paloalto NETWORKS | UNIT 42

# Global Incident Response Report

## 2025

# Table of Contents

# Executive Summary

We see five major emerging trends reshaping the threat landscape.

- **First**, threat actors are augmenting traditional ransomware and extortion with attacks designed to intentionally disrupt operations. In 2024, 86% of incidents that Unit 42 responded to involved business disruption — spanning operational downtime, reputational damage or both.
- **Second**, software supply chain and cloud attacks are growing in both frequency and sophistication. In the cloud, threat actors often embed within misconfigured environments to scan vast networks for valuable data. In one campaign, attackers scanned more than 230 million unique targets for sensitive information.
- **Third**, the increasing speed of intrusions — amplified by automation and streamlined hacker toolkits — gives defenders minimal time to detect and respond. In nearly one in five cases, data exfiltration took place within the first hour of compromise.
- **Fourth**, organizations face an elevated risk of insider threats, as nation-states like North Korea target organizations to steal information and fund national initiatives. Insider threat cases tied to North Korea tripled in 2024.
- **Fifth**, early observations of AI-assisted attacks show how AI can amplify the scale and speed of intrusions.

Amid these trends, we're also seeing a multi-pronged approach in attacks, as threat actors target multiple areas of the attack surface. In fact, 70% of the incidents Unit 42 responded to happened on three or more fronts, underscoring the need to protect endpoints, networks, cloud environments and the human factor in tandem. And on the human element — nearly half of the security incidents (44%) we investigated involved a web browser, including phishing attacks, malicious redirects and malware downloads.

Drawing from thousands of incident responses over years of experience, we've identified three core enablers that allow adversaries to succeed: **complexity, gaps in visibility and excessive trust**. Fragmented security architectures, unmanaged assets and overly permissive accounts all give attackers the space they need to succeed.

To confront these challenges, security leaders must **accelerate their journey to Zero Trust**, reducing implicit trust across the ecosystem. Equally crucial is **securing applications and cloud environments** from development to runtime, ensuring that misconfigurations and vulnerabilities are swiftly addressed. Finally, it's essential to **empower security operations to see more and respond faster** — with consolidated visibility across on-premises, cloud and endpoint logs, as well as automation-driven threat detection and remediation.

# 1 Introduction

Over my two-decade career as an incident responder, I've witnessed **countless shifts in the threat landscape and attacker tactics.**

When ransomware first appeared, file encryption became the tactic of choice for cybercriminals. Locking up files, getting paid for an encryption key, and moving on. Backups got better, and double extortion became more popular. Cybercriminals leveraged harassment (and still do) to tell companies "pay, or we will leak sensitive data." But even that is losing its luster.

Almost every month, I receive notice of a data breach. Occasionally, I open and read these letters; admittedly other times, they go directly into the trash. Like many people, I've invested in identity theft protection software and adhere to best practices in cyber hygiene. With the onslaught of these notifications, it's hard not to imagine the everyday person thinking: My data has been leaked again, so what? This desensitized mindset is unsettling. And yet, despite this public apathy, a data breach can still cause substantial damage to a company.

**The past year has marked yet another shift in attacker focus to intentional operational disruption.** This new phase in financially motivated extortion prioritizes sabotage — where attackers are intentionally destroying systems, locking customers out of their environments, and forcing prolonged downtime — so threat actors can maintain their ability to have maximum impact with their attacks and command payment from organizations.

In 2024, Unit 42 responded to over 500 major cyberattacks. These incidents involved large organizations grappling with extortion, network intrusions, data theft, advanced persistent threats and more. The targets of these attacks spanned **all major industry verticals and 38 countries.**

We've responded to breaches occurring at unprecedented speed, causing severe operational disruption and cascading impacts — **from downtime and service outages to costs reaching *billions* of dollars.** In every case, the situation had escalated to the point where the security operations center (SOC) called for backup.

When Unit 42 is called, our Incident Response team works swiftly to contain threats, investigate incidents, and restore operations. After the crisis, we partner with clients to strengthen their security posture against future attacks.

**The Unit 42 mission is clear: protecting the digital world from cyberthreats. Operating 24/7 across the globe,** our team is united by the purpose of stopping threat actors, hunting evolving threats and helping organizations prepare for and recover from even the most sophisticated attacks.

This report is organized to guide you through our key findings and actionable insights:

- **Emerging Threats and Trends:** A look at what's coming, including the rise of disruption-driven extortion, AI-assisted attacks, cloud and software supply chain-based attacks, nation-state insider threats, and speed.
- **How Threat Actors Succeed:** Analysis of the most common effective tactics, techniques and procedures, from initial access to impact.
- **Recommendations for Defenders:** Practical guidance for executives, CISOs and security teams to fortify their defenses, build resilience and stay ahead of the threat.

As you read, consider not just what's happening, but what's next and how your organization can prepare to meet the challenges of an increasingly complex threat environment.

**Sam Rubin**
SVP of Consulting and Threat Intelligence
Unit 42

# 2 Emerging Threats and Trends

In 2025, organizations face a complex mix of threats from financially driven cybercriminals, well-resourced nation-states, insider schemes and ideologically motivated hacktivists. While extortion attacks remain dominant among criminal groups, sophisticated nation-state adversaries target critical infrastructure, supply chains and key industries. Insider risks intensify as contractors and employees with privileged access can bypass external defenses, and hacktivists exploit social media networks to coordinate large-scale disruptions.

Against this backdrop, Unit 42 has identified five key trends where we see the most significant and immediate impact on organizations: **intentionally disruptive extortion attacks, software supply chain and cloud exploitation, the increasing speed of attacks, North Korean insider threats and AI-assisted threats.**

## Trend 1. Disrupting Business Operations: The Third Wave of Extortion Attacks

As defenses improve, backups become more common and successful as cyber hygiene matures. Attackers have been forced to innovate their approaches to ensure they can command consistent — and higher — payments.

Extortion attacks evolved over the past decade: from encryption, to exfiltration and multi-extortion techniques, to intentional disruption. Though ransomware remains a headline threat, attackers have shifted from solely encrypting data to more disruptive tactics like harassing stakeholders and threatening critical operations resulting in long periods of downtime.

In 2024, 86% of incidents that Unit 42 responded to had some sort of impact-related loss. This includes:

- Outright business disruption
- Asset and fraud-related losses
- Brand and market damage as a result of publicized attacks
- Increased operating costs, legal and regulatory costs, and more

We can define the evolution of extortion attacks in terms of three waves.

## Wave 1: In the Beginning, There Was Encryption

The rise of cryptocurrency enabled larger-scale crime with smaller-scale risk to the criminal. Threat actors quickly adopted ransomware as a profitable attack method, locking up critical files, holding them for ransom and demanding a cryptocurrency payment to unlock them. Cryptocurrency has since become a critical enabler of ransomware attacks:

- Reducing the attacker's risk of being identified
- Lowering the barrier to entry for cybercriminals
- Helping the attacker evade law enforcement and international sanctions

In those early ransomware cases, the playbook was simple. Get in, encrypt the files and get out. Unit 42 investigations from this period rarely uncovered signs of data exfiltration.

Attackers are now more sophisticated, often combining encryption with data theft and double extortion threats, but encryption itself is still a go-to tactic. In fact, Unit 42's latest incident response data shows that encryption remains the most common tactic used in extortion cases, holding relatively steady over the past 4 years.

Over time, as organizations have improved their data backup practices, encryption as the sole extortion tactic has become less effective. Backups have helped more organizations recover faster — nearly half (49.5%) of impacted victims were able to restore from backup in 2024. As seen in Figure 1, this is about five times as many as in 2022, when only 11% of victims were able to restore from backup.

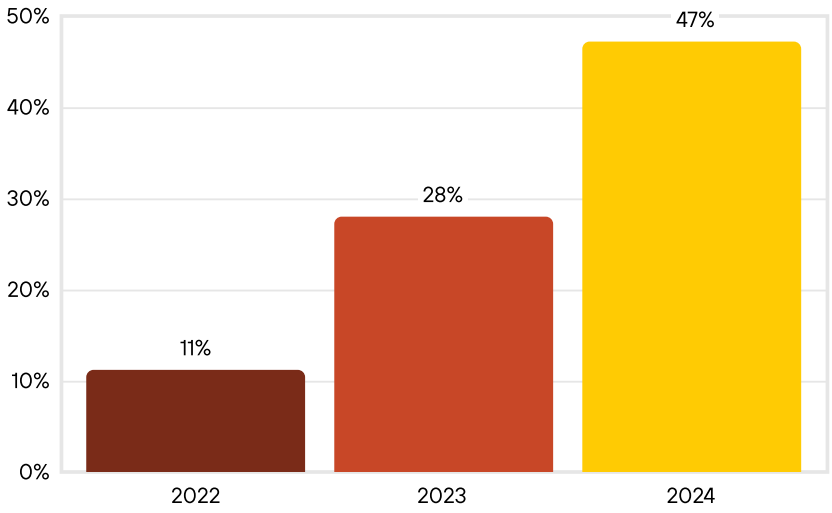



**Figure 1.** The percentage of victims who successfully restored encrypted files from backup rose 360% between 2022-2024.

However, these defensive measures do little to counter the risk of attackers publishing or selling stolen data.

## Wave 2: Upping the Ante With Data Exfiltration

As focusing solely on encryption became less effective, attackers pivoted to a new extortion tactic: data exfiltration and subsequent harassment. In addition to using exfiltrated data to pressure victims through blackmail and harassment, financially motivated actors gained additional revenue streams, such as auctioning data on dark-web marketplaces.

Attackers threatened to leak sensitive information publicly, often hosting leak sites touting their alleged victims. Some bombarded employees and customers with malicious messages.

However, while data theft remains a popular tactic, its effectiveness has started to decline for several reasons. Data breach fatigue has made dark web leaks less impactful in pressuring victims to pay.

According to the Identity Theft Resource Center's 2023 Data Breach Report, 353 million victims had their data leaked in 2023 alone. Additionally, while attackers do keep their promises more often than not, organizations are increasingly concerned about the times when they don't.

In fact, in fewer than two thirds of cases with data theft in 2024 did attackers provide any proof of data deletion (only 58%). In some cases, Unit 42 became aware that despite providing such alleged "proof," the threat actor had retained at least some of the data. While two thirds of the time is still most of the time, that's far from the level of certainty most would expect when paying an (often exorbitant) fee for something.

Public leak site data supports this trend. After a 50% increase in leak site victims from 2022-2023, the number rose by only 2% in 2024. This may indicate that threat actors are finding leak site extortion less effective in compelling payments.

Extortion tactics rely on instilling fear and keeping the victim's full attention. To achieve this, threat actors will continue to evolve their methods to remain at the forefront of disruption.

This doesn't mean that attackers are abandoning exfiltration. As seen in Table 1, threat actors continue to steal data more than half the time, and their use of harassment is steadily rising. However, threat actors are piling on additional tactics to ensure they get their payouts.

| Extortion Tactic | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|
| Encryption | 96% | 90% | 89% | 92% |
| Data Theft | 53% | 59% | 53% | 60% |
| Harassment | 5% | 9% | 8% | 13% |

**Table 1.** Prevalence of extortion tactics in extortion-related cases.

Deliberate disruption is the next phase in the evolution of financially motivated attacks as threat actors continue to turn up the volume to get their victims' attention.

## Wave 3: Intentional Operational Disruption

Attackers are increasing the pressure by focusing on a third tactic: intentional disruption. In 2024, 86% of incidents that Unit 42 responded to involved some sort of loss that disrupted the business either operationally, reputationally or otherwise.

Unit 42 observed attackers combining encryption techniques with data theft and then going even further with other tactics to visibly disrupt organizations. They damaged victims' brand reputation or harassed their customers and partners. Attackers also deleted virtual machines and destroyed data (section 5.1 offers a full breakdown of MITRE techniques attackers used for this type of impact).

We have seen attackers disrupt victims who have deep partner networks that they rely on to conduct business. When an organization has to lock down parts of its network to contain the threat actor and remediate the attack before resuming operations, their partners are forced to disconnect. Once back online, the recertification process creates further disruption as partners reconnect to the network.

Sophisticated attackers have targeted enterprises leveraging these tactics — including in healthcare, hospitality, manufacturing and critical infrastructure — with the goal of causing widespread disruption not only to the business but their partners and customers as well.

As businesses grapple with extended downtime, strain on partner and customer relationships and bottom-line impacts, threat actors are taking advantage and demanding increased payments. Businesses looking to get their systems back online and minimize the financial impact (which can stretch to the millions and sometimes even billions) are being extorted for higher payments. The median initial extortion demand increased nearly 80% to $1.25 million in 2024 from $695,000 in 2023.

We also examined demands in terms of how much a threat actor perceives an organization can pay. (We based this on what the threat actor would find by searching for public sources of information about an organization.) The median initial demand in 2024 is 2% of the victim organization's perceived annual revenue. Half of the initial demands fell between half a percent (0.5%) and 5% of the victim's perceived annual revenue. On the high end, we have seen attackers attempt to extort amounts that are more than a victim organization's perceived annual revenue.

However, whereas demands have increased, Unit 42 continues to find success when negotiating the ultimate payment (for clients who pay). As a result, the median ransom payment has risen only $30,000 to $267,500 in 2024. When organizations pay, the median amount is less than 1% of their perceived revenue (0.6%). The median percent reduction negotiated by Unit 42 is therefore more than a 50% decrease from the initial demand.

### Countermeasures: Remaining Resilient in the Face of Increasing Disruption

An important factor to consider when facing disruption-minded threat actors is operational resilience: Can you continue to function if critical systems go down or sensitive data is locked out of reach? Which business operations are essential to maintain? What are your disaster recovery and backup strategies? Are critical partners prepared to shift to new systems in the face of an attack?

The best way to find out is through regular testing and incident simulations, which validate your technical controls, train your response teams, and gauge your capacity to maintain essential services. By focusing on resilience, you not only mitigate the immediate financial impact of an attack, but also protect your long-term reputation and stakeholder trust — key assets in an increasingly volatile cyber landscape.

Extortion attacks and all that comes with them — encryption, data theft, harassment and intentional disruption — are no passing trend. Cybersecurity strategies must continuously evolve to counter the shifting technical tactics of attackers — while also recognizing that threat actors will continuously adapt to overcome stronger defenses.

## Trend 2. Increasing Impact in Software Supply Chain and Cloud Attacks

As organizations increasingly rely on cloud resources for both operations and the storage of valuable data, incidents related to the cloud or SaaS applications are some of the most impactful we see.

A little less than one third of cases (29%) in 2024 were cloud-related. This means that our investigation involved collecting logs and images from a cloud environment or touched on externally hosted assets such as SaaS applications.

Those cases don't necessarily represent the situations in which threat actors are doing damage to cloud assets. We see this in about one in five cases in 2024 (21%), where threat actors adversely impacted cloud environments or assets.

### Identity and Access Management as Contributing Factor

Issues with identity and access management (IAM) continue to be contributing factors in a significant number of cases. Cybercriminals such as Bling Libra (distributors of ShinyHunters ransomware) and Muddled Libra gain access to cloud environments by exploiting misconfigurations and finding exposed credentials.

While lack of multi-factor authentication (MFA) is still the most prevalent contributing factor of this type, we are seeing that issue less frequently. We saw it about one fourth of the time in 2024, compared to about a third of the time in 2023.

Other identity and access management issues are trending in the wrong direction. Excessive policy access, excessive permissions and password issues all became more prevalent in 2024, as shown in Figure 2.

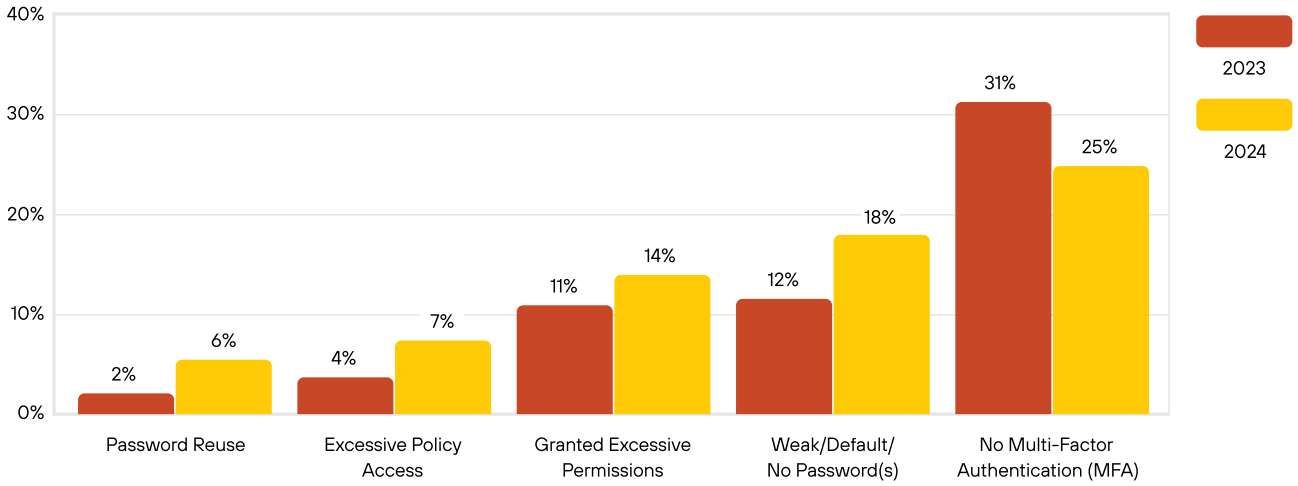



**Figure 2.** Trends in identity and access management issues from 2023 to 2024.

IAM misconfigurations were the initial access vector in about 4% of cases, but this figure should be considered alongside the scale and impact of cloud attacks. Incidents of this type can affect an organization on a wide scale, and can also affect other organizations if threat actors are able to commandeer cloud resources.

One extortion campaign's cloud operation took advantage of exposed environment variables, the use of long-lived credentials and the absence of least-privilege architecture. Once the threat actors succeeded in embedding attack infrastructure within multiple organizations' cloud environments, they used this as a jumping off point to attack other organizations on a large scale. This included scanning more than 230 million unique targets for additional exposed API endpoints. As a result, the threat actor was able to target exposed files from at least 110,000 domains, collecting more than 90,000 unique leaked variables. Of these variables, 7,000 were associated with cloud services and 1,500 with social media accounts, often including account names in addition to information needed for authentication.

On multiple occasions, Unit 42 has observed threat actors using leaked API/access keys for initial access. This often gives threat actors leverage for further compromise. The use of valid cloud accounts (T1078.004) appears repeatedly in our case data in relation to the following tactics:

- Initial Access (13% of cases where we observed this tactic)
- Privilege Escalation (8%)
- Persistence (7%)
- Defense Evasion (7%)

## Exfiltration and Cloud Storage

We responded to multiple cases of threat actors accessing, exfiltrating and then deleting organizations' cloud storage. The speed of exfiltration (often less than a day), combined with data destruction can put extreme pressure on organizations to comply with extortion demands.

In some cases, attackers have also exfiltrated cloud snapshots, which are point-in-time copies of the contents of a cloud storage volume. This activity can expose critical data and can also be difficult to detect amid legitimate uses of snapshots for backup purposes.

The use of cloud resources for exfiltration is very common, even though cloud dataplane compromises represent a small percentage of overall cases (less than 5%). In 45% of cases where we observed exfiltration, attackers sent the data to cloud storage (T1567.002 - Exfiltration Over Web Service: Exfiltration to Cloud Storage), a technique that can also mask the attackers' activity within legitimate organizational traffic.

## Poor Visibility and Control of SaaS and Cloud-Based Systems

A common issue for SaaS and cloud-based systems is lack of visibility into or attention to issues on those systems.

In one investigation, the organization successfully mitigated an attack, only to be compromised again a short time later.

Our investigators discovered that threat actors had automated exploitation of a vulnerability within a service used within the organization's cloud-based products. By combining this with using anti-forensic techniques to hide activity, the threat actor was able to regain access to the organization and its clients even after internal teams appeared to have successfully removed them.

## Web Scraping and API Abuse

Though data scraping is not always malicious, its weaponization emerged as a significant threat in 2024. In one case, a threat actor executed billions of daily unauthorized scraping requests. This was an operation that would have cost more than $6 million annually in compute resources had we not identified the activity and aided with its mitigation.

Our incident response teams responded to attacks leveraging advanced techniques to bypass security controls, while cybercrime groups integrated scraping into their attack lifecycle to fuel fraud operations. In another case, attackers' systematic, unauthorized scraping of documents forced an organization to completely re-architect their API infrastructure.

With privacy laws evolving to address automated collection, organizations face pressure to implement unauthorized scraping detection measures. Yet many struggle to differentiate between legitimate access and malicious scraping, often discovering data harvesting only after significant exposure has occurred.

## Cloud-Enabled Attacks

Attackers frequently use compromised cloud resources to attempt to exploit or brute force other unrelated targets.

Another emerging trend is adversaries manipulating environment configurations (beyond a single host) to further enable or conceal their activity.

In cloud environments, threat actors can perform the following activities, for example:

- Abuse admin-level access (or the equivalent user account permission misconfigurations, T1098 - Account Manipulation)
- Hijack cloud resources (T1578 - Modify Cloud Compute Infrastructure, T1496.004 - Resource Hijacking: Cloud Service Hijacking)
- Infect critical centrally managed configuration settings (T1484 - Domain or Tenant Policy Modification).

## Software Supply Chain Attacks and Third-Party Software

In 2024, we responded to a number of incidents related to the software supply chain.

A critical vulnerability in the data compression library XZ Utils was identified before it could do large-scale damage. However, it remains a lesson in the potential impact of supply chain compromises. According to Red Hat at the time of the disclosure, the XZ tools and libraries contained "malicious code that appears to be intended to allow unauthorized access." Since XZ Utils is included in a variety of major Linux distributions – which are used in turn by countless organizations around the world – successful deployment of this malicious code could have exposed thousands of organizations around the world. The result of a "multi-year effort," the issue in XZ Utils underscores the need for all organizations to implement best practices around the open source software incorporated into their systems.

Several vulnerabilities in VPN appliances also raised concerns about the integrity of third-party software. We saw these vulnerabilities used as initial access vectors by both nation-state threat actors and cybercriminals.

Threat actors do not always need to use vulnerabilities to attack organizations through third-party software. In June 2024, the cloud-based data platform Snowflake warned that threat actors were targeting some of its customers' accounts. The company said its research indicated that attackers were using previously compromised credentials (T1078 - Valid Accounts) and cited "ongoing industry-wide, identity-based attacks with the intent to obtain customer data."

In a different matter worked by Unit 42, threat actors spent months brute-forcing a VPN (T1110 - Brute Force). Their eventual success allowed them to gain access to and maintain persistence in the organization's environment.

The complexity of infrastructure and resulting lack of visibility can make it challenging to fully remediate attacks, particularly when incorporating third-party software.

### Countermeasures: Defending Against Software Supply Chain and Cloud Attacks

To reduce risk from supply chain and cloud-based attacks, focus on a few key tactics:

- **Limit credential abuse:** Enforce strict IAM controls, granting only the privileges necessary for each role. Use short-lived credentials and multi-factor authentication wherever possible.
- **Centralize logging and auditing of production cloud resources:** Forward logs off the originating host to prevent tampering, and aggregate them for correlation across services. Track anomalies such as unusual API calls or large data transfers.
- **Monitor usage patterns:** Use log analytics to establish baselines for normal resource consumption and trigger alerts for deviations. Attackers frequently spike CPU or bandwidth usage during data exfiltration or cryptomining.
- **Patch promptly:** Treat third-party libraries, container images and open-source components as part of your operational infrastructure. Develop a process to regularly review and quickly deploy security updates.
- **Secure APIs and supply chain integrations:** Apply rate limiting to thwart excessive scraping or brute-force attempts, and use robust scanning tools to assess new dependencies before integrating them into production.

By applying these measures consistently, security teams can identify attacks early, limit their impact and maintain confidence that cloud resources and software pipelines remain under control.

## Trend 3. Speed: Attacks are Getting Faster, Giving Defenders Less Time to Respond

Unit 42 has observed a notable acceleration in cyberattacks as threat actors increasingly adopt automation, ransomware-as-a-service (RaaS) models and generative AI (GenAI) to streamline their campaigns. These tools allow attackers to rapidly identify vulnerabilities, craft convincing social engineering lures and ultimately execute attacks at scale, faster.

The speed of attacks forces global organizations to reassess their response capabilities and prioritize early detection. In many cases, just a few hours can determine whether an attacker succeeds in completing their mission, including data theft, encryption or operational disruption. As attackers continue to refine their methods and accelerate their timelines, the need for proactive security measures and rapid incident response is critical.

One of the ways Unit 42 gauges attack speed is by measuring time to exfiltration — how quickly an attacker exfiltrates stolen data following initial compromise.

In 2024, the median time to exfiltration in attacks that Unit 42 responded to was about two days. This time frame is notable because organizations often take several days to detect and remediate a compromise.

Examining the subset of cases where exfiltration happened most quickly, the speed of exfiltration is even more concerning.

- **In a quarter of cases, the time from compromise to exfiltration was less than five hours.** This is three times faster than in 2021, when for the first quartile of cases, exfiltration took place in less than 15 hours.

For a large proportion of incidents, attackers are even faster.

- **In one in five cases (19%), the time from compromise to exfiltration was less than one hour.**

In three recent cases that Unit 42 responded to, we observed attacker speed in action:

- RansomHub (tracked by Unit 42 as Spoiled Scorpius) accessed a municipal government's network through a VPN that lacked multi-factor authentication (MFA). Within seven hours of gaining a foothold, the threat actor exfiltrated 500 GB of data from the network.
- A threat actor brute-forced a VPN account to gain access to a university. After identifying a system without XDR protection, they deployed ransomware and exfiltrated data within 18 hours.

Muddled Libra (also known as Scattered Spider) successfully social-engineered a service provider's helpdesk to gain access to a privileged access manager (PAM) account. Using this access, they retrieved stored credentials and compromised a domain-privileged account — all within just 40 minutes. With domain access secured, the threat actor breached a password management vault and added a compromised account to the client's cloud environment, escalating permissions to enable data exfiltration.

Defenders have less time than ever to identify, respond to and contain an attack. In some cases, they have less than an hour to respond.

However, we are making progress in reducing dwell time, which is measured as the number of days an attacker is present in a victim environment before an organization discovers or detects the attacker. Dwell time in 2024 decreased 46% to 7 days from 13 days in 2023. This continues a trend of decreasing dwell time that we have observed since 2021, when dwell time was 26.5 days.

## Countermeasures: Defending Against Faster Attacks

To improve your defense against ever faster attacks, consider the following tactics:

- **Measure detection and response times:** Tracking and driving continuous improvement in mean time to detect (MTTD) and mean time to respond (MTTR) means your SOC is getting faster.
- **Leverage AI-driven analytics:** Centralize data sources and identify anomalies in real time, surfacing critical alerts faster than manual methods.
- **Use automated playbooks:** Predefine containment actions to isolate compromised endpoints or lock down user accounts within minutes.
- **Test continuously:** Conduct regular tabletop and red-team exercises to ensure your SecOps team can pivot seamlessly from detection to response.
- **Prioritize high-risk assets:** Focus swift-response capabilities on your most critical systems, where downtime or data loss would be most damaging.

By integrating real-time visibility, AI insights and automated workflows, you can outpace even the fastest-moving adversaries.

## Trend 4. The Rise of Insider Threats: North Korea's Insider Threat Spree

Insider threats pose some of the most elusive risks for any organization, as they exploit the privileged access and trusted relationships that businesses depend on to operate. The ability to sidestep many external defenses makes these threats exceptionally challenging to detect.

North Korean nation-state threat groups have recently engaged in even more disruptive insider threat attacks by placing operatives in technical positions in international organizations. The campaign we track as Wagemole (also known as "IT Workers") has transformed engineering roles themselves into another attack surface. This generates hundreds of millions of USD and other hard currencies for the North Korean regime in the process.

North Korean threat actors exploit traditional hiring processes with stolen or synthetic identities backed by detailed technical portfolios. These portfolios can include legitimate references obtained through identity manipulation and previous real work histories that pass basic verification.

About 5% of our incident response cases in 2024 related to insider threats, and the number of those tied to North Korea tripled compared to the previous year. While greater awareness of the threat may have led to more clients looking for it, it is significant that these threat actors continue to operate.

No sector is immune from this threat. In 2024, these actors expanded their reach to include financial services, media, retail, logistics, entertainment, telecommunications, IT services and government defense contractors. Large technology companies remained primary targets.

### Contract Workforce

These campaigns typically target organizations utilizing contract-based technical roles. Staffing firms become unwitting facilitators for North Korean IT worker schemes due to:

- Abbreviated verification processes to meet rapid staffing demands
- Limited identity verification mechanisms
- Poor visibility into subcontracted workforce providers
- Pressure to quickly fill positions in a competitive market

While North Korean operatives have successfully obtained full-time positions, the contract workforce remains their most utilized vector of infiltration.

### Evolving Tactics

The technical sophistication of these operatives has evolved. Where they once relied heavily on commercial remote management tools, they've recently shifted toward more subtle approaches.

Most concerning is the increasing use of hardware-based KVM-over-IP solutions — small devices that connect directly to target systems' video and USB ports, providing remote control capabilities that can bypass most endpoint monitoring tools. These devices are attached to the computers that the target organization themselves provided to further the threat actors' aims.

Visual Studio Code tunneling features, originally designed for legitimate remote development, now serve as covert channels for maintaining access.

The nature of these operations presents detection challenges because many operatives possess genuine technical skills. Their access appears legitimate because it is. They perform their assigned work while simultaneously serving their true objectives.

### Threats Posed by Fake IT Workers

Once embedded within a company, in addition to illegally collecting salaries that help support the regime, these insiders engage in a range of malicious activities:

- **Data exfiltration:** Systematic exfiltration of sensitive business data and internal documentation — using security policies, vulnerability reports and interviewing guides to better evade detection while targeting client data, source code and intellectual property.
- **Unauthorized tool deployment:** Introducing remote management and other unauthorized tools to maintain access or prepare for further exploitation.
- **Altering source code:** With access to a source code repository, the threat actor may insert backdoor code, potentially enabling unauthorized system access across broader organizations or tampering with financial transactions.
- **Extortion:** In some cases, operatives leverage stolen data to demand ransoms, threatening to leak proprietary information. In some cases, they followed through on these threats.
- **Fake referrals:** Threat actors may refer their associates to the organization, leading to the hiring of additional fake IT workers. In some cases, the referred hires are merely clones of the original referrer, using different fake identities to pose as multiple individuals.

### Countermeasures: Defending Against Fake IT Workers

The North Korean IT worker scheme has shifted from simply collecting revenue to a more evasive insider threat strategy, targeting a wide range of organizations globally. The regime's strategic investment in these operations is a long-term commitment to this approach.

Defending against this threat requires a shift in how organizations approach both workforce management and security.

Addressing insider threats requires more than just technical controls. It demands a culture of security awareness and active monitoring of user activities, particularly among individuals with elevated privileges.

Measures such as implementing least privilege policies and acting on the results of thorough background checks can help minimize the potential for abuse. Additionally, organizations should pay close attention to behavioral indicators, such as unusual data transfers or last-minute system access by employees nearing their departure date. As part of this, it's important to have the ability to put together indicators from various data sources. A behavior may seem innocuous on its own but, in combination with other signals, may indicate the need for an investigation.

Ultimately, trust must be balanced with verification. A single insider incident can undermine years of organizational progress, threaten intellectual property and inflict reputational harm. By fortifying internal processes, monitoring privileged access and emphasizing security at every level, businesses can significantly reduce the likelihood of a damaging insider event.

## Trend 5. The Emergence of AI-assisted Attacks

Although still in early stages, malicious use of GenAI is already transforming the cyberthreat landscape. Attackers use AI-driven methods to enable more convincing phishing campaigns, automate malware development and accelerate progression through the attack chain, making cyberattacks both harder to detect and faster to execute. While adversarial GenAI use is more evolutionary than revolutionary at this point, make no mistake: GenAI is already transforming offensive attack capabilities.

### Enhancing Attack Capabilities with GenAI

GenAI tools, particularly LLMs, are being harnessed by both nation-state APTs and financially motivated cybercriminals to streamline and amplify attacks. These technologies automate complex tasks that previously required significant manual effort, accelerating the entire attack lifecycle.

For example, LLMs can craft highly convincing phishing emails that mimic legitimate corporate communications with unprecedented accuracy, increasing the success rate of phishing campaigns and making them harder to detect with traditional signature-based defenses. Malicious groups are already selling tools that can make convincing deepfakes (these range from free offerings to "enterprise plans" that offer deepfakes for as little as $249/month).

In malware development, LLMs assist in generating and obfuscating malicious code, enabling attackers to create polymorphic malware that can evade standard detection mechanisms. By automating the creation of exploit scripts and refining malware payloads, adversarial AI lowers the technical barriers for less-skilled threat actors, broadening the pool of potential attackers. Additionally, AI-driven tools enhance the capability to identify and exploit vulnerabilities.

## Speed and AI

One of the most profound impacts of AI-assisted attacks is the increase in the speed and efficiency of cyberattacks. Tasks that traditionally took days or weeks can now be completed in minutes.

To test this, Unit 42 researchers simulated a ransomware attack integrating GenAI at each stage of the attack. Figure 3 below demonstrates the speed of an attack before the use of GenAI — as benchmarked by the median time actually observed in our IR investigations — compared with the time when using GenAI.

Our testing took the time to exfiltration from the median of two days down to 25 minutes — about 100 times faster. While these are lab-based results, it's easy to see how this rapid progression from reconnaissance to exploitation significantly shortens the "time-to-impact," making it challenging for organizations to respond in time to mitigate the damage.

## Countermeasures: Defending Against AI-assisted Attacks

These tactics can help you defend against AI-assisted attacks:

- **Deploy AI-driven detection** to spot malicious patterns at machine speed, correlating data from multiple sources.
- **Train staff** to recognize AI-generated phishing, deepfakes and targeted social engineering attempts.
- **Incorporate adversarial simulations** using AI-based tactics in tabletop exercises to prepare for rapid, large-scale attacks.
- **Develop automated workflows** so your SOC can contain threats before they pivot or exfiltrate data.

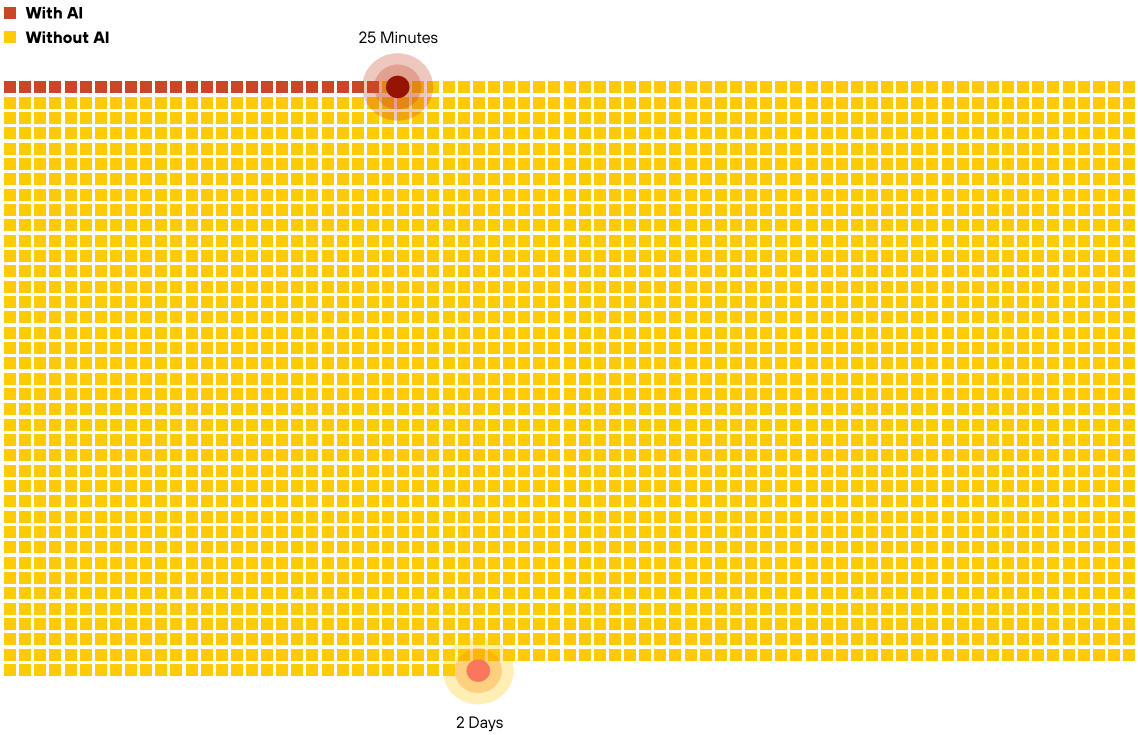



**Figure 3.** Speed differences in a simulated attack, before and after using AI-assisted techniques.

# 3 How Threat Actors Succeed: Common Effective Tactics, Techniques and Procedures

Threat actors continue to increase the speed, scale and sophistication of their attacks. This enables them to do widespread damage in a short time, making it difficult for organizations to detect their activity and mitigate it efficiently.

In our case data, we noted two key trends:

**Threat actors frequently attack organizations on multiple fronts.**

When we looked into how threat actors pursued their objectives, they pivoted from social engineering to attacking endpoints, cloud resources and other fronts, as shown in Table 2.

| Fronts of Attack | Percentage of Cases |
|---|---|
| Endpoints | 72% |
| Human | 65% |
| Identity | 63% |
| Network | 58% |
| Email | 28% |
| Cloud | 27% |
| Application | 21% |
| SecOps | 14% |
| Database | 1% |

**Table 2.** Fronts of attack where we saw threat actors operating.

In 84% of incidents, threat actors attacked their intended victim across multiple fronts (70% of the time, across three or more). In some incidents we responded to, threat actors attacked across as many as eight fronts.

The growing complexity of attacks demands a unified view across all data sources. In 85% of cases, Unit 42 incident responders had to access multiple types of data sources to complete their investigation. Defenders should prepare to access and efficiently process information from these various sources across an organization.

**The browser is a key conduit for threats.**

Nearly half of the security incidents we investigated (44%) involved malicious activity launched or facilitated through employees' browsers. This included phishing, abuse of URL redirects and malware downloads, each exploiting the browser session without adequate detection or blocking.

The user's interaction with malicious links, domains or files, combined with insufficient security controls led to compromise. Organizations must improve visibility and implement robust controls at the browser level to detect, block and respond to these threats before they spread.

The sections that follow cover our observations about intrusion, as well as insights about common attack techniques that we've gleaned from Unit 42 case data.

## 3.1. Intrusion: Growing Social Engineering, Both Widespread and Targeted

In 2024, phishing reclaimed its spot as the most common initial access vector in Unit 42 cases, accounting for about a quarter of our incidents (23%), as shown in Figure 4.

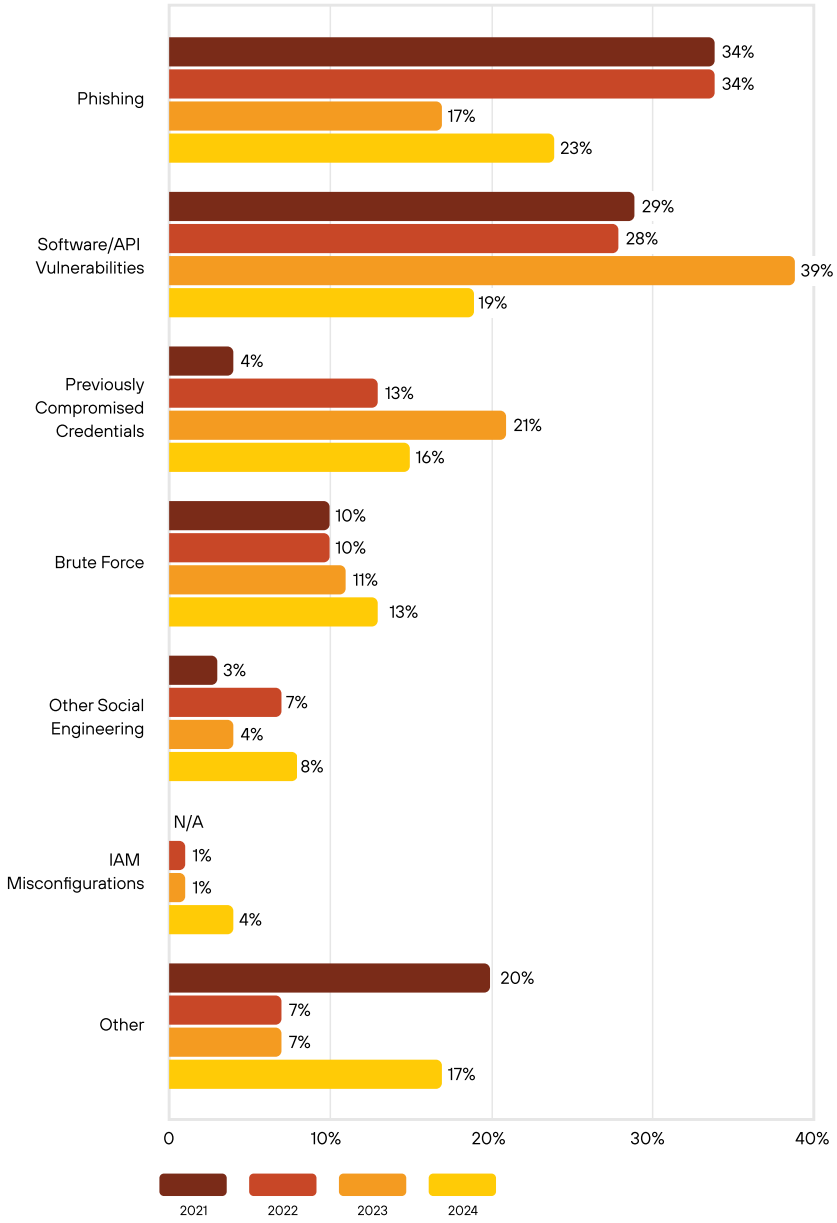



**Figure 4.** Initial access vectors observed in incidents Unit 42 responded to over the years. Other social engineering includes SEO poisoning, malvertising, smishing, MFA bombing and compromising the help desk. Other initial access vectors include abuse of trusted relationships or tools, as well as insider threats.

The initial access vectors alone don't tell the whole story. Different initial access vectors often corresponded to different threat actor profiles and objectives. For example, when threat actors gained access through phishing, the associated incident type was most often business email compromise (76% of cases), followed distantly by extortion, specifically ransomware (nearly 9%).

Nation-state actors, which account for a small but impactful percentage of incidents, favor software/API vulnerabilities as the initial access vector.

Defenders should be aware of how commonly threat actors use previously compromised credentials, which they often purchase from initial access brokers. Searches of the deep and dark web can often reveal previously compromised credentials.

Some less common initial access vectors can lead to significant compromises. For example, Unit 42 continues to observe the cybercrime group Muddled Libra gaining access to organizations by social engineering the help desk. However, other threat actors are also leveraging the technique, such as a financially motivated actor based in Nigeria.

Actors using this type of technique perpetuate fraud without the use of malware, armed with forged identity documents or VoIP phone numbers geo-located in the city where their intended victims are based. The percentage of targeted attacks in our data has risen from 6% of incidents in 2022 to 13% in 2024.

### Countermeasures: Defending Against Social Engineering Attacks

Defenders should continue to use defense-in-depth strategies to prepare for common initial access vectors and minimize the impact of threat actors who do gain access to systems.

Security training is a must to help prepare employees to resist social engineering attacks. Training should go beyond phishing and spear phishing. Training should also include:

- Strategies for improving physical security (such as preventing badge tailgating)
- Best practices against device loss
- What to do if devices are stolen or left unattended
- Insider threat indicators
- Red flags to be aware of in help desk calls
- Signs of deepfakes

## 3.2. Attack Technique Insights From Unit 42 Case Data

Based on the tactics and techniques we observed the most sophisticated attackers using in 2024, our threat intelligence analysts identified three key insights for defenders:

- Any sort of access can help attackers. Even if a threat group seems focused on other targets, it's still important to be prepared to defend your organization against them.
- Advanced threat actors don't always use complex attacks. If a simpler approach will work, they will use it.
- Despite the prevalence of extortion, not all threat actors announce their presence. Nation-state threat actors, for example, often specialize in remaining in a compromised network quietly, especially through "living off the land" techniques.

The following sections go into more detail about techniques used by nation-state threat groups and other motivated actors.

### All Access Is Important Access

Organizations often deprioritize defending against specific actors, believing those groups are focused on other targets. However, many actors have repeatedly shown us that persistent groups tend to impact many organizations along the path to achieving their final objectives.

Throughout 2024, Unit 42 has tracked many organizations breached by nation-state actors. These actors aren't always directly satisfying espionage objectives. Sometimes, they are commandeering devices to support their future activity (T1584 - Compromise Infrastructure).

For example, Insidious Taurus, aka Volt Typhoon, has been known to abuse these opportunistically compromised devices (often internet-facing network routers and internet-of-things assets) to create botnets that proxy command and control network traffic delivered to or from additional victims.

Actors have also been observed targeting and compromising technology vendors to collect specific sensitive customer information or even to exploit interconnected access to downstream victims (T1199 - Trusted Relationship).

Your network may still be at risk of compromise by threat actors, even if you are not their direct target.

## Successful Trade Craft Isn't Always New or Sophisticated

The term "advanced persistent threat" has created an illusion that all these adversaries' activities will be novel and complex. In reality, even well-resourced actors often take the path of least resistance. This includes exploiting known (and even old) vulnerabilities (T1190 - Exploit Public-Facing Application), simply abusing legitimate remote access features (T1133 - External Remote Services), or stealing information using popular existing online services (T1567 - Exfiltration Over Web Service).

We see systemic issues and mistakes commonly repeated across networks, such as misconfigurations and exposed internet-facing devices. This lowers the barrier for malicious actors.

## Post-Compromise Activity Can Be Patient and Quiet

The majority of incidents involved financially motivated threat actors, many of whom move quickly and announce their presence for the purpose of extortion. However, we also see incidents in which adversaries avoid triggering alerts and make an effort to evade defensive mechanisms, for purposes such as espionage.

Attackers sometimes further exploit the complexity of networks by hiding within the "noise" of expected user activity. They abuse otherwise legitimate features of a compromised environment, an approach known as "living off the land." The success attackers can garner with this approach highlights the often unmanageable challenge for defenders to categorize benign versus malicious activity.

As a very common real-world example, can you immediately tell the difference between administrators or an APT when observing the following actions?

- Executed commands
- System configuration changes
- Logins
- Network traffic

| Technique | 2024 Trends |
|---|---|
| T1078 - Valid Accounts | This was one of the top techniques observed as an **Initial Access** vector, which represents more than 40% of the kinds of grouped techniques observed in association with this tactic. It is likely enabled by weaknesses in identity and access management and attack surface management (ASM) such as:<br>• No MFA (28% of cases)<br>• Weak/default passwords (20% of cases)<br>• Insufficient brute force/account lockout controls (17% of cases)<br>• Excessive account permissions (17% of cases) |
| T1059 - Command and Scripting Interpreter | This was the top **Execution** technique (more than 61% of cases associated with the Execution tactic abuse PowerShell in this way, for example). Other commonly abused system utilities include other native Windows, Unix, network devices and application-specific shells to perform various tasks. |
| T1021 - Remote Services | Abuse of these services was overwhelmingly the most observed technique for **Lateral Movement** (of the kinds of grouped techniques observed in association with this tactic, over 86% involved remote services). This further extends the trend highlighting reuse of legitimate credentials. Instead of more traditional uses of these credentials, here we see them used to authenticate through internal network protocols such as RDP (over 48% of cases), SMB (over 27% of cases), and SSH (over 9% of cases). |

**Table 3.** Most prominent living off the land techniques from Unit 42 IR cases.

In addition to living off the land, we have observed a number of actors — particularly involved with ransomware — attempting to use EDR disabling tools to "modify the land" as part of their operations. Nearly 30% of the kinds of grouped techniques observed associated with **Defense Evasion** involved T1562 - Impair Defenses. This includes sub-techniques such as:

- Disable or Modify Tools
- Disable or Modify System Firewall
- Disable Windows Event Logging

While there are many tricks, we are seeing more breaches involving threat actors abusing bring your own vulnerable driver (BYOVD) trade craft. They use this technique to gain the required permissions to bypass then even attack EDR and other defensive protections installed on a compromised host. Related techniques include:

- T1543.003 - Create or Modify System Process: Windows Service
- T1068 - Exploitation for Privilege Escalation

## Countermeasures: Defending Against Common Effective TTPs

Defenders should maintain a clear understanding of the organization's internal and external attack surface. Periodically evaluate what data or devices are accessible or exposed on the public-facing internet, and minimize dangerous remote access settings and misconfigurations. Remove systems running on operating systems that are no longer supported with regular security updates, and be aware of vulnerabilities for your systems, including older ones – especially those with published PoC code.

Maintain an actionable baseline of your environment, including accounts, software/applications, and other activity that is approved for use. Implement robust logging and take advantage of analytic tools that can help quickly make connections between multiple data sources to detect unusual behavioral patterns.

# 4 Recommendations for Defenders

This section takes a closer look at systemic issues most frequently exploited by attackers and the targeted strategies to counter them. By proactively addressing these factors, organizations can significantly reduce cyber risk, strengthen resilience, and maintain a decisive edge against current and emerging threats.

## 4.1. Common Contributing Factors

Common contributing factors are systemic issues that enable threat actors to succeed time and again. By addressing these issues proactively, organizations reduce both the likelihood and impact of cyberattacks.

Drawing from thousands of incidents, we've identified three main enablers: complexity, gaps in visibility and excessive trust. These factors enable initial access, allow threats to escalate unchecked and amplify overall damage. Confronting them head-on will significantly strengthen defenses and improve resilience.

### 1. Security Complexity: A Killer for Effective SecOps and Incident Response

Today's IT and security environments often resemble a patchwork of legacy applications, bolt-on infrastructure, and incomplete transformation initiatives. This leads many organizations to rely on 50 or more disparate security tools. Acquired piecemeal to address individual threats, these tools typically lack integration, creating data silos and preventing teams from maintaining a unified view of their environments.

In 75% of incidents we investigated, critical evidence of the initial intrusion was present in the logs. Yet, due to complex, disjointed systems, that information wasn't readily accessible or effectively operationalized, allowing attackers to exploit the gaps undetected.

At the same time, multiple data sources are essential to detect and respond effectively. About 85% of incidents required correlating data from multiple sources to fully understand the scope and impact. Nearly half (46%) required correlating data from four or more sources. When these systems don't communicate — or the telemetry is incomplete — essential clues remain buried until it's too late.

**Case in Point:**
In one ransomware attack, the endpoint detection and response (EDR) system captured lateral movement, while the initial compromise was buried in unmonitored network logs. This fractured visibility delayed detection for an extended period of time, granting attackers ample time to exfiltrate data and deploy ransomware payloads.

### 2. Gaps in Visibility: You Can't Secure What You Don't Know About

Enterprise-wide visibility is the backbone of effective security operations, yet gaps remain common. Cloud services, in particular, present a significant challenge.

Unit 42 found that organizations spin up an average of 300 new cloud services each month. Without proper runtime visibility, SecOps teams are unaware of both exposures and attack. Unmanaged and unmonitored assets — whether they're endpoints, applications or shadow IT — provide attackers with easy entry points into an organization's environment.

In fact, issues with security tools and management were a contributing factor in nearly 40% of cases. These gaps allowed attackers to establish a foothold, move laterally and escalate privileges without being detected.

**Case in Point:**
In one incident, Muddled Libra used a privileged user account to elevate permissions in the client's AWS environment, granting it permissions for data exfiltration. Because the cloud service was not integrated with the organization's SOC or SIEM, the suspicious activity initially went undetected.

### 3. Too Much Trust Expands the Impact

Overly permissive access is a dangerous liability. In the incidents we respond to, attackers consistently exploit overly permissive accounts and inadequate access controls to escalate their attacks.

In fact, in 41% of incidents, there was at least one contributing factor related to issues with identity and access management, including overly permissioned accounts and roles. This leads to lateral movement, access to sensitive information and applications, and ultimately enables attackers to succeed.

Here too, cloud environments are especially vulnerable: Unit 42 researchers found that in nearly half of cloud-related incidents, there was at least one contributing factor related to issues with identity and access management, including overly permissioned accounts and roles.

In many cases, attackers gained far more access than they should have given the types of roles they compromised. Once initial access is gained — through phishing, credential theft or exploiting vulnerabilities — this excessive trust allows attackers to rapidly escalate privileges, exfiltrate data and disrupt operations.

**Case in Point:**
In the case of an IT services company, attackers exploited overly permissive admin accounts to move laterally and escalate privileges after brute-forcing a VPN without multi-factor authentication. This excessive trust allowed the attackers to deploy ransomware across 700 ESXi servers, ultimately disrupting the company's main business operations and impacting over 9,000 systems.

## 4.2. Recommendations for Defenders

By tackling complexity, gaps in visibility and excessive trust, organizations can materially reduce the risk and impact of cyberattacks. This not only avoids extended downtime and expensive breach remediation but also preserves operational continuity and stakeholder confidence. The following recommendations include strategies to address these systemic issues head-on.

### 1. Empower Security Operations to See More and Respond Faster

The SOC is your last line of defense. When network, identity, endpoint or application controls fail, this team needs the tools and capabilities to detect and respond fast — before threats escalate. Empower your SOC with comprehensive visibility across the enterprise, and the technology to identify the signal in the noise.

- **Ingest all relevant security data:** Aggregate and normalize telemetry from cloud infrastructure, on-premises systems, identity, endpoints and applications to create a single source of truth. This unified view not only shrinks gaps but also reduces the complexity of juggling multiple tools. Map the internal and external attack surface to inventory all assets and owners and integrate threat intelligence to prioritize high-risk indicators.
- **Detect and prioritize threats with AI-driven capabilities:** Use artificial intelligence and machine learning to sift through vast datasets, identifying hidden threats and anomalous behaviors. AI-assisted behavioral analytics help predict attacks before they fully materialize. The SOC should measure MTTD to gauge improvements. Regular threat hunting and correlation of signals from multiple sources tackle the "needle in a haystack" problem.

- **Enable real-time threat response with automation:** Automating incident response workflows is critical for containing threats at machine speed, before an attacker can escalate privileges or exfiltrate sensitive data. The SOC should track MTTR to drive continuous improvement. Seamless integration between SOC platforms, IT systems and business applications also removes manual bottlenecks that delay remediation.
- **Transition from reactive to proactive security:** Combine red team exercises, incident simulation, and continuous security assessments to refine detection logic and response playbooks. This consistent feedback loop ensures the SOC adapts as new threats emerge. Elevating SOC skills through advanced training closes knowledge gaps and ensures that your organization is prepared for the next wave of attacks.
- **Deepen your bench with IR experts:** Having a dedicated IR team on retainer — such as Unit 42 — ensures you have expert support on speed dial when incidents escalate. Beyond emergency response, retainer credits can fund proactive services like threat hunting, tabletop exercises and purple team assessments, fortifying your readiness and sharpening defenses before attackers strike.

By aligning your SOC with these core principles, your organization can outmaneuver adversaries, contain incidents swiftly and evolve defenses in ahead of emerging risks.

## 2. Accelerate Your Journey to Zero Trust

Zero Trust is a strategic security model centered on eliminating implicit trust and continuously validating every user, device and application — no matter the location or platform. While full adoption can be complex, even incremental progress will reduce risk, protect sensitive data and build resilience. These high-level recommendations map to the three common contributing factors (complexity, gaps in visibility and excessive trust), ensuring your Zero Trust journey directly addresses those pain points.

- **Identify and verify all users, devices and applications:** Consistently authenticate every entity — human or machine — before granting access, whether on-site or remote. This closes gaps and reduces complexity by ensuring a single source of truth for identity. Verified entities should then be monitored continuously, minimizing unauthorized access.
- **Enforce strict least privilege access:** Grant roles only the access they need, guided by context-aware rules that factor in identity, device posture and data sensitivity. This neutralizes the "excessive trust" issue by limiting the range of damage if an account is compromised. Network segmentation further isolates critical assets and prevents attackers from moving laterally.
- **Apply holistic security inspection:** Analyze network traffic — including encrypted streams — to prevent and detect active threats without degrading performance. Tailor controls for distinct environments (e.g., cloud, IoT) to reduce operational complexity and avoid gaps in visibility. This integrated inspection approach boosts threat detection accuracy and speeds incident response.
- **Control data access and movement:** Safeguard sensitive information by classifying data and enforcing robust handling policies. Data loss prevention (DLP) technologies monitor flows and stop unauthorized transfers, shielding your organization from intellectual property theft, compliance violations and financial repercussions.

By adopting these Zero Trust principles — even one actionable step at a time — you not only address the core factors that enable attackers but also build a sustainable security model that your executive team can stand behind.

### 3. Secure Apps and Cloud From Development to Runtime

As adversaries target cloud environments and software supply chains, embedding security into DevOps, getting real time visibility into misconfigurations and vulnerabilities, and enabling your SecOps team to continuously monitor and respond to cloud-based attacks is crucial to staying ahead of the threat. The following recommendations detail how to integrate security into every stage — preventing breaches before production and rapidly containing threats in real time.

- **Prevent security issues from reaching production:** Integrate security early in the development lifecycle. Harden development and DevOps tools, govern third-party and open-source components, and run continuous scans during the CI/CD process. This shift-left approach uncovers vulnerabilities before they reach production.
- **Remediate newly discovered security weaknesses:** Continuously monitor cloud infrastructure for misconfigurations, vulnerabilities and excessive permissions. Automated scanning and risk-based remediation ensure that once issues emerge, they are swiftly identified and contained. This is critical for stopping attackers before they gain a foothold.
- **Identify and block runtime attacks:** Protect applications, APIs and workloads with real-time threat detection and preventive controls. Ongoing monitoring helps neutralize malicious activity in progress, minimizing operational disruption and cutting off attackers before threats escalate.
- **Automate cloud detection and response:** Leverage native cloud services and third-party security tools to orchestrate automated incident response. By removing manual bottlenecks, you reduce the time attackers have to pivot, exfiltrate data or escalate privileges.

Focusing on these capabilities counters emerging threats in the cloud and software supply chain, ensuring that attempts to breach your environment are shut down early.

# 5 Appendix: MITRE ATT&CK® Techniques by Tactic, Investigation Types and Other Case Data

## 5.1 Overview of Observed MITRE ATT&CK Techniques by Tactic

The following series of charts (Figures 5-16) show the MITRE ATT&CK® techniques we observed in association with specific tactics. Note that the percentages shown represent the prevalence of each technique when compared across the other kinds of techniques identified for each respective tactic. These percentages don't represent how often the techniques showed up in cases (see the website version to explore data about unique techniques and cases).

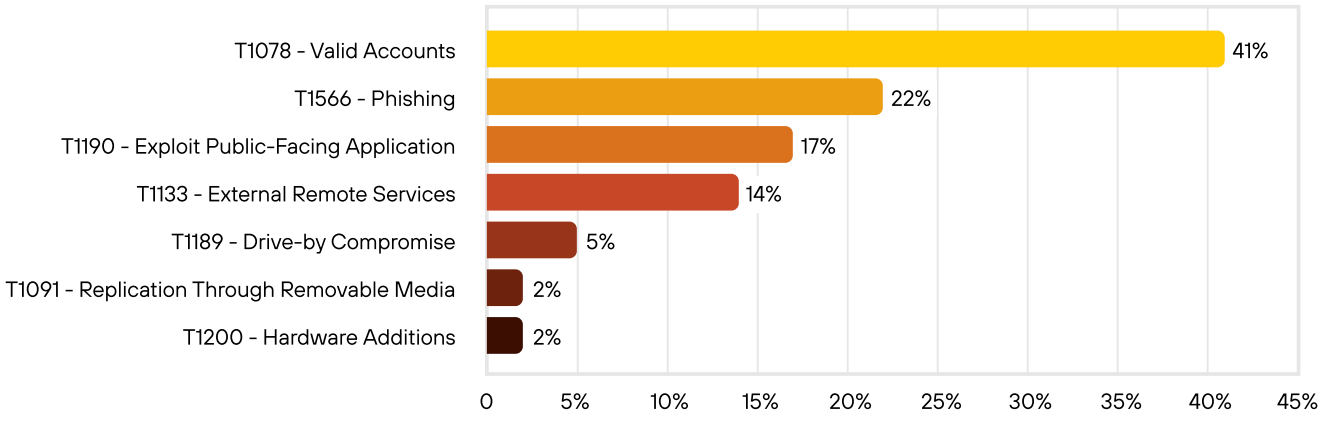



**Figure 5.** Relative Prevalence of Techniques Observed in Association With the Initial Access Tactic

## 5.1 Overview of Observed MITRE ATT&CK Techniques by Tactic (Cont.)

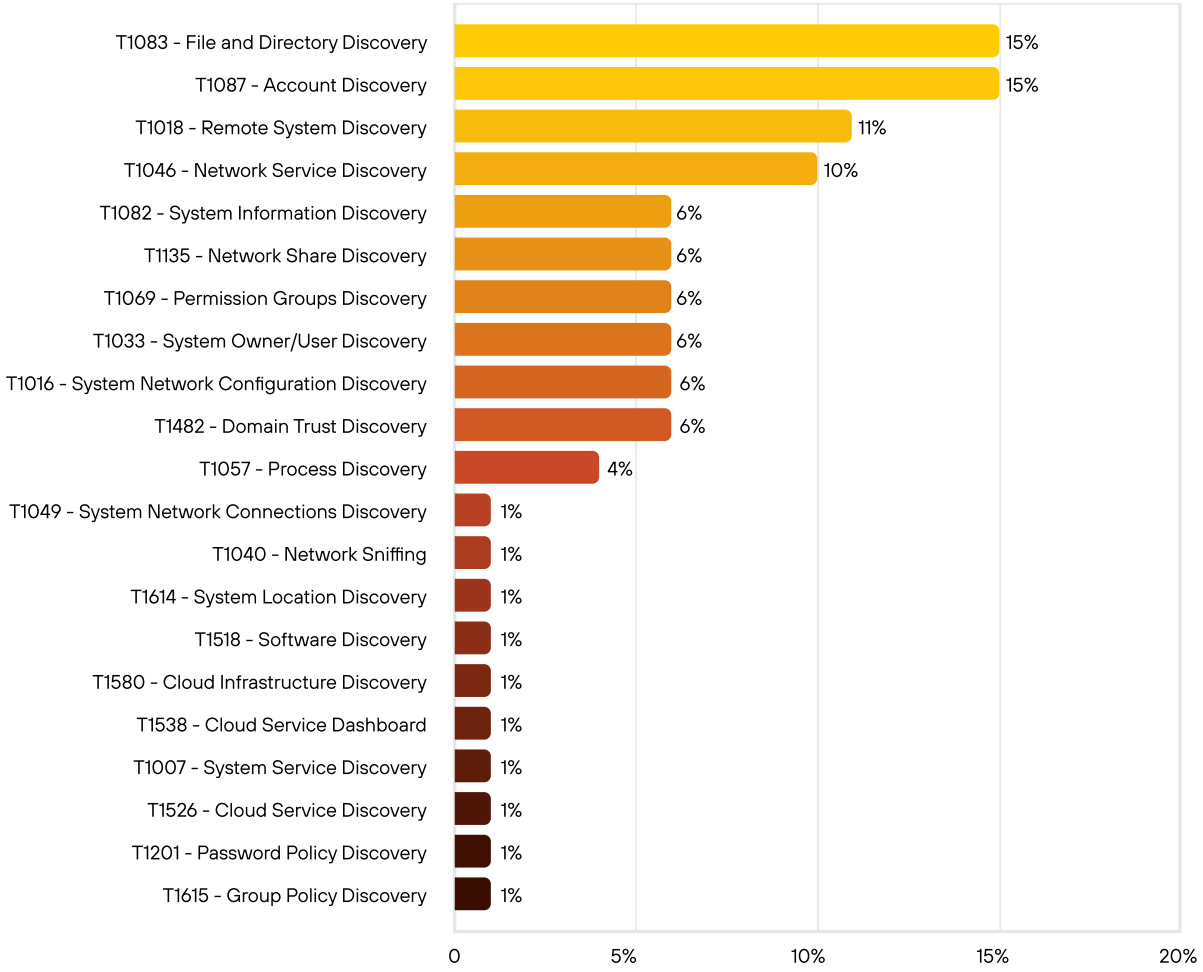



**Figure 6.** Relative Prevalence of Techniques Observed in Association With the Discovery Tactic

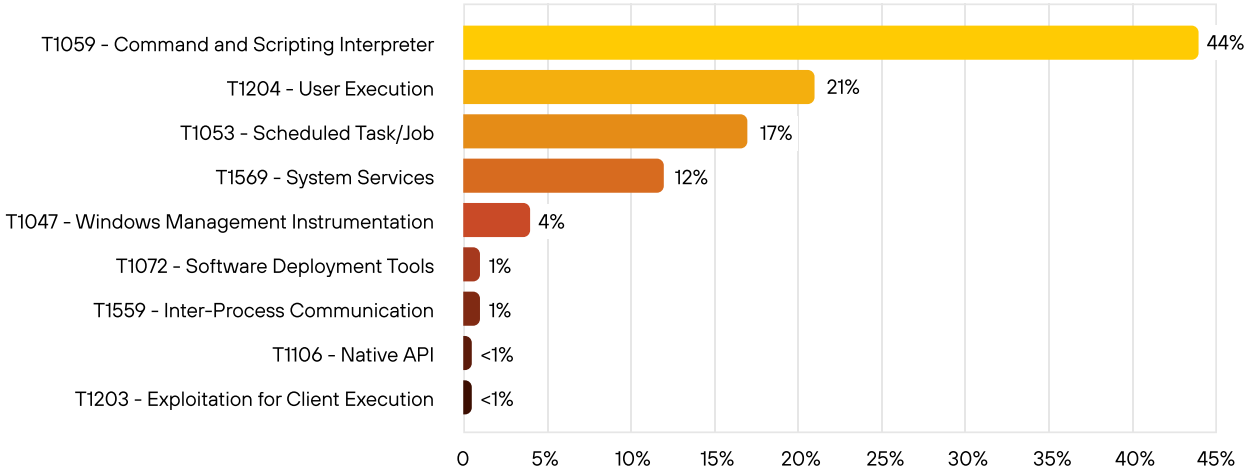



**Figure 7.** Relative Prevalence of Techniques Observed in Association With the Execution Tactic

## 5.1 Overview of Observed MITRE ATT&CK Techniques by Tactic (Cont.)

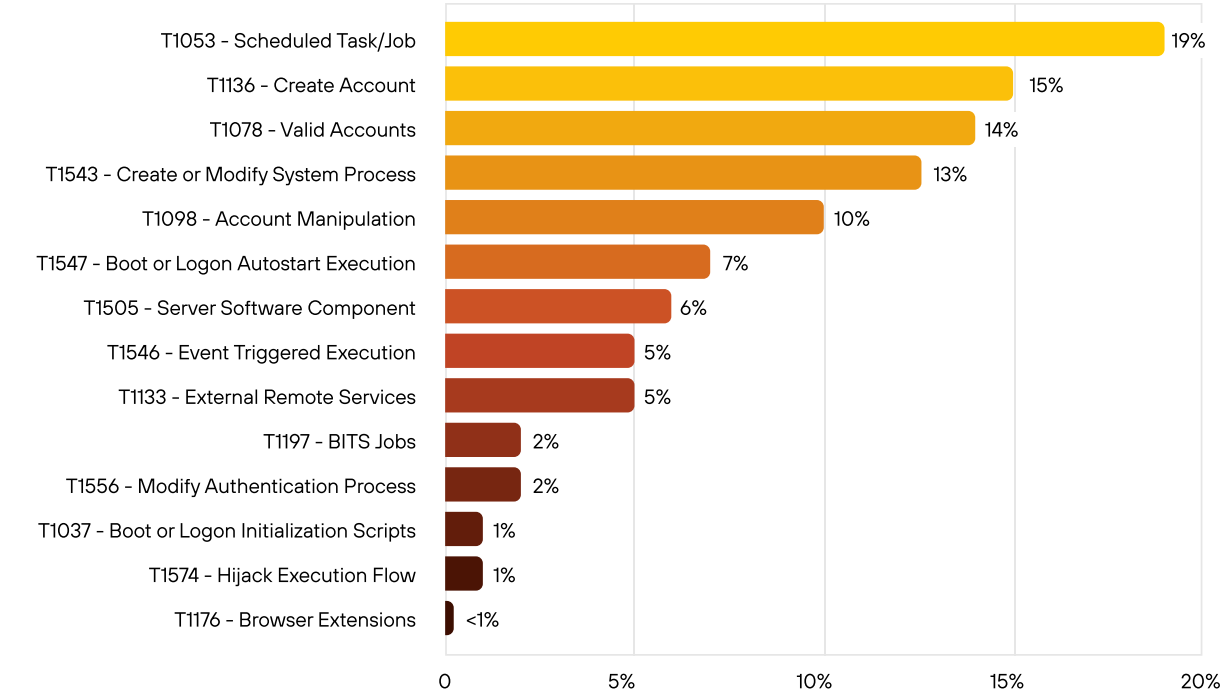



**Figure 8.** Relative Prevalence of Techniques Observed in Association With the Persistence Tactic

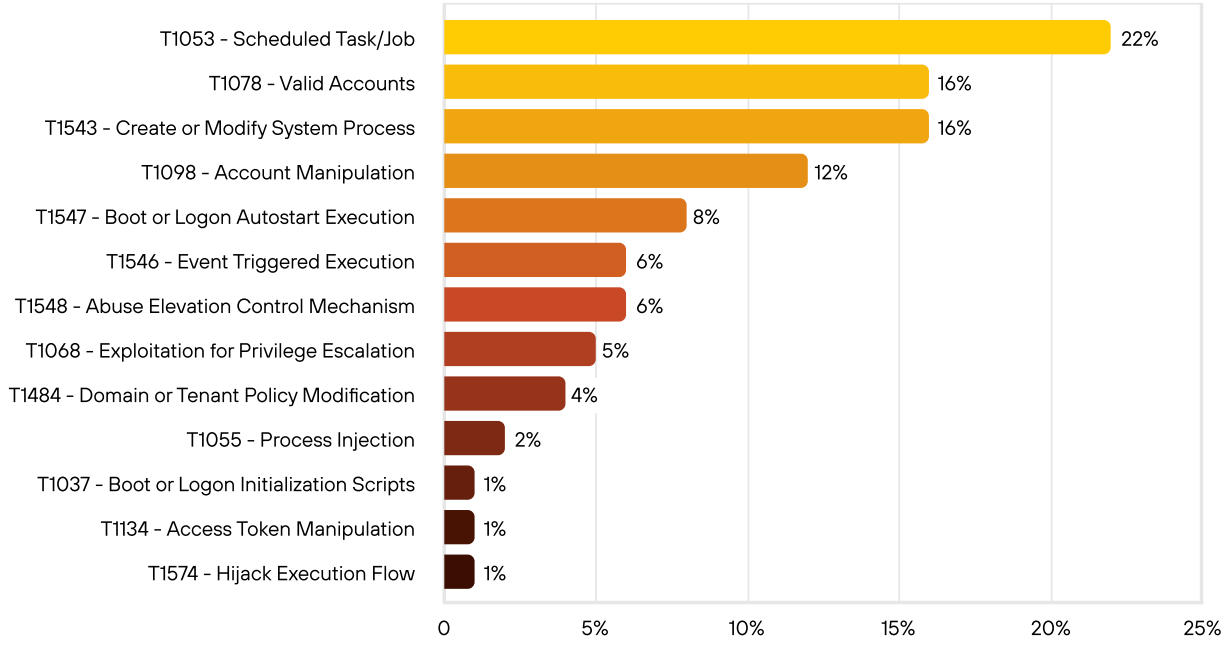



**Figure 9.** Relative Prevalence of Techniques Observed in Association With the Privilege Escalation Tactic

## 5.1 Overview of Observed MITRE ATT&CK Techniques by Tactic (Cont.)

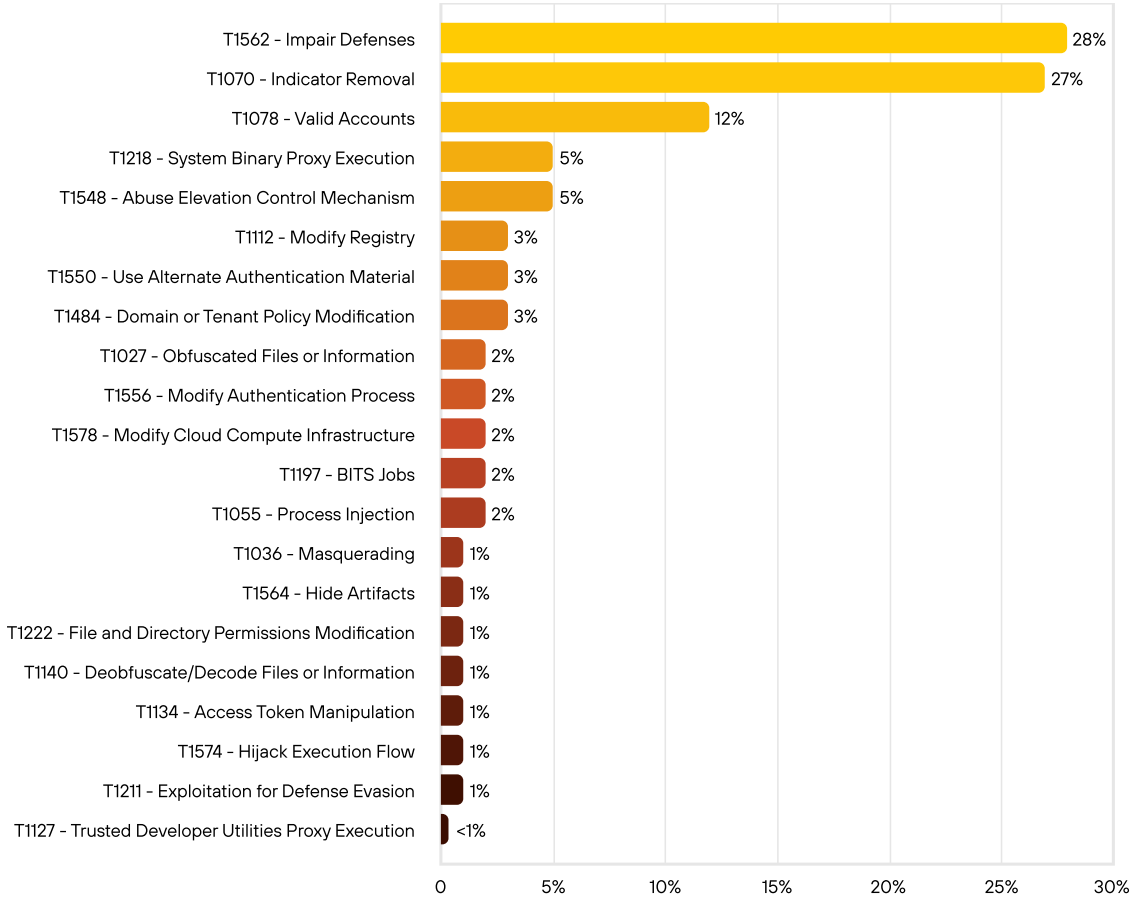



**Figure 10.** Relative Prevalence of Techniques Observed in Association With the Defense Evasion Tactic

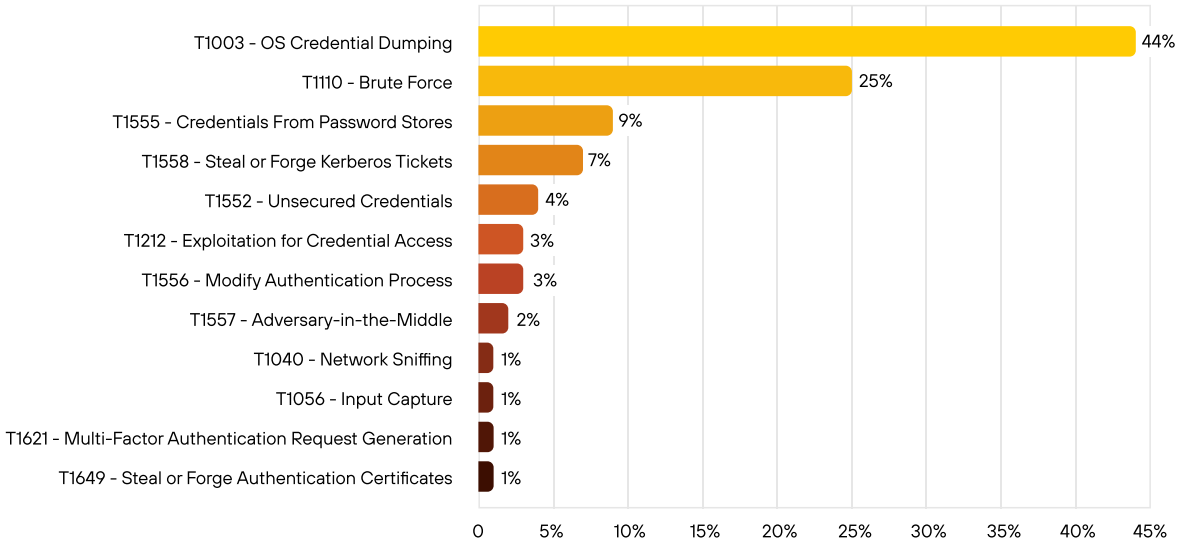



**Figure 11.** Relative Prevalence of Techniques Observed In Association With the Credential Access Tactic

## 5.1 Overview of Observed MITRE ATT&CK Techniques by Tactic (Cont.)

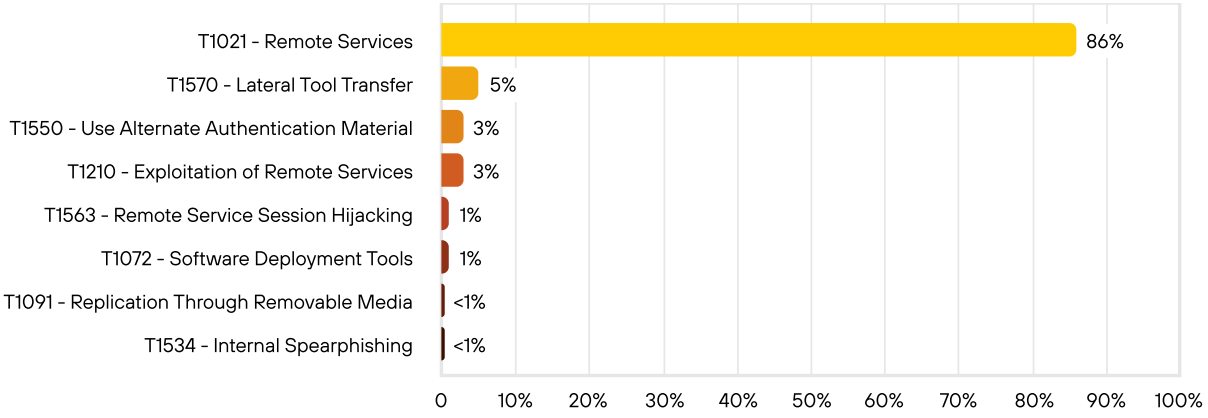



**Figure 12.** Relative Prevalence of Techniques Observed in Association With the Lateral Movement Tactic

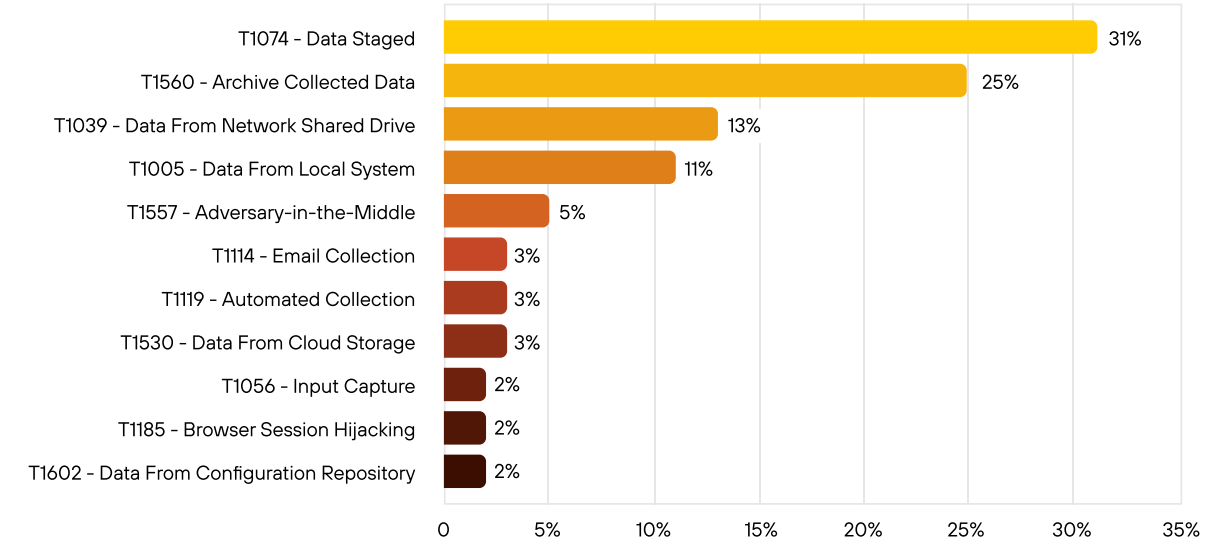



**Figure 13.** Relative Prevalence of Techniques Observed in Association With the Collection Tactic

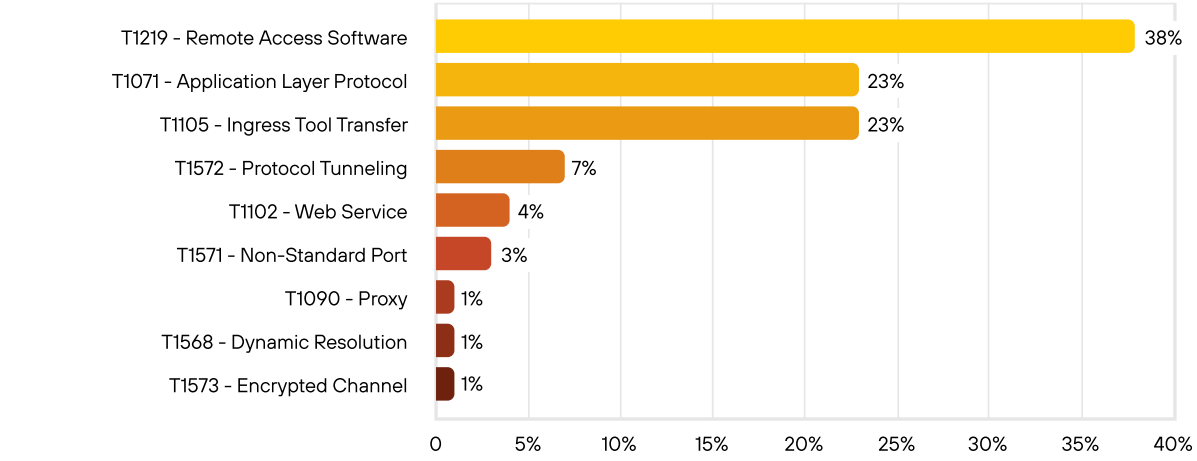



**Figure 14.** Relative Prevalence of Techniques Observed in Association With the Command and Control Tactic

## 5.1 Overview of Observed MITRE ATT&CK Techniques by Tactic (Cont.)

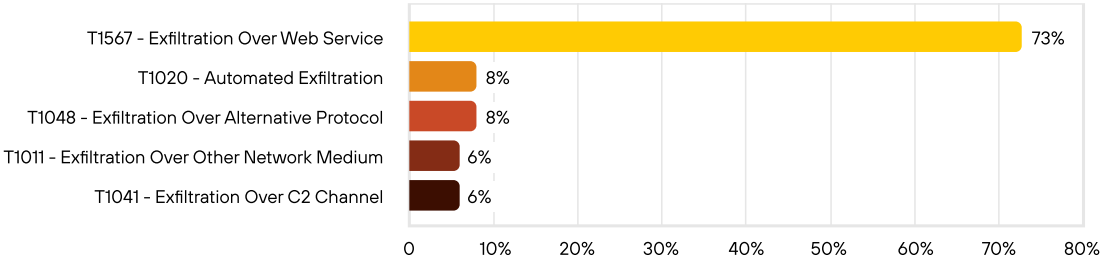



**Figure 15.** Relative Prevalence of Techniques Observed in Association With the Exfiltration Tactic

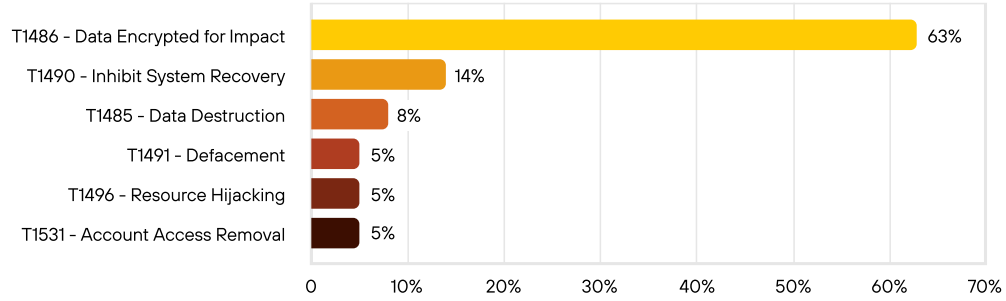



**Figure 16.** Relative Prevalence of Techniques Observed in Association With the Impact Tactic

## 5.2. Data by Region and Industry

The most common type of investigation we performed in 2024 was network intrusion (roughly 25% of cases). Seeing so much of this investigation type is good news, since we use this classification when intrusion into the network is the only malicious activity we observe. We believe that the rise in this investigation type means that, in at least some cases, clients are calling us earlier in the attack chain, which can lead to stopping attackers before they have a chance to succeed at their other objectives.

While defenders in all industries and regions share many of the same concerns, we saw some variation by region and industry.

In North America, business email compromise was a close second to network intrusion (19% of cases versus 23%). In EMEA, if all extortion types are considered (with and without encryption), extortion slightly surpasses network intrusion in our data (31% of cases versus 30%).

It is clear how significant a concern extortion is when looking at our industry data. In the high technology industry, extortion with and without encryption was also the top investigation type (22%). This is also the case in manufacturing, the industry most commonly represented on ransomware groups' dark web leak sites (25%).

Business email compromise remains a substantial threat, particularly for financial services (25% of cases), professional and legal services (23%), and wholesale and retail (21%).

Aside from the substantial proportion of cases that involve or impact organizations' cloud services, we see a small but growing trend of cases primarily focused on cloud control plane or dataplane compromises. This includes 4% of cases overall, but it's higher in industries such as high technology and professional and legal services (9% of cases for both). These specifically cloud-focused attacks have the potential for significant impact. In the case of attacks on the cloud control plane, attackers can gain access to an organization's entire cloud infrastructure. Attacks on the dataplane have the potential to harvest a large amount of sensitive data, given the type and scope of data typically stored in the cloud.

## 5.2. Data by Region and Industry (Cont.)

### Investigation Type by Region

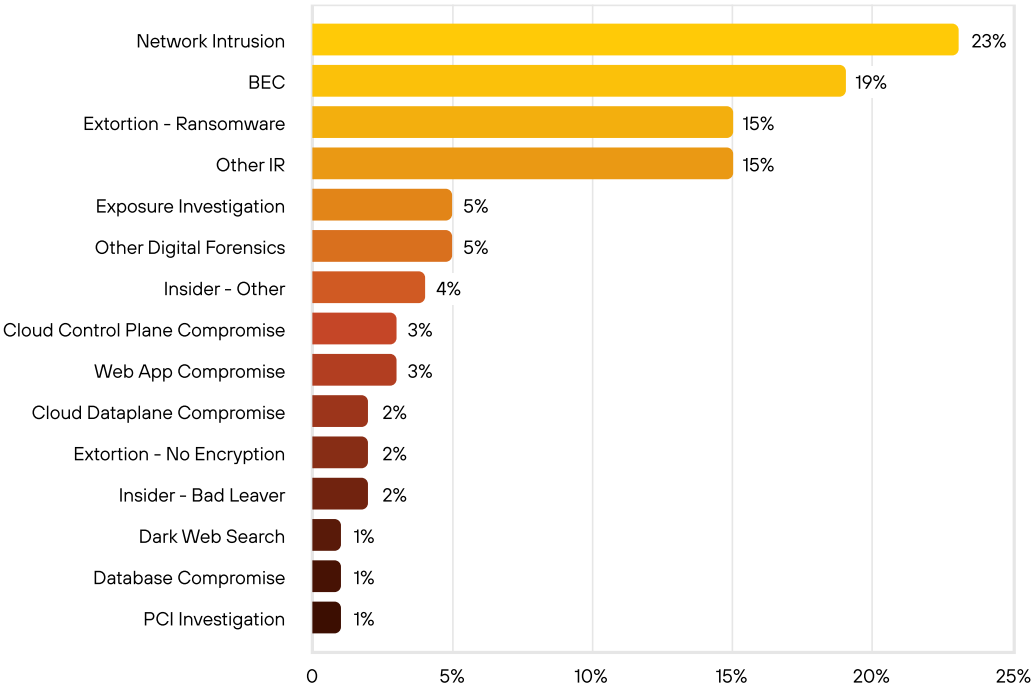



**Figure 17.** Investigation Type by Region – North America

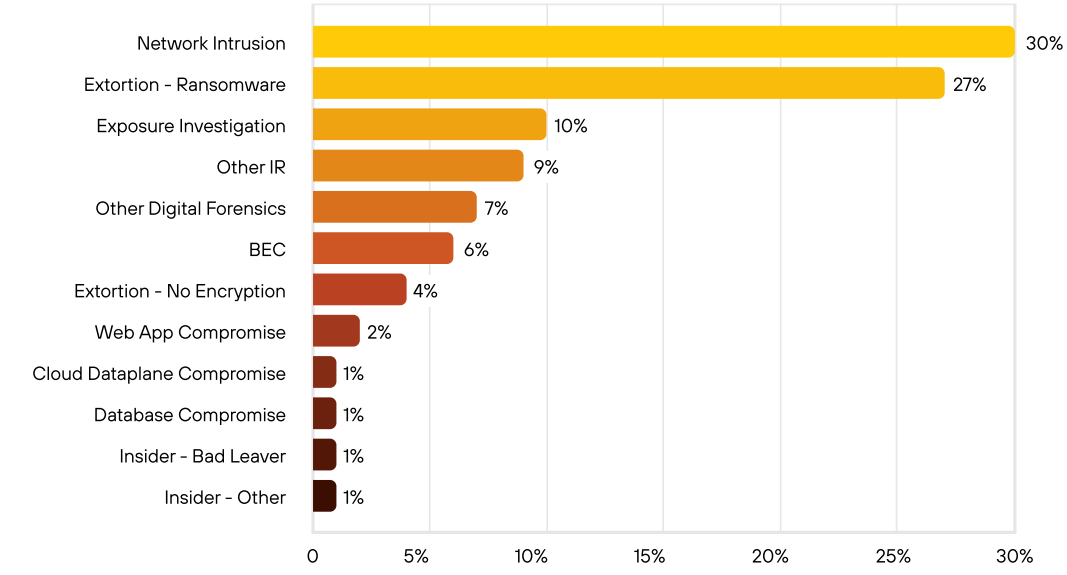



**Figure 18.** Investigation Type by Region – Europe, the Middle East and Africa

## 5.2. Data by Region and Industry (Cont.)

### Investigation Type by Industry

Figures 19-24 below show a breakdown of the top investigation types associated with the six industries most represented in our incident response data.

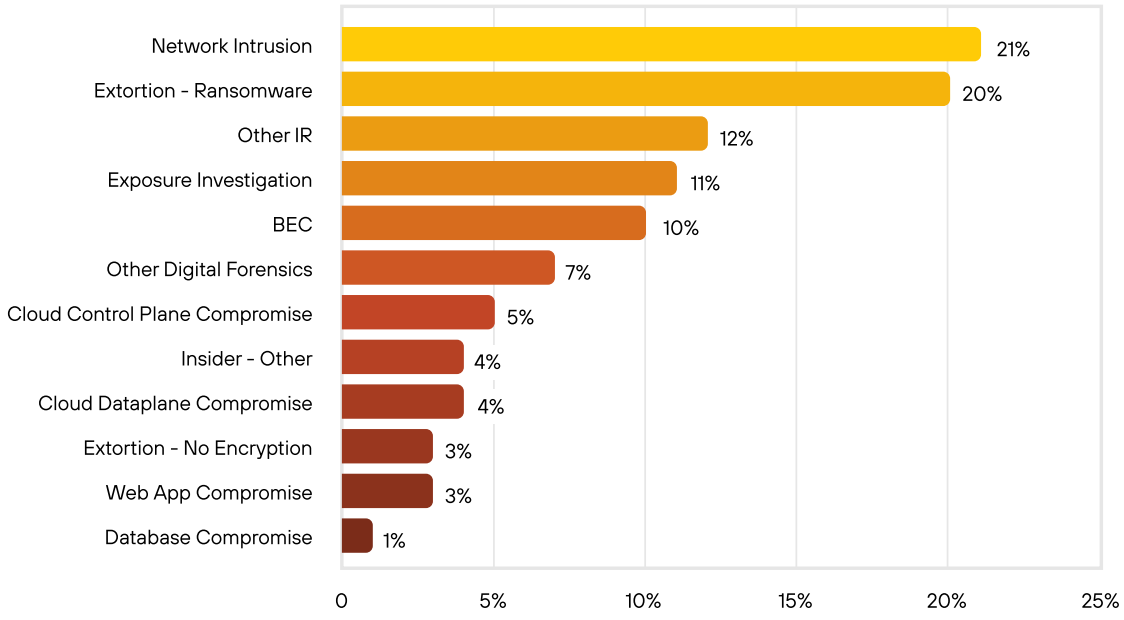



**Figure 19.** Investigation Type by Industry – High Technology

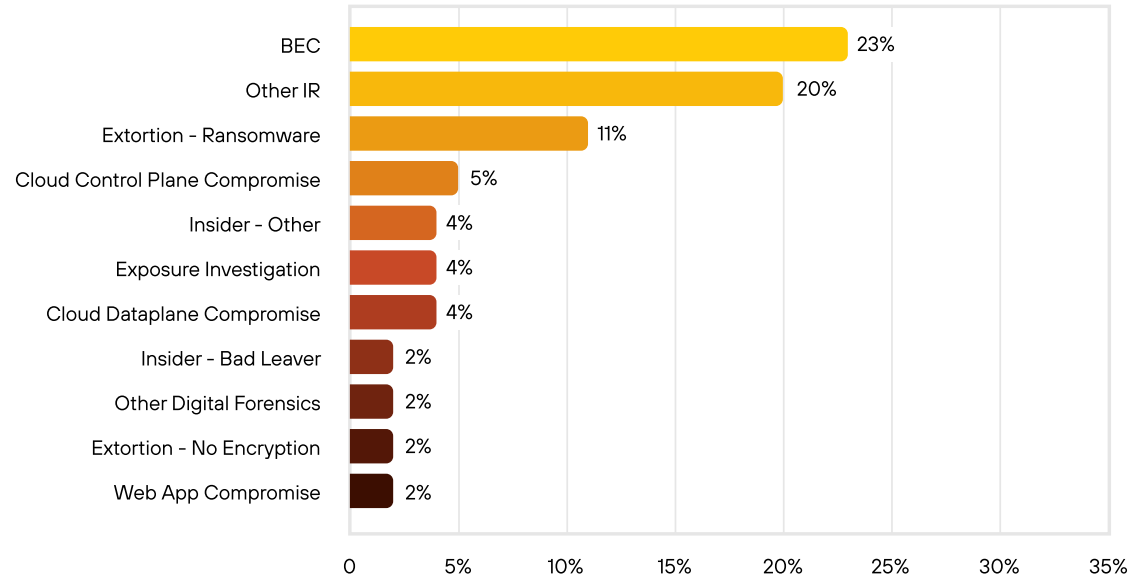



**Figure 20.** Investigation Type by Industry – Professional & Legal Services

## 5.2. Data by Region and Industry (Cont.)

### Investigation Type by Industry

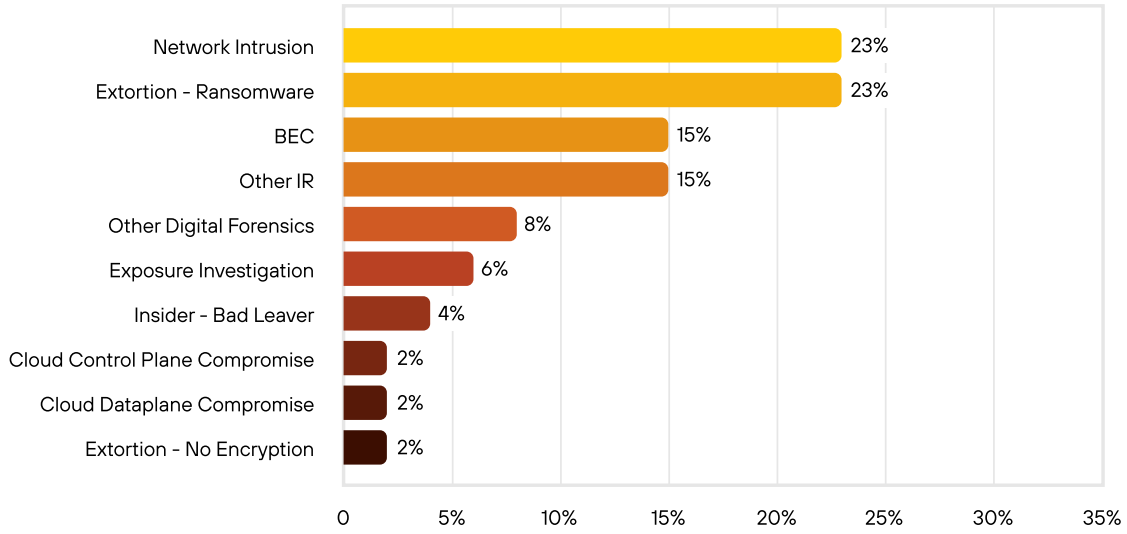



**Figure 21.** Investigation Type by Industry – Manufacturing

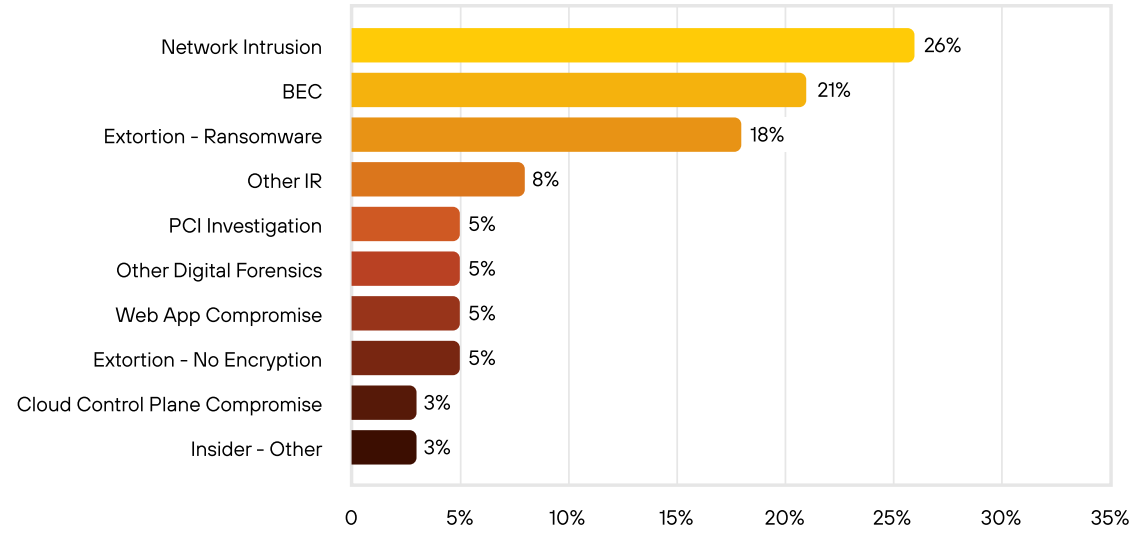



**Figure 22.** Investigation Type by Industry – Wholesale & Retail

## 5.2. Data by Region and Industry (Cont.)

### Investigation Type by Industry

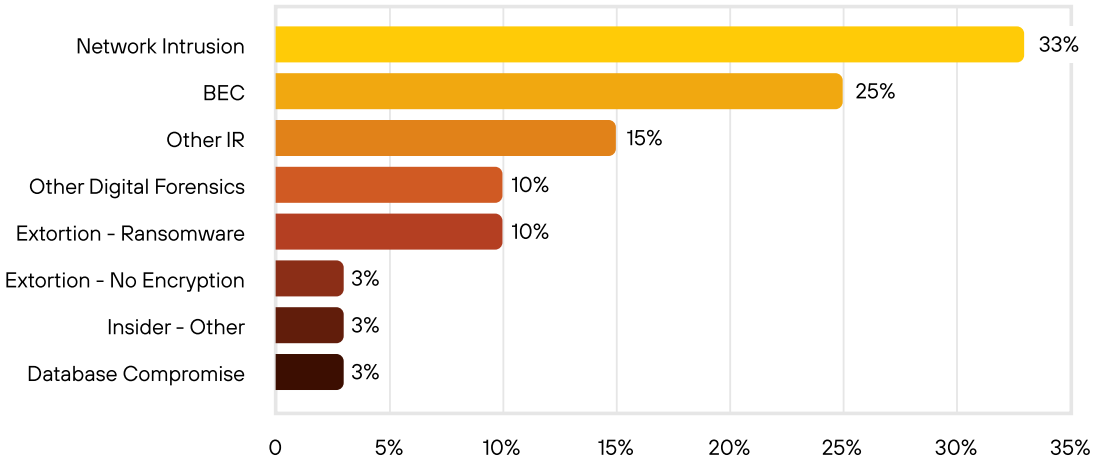



**Figure 23.** Investigation Type by Industry – Financial Services

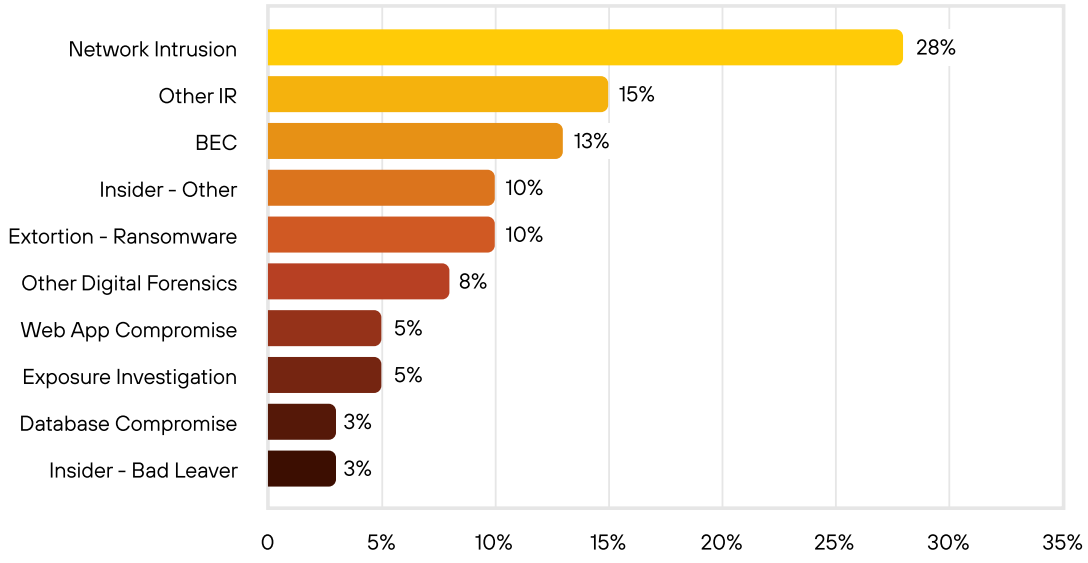
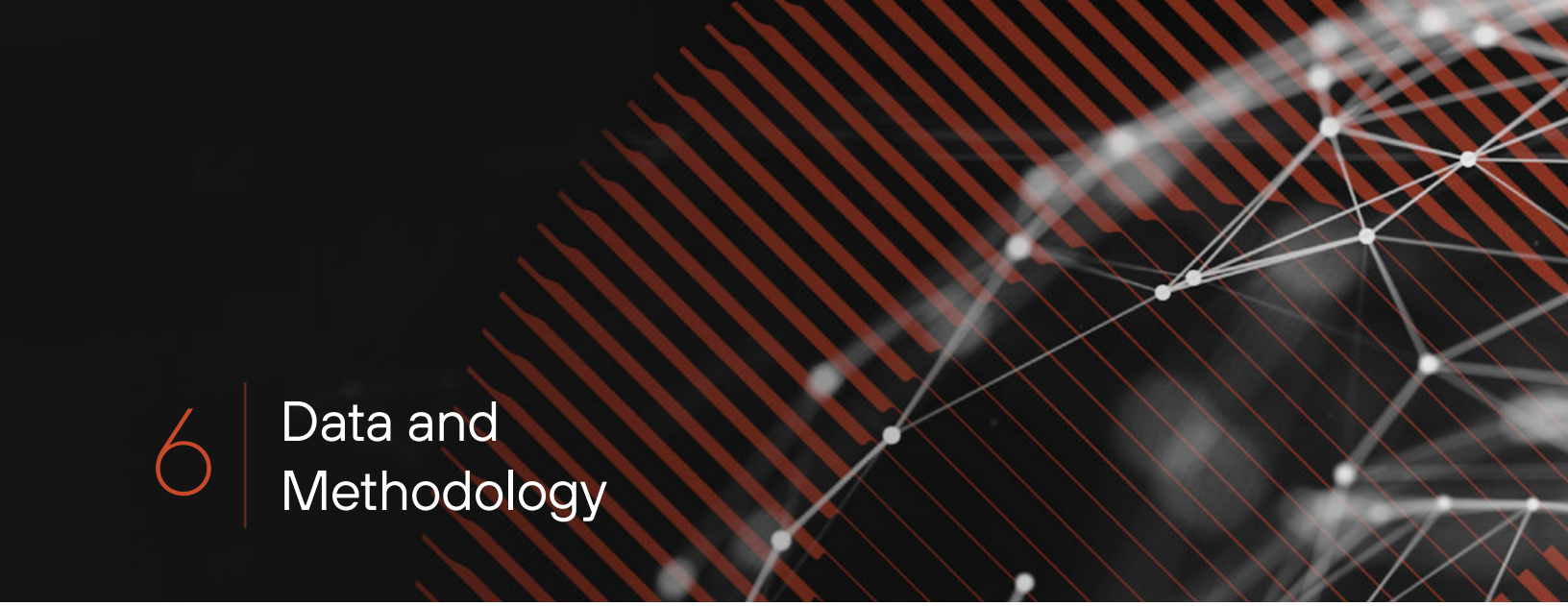



**Figure 24.** Investigation Type by Industry – Healthcare



# 6 Data and Methodology

We sourced data for this report from more than 500 cases Unit 42 responded to between October 2023-December 2024, as well as from other case data going back as far as 2021.

Our clients range from small organizations with fewer than 50 personnel to Fortune 500 and Global 2000 companies and government organizations with more than 100,000 employees.

The affected organizations were headquartered in 38 unique countries. About 80% of the targeted organizations in these cases were located in the U.S. Cases related to organizations based in Europe, the Middle East and Asia-Pacific form the other 20% of the work. Attacks frequently have impact beyond the locations where organizations are headquartered.

We combine this case data with insights from our threat research, which is based on product telemetry as well as on observations of dark web leak sites and other open-source data.

Incident responders have also shared their observations of key trends based on working directly with clients.

Several factors may impact the nature of our data, including a trend toward working with larger organizations with more mature security postures. We have also chosen to emphasize cases that we believe reveal emerging trends, which for some topics means focusing on smaller segments of the dataset.

For some topics, we chose to filter our data to remove factors that could skew our results. For example, we offered our incident response services to help our customers investigate potential impacts of CVE-2024-3400, which caused that vulnerability to be overrepresented in our dataset. In places, we corrected the data to remove this overrepresentation.

Our guiding principle throughout has been to provide the reader with insights into the present and future threat landscape, enabling improved defense.

## Contributors


**Aditi Adya**
Consultant

**Jim Barber**
Senior Consultant

**Richard Emerson**
Manager, Intel Response Unit

**Evan Gordenker**
Consulting Senior Manager

**Michael J. Graven**
Director, Global Consulting Operations

**Eva Mehlert**
Senior Executive and Internal Communications Manager, Unit 42

**Lysa Myers**
Senior Technical Editor

**Erica Naone**
Senior Manager, Unit 42 External Engagement

**Dan O'Day**
Consulting Director

**Prashil Pattni**
Senior Threat Researcher

**Laury Rodriguez**
Consultant

**Sam Rubin**
SVP, Unit 42 Consulting and Threat Intelligence

**Doel Santos**
Principal Threat Researcher

**Mike Savitz**
Senior Consulting Director

**Michael Sikorski**
CTO & VP of Engineering, Unit 42

**Samantha Stallings**
Senior Production Editor

**Jamie Williams**
Principal Threat Intelligence Researcher

## About Palo Alto Networks

Palo Alto Networks® is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2023, 2022, 2021), with a score of 100 on the Disability Equality Index (2023, 2022), and HRC Best Places for LGBTQ equality (2022). For more information, visit www.paloaltonetworks.com.

## About Unit 42

Palo Alto Networks® Unit 42® brings together world-renowned threat researchers, elite incident responders and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster. Visit paloaltonetworks.com/unit42.

3000 Tannery Way
Santa Clara, CA 95054

Main +1.408.753.4000
Sales +1.866.320.4788
Support +1.866.898.9087

**www.paloaltonetworks.com**



2025 Unit 42 Incident Response Report | February 2025