTrader, and LexiCom
- CVE-2024-3400 targeting Palo Alto GlobalProtect

When PoCs are released, the clock starts ticking; attackers rush to exploit vulnerabilities at scale before organizations can respond.



To stay ahead, organizations across all sectors must prioritize securing external-facing assets, as these are prime targets for rapid, opportunistic attacks the moment exploits become available.



The **information sector** emerged as the primary target for public-facing application attacks, largely due to its reliance on software that often inadvertently leaves critical assets exposed, like customer service platforms, hosting infrastructure, and interconnected systems.

LockBit Finds a Key in ScreenConnect

In February 2024, a “LockBit” ransomware affiliate successfully exploited CVE-2024-1708 to gain access to a customer’s on-premises ConnectWise ScreenConnect server.

Using this access, the adversary executed a ransomware encryptor via ScreenConnect, impacting numerous hosts within the environment.

The affected hosts had adequate visibility through logging and endpoint security tools, enabling a swift and effective response that ultimately prevented a successful attack.

Take Action

Against Exploitation of Public-Facing Applications

- ✓ Maintain an accurate inventory of public-facing software like VPNs, firewalls, and file-transfer software. Minimize the external attack surface by disabling unused services or applications and limiting the public exposure of systems to only those that are essential for business operations. For devices that need to be externally facing, enforce strict access controls and incorporate a web application firewall (WAF) to monitor and block malicious requests.
- ✓ Prioritize patching these critical systems and establish fallback plans to mitigate risks when patching isn’t immediately possible.
- ✓ Equip internal devices and servers relying on this software with adequate logging and security tools to enhance visibility and enable swift responses to threats.


Voice Phishing Behind 14% of Breaches

Social engineering is far from new, but it remains one of threat actors' most effective tools, allowing them to exploit human trust to infiltrate organizations.

Attackers frequently deceive users into [downloading malicious software](#) or manipulate IT help desks into resetting credentials and disabling MFA. To deceive help-desk personnel, attackers gather employee information such as full names, addresses, and Social Security numbers.

Voice phishing is especially concerning.

It circumvents all technical defenses, instead directly targeting an organization's people. Employees tricked by these tactics not only risk exposing sensitive information but also open the door for attackers to deploy malware, allowing them to steal the data themselves.



The manufacturing sector was the top target for phone-based social engineering attacks, with attackers likely taking advantage of its frequent IT interactions and lenient help-desk policies designed to handle high volumes of support requests.

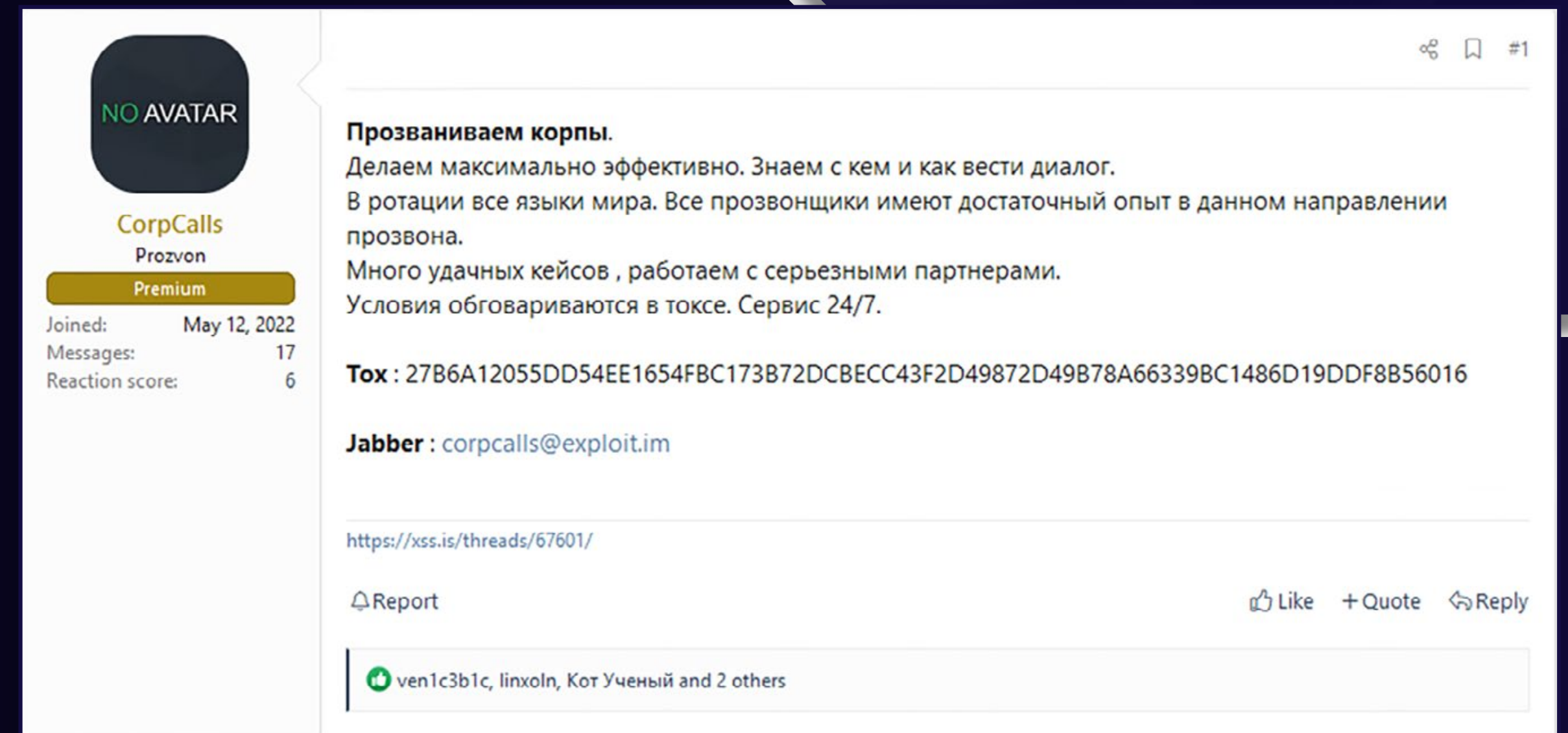


Figure 8: A user offers corporate calling services in multiple languages on forum XSS

To overcome language barriers, threat actors are now advertising multilingual calling services, while English-speaking attackers are using their language fluency to [secure initial access on behalf of Russian-speaking ransomware groups](#).

These attackers are using messaging apps like Telegram and traditional cybercriminal forums to advertise their services, as shown in Figure 8. The post advertises:



We call corporations, doing it as effectively as possible. We know who to contact and how to communicate with them. Every language in the world is available.

Our callers are experienced in this type of calling. Backed by many successful cases, we work with serious partners. Terms can be discussed via Tox. 24/7 service (translated from Russian)

This new shift shows that social engineering has evolved into a globalized and increasingly sophisticated threat.

When Help Desks Become Gateways: Social Engineering Hits Health Care

In April 2024, we uncovered a [social engineering campaign](#) targeting multiple health-care customers.

The threat actor attempted to access the organizations' VPN portals and, when blocked by MFA, called help desks while posing as employees. Due to procedural flaws in help-desk operations, the attacker was given access to employee accounts.

To remediate the incident, we identified the attacker's infrastructure and initiated hunts across our health-care customers' environments. Impacted organizations were promptly notified, and the attacker's access was revoked.

Take Action

Against Voice Phishing

- ✓ Educate IT help-desk employees to follow established policies and verify requests through official communication channels.
- ✓ Encourage employees to confirm a caller's identity via a secondary channel, like email or direct message.
- ✓ Use social engineering scenarios in red team exercises to test processes and strengthen employee defenses.

Access via Cloud Accounts and Trusted Relationships Achieved in 9% of Intrusions

Attacks on customer [cloud services](#) like Amazon Web Services (AWS) and Azure rose by 4% between 2023 and 2024, a trend driven by the growing adoption of cloud platforms and the improved resiliency of on-premises systems.

But attackers are adapting to this shift, lured by the broad attack surface and vast amounts of sensitive data these platforms offer.

Adversaries are also abusing trusted relationships, like those with third-party service providers that offer on-premises or cloud services, to infiltrate organizations.

By targeting partners with weaker security controls, attackers can follow a “one-to-many” approach:

Compromise one organization and exploit its connections to breach more-secure partners.

In some cases, attackers return to previously breached entities that have since been acquired to exploit weaknesses a second time around.

As cloud adoption grows and business ecosystems become more interconnected, organizations need robust security across every link in the chain.



Organizations in the professional, scientific, and technical services (PSTS) sector are the most frequent targets of cloud-based attacks, likely due to the sensitive nature of the data they manage, such as intellectual property and client information.

The following factors also make cloud environments ripe for exploitation:

Misconfigurations

Weak Access Controls

Gaps in the Shared Responsibility Model

When Trust Backfires: How Silk Typhoon Exploited a Third-Party Account for Azure Access

In September 2024, we responded to an intrusion attributed to “Silk Typhoon” where the attacker gained access to a customer’s Azure cloud environment by leveraging an overprivileged Azure account. The account, which belonged to a third-party vendor, lacked MFA and had been previously compromised.

Once inside, the attacker attempted to escalate privileges by adding credentials to service principal accounts.

To remediate the incident, the attacker’s access was revoked for the compromised vendor account, credentials were reset, and MFA was added to secure the account going forward.

Take Action

Against Cloud and Trusted Relationship Attacks

- ✔ Enable MFA for AWS Identity and Access Management (IAM) users and root accounts, prioritizing phishing-resistant options like passkeys and security keys for critical accounts.
- ✔ Set conditional access policies in Microsoft Entra ID (formerly Azure Active Directory) for external contractors.
- ✔ Limit session durations for external users, enforce access restrictions to only the applications and data required for job functions, and ensure device compliance.

GreyMatter Automations for Combatting Unauthorized Access

For the best protection against the initial access techniques outlined in this section, ReliaQuest customers should use the following Automated Response Playbooks and threat hunting packages in GreyMatter.

These tools are designed to disrupt and respond to unauthorized access attempts, reducing the risk of further compromise and lateral movement within an environment.

Recommended Automated Response Playbooks



Block IP: Denies communication with specific IP addresses associated with malicious activity, cutting off attacker access and disrupting their operations.



Reset Password: Forces a password change to invalidate stolen credentials harvested through phishing, preventing attackers from maintaining access.

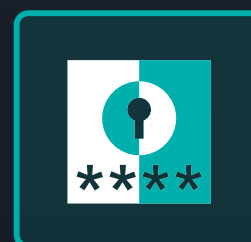
Recommended Threat Hunting Packages



Successful MFA from High-Risk Country: Identifies successful MFA attempts originating from high-risk countries to detect potential unauthorized access. This threat hunting package focuses on unusual login locations that could indicate compromised credentials or malicious activity.



AWS Enumeration: Detects the use of AWS commands commonly used by threat actors for enumeration and discovery. This threat hunting package identifies activities such as user and policy enumeration, role identification, infrastructure discovery, and bucket listing to uncover unauthorized access and reconnaissance efforts in cloud environments.



Password Manager Access to Sensitive Secrets—Credential Access: Audit access to secrets stored in password managers to monitor how often these secrets are accessed, who is accessing them, and from which locations. This enables organizations to detect potential unauthorized activity by threat actors.

SocGholish Secures Top Spot Again in 2024 Malware List

The malware threats observed in customer environments throughout 2024 revealed a relentless evolution in tactics and preferred variants, as attackers continued refining their methods to outpace defenders.

AsyncRAT used legitimate software like ScreenConnect to infiltrate systems with stealth and precision. Lumma, on the other hand, doubled its sales of stolen credentials and turned to novel techniques, such as coercing users to copy and paste malicious PowerShell code via fake CAPTCHAs. With over 478,000 Lumma-related listings on criminal marketplaces, including credentials used to breach major platforms like Snowflake, the stakes for defenders are at an all-time high.

In this section, we'll examine these malware variants in detail, focusing on their new tactics and the factors behind their increased popularity.

While SocGholish held its top spot as the biggest malware threat—largely thanks to its new Python infection chain used for persistence—the “AsyncRAT” remote-access trojan (RAT) and “Lumma” (aka LummaC2) infostealer climbed the ranks.

Percentage of 2024 Incidents by Malware Variant



Percentage of 2023 Incidents by Malware Variant



SocGholish Persists in First Place with Python

Named for its deceptive use of social engineering and “ghoulish” tactics, SocGholish remains a dominant force on the malware scene.

It’s primarily distributed through infected websites that rank highly in search engine results or through phishing emails that redirect victims to these sites.

Once on the infected website, victims are tricked into downloading a malicious JavaScript file disguised as a legitimate browser update.

This file grants attackers remote access to the victims’ systems, enabling serious consequences like data exfiltration, system encryption, and other high-impact threats that can devastate organizations.

Although SocGholish maintained its position as the most frequently observed malware in 2024, we saw infostealers written in C, Rust, and C++ rise in popularity, as evidenced by Lumma’s ascent to third place.

Windows Command Shell

44%

PowerShell

30%

JavaScript

11%

Visual Basic

6%

Unix Shell

4%

Python

2%

AutoHotKey & AutoIT

2%

Additionally, 2024 saw a surge in “one-off” malware variants like “[Broomstick](#)” and “[Matanbuchus](#).”

These evolving trends highlight the increasingly diverse and unpredictable nature of the malware landscape, emphasizing the critical need for proactive defenses and rapid response strategies.

Figure 9: Top command and scripting interpreters

Despite the shifting statistics, SocGhosh continues to pose a significant global threat to organizations.

February 2024 saw its biggest advancement:

A new infection chain that uses [Python for persistence](#), likely as a means to evade traditional security tools.



By using a second-stage download from the trusted domain python[.]org, this adaptation significantly enhances the malware's ability to bypass defenses and remain undetected.

While defenders are well-prepared to detect malicious activity through common tools like the Windows command shell and PowerShell (see Figure 9), Python is rarely seen in malware deployments.

This relative unfamiliarity and limited detection coverage likely prompted the SocGhosh team to incorporate Python into their operations, exploiting a blind spot in many security strategies. This change in tactic underscores that adversaries are not only aware of existing security controls but are actively engineering ways to outmaneuver them.

As a result, SocGhosh continues to cement its position as a persistent and sophisticated threat to organizations worldwide.

Take Action

Against SocGhosh

- ✔ Use a Group Policy Object (GPO) to set Notepad as the default application for JavaScript files to prevent SocGhosh from executing via WScript.
- ✔ Set Microsoft attack surface reduction (ASR) rules to block JavaScript or Visual Basic Script (VBScript) from launching downloaded executable content.
- ✔ Enable the "include command line in process creation events" policy setting in Group Policy to ensure adequate command-line auditing.

Figure 10: AsyncRAT x ScreenConnect infection chain

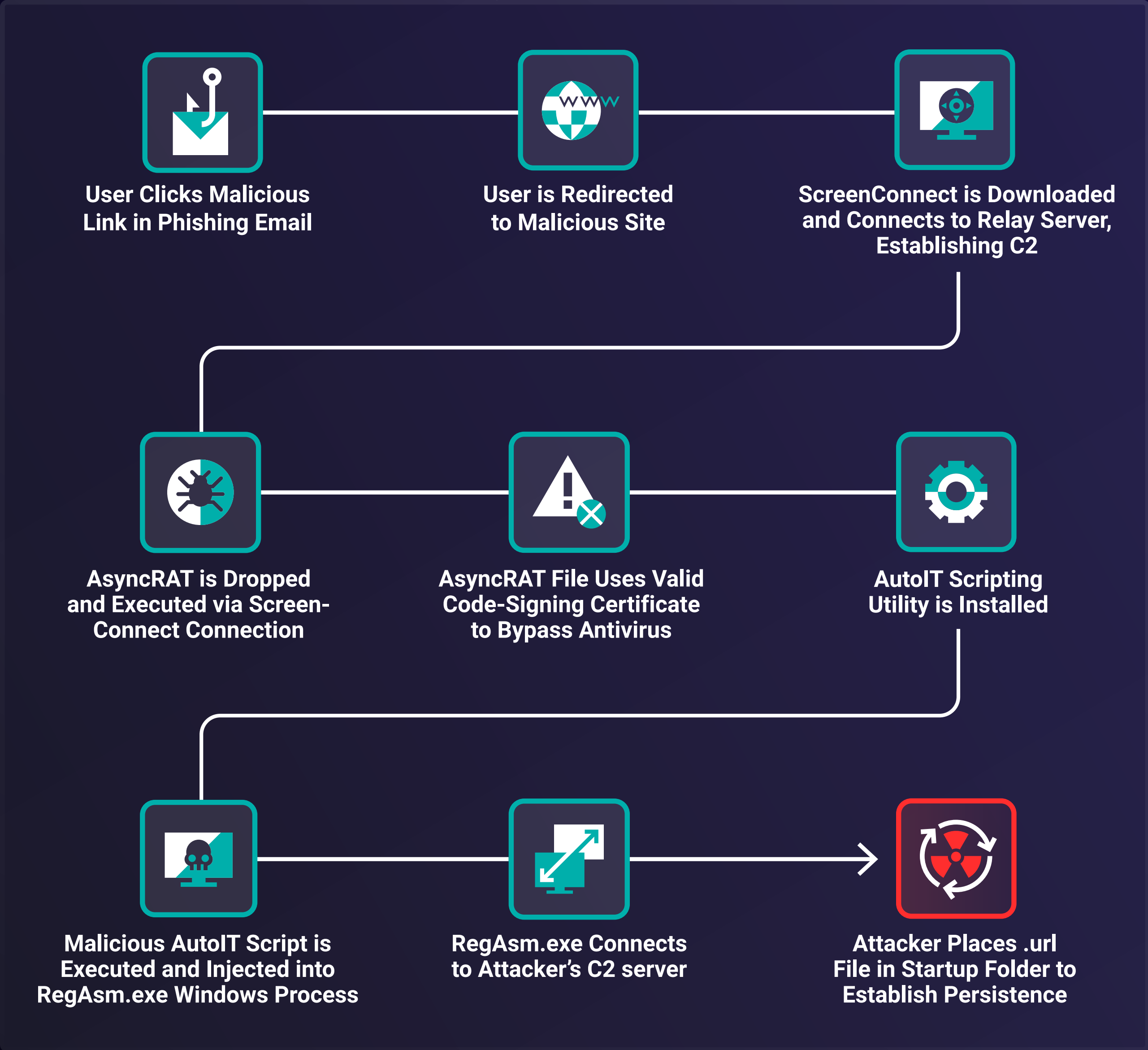
ScreenConnect Abuse Propels AsyncRAT to Second Place

The powerful AsyncRAT gives attackers full control over infected hosts, enabling keylogging, credential theft, malware delivery—including ransomware—as well as C2 operation.

To complicate matters, it also has botnet capabilities for launching denial-of-service (DoS) attacks.

This versatility has made AsyncRAT a favorite among threat actors, and 2024 marked a defining year for the trojan, as it contributed to the second-most customer incidents over the year, up from fourth in 2023.

AsyncRAT uses the guise of legitimate software to infiltrate systems, exploiting users' trust to evade security mechanisms, blend into normal network traffic, and deceive users into downloading malicious files—all while remaining undetected.



By incorporating ScreenConnect into its methodology, AsyncRAT has achieved increasing success.

However, as defenders adapt to these tactics, **we expect its dominance to wane in 2025.**

In July 2024, we identified a campaign in which phishing emails were sent to trick individual recipients into downloading ScreenConnect software (see Figure 10).

Once installed and connected to the attackers' ScreenConnect server, an executable—equipped with a code-signing certificate capable of bypassing antivirus and Endpoint Detection and Response (EDR) tools—deployed AsyncRAT onto the victim's system.

This incident demonstrates the critical importance of understanding what's "normal" in your environment to quickly detect and respond to anomalies.

Take Action

Against AsyncRAT

- ✓ Enforce application control policies to control the execution of JavaScript, AutoIT scripts, and Program Information files commonly exploited by AsyncRAT.
- ✓ If ScreenConnect isn't used in your organization, block screenconnect[.]com at the network edge to eliminate this attack vector.
- ✓ Certain versions of AsyncRAT exploit VBScript for execution. Configure a Group Policy to open VBScript files with Notepad to prevent their execution.

Copy, Paste, Compromised: Lumma Rises to Third Place with Innovative Tactics

1	SocGhosh	—
2	AsyncRAT	↑
3	Lumma (+8)	↑
4	Gootloader	↑
5	Cobalt Strike	↑
6	Impacket	↑
7	Netsupport RAT	—
8	Raspberry Robin	↓
9	Clearfake	↑
10	DanaBot	↑
11	DarkGate	↑

Climbing from eleventh place in our 2023 rankings to third in 2024, Lumma is an infostealer malware that harvests sensitive data like browsing history, cookies, saved credentials, and cryptocurrency wallets.

The stolen data is sold on criminal marketplaces as infostealer logs, typically priced around \$10 each. Distributed through malicious websites, trojanized software, and phishing attacks, Lumma operates as a MaaS model, providing subscribers with continuous updates and support.

Lumma's growth has been explosive.

[Its credential sales nearly doubled](#) each quarter in 2023, and it maintained an upward trajectory in 2024.

478,000 Listings

Last year alone, more than 478,000 listings on criminal marketplaces originated from Lumma infections, which coincided with a 4% increase in infected customer environments.

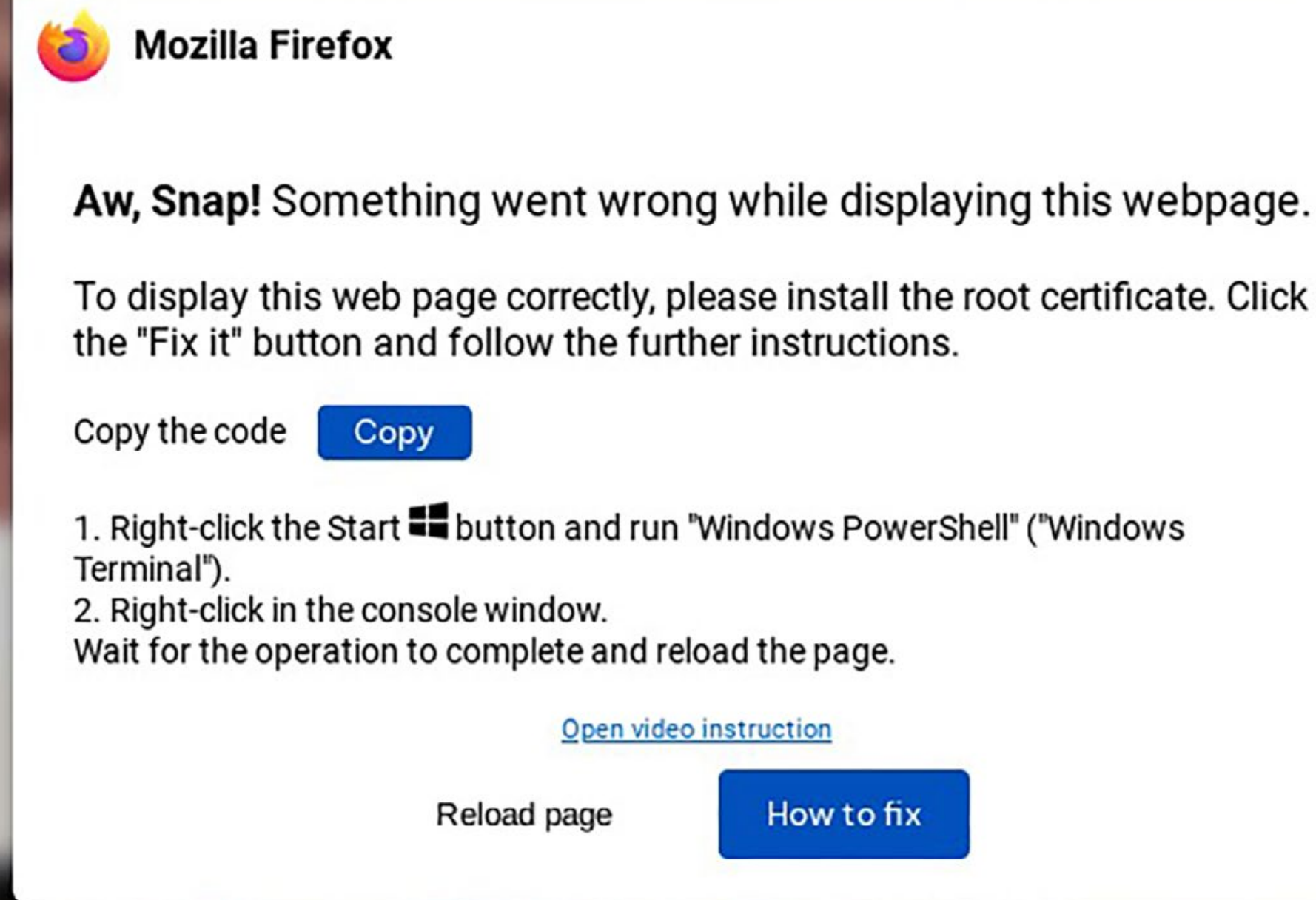


Figure 11: Fake prompt containing malicious code

In May 2024, ReliaQuest observed Lumma being installed via a novel execution technique: coercing users into manually [copying and pasting](#) malicious PowerShell code into the console via fake browser errors or CAPTCHAs (see Figure 11).

This tactic was likely designed to evade traditional signature-based security detections, showcasing the attackers' relentless innovation to ensure the malware's continued success.

Lumma's popularity among threat actors stems from its active support for its users, frequent updates, and advanced evasion capabilities that make it highly effective for data exfiltration.

Its logs provide attackers with direct access to internal networks and cloud platforms.

Despite Lumma's steep subscription fees—as high as \$1,000 per month—many attackers are willing to pay the price, as the stolen credentials yield far greater returns.

**\$1,000/
Month**

Corporate

**\$500/
Month**

Professional

**\$250/
Month**

Experienced

To defend against Lumma and similar infostealer malware, organizations must include infostealers in their threat models, as stolen data can provide attackers with access to critical assets. Notably, the May 2024 breach of the Snowflake cloud platform² was allegedly traced back to stolen credentials obtained from infostealer logs.

Take Action

Against Lumma

- ✔ Restrict employees from using personal devices to access employer portals to prevent the risk of corporate credentials being stolen from infected devices.
- ✔ Implement a Group Policy to prevent passwords from being saved in browsers, minimizing potential data theft if malware infiltrates.
- ✔ Disable QuickEdit Mode in PowerShell and the Windows Run command prompt via Group Policy for unaffected employees to mitigate malware that exploits copy-paste functionality.

GreyMatter Automations for Combatting **Malware**

To combat the sophisticated techniques used by top malware threats, ReliaQuest customers can enable targeted detection rules that identify malicious activity, such as obfuscated PowerShell scripts and drive-by downloads.

In addition, deploying appropriate Automated Response Playbooks in GreyMatter allows for rapid containment and removal of threats.

Together, these proactive measures help organizations minimize the impact of malware infections and prevent further compromise.

Recommended Detection Rules



PowerShell Obfuscated Script: To evade detection, attackers obfuscate PowerShell scripts by inserting escape characters (special characters written to overcome programming language limitations) between normal characters when sending function calls to the system. This technique makes pattern matching more difficult. This detection rule identifies such obfuscated PowerShell commands, as they are strong indicators of malicious activity.



WScript Executing Suspicious File: Many initial access tools rely on users interacting with web popups to download ZIP files and execute JavaScript files. On Windows 10, double-clicking a JavaScript file automatically executes the malicious payload via wscript.exe. This rule monitors drive-by download activity, including WScript usage, files in local/temp directories, and script execution from these files.

Recommended Automated Response Playbooks



Isolate Host:

Disconnects compromised hosts from the network to prevent lateral movement and contain the threat while enabling further investigation.



Delete File:

Removes malicious files from endpoints to eliminate threats such as malware or ransomware before they can be executed.

48 Minutes to Breakout: Unmasking Post-Compromise Trends

Once attackers have a foot in the door, their path forward is clear:

Escalate privileges, move laterally, and achieve their objectives—whether that’s stealing sensitive data or crippling operations. Post-exploitation is where the real damage happens, and attackers are moving faster than ever, with lateral movement now taking an average of just 48 minutes. Armed with increasingly sophisticated tools, they maximize their impact while staying under the radar.

In the section we break down...

The top techniques used by attackers in 2024 to navigate networks and escalate privileges



The tools they employed to stay hidden



The growing trend of prioritizing data theft over encryption.

We'll also explore

the turbulent ransomware landscape that defined 2024 and its implications for organizational defenses.

An Attacker's Route to Control

First, we'll look at the top techniques: RDP became the most common method for lateral movement, while internal spearphishing doubled year over year, leveraging employee trust and dark-web phishing kits to compromise multiple accounts.

Then, we'll explore how privilege escalation centered around valid accounts, with 85% of breaches involving compromised service accounts. This enabled attackers to evade detection and move laterally within minutes of initial access.

Finally, we'll highlight their growing reliance on legitimate tools like Impacket, WinRAR, and RMM software to maintain control and execute attacks. These tools, used in 60% of hands-on-keyboard incidents, seamlessly blend into normal activity, making their abuse significantly harder to detect.

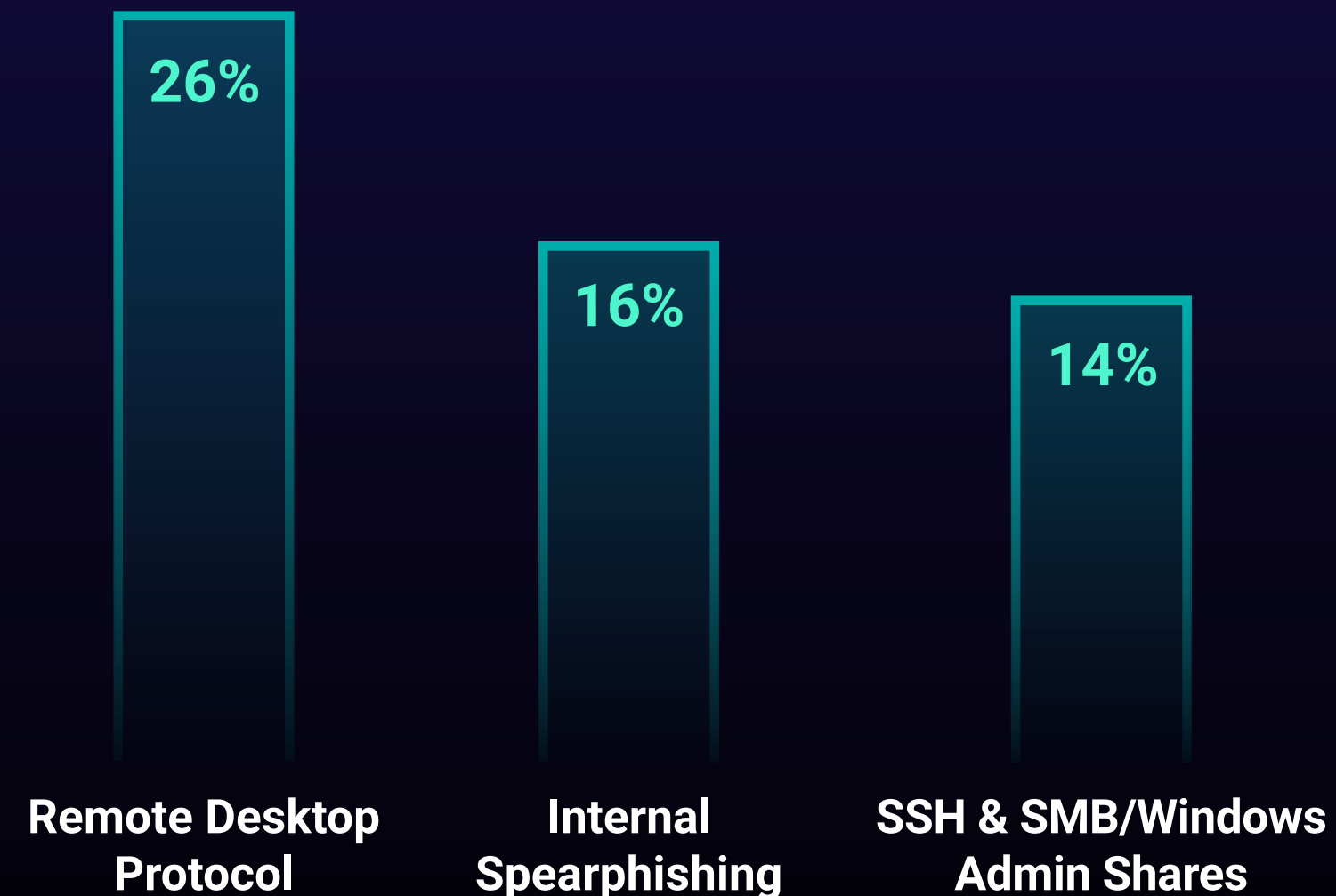
The period between initial access and lateral movement is known as breakout time. In our analysis of customer incidents from 2024, we found that attackers achieved an average breakout time of just 48 minutes.

Why RDP Became the Tool of Choice for Lateral Movement

In 2024, RDP topped the list as the most-used tool for lateral movement, giving attackers a straightforward method to connect to other internal systems within an environment. Originally designed as a legitimate remote management tool for IT help desks to assist global workforces, RDP's built-in presence on Windows systems has made it a favorite among attackers.

Armed with stolen credentials, attackers can use RDP to discreetly move between systems, blending into regular network activity without triggering alarms that malware might. Its simplicity, stealth, and ability to easily connect to systems makes RDP a go-to tactic for lateral movement—and its misuse shows no signs of slowing down.

Percentage of 2024 Incidents by Lateral Movement Technique



Percentage of 2023 Incidents by Lateral Movement Technique

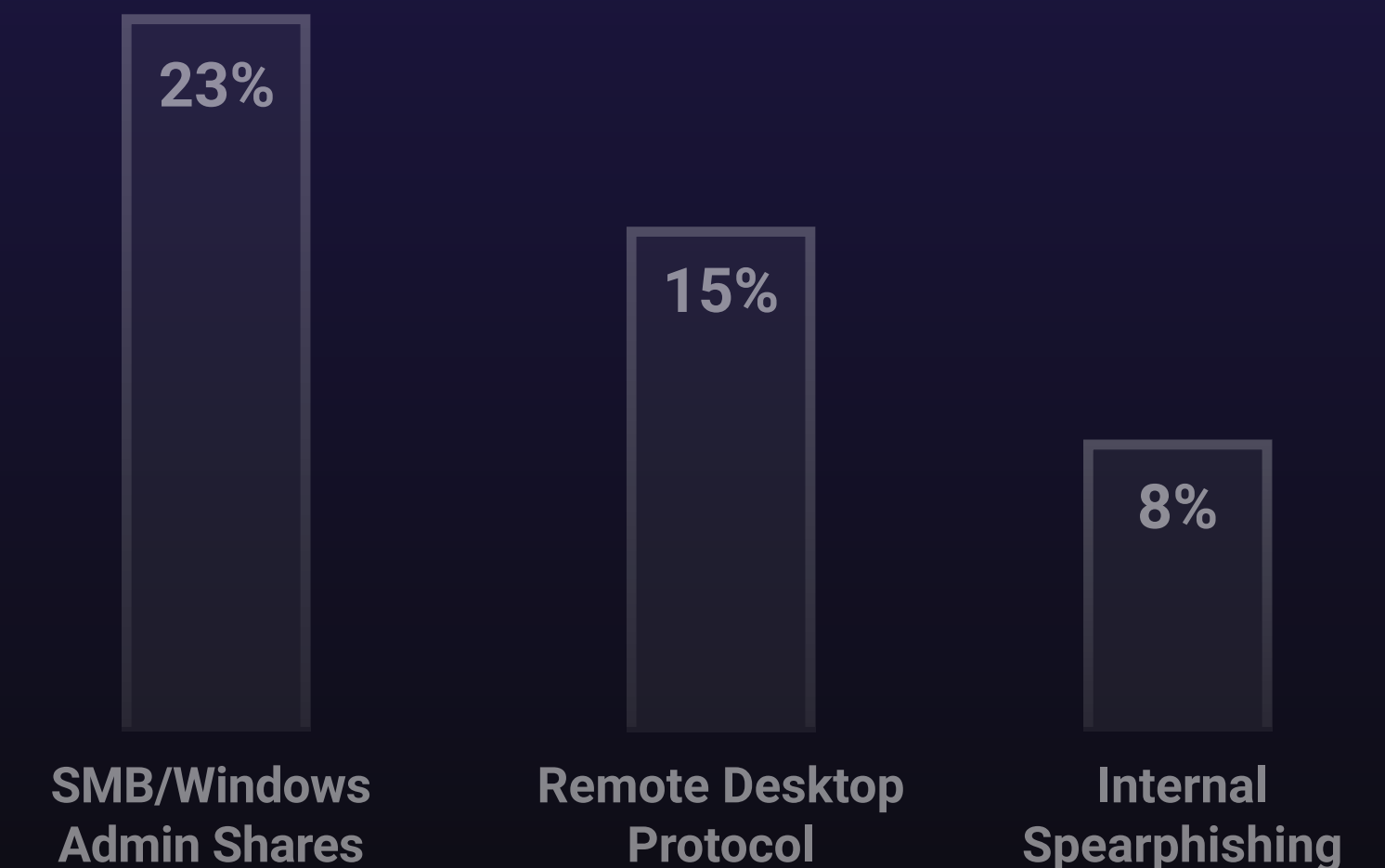
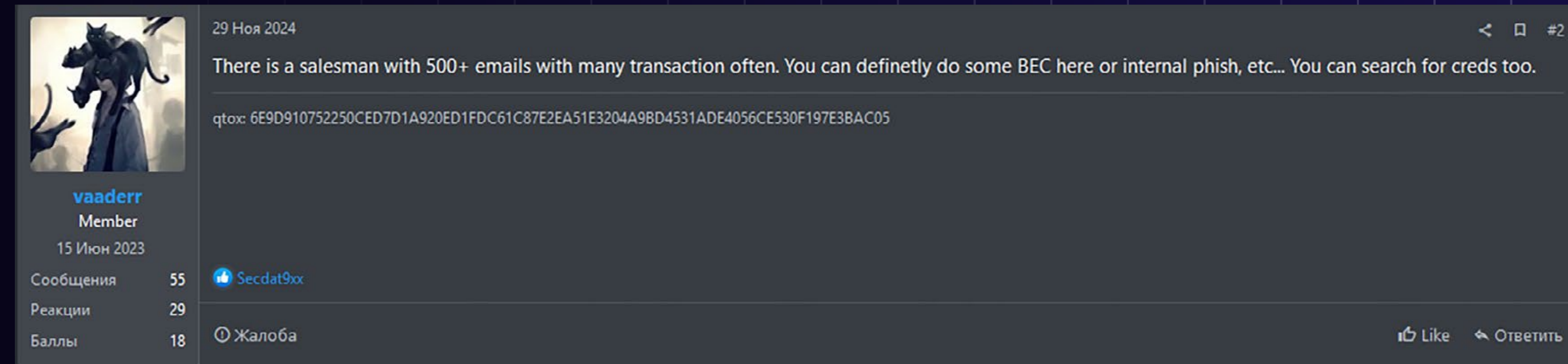


Figure 12: RAMP forum user selling access and suggesting phishing internal users



Internal spearphishing, a technique sometimes used in BEC attacks, doubled in frequency from 2023 to 2024, rising to become the second most common tactic for lateral movement.

Internal spearphishing involves attackers compromising a user account and using it to send phishing emails to other users within the same organization, potentially compromising multiple accounts at once.

The significant rise in internal spearphishing can likely be attributed to the **200% increase** in phishing kit mentions on the dark web between 2023 and 2024.

These phishing kits—tools designed to help attackers with little to no technical expertise launch phishing attacks—can bypass MFA and lower the barrier to entry for attackers. This is especially true when paired with services on cybercriminal forums that offer or sell access to hundreds of active email accounts (see Figure 12).

As a result, advanced phishing campaigns have become accessible to attackers of any skill level.

By exploiting the inherent trust that employees place in internal emails, attackers achieve far higher success rates with internal phishing compared to external campaigns. Given its success, this growing threat demands that organizations prioritize security awareness training and implement internal phishing simulations to assess system and user readiness.

Take Action

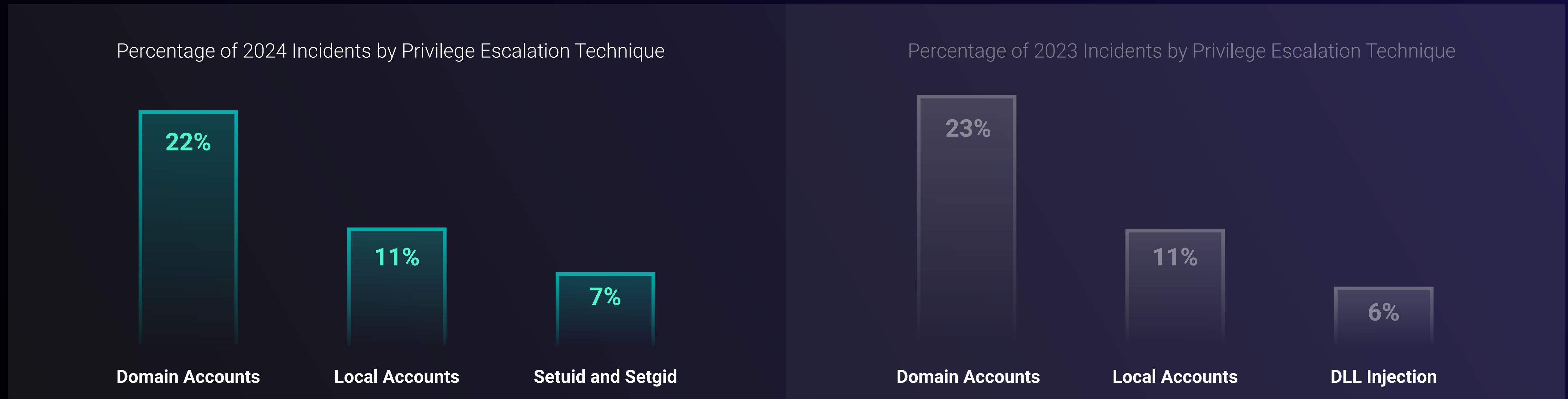
Against Lateral Movement Techniques

- ✔ Enforce MFA for RDP and, to minimize exposure to potential threats, limit its use to essential systems only.
- ✔ Enable the scanning of internal emails to analyze messages exchanged between internal accounts and those sent externally to detect phishing attempts and malicious activity originating from compromised accounts.
- ✔ Use tools like AllowUsers or AllowGroups in sshd_config to restrict Secure Shell (SSH) access to specific users or groups.

Valid Accounts, Invalid Intent: Easy Access to Privilege Escalation

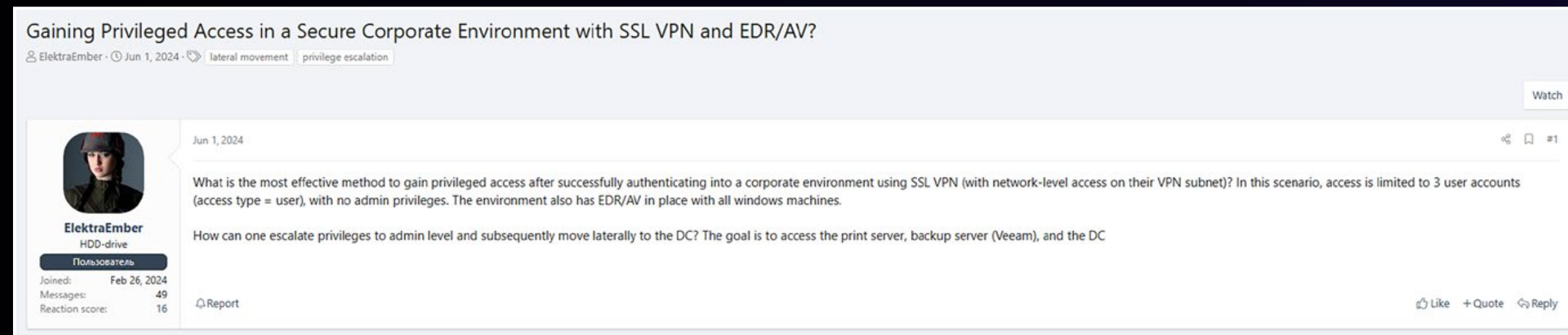
Attackers are abusing high-privileged, valid accounts at both the domain and local levels to achieve short breakout times. Once inside an environment, attackers quickly assess the permissions of the compromised account. Basic accounts rarely provide the keys to the castle, so to establish persistence or move laterally, attackers must escalate privileges to gain the elevated access they need.

Our findings revealed that when attackers needed to escalate privileges, valid domain accounts were their primary targets—a trend unchanged from 2023. These accounts, whether owned by users, administrators, or services, are frequently exploited because they offer the access and stealth attackers need to advance their operations without detection. This trend is reflected on cybercriminal forums: For instance, we observed a user on the Russian-language forum XSS seeking advice on how to gain admin-level privileges to compromise a domain controller (DC) (see Figure 13). Control over a DC opens the door to countless opportunities for attackers—they can map the network, access most connected devices, and steal sensitive data—making them a prized target.



Local accounts also remain a key focus for threat actors, ranking second place for most-common privilege escalation technique year after year. Stored on individual systems, local accounts include standard user accounts, service accounts, and the Windows default administrator account, and are often targeted in brute-force attacks. Because systems are guaranteed to have local accounts, attackers can bypass the need to identify specific users, speeding up their efforts to compromise systems.

Figure 13: XSS user turns to other forum users for help on escalating privileges



Malware- or exploit-based attacks are noisy and can be easy to detect. But, by exploiting valid accounts, attackers make it difficult for organizations to distinguish malicious actions from legitimate activity, a fact they take advantage of.

The longer attackers remain undetected, the greater the risk they pose—whether through lateral movement, data theft, or deploying malicious payloads.



Without strong security controls, these trusted accounts can turn into an organization's biggest vulnerability. Between January and July 2024, 85% of customer breaches involved [compromised service accounts](#), allowing attackers to operate under the radar for extended periods.

Take Action

Against Privilege Escalation

- ✔ To mitigate the risk of domain account compromise, restrict domain account permissions, harden administrator accounts, implement stringent help-desk procedures, regularly clean up unused service accounts, and implement group managed service accounts (gMSAs).
- ✔ To secure systems from local account abuse, enforce strong and unique passwords for all local accounts and disable unused or default accounts, such as the Windows Administrator account.
- ✔ To secure systems against Setuid and Setgid abuse, audit files using `find / -perm -4000` and `find / -perm -2000` to identify risky binaries. Remove unnecessary Setuid and Setgid bits with `chmod u-s` or `chmod g-s` to prevent attacks from abusing them for privilege escalation.

Scattered Spider's Web of Social Engineering Unravels Privileges

In October 2024, [Scattered Spider](#) convinced a customer's IT help-desk staff to reset the CFO's password in a social engineering attack. The group later convinced another help-desk employee to reset MFA controls and successfully enrolled its own device.

Although the CFO's account lacked the privileges necessary to further its attack, Scattered Spider identified a domain administrator account in SharePoint that could provide elevated privileges. Recontacting the help desk, it achieved a password reset, which granted the group access to the organization's password manager.

Within six hours of initial access, Scattered Spider began encrypting the organization's systems. The group created a virtual machine within the organization's VMware ESXi environment to maintain persistence, concealing its activities until encryption was complete and backups were sabotaged.

The Adversary's Toolkit: Post-Exploitation Essentials

In the past, adversaries relied heavily on frameworks like Cobalt Strike and PowerShell exploits for C2. However, enhanced detection measures have made these methods increasingly risky for attackers.

To evade modern defenses, they are now turning to commercial applications for malicious operations ([CAMO](#)), leveraging legitimate tools such as AnyDesk and PDQ Deploy to maintain C2 and progress through every stage of the kill chain—from scanning networks to deploying ransomware.

Between January and August 2024, ReliaQuest saw a **16% increase** in the use of legitimate tools in hands-on-keyboard incidents compared to 2023, with such tools accounting for **60% of cases**.

These trusted tools have become the backbone of modern attacks, enabling attackers to avoid detection while inflicting maximum damage. Cybercriminals' increased reliance on legitimate tools outlines the need for organizations to understand how these applications are being weaponized to bypass defenses.

Next, we'll detail the most common tools attackers used in breaches during 2024 and steps you can take to mitigate these risks.

Legitimate RMM Tools Top Choice to Maintain C2

Originally designed for IT professionals to manage infrastructure, RMM tools pose [serious security risks](#) when left unsecured. Their legitimacy allows attackers to slip past defenses, evading detection by appearing benign. Attackers also exploit RMM tools in social engineering campaigns, posing as help-desk support to trick users into granting remote access.

By mimicking routine IT operations, they seamlessly integrate into workflows, maximizing the effectiveness of their attacks while avoiding suspicion.

To mitigate these risks, organizations must recognize the risks of RMM tool abuse, incorporate it into their threat models, and establish a baseline for normal RMM tool usage to quickly distinguish normal activity and malicious behavior.

1. AnyDesk

2. TeamView

3. QuickAssist

4. Jwrapper

5. Dameware

6. ATERA

Figure 14: RMM tools favored by attackers

Impacket Now Go-To Post-Compromise Tool

Originally designed to interact with network protocols like SMB, New Technology Local Area Network Manager (NTLM), and Lightweight Directory Access Protocol (LDAP), Impacket has become a go-to post-compromise tool for attackers, appearing in 33% of breaches in 2024.

This Python-based tool set is favored for lateral movement but also offers extensive capabilities—such as credential dumping, Kerberoasting, and more—that make it highly versatile and portable for post-compromise operations.

Although Impacket is susceptible to signature-based detections, adversaries often exploit poorly monitored environments and take advantage of Impacket's use of legitimate protocols like SMB, Windows Management Instrumentation (WMI), and LDAP. It's realistically possible that adversaries adapt how they use Impacket to mimic normal network activity, making their actions harder to distinguish from legitimate behavior and appear non-malicious.

These shifting tactics emphasize the importance of ensuring comprehensive network traffic logging and adequate security tool coverage to detect Impacket itself as well as the network behaviors it generates.

Medusa Turns Everyday Tools into Weapons

In April 2024, a customer in the information sector was infiltrated through an insecure VPN. In June, a “[Medusa](#)” ransomware affiliate launched follow-on attacks. While not confirmed, it’s realistically possible that an IAB obtained network access and later sold it to the Medusa affiliate.

The Medusa affiliate used legitimate tools to compromise the organization’s network: Netscan and PDQ Inventory Scanner for network discovery, AnyDesk for C2, and PDQ Deploy to spread ransomware across the environment, all while remaining hidden.

The organization’s vulnerabilities—including an insecure VPN, significant blind spots, and unmanaged devices—contributed to the success of the attack, resulting in the encryption of a portion of the environment.

File-Compression Tools Gain Popularity Among Attackers

Attackers are increasingly using legitimate file-compression tools like WinRAR and 7-Zip to compress staged data before exfiltration, replacing the compression features traditionally built into C2 frameworks.

Adversaries often use these tools in combination with cloud utilities like Rclone and MegaSync to exfiltrate data to cloud storage. Because the activity generated by these tools often doesn’t appear inherently malicious, organizations should establish a baseline for their usage and implement security controls to differentiate between legitimate and malicious activity.

The message is clear: Attackers lean on legitimate tools because they’re easily accessible—many are open source—and incredibly versatile, allowing them to execute multiple actions at once. By using trusted tools, attackers blend seamlessly into legitimate network traffic, avoiding suspicion and complicating detection efforts, especially if an organization has no baselines for normal use in place. For businesses, this camouflage can have devastating consequences. The longer attackers remain undetected in a network, the greater the risk of major data breaches or operational disruptions—both of which can shatter an organization’s reputation and result in the loss of key talent or critical business opportunities.

Take Action

Against Abuse of Legitimate Tools

- ✓ Implement endpoint segmentation by blocking SMB communication from workstations to servers that don’t require it. This measure reduces the attack surface and helps prevent Impacket-based intrusions.
- ✓ Implement an Active Directory (AD) Group Policy or application control tool that can be used to add approved RMM software to the allowlist.
- ✓ Implement firewall rules to block domains associated with unauthorized cloud syncing and RMM tools.

GreyMatter Automations for Combatting **Legitimate Tool Abuse**

To combat threat actors' misuse of legitimate tools, ReliaQuest customers can leverage GreyMatter Automated Response Playbooks to quickly contain attacker activity.

Additionally, GreyMatter threat hunting packages enable customers to proactively detect abuse of legitimate tools within their networks.

Together, these actionable measures empower security teams to disrupt attacker access and put a stop to the unauthorized use of commonly trusted tools.

Recommended Automated Response Playbooks

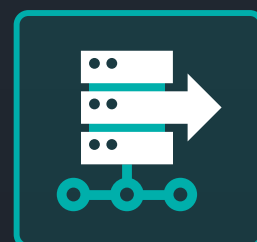


Terminate Active Sessions: Ends the user's active sign-ins and revokes session cookies, cutting off any unauthorized access in real time.



Reset MFA: Resets the user's MFA, effectively blocking attackers who may have intercepted tokens or bypassed MFA during a phishing attack.

Recommended Threat Hunting Packages



Network Discovery Tooling: Detects the use of common network discovery tools, such as Advanced IP Scanner and Angry IP Scanner, which threat actors use to map network topology and identify targets for lateral movement. By analyzing telemetry from network traffic logs and EDR tools, organizations can identify reconnaissance efforts and mitigate risks early in the intrusion process.



Remote Desktop Audit: Identifies suspicious RDP activity, such as unusual logins or session behaviors, that may indicate access or lateral movement by threat actors. By analyzing event logs, processes, and registry changes, this threat hunting package helps organizations detect potential threats and strengthen defenses against RDP-based attacks.



Impacket Utilization: Detects the use of Impacket, a tool set often leveraged by threat actors to exploit Windows network protocols. By analyzing telemetry from Windows Event logs and command-line logging on destination hosts, organizations can detect malicious activity involving Impacket tools.

Ransomware Decoded: Exfiltration Is the New Encryption

Ransomware tactics have undergone a dramatic transformation. What began as straightforward extortion through system encryption grew into “double extortion,” where attackers compounded encryption with the threat of leaking stolen data to maximize pressure on victims. Now, many attackers are abandoning encryption altogether, focusing solely on data theft—a faster, more profitable approach. In 2024, this trend accelerated, with only 20% of breaches still featuring encryption. **In this section, we’ll...**

Examine this rise of exfiltration-only attacks

Uncover the tools and methods driving these campaigns

Break down the major developments in the 2024 ransomware landscape

From the decline of key players to the emergence of new ones, we’ll explore the twists, turns, and trends to watch. Most importantly, we’ll provide actionable recommendations to help organizations defend against these evolving threats—and demonstrate how ReliaQuest can keep organizations ahead of the curve.

Exfiltration Outpaces Encryption in Modern Breaches

When most people think of ransomware, they picture locked systems, black screens, and ransom notes—but that’s no longer always the case.

Our data reveals a major shift in ransomware tactics: Of all breaches we observed in 2024, 80% involved data exfiltration, while only 20% included encryption.

This sea change is almost certainly driven by the growing adoption of advanced security tools and robust backups, which have diminished the impact of encryption-based attacks. Additionally, the process of restoring encrypted systems can be so lengthy and complex that organizations are likely choosing to rebuild their systems instead. This approach has the added benefit of ensuring that any persistence mechanisms left by the attacker are completely removed. As encryption becomes less effective, groups like “[Inc Ransom](#)” now weaponize stolen data for extortion, resale, or access to additional targets, preying on organizations’ fears of reputational damage, regulatory fines, and the exposure of sensitive information.

The time required for an adversary to progress from initial access to executing data exfiltration is 34% faster than the time needed for encryption; the quickest exfiltration time we saw in 2024 clocked in at just 4 hours and 29 minutes, compared to 6 hours for encryption. This leaves defenders with even less time to detect and respond before critical data is stolen. By bypassing the technical complexities of encryption, attackers have embraced data exfiltration as their ultimate tool to strike quickly, inflict maximum harm, and maintain leverage over their victims.

Fastest Exfiltration in 2024

4 hours 29 mins

Fastest Encryption in 2024

6 hours

In 2024, 60% of attackers who successfully exfiltrated data in the incidents we examined sent the stolen data to cloud storage platforms such as Google Drive, Mega, or Amazon S3.

These services are highly useful for stealthy exfiltration, as stolen data can be uploaded quickly and disguised within legitimate traffic from commonly used platforms. This makes detection more difficult for defenders because the exfiltration activity blends in with normal business operations. Given the potential for business disruption, blocking access to widely used cloud platforms is rarely a viable option for businesses. This limits defenders' ability to be proactive, instead forcing them to rely on advanced monitoring and alerting to identify and respond to malicious activity.

Accounting for the remaining 40% of attacks, exfiltration over C2 channels enables attackers to funnel data directly to their own infrastructure.

This method requires a direct connection from the compromised system to the attacker's infrastructure, making the malicious activity more likely to be detected. However, despite this increased risk, C2-based exfiltration offers attackers greater control over the stolen data compared to third-party platforms like cloud services. This method is utilized by adversaries who don't use legitimate tools in their operations, such as RMM tools, and instead prefer the built-in capabilities of C2 frameworks to compress, encrypt, and exfiltrate data.

Looking ahead to 2025, we expect the [trend of exfiltration-only attacks](#) to persist, with exfiltration times likely to drop even further. For organizations, this shift demands a rethink of ransomware recovery strategies. The focus can no longer be solely on restoring encrypted systems—strategies must also address protecting data privacy, managing reputational risks, and ensuring compliance with regulatory requirements. To prepare, CISOs must implement defenses to detect and prevent exfiltration attempts while developing playbooks that prioritize business continuity and resilience against these evolving ransomware tactics.

Take Action

Against Exfiltration

- ✔ Deploy web proxies to block access to malicious or unauthorized websites that attackers could use for data exfiltration.
- ✔ Enforce strict access control policies to prevent connections to unapproved external services, reducing the risk of data leaks or unauthorized data transfers.
- ✔ Regularly monitor cloud service usage for unusual behavior like unexpected file uploads or downloads and block unauthorized cloud services at the network edge to prevent abuse.

Ransomware in 2024: Increased 11.9%, Hit New Highs

In 2024, the names of 5,253 organizations were listed on ransomware data-leak sites—559 more than in 2023.

Although this growth may seem modest, much of 2024 actually saw a slowdown in ransomware activity. Instability within the ransomware ecosystem played a significant role, as ransomware-as-a-service (RaaS) providers focused more on competing for affiliates than refining their attack techniques. Operations were further disrupted by law enforcement actions dismantling key ransomware infrastructure, improvements in security tool detection capabilities, and advancements in cybersecurity practices.

But the slowdown didn't last. [December 2024 marked a grim turning point](#), recording the highest-ever victim count in a single month. This surge can be attributed to the explosion of new ransomware groups, which have grown from around 60 active groups in 2022 to nearly 100 today. To avoid the spotlight and scrutiny faced by larger operations like LockBit, smaller, decentralized groups are forming, fueling an increasingly crowded and competitive landscape. As a result, attackers are likely to push for higher ransoms and adopt more sophisticated strategies to outpace defenses and secure their share of the profits.

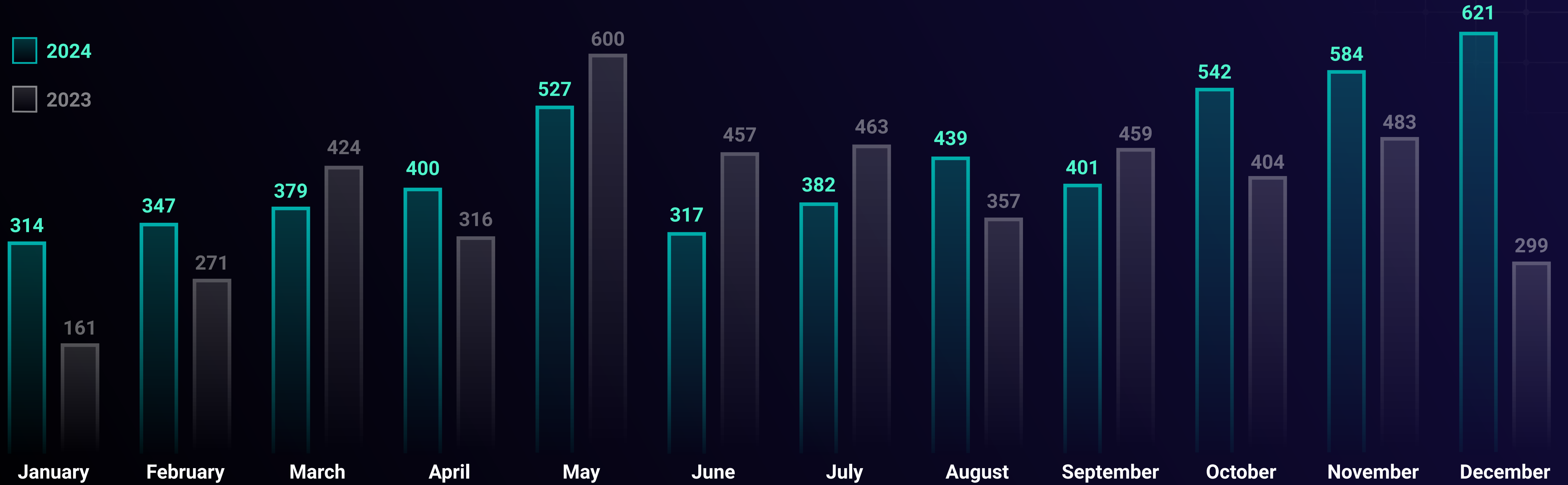


Figure 15: Ransomware volume trends, 2024 vs. 2023

From Extortion to Exit Scams: The Big Ransomware Group Shake-Up of 2024

LockBit Affects 93% Fewer Organizations



2024 marked the year that LockBit—the omnipresent ransomware threat throughout 2023—became the target of multiple law enforcement operations that disrupted its infrastructure.³

While LockBit attempted a comeback in May by naming 176 organizations on its data-leak site, it failed to sustain momentum, ending the year with only 19 victims in its final quarter—a staggering 93% decrease compared to the same period in 2023.

ALPHV Exits with Big Profits



“ALPHV’s” sudden exit in March 2024, following a reported \$22 million payday from its attack on Optum, added to the turbulence in the ransomware landscape.

With LockBit in decline and “Clop” sticking to its strategy of infrequent but high-reward attacks, the absence of these dominant players created an opening for smaller, fragmented groups to rise to prominence throughout 2024.

RansomHub Ups the Ante

RansomHub

“RansomHub” wasted no time capitalizing on the void left by declining giant, LockBit. Its game-changing affiliate model—paying affiliates 90% of the profits upfront while retaining just 10%—made it a top choice among cybercriminals, driving a surge in activity.

By the second half of 2024, RansomHub had firmly established itself as the most active ransomware group, naming 326 more victims than LockBit.



Figure 16: Top ransomware groups by number of data-leak postings, 2024 vs. 2023

Groups to Watch Out for in 2025

The “BlackLock” (aka Eldorado) ransomware group, active since at least March 2024, gained prominence in July but truly made its mark in October. Its victim count skyrocketed by over 1,000% from Q3 to Q4 2024.

Likely tied to Russia (evidenced by its refusal to target countries in the Commonwealth of Independent States), BlackLock’s rapid ascent mirrors that of groups like RansomHub, proving how quickly a group can move from obscurity to dominance.

In September 2024, new group “FunkSec” emerged on the ransomware scene, making a major impact by December by listing 82 victims—more than any other group that month.

FunkSec targeted a wide range of sectors, including retail, manufacturing, health care, education, and professional services, across countries like the US, France, India, and Thailand. The group promotes its technical expertise on cybercriminal forums, boasting a free distributed denial-of-service (DDoS) tool, a Tor-based data-leak site, and a suite of self-developed tools.

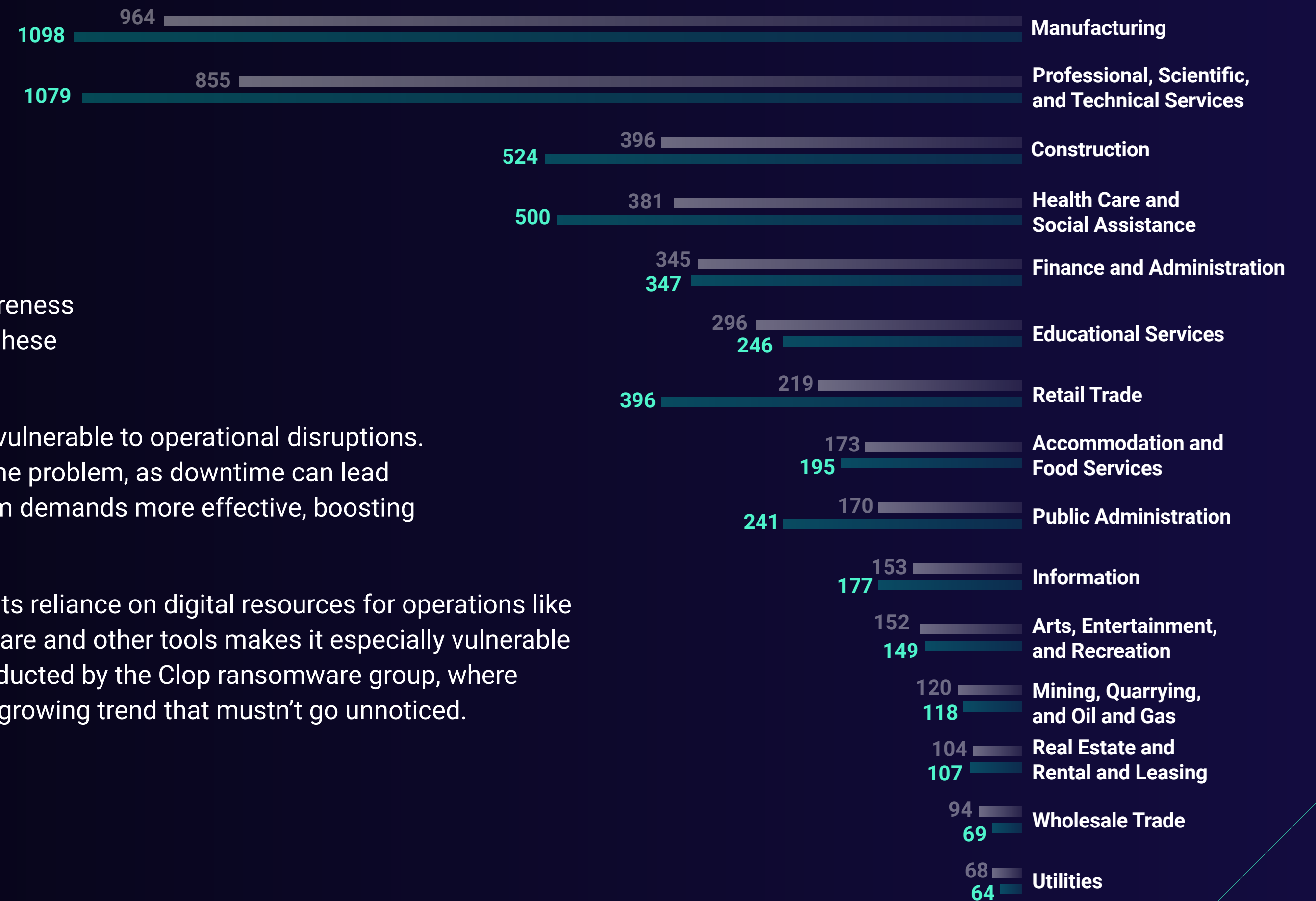
It’s realistically possible that both BlackLock and FunkSec stockpiled victims and chose to publish them all on their respective data-leak sites before the year ended. However, our analysis suggests it’s more likely that both groups capitalized on the turbulence amongst ransomware groups, scooping up affiliates from faltering groups and thriving in the absence of dominant players.

The constantly changing ransomware threat means that traditional defenses won’t cut it anymore. Organizations must adopt proactive, multi-layered strategies that combine technology, processes, and people. In 2025, ransomware will remain largely opportunistic, but the explosion of new groups and affiliates will make attacks more unpredictable and widespread than ever before.



Figure 17: Number of victims by region added to ransomware data-leak sites, 2024 vs 2023

Figure 18: Number of victims by industry added to ransomware data-leak sites, 2023 vs 2024



As anticipated, the US remained the overwhelmingly popular target for ransomware operators and affiliates in 2024.

This trend is highly likely to continue, as attackers perceive that organizations in English-speaking countries have the financial means to pay ransoms.

Additionally, well-developed insurance markets and heightened cybersecurity awareness in these countries have driven higher adoption of ransomware insurance, making these regions more attractive to attackers.

Ransomware operators are acutely aware that the manufacturing sector is highly vulnerable to operational disruptions. The integration of IT with operational technology (OT) in this sector exacerbates the problem, as downtime can lead to major productivity, financial, or legal consequences. These factors make ransom demands more effective, boosting ransomware groups' profits and attack success rates.

The PSTS sector is a lucrative target because of the sensitive data it handles and its reliance on digital resources for operations like client collaboration and secure file transfers. Its dependence on file-transfer software and other tools makes it especially vulnerable to exploitation. This vulnerability was evident in multiple supply-chain attacks conducted by the Clop ransomware group, where adversaries compromised widely used tools to target numerous organizations—a growing trend that mustn't go unnoticed.

Take Action

Against Ransomware

- ✔ Use GreyMatter Digital Risk Protection (DRP) to detect exposed credentials on cybercriminal forums and thwart initial access attempts by ransomware groups.
- ✔ Prioritize employee awareness training on social engineering tactics, as groups like Black Basta and RansomHub continue to exploit human vulnerabilities with success.
- ✔ Use GPOs to restrict PowerShell usage to only those users who require it for their role. This will prevent ransomware actors from abusing PowerShell to execute malicious scripts.

GreyMatter Detections and Automations for Combatting Ransomware

To combat ransomware and data exfiltration threats, we advise customers to use the following targeted detection rules and GreyMatter threat hunting packages that are designed to identify specific malicious activity, such as the use of exfiltration tools and ransomware-specific behaviors.

These solutions help organizations detect and disrupt data theft, unauthorized access, and ransomware deployments, minimizing the impact of attacks and protecting critical assets.

Recommended Detection Rules



Rclone Execution via Command Line: Rclone is a powerful and effective tool for copying data to various cloud storage providers, making it a popular choice for ransomware operators to facilitate exfiltration. This rule detects the use of Rclone by looking for common arguments in PowerShell or the Command Prompt.



Data Exfiltration via Command Line: After retrieving the information they want to exfiltrate—such as credentials or sensitive documents—threat actors can use the command line to execute data exfiltration commands. This rule specifically detects the different methods threat actors use to leverage command-line arguments for exfiltrating data.

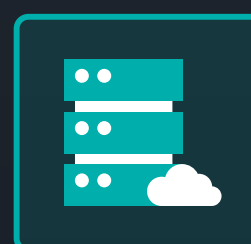


Ransomware File Extension: Once ransomware is deployed, it encrypts many files at once with a unique file extension typically only associated with ransomware attacks. This rule identifies file modifications that change extensions to those known to be used in ransomware operations.

Recommended Threat Hunting Packages



Exfiltration Tools: Identifies the use of legitimate or native tools abused by threat actors to exfiltrate data. By detecting unusual patterns or activity from unexpected sources, this threat hunting package helps uncover malicious intent and mitigate the risk of data breaches.



Proxy and Protocol Tunneling Tools: Detects unauthorized or suspicious use of proxy and tunneling software within an environment. By analyzing endpoint telemetry, this threat hunting package identifies deviations from normal usage patterns, enabling organizations to uncover malicious activities such as bypassing security controls, data exfiltration, or maintaining stealthy persistence.



RMM Software: Identifies suspicious or unauthorized use of RMM software within an environment by analyzing process events. This threat hunting package detects threat actors abusing RMM software as backdoors or for data exfiltration by focusing on deviations from expected usage baselines, exposing malicious activity disguised as legitimate business operations.

Next Steps: A CISO's Checklist

The biggest takeaway from 2024? Cyber threats are outpacing and outsmarting traditional or poorly implemented security controls.

Attackers are now averaging just 48 minutes to move laterally, adapting to security controls, bypassing MFA in 100% of successful BEC incidents we investigated, and blending into environments by exploiting the very software and tools organizations rely on daily.

In 80% of breaches, attackers exfiltrated data by mimicking normal activity, thereby avoiding detection. Our analysis also revealed that the top cause of major incidents was visibility gaps.



Armed with this knowledge, it's time to act. Throughout this report, we've shared targeted recommendations to mitigate the threats we've identified—but there's more that organizations can do.

We've compiled the main takeaways every CISO needs to know. By adopting these measures, organizations will be better positioned to minimize their exposure and outmaneuver this year's biggest threats.

Read on to explore

our top strategies for tackling the three core issues highlighted in this report.

To Respond at Top Speed, Automate

- ✓ Automated responses excel in scenarios where speed is critical. GreyMatter Automated Response Playbooks can reduce MTTC to as low as three minutes when incorporated into incident response plans.
- ✓ Alternatively, set GreyMatter Response Playbooks to “RQ Approved” to allow ReliaQuest to remediate incidents directly, significantly improving MTTC and accelerating response times.
- ✓ Implement the GreyMatter AI Agent to entirely eliminate the Tier 1 and Tier 2 tasks that slow down analysts.
- ✓ Use GreyMatter Phishing Analyzer to automate the analysis of user-submitted phishing emails. This significantly accelerates the triage and remediation process for phishing email inboxes, executing actions like email deletion, URL blocking, and host isolation.



Block Initial Access by Shoring Up Foundations

- ✓ Implement MFA, but don't rely on it as a silver bullet solution. Strengthen MFA by incorporating additional safeguards, such as conditional access policies, restricting access to trusted devices, and shortening token expiration times.
- ✓ For VPNs, implement client-based certificates and access policies to restrict authentication, which will reduce the likelihood of unauthorized access. Make an inventory of public-facing devices, prioritize patching to address vulnerabilities, and prepare continuity plans if critical devices must be temporarily disconnected to prevent exploitation.
- ✓ Train employees to recognize social engineering tactics, particularly employees in IT help-desk roles. Focus on robust training programs, testing, and clear standard operating procedures to prevent successful social engineering attacks.



Disrupt and Contain Attackers with Defense-in-Depth

- ✓ Rotate potentially compromised credentials at the earliest opportunity. Acting quickly prevents attackers from exploiting valid accounts to move laterally within compromised networks.
- ✓ Verify that service accounts are not overprivileged with domain admin rights, enforce password length and complexity requirements for service accounts, and enable Advanced Encryption Standard (AES) encryption for Kerberos to mitigate cracking.
- ✓ Ensure comprehensive logging and coverage for endpoint security tools, including critical assets. This approach will eliminate blind spots and enhance security monitoring, allowing for faster threat detection.
- ✓ Implement detection rules to identify the unauthorized use of tools or software and engage in frequent threat hunting to detect anomalous activities. Serious threats fly under the radar, so a defense-in-depth strategy is key to staying ahead.



Our Threat Forecast for 2025

Looking ahead, **ransomware attacks** are set to surge [throughout 2025](#), surpassing their 2024 levels and rivaling December's record-breaking activity.

While RansomHub may dominate early in the year, we expect BlackLock to take the lead by Q3.

Meanwhile, we anticipate that **8–10%** of investigations will likely involve threat actors leveraging large language model (LLM) tools, alongside a projected **10%** increase in non-human identity (NHI)-based attacks, such as the compromise of API keys, service accounts, and digital certificates.

Spearphishing, exploiting public-facing applications, and targeting external remote services will remain key tactics, fueled by rapid vulnerability exploitation, human error, exposed credentials, and ever-expanding attack surfaces.

ReliaQuest Exists to Make Security Possible

ReliaQuest's AI-powered security operations platform, GreyMatter, is purpose-built to confront these challenges, providing customers with the capabilities they need to secure their environments against the threats detailed in this report.

To accelerate containment and response, we've created our own agentic AI Agent as well as developed Automated Response Playbooks that prevent cybercriminals from gaining or maintaining a foothold—all without manual effort.

RELIAQUEST GREY MATTER®

The GreyMatter AI Agent autonomously handles **100%** of security alerts end-to-end. Combining this capability with Automated Response Playbooks has enabled our customers to achieve containment and response times as low as 3 minutes. When customers pair Digital Risk Protection with GreyMatter, they achieve 360-degree visibility into the threats facing their organization, both within their environment and outside it. DRP identifies threats on the open, deep, and dark web, allowing customers to counter them before they reach their attack surface.

GreyMatter also uses external threat data, including the latest threat actor TTPs, to develop threat hunting packages that customers can use to proactively identify early indicators of compromise. By spotting known tactics early, customers prevent attacks from progressing.



With GreyMatter, ReliaQuest customers are well armed against the threats facing us in 2025 and beyond. To see how GreyMatter can help protect your organization, visit reliaquest.com to request a demo tailored to your environment.

The last year in cyber threats has emphasized again and again the critical importance of speed, automation, visibility, and proactiveness in modern security operations.

Organizations must have the right weapons in their arsenal to defend against attackers who are getting smarter and more efficient.

About ReliaQuest

ReliaQuest exists to Make Security Possible.

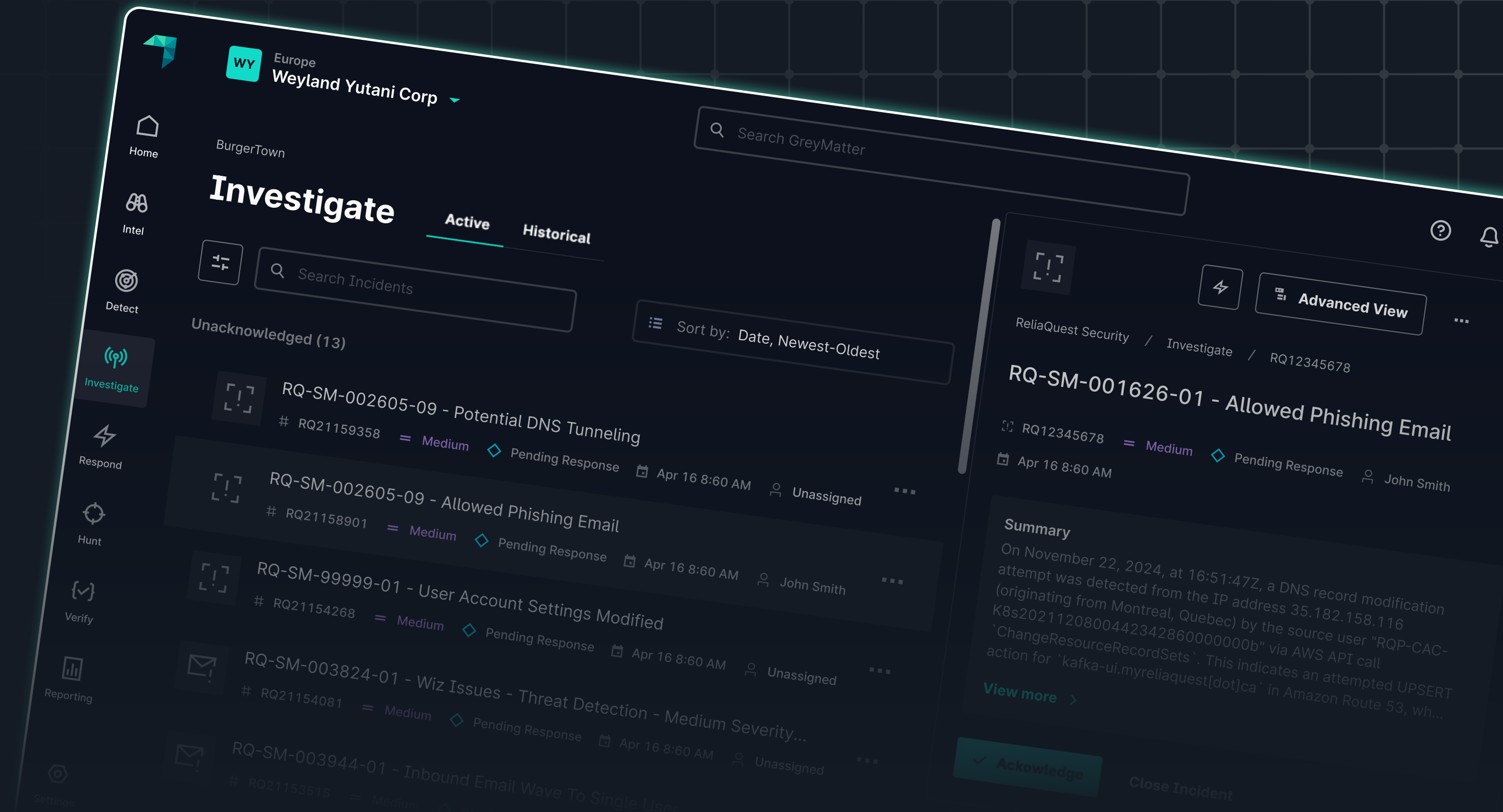
Our agentic AI-powered security operations platform, GreyMatter, allows security teams to detect threats at the source, and contain, investigate, and respond in less than 5 minutes—eliminating Tier 1 and Tier 2 security operations work.

GreyMatter uses data-stitching, detection-at-source, AI, and automation to seamlessly connect telemetry from across cloud, multi-cloud, and on-premises technologies.

ReliaQuest is the only cybersecurity technology company that delivers outcomes specific to each organization's unique architecture, technology, and business needs.

With over 1,000 customers and 1,200 teammates across six global operating centers, ReliaQuest Makes Security Possible for the most trusted enterprise brands in the world.

[Learn more at www.reliaquest.com](http://www.reliaquest.com) →



[ReliaQuest's ShadowTalk](#) is a weekly podcast featuring discussions on the latest cybersecurity news and threat research.

Listen to the latest episodes on your favorite podcast channels.



reliaquest.com

[800.925.2159](tel:800.925.2159)

info@reliaquest.com

Endnotes

1. https://nvd.nist.gov/vuln/search/statistics?form_type=Advanced&results_type=statistics&search_type=all&isCpeNameSearch=false&cvss_version=3&cvss_v3_metrics=AV%3AN%-2FAC%3AL%2FPR%3AN%2FUI%3AN&cvss_v3_severity=CRITICAL
2. <https://www.darkreading.com/cyberattacks-data-breaches/canadian-authorities-arrest-snowflake-data-thief>
3. <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>