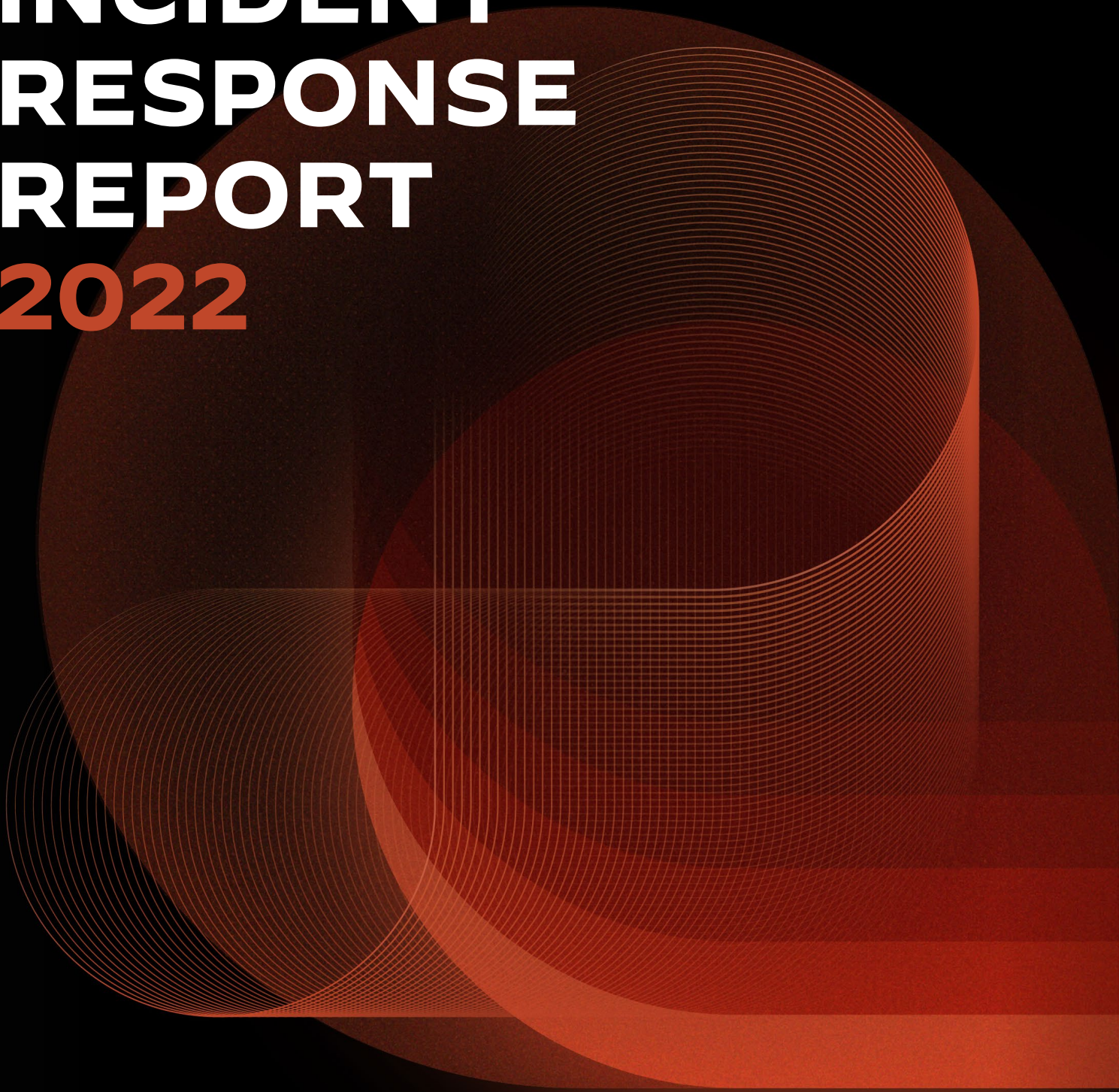
UNIT 42™
BY PALO ALTO NETWORKS

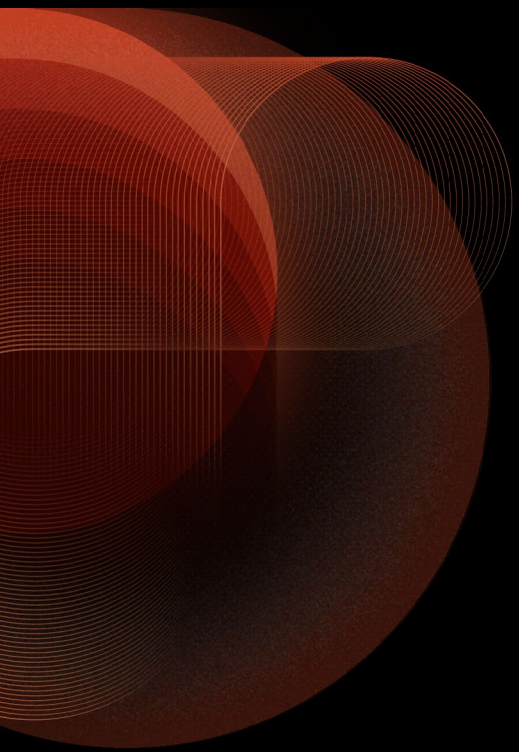
INCIDENT RESPONSE REPORT 2022



paloalto® NETWORKS

INCIDENT RESPONSE REPORT
2022

Table of Contents



Foreword

When it comes to cybersecurity, there is a risk to government, industry, and individual citizens alike. The world's infrastructure, economy, and healthcare are increasingly dependent on digital systems, making it even more critical to align strategies and resources to best mitigate the risks and threats we are facing.

It is important to recognize that cybersecurity is no longer the responsibility of the few. It requires the constant vigilance and efforts of everyone throughout your organization. Because of the far-reaching ripple effects an attack can have across the digital ecosystem, we are seeing everyone, from boards to regulators, take a more active role, demanding greater transparency and the continuous demonstration of an organization's preparedness to respond to the ever-evolving threat landscape.

A series of recent high-profile cyber attacks has spurred governments across the globe to propose new laws or regulations related to reporting significant cyber incidents, from the United States to the European Union, United Kingdom, Canada, Australia, India, and elsewhere. These requirements, if implemented appropriately, would serve to ensure governments have the visibility necessary to adequately respond to incidents affecting critical services and infrastructure, and ensure industry partners can effectively collaborate to defend against these threats.

In other cases, proposed rules would enhance public disclosure of material incidents by publicly traded companies, with a goal of ensuring boards and company executives are appropriately resourcing and implementing cybersecurity policies and procedures commensurate with that organization's risk. The ultimate goal would be to improve an organization's preparedness to withstand a cyberattack by ensuring executive-level oversight.

In order to prepare, organizations must first understand what they are up against. The "2022 Unit 42 Incident Response Report" sheds light on the risks and threats that organizations are facing. It provides insights into threat actors and their methods that can then be used to help organizations identify potential gaps in their defenses and areas to focus on to improve their cybersecurity stance going forward.

This year, business email compromises (BEC) and ransomware were the top incident types Unit 42 handled. Both types of attacks are prevalent because they generate fast, easy money for criminal groups. Beyond lining an attacker's pockets, these breaches can be used to fund and inform subsequent criminal acts, including those sponsored by nation-states.

Ransomware in particular has been a focus area for many in the cybersecurity industry because of the impact on targeted organizations and those who depend on them. Ransomware threat actors gain control over critical data and resources and then leverage this control to coerce high-dollar payments from their victims. Unfortunately, these attacks have been made even easier with the rise of ransomware-as-a-service (RaaS) offerings.

Our job is to help break the cycle of illicit activity to protect the greater digital ecosystem. This report outlines recommendations that any organization can employ to strengthen its security posture and mitigate the impact of an incident. Implementing these best practices will go a long way toward making it harder and, therefore, less lucrative and appealing for threat actors to attack. Patching vulnerabilities, implementing multifactor authentication and fixing misconfigurations may not be exciting, but these foundational steps reduce an organization's attack surface and ensure it is not an easy target.

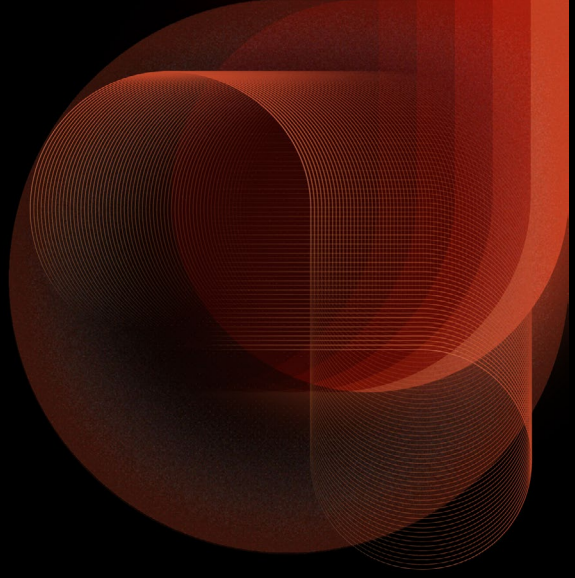
Once the basics are covered, organizations can move to implement additional capabilities and defenses to address the more advanced hackers and tactics. The goal is to make it as difficult and costly as possible for attackers to succeed at any attack stage. It will take everyone being vigilant and working tirelessly to protect our connected, digital ecosystem, but this effort is vital if we are to ensure that ecosystem is always there and functioning to the benefit of us all.

Ciaran Martin

Founder and former CEO of the United Kingdom's National Cyber Security Centre

Executive Summary

Every week brings news about threat actors—new campaigns, new groups, new types of attacks, new targets. Defenders can easily wind up playing catchup, but what does it take to flip the script?



SOC teams need to know where to focus defensive and network security efforts in a dynamic cyberthreat landscape. CISOs need to understand the greatest security risks they face, and where to prioritize scarce resources to reduce them.

Unit 42 has insights into hundreds of incident response cases, as well as global telemetry and threat intelligence gathered at a large scale, and we can use that to provide insights into today's cyberthreat landscape—and where it might be headed.

Using a selection of over 600 incident response cases conducted over the past year, we identified these key patterns and trends:

70% **of incident response cases** over the past twelve months were ransomware and business email compromise (BEC).

77% **of intrusions** are suspected to be caused by three initial access vectors: phishing, exploitation of known software vulnerabilities and brute-force credential attacks—focused primarily on remote desktop protocol (RDP).

MORE THAN 87% **of positively identified vulnerabilities** fell into one of six major categories: ProxyShell, Log4j, SonicWall, ProxyLogon, Zoho ManageEngine ADSelfService Plus and Fortinet.

7 **most targeted industries** were finance, professional and legal services, manufacturing, healthcare, high tech, and wholesale and retail.

50% **of targeted organizations** lacked multifactor authentication on key internet-facing systems such as corporate webmail, virtual private network (VPN) solutions and other remote access solutions.

While there is no one-size-fits-all solution to protect your organization from cyberattacks, CISOs, SOC leaders, incident responders, security analysts, network defenders, and other professionals can use commonalities in our cases to understand what attackers are going after and how they've been successful. We accompany these insights with concrete recommendations on how to protect your organization. This is our way of sharing lessons from the incident response trenches to help bolster your security efforts.

We also asked our incident responders to look ahead to the cyberthreats on the horizon. They shared the following predictions:

- The window of time to patch high-profile vulnerabilities before exploitation will continue to shrink.
- The widespread availability attack frameworks and hacking-as-a-service-based platforms will continue to increase in the number of unskilled threat actors.
- Reduced anonymity and increased instability with cryptocurrency could lead to a rise in business email compromise or payment card-related website compromise.
- Declining economic conditions could push more people into cybercrime as a way to make ends meet.
- Hacktivism and politically motivated attacks will increase as motivated groups continue to hone their ability to leverage social media and other platforms to organize and target both public and private sector organizations seen as adversarial.

Alongside these predictions, we offer strategies for how you can get ahead of these future threats today.

In the pages that follow, we identify the top methods attackers used to gain initial access, as well as details on what led to the incident or allowed it to escalate. We provide an in-depth spotlight on several key incident types—ransomware, business email compromise, and cloud incidents. Finally, we share our top actionable recommendations for securing organizations based on our experience helping clients.

01

How Incident Response Data Can Help Prevent Bad Days

Incident response services are there for you on a bad day. When you need to use them, every second counts. At that moment, you likely have a critical security incident to address and the top priority is to contain and eradicate threats, recover, and restore your organization's ability to function as quickly as possible.

Reading about incident response can be a totally different experience.

You can do this at a much calmer moment, gaining insights from what's gone wrong in the larger world so you know how to prepare your organization—and, we hope, successfully prevent some of those bad days.

For any type of incident response, the key questions remain the same: What did they do? How did they do it? Did they take anything? When our experts ask those questions, we learn what we need to help an individual client, and we build up a body of knowledge about how threat actors operate and how they gain access to systems.

Our incident responders say there are key pieces of advice they give to almost every client about how to recover from an incident and close security gaps moving forward.

You don't have to wait until a bad day to get that advice. We've gathered our top insights from hundreds of recent cases and are sharing them here along with key tips for prevention and preparedness. You may still need to call on incident response services one day – threat actors can be determined and innovative.

Our hope is that if you do, you'll have some peace of mind even if you're having a bad day as you make that call.

If you apply the top recommendations we share here, you'll know that you've made a strong start toward preparing your organization for today's threat landscape. You'll have an understanding of your organization's security posture so that if you do need to respond to a critical security incident, you'll come at that effort with a foundation of confidence. You'll know that you've taken steps to limit the damage threat actors can do within your systems and put measures in place to ease the recovery process.

How to Use This Report

If you're a security leader:

Use the data in this report to help determine where to focus your resources. Pay close attention to What Attackers Are Going After in 2022 and Predictions: Follow the Money, and use these views of the current and future threat landscape to help you strategize about where your organization most needs protection.

Sharing the report with your Board could help start and support conversations about the resources you need to properly protect your organization and the potential impact of a breach. You may benefit from spotlights on specific challenges, including ransomware, business email compromise and cloud incidents—especially if these are areas of particular concern for you or your board. Consider sharing the report with your direct reports and security teams, too, so they can evaluate and implement recommendations in the areas you prioritize.

However you decide to steer your team, it's worth taking a look at our incident responders' top recommendations: If You Take Any Action to Protect Your Organization, Start With These Six Things. We recommend ensuring that your organization has these fundamentals covered since they would help prevent and mitigate many types of incidents that organizations commonly face.

If you're a security practitioner:

This report includes many practical recommendations based on our incident responders' on-the-ground experiences. Start with our team's top recommendations—a set that is tailor-made to help prevent and mitigate many types of incidents that organizations commonly face. You'll find them in the section titled, If You Take Any Action to Protect Your Organization, Start With These Six Things.

Once you've laid the foundation, move to the more in-depth recommendations that follow the conclusion. These are grouped based on the incident types they're designed to address so you can focus your efforts on the issues that matter most to you and your leadership.

It may also benefit you to look closely at the sections on threat actor behavior. Seven Issues Threat Actors Don't Want You to Address covers the seven security gaps that we most commonly observed threat actors using to their advantage. What Threat Actors Do Once They're Inside a Network includes our observations of threat actors' most commonly used capabilities after initial access. Both these sections can translate to practical guidance on where to shore up your organization's defenses.

Consider sharing the report with your peers and leadership to coordinate your defense efforts and obtain buy-in on key approaches to protecting your organization.

02

What Attackers Are Going After in 2022

If you know what attackers are going after, you know what you most need to protect. Here's what we found in our case data about the most common incident types, how attackers are gaining initial access, what vulnerabilities they're exploiting, and which industries they're targeting.

Attackers' financial motivations drive heavy use of ransomware and business email compromise.

Incident Types

Ransomware and BEC were the top attacks we responded to over the past 12 months, accounting for approximately 70% of our incident response cases.

While these two attacks are the primary ways threat actors can monetize illicit access to networks, attackers have and use additional strategies for financial gain. Threat actors have increasingly paired extortion with encryption (sometimes including added threats of informing customers or the press, or conducting a distributed denial-of-service attack). Some attackers focus on extortion alone. For example, 4% of our cases involved extortion without encryption—a technique distinct from ransomware that can be simpler to execute. In these cases, attackers coerce organizations into paying by threatening the release of customers' data.

Our incident responders and threat intelligence analysts note that extortion without encryption is likely to rise. The efficacy of extortion tactics has even led some prominent threat actors associated with the Conti ransomware group to publicly state that they envision focusing their future efforts on attacking organizations through extortion alone.

Ransomware is a type of malware used by cybercriminals for financial gain. It is delivered in the same way any type of malware makes its way onto targeted systems (e.g., through known vulnerabilities, already compromised systems, social engineering tactics, etc.). Once deployed, the ransomware will encrypt the organization's files and render them unusable to the organization. The attacker demands ransom, promising to provide a decrypter and not further disclose the client's data or identity in exchange.

Business Email Compromise (BEC) is a category of threat activity involving sophisticated scams which target legitimate business email accounts through social engineering (e.g., phishing) or other computer intrusion activities. Once businesses are compromised, cybercriminals leverage their access to initiate or redirect the transfer of business funds for personal gain.

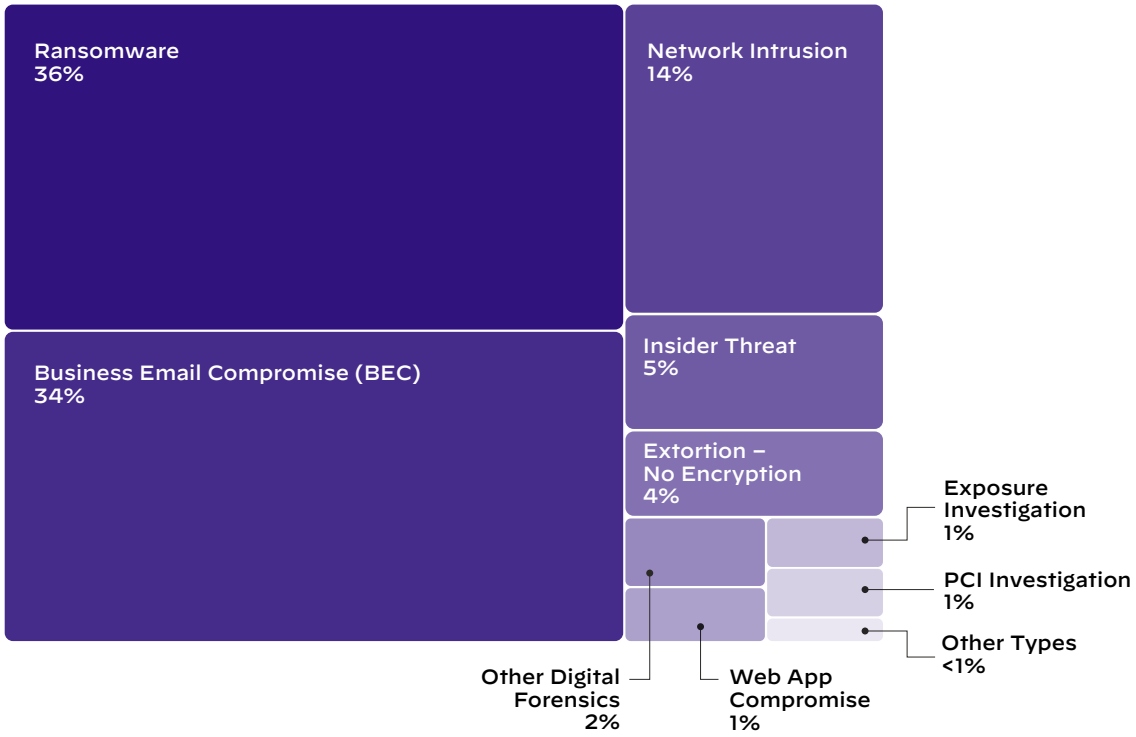


Figure 1: Types of Investigations Conducted by Unit 42 in 2022

Attackers are looking for easy ways in.

Suspected Means of Initial Access

The top three access vectors for threat actors were phishing, exploitation of known software vulnerabilities and brute-force credential attacks—focused primarily on remote desktop protocol (RDP). These three attack vectors totaled over 77% of the suspected root causes for intrusions. Of note, the next most commonly used means of access for threat actors was leveraging previously compromised credentials.

Remote Desktop Protocol (RDP) is a protocol on Microsoft Windows systems that is designed to allow users to connect to and control a remote system. Common legitimate uses include allowing IT support to remotely control a user's system to fix an issue, allowing access to virtual machines in cloud environments and remotely managing cloud assets. Unfortunately, it is easy to expose RDP unintentionally, which has led to it becoming a popular initial attack vector among threat actors.

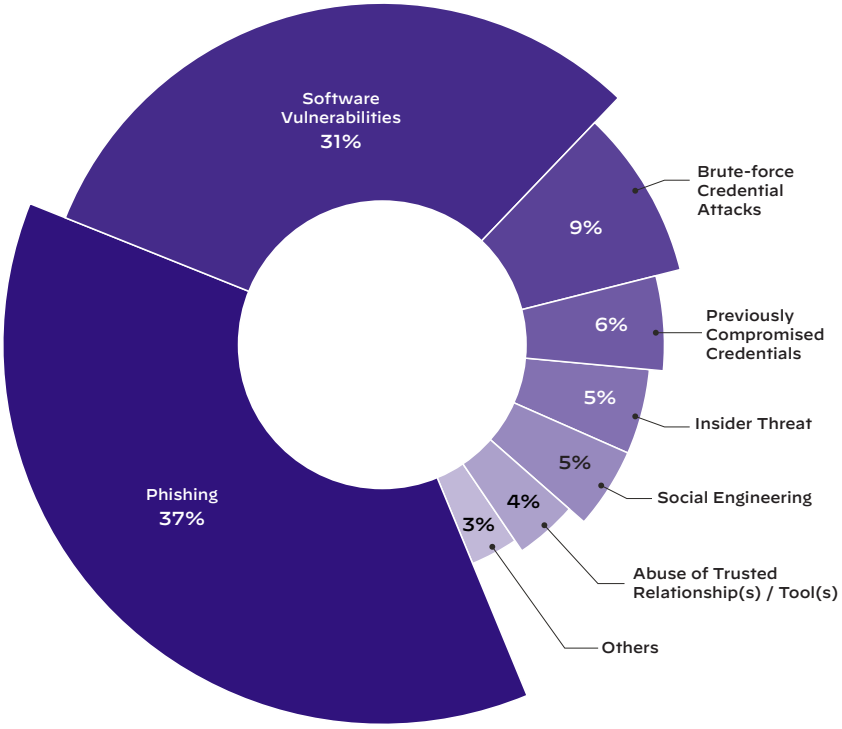


Figure 2: Suspected Means of Initial Access

How do organizations find out they've been compromised?

Often, organizations notice an alert or find software that shouldn't be installed, signaling that something odd is going on in the network.

Other times, the threat actor reveals their presence by popping up with a ransom note.

Sometimes, it gets stranger than that. In one case, a threat actor compromised a series of identification photos and other sensitive scanned documents, then stitched the images into a mosaic depicting a famous character related to the threat actor's moniker as proof of exfiltration.

A few key vulnerabilities have become attackers' favorites.

Exploited Vulnerabilities

For cases where responders positively identified the vulnerability exploited by the threat actor, more than 87% of them fell into one of six CVE categories.

The primary categories are and their corresponding CVEs, where available, are:

- ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
- Log4j
- SonicWall CVEs
- ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)
- Zoho ManageEngine ADSelfService Plus (CVE-2021-40539)
- Fortinet CVEs

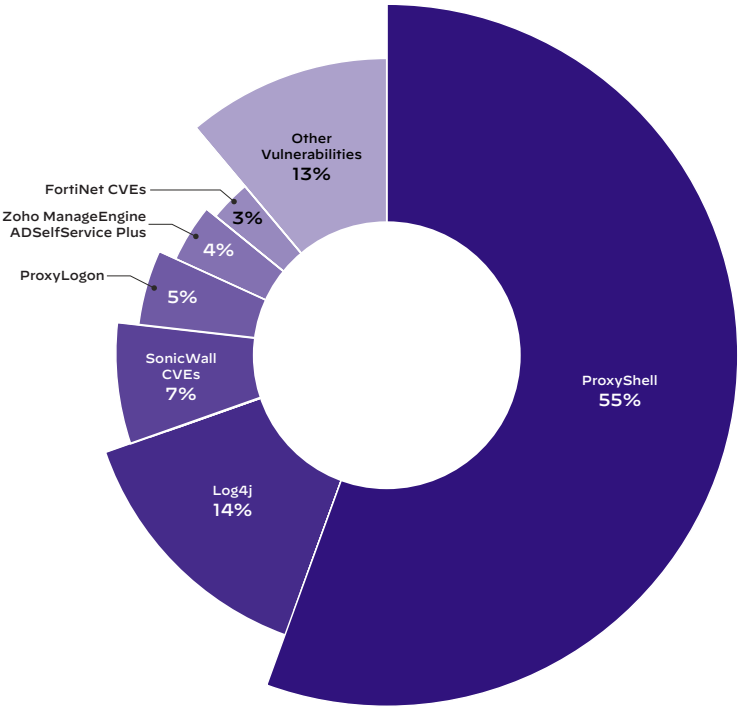


Figure 3: Exploited Vulnerabilities in Unit 42 Cases

Log4Shell

On Dec. 9, 2021, a zero-day remote code execution (RCE) vulnerability in Apache Log4j 2 was identified as being exploited in the wild. Public proof-of-concept (PoC) code was released and subsequent investigation revealed that exploitation was incredibly easy to perform. What followed was a series of events that will go down in cybersecurity history.

RCE vulnerabilities are often high severity because they allow an attacker to execute malicious code on a system, but this vulnerability had a particularly far-reaching impact. Log4Shell was rated a 10 on the Common Vulnerability Scoring System (CVSS)—the highest possible score. And while Apache Log4j 2 may not have been a household name outside the technical community, the software underlies a large number of well-known services and systems. Organizations all over the globe had vulnerable systems (whether or not they knew it), and mass scanning activities seeking these vulnerable systems began almost immediately.

Unit 42 researchers monitored hits on the Apache Log4j Remote Code Execution Vulnerability Threat Prevention signature, which allowed us to gain visibility into exploitation attempts. Between Dec. 10, 2021, and Feb. 2, 2022, we observed almost 126 million hits triggering the signature. While the largest number of hits occurred in days immediately following public knowledge of the vulnerability (Dec. 12-16), spikes of hits continued to take place throughout that entire period.

When we investigated what would have happened had the hits on our Threat Prevention signature been successful, we observed a wide range of attempted activities: vulnerable server identification via mass scanning, the installation of backdoors to exfiltrate sensitive information and to install additional tools, the installation of coin mining software for financial gain and many more.

Before long, incident response cases also began to appear. Log4j accounts for 14% of cases where responders positively identified the vulnerability exploited by the threat actor—despite only being public for a few months of the time period we studied.

> "Log4Shell is not the first vulnerability garnering significant public interest, and it almost certainly won't be the last. That's why it's important to look at Log4Shell both as a standalone vulnerability that demands discrete analysis and reflection, and as the latest in a string of national-level vulnerabilities that impact federal systems, critical infrastructure, and state and local networks alike."
>
> **Jen Miller-Osborn, Unit 42 Deputy Director of Threat Intelligence**
> Written testimony submitted to the Homeland Security and Governmental Affairs Committee of the U.S. Senate

Zoho Manage Engine AD SelfService Plus

On Sept. 16, 2021, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released an alert warning that advanced persistent threat (APT) actors were actively exploiting newly identified vulnerabilities in a self-service password management and single sign-on solution known as Zoho ManageEngine ADSelfService Plus.

Building upon the findings of that initial report, on Nov. 7, Unit 42 disclosed a second, more sophisticated, active and difficult-to-detect campaign that had resulted in the compromise of at least nine organizations.

By Dec. 2, the number of targets had grown to 13 across the technology, defense, healthcare, energy, finance and education industries, and we had identified patterns consistent with a persistent campaign (tracked as TiltedTemple). The actor continued to conduct reconnaissance against these industries and others, including infrastructure associated with five U.S. states.

Our threat intelligence analysts believe that the actor's primary goal involved gaining persistent access to the network and the gathering and exfiltration of sensitive documents from compromised organizations.

While the vulnerability in Zoho ManageEngine ADSelfService Plus accounts for only 4% of cases where responders positively identified the vulnerability exploited by the threat actor, the TiltedTemple campaign illustrates how a determined threat actor can use a vulnerability as a doorway to extensive malicious activity.

Attackers follow the money when targeting industries.

Industries Affected: Cases by Industry

The top affected industries were finance, professional and legal services, manufacturing, healthcare, high tech, and wholesale and retail. These industries accounted for over 60% of our cases. Organizations within these industries store, transmit and process high volumes of monetizable sensitive information that attracts threat actors.

Attackers may at times purposely target certain industries—for example, financial organizations because they frequently conduct wire transfers, or healthcare organizations because they may be particularly motivated to avoid operational disruptions. However, many attackers are opportunistic, simply scanning the internet in search of systems where they might leverage specific vulnerabilities. In some cases, industries may have been particularly affected not because attackers intended to target them but because, for example, organizations in those industries happen to make widespread use of certain software with known vulnerabilities.

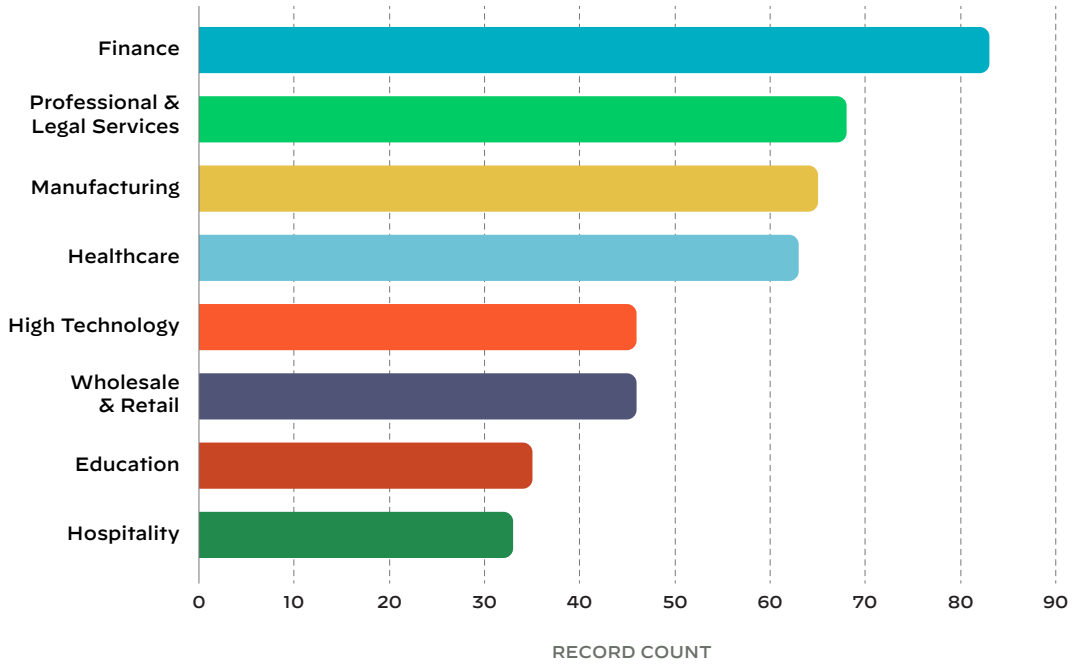


Figure 4: Top Affected Industries in 2022

But not all motivations are financial. Grudges matter, too.

Insider Threats

Insider threats were not the most common type of incident we handled—5.4%—but they can be significant because they involve a malicious actor who knows exactly where to look to find sensitive data. Seventy-five percent of our insider threat cases pertained to a disgruntled ex-employee who left with company data, destroyed company data, or accessed company networks after their departure.

However, our consultants note that many attacks that appear initially to be insider threats turn out to come from cybercriminals who, for instance, purchased stolen credentials. With mature markets for illicit initial access available, differentiating between legitimate user access and malicious user access is becoming more challenging.

Key Insight: Insider threats often involve theft of intellectual property.

Our incident responders report many ways this can happen, including:

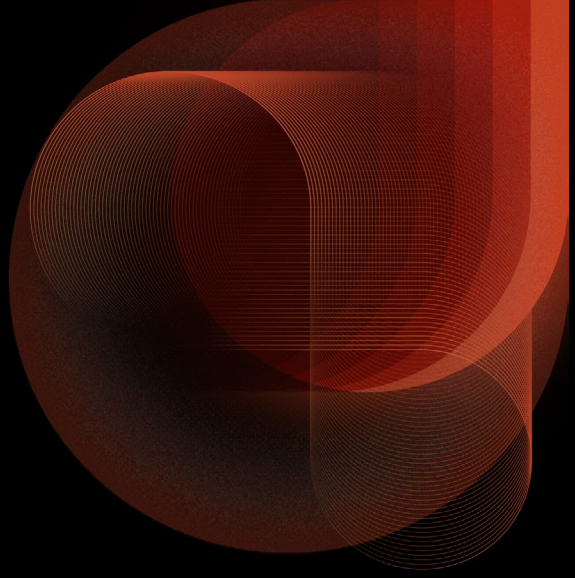
- Transferring data to personal accounts (especially possible when remote work allows an employee to simply shut off a VPN).
- Physically transporting corporate property to a competitor's location.
- Using inside knowledge to locate and hire the same contractors and support staff, who then may have access to privileged information.

75%

of insider threat cases were caused by a disgruntled ex-employee with enough sensitive data to become a malicious threat actor.

03
Spotlight: Ransomware

A FAVORITE CASH COW FOR CYBERCRIMINALS



Ransomware has grabbed attention in recent years. It sometimes seems as if every week brings new high-profile headlines about multimillion dollar demands from threat actors. The choice of targets has at times been disturbing, including hospitals and other organizations that people depend on for the needs of daily life.

Ransomware can disrupt daily operations, causing significant headaches and financial pressure. Increasingly, affected organizations can also expect threat actors to use double extortion, threatening to publicly release sensitive information if a ransom isn't paid.

Cybercriminals have displayed innovation on the one hand—introducing sophisticated attack tools, extortion techniques, and marketing campaigns. On the other hand, the RaaS business model has lowered the technical bar for entry by making powerful tools accessible to wannabe cyber extortionists with easy-to-use interfaces and online support.

What follows is a set of observations from our case data that highlight the impact that ransomware has had on various industries.

Multi-extortion techniques, including double extortion, occur when attackers not only encrypt the files of an organization, but also name and shame the targets and/or threaten to launch additional attacks (e.g., distributed denial of service, known as DDoS) to encourage organizations to pay more quickly. Many ransomware groups maintain dark web leak sites for the purpose of double extortion.

Ransomware as a service (RaaS) is a business for criminals, by criminals, with agreements that set the terms for providing ransomware to affiliates, often in exchange for monthly fees or a percentage of ransoms paid. RaaS makes carrying out attacks that much easier, lowering the barrier to entry for would-be threat actors and expanding the reach of ransomware. Unit 42 is actively tracking at least 56 active RaaS groups, some of which have been operating since 2020. Due to the success of these groups, we expect activity of this type to continue to grow.

Case Study: LockBit 2.0 Ransomware

LockBit 2.0 is a rebrand of LockBit ransomware and has become one of the most common ransomware variants that organizations are facing this year.

LockBit 2.0 is offered as ransomware as a service (RaaS), but represents a departure from the usual RaaS storyline. While in many cases, RaaS appeals to less technically savvy threat actors, LockBit 2.0 operators allegedly only work with experienced penetration testers, especially those experienced with tools such as Metasploit and Cobalt Strike. This can make it more challenging for organizations to defend against the variant. Affiliates are tasked with gaining initial access to the targeted network, allowing LockBit 2.0 to conduct the rest of the attack.

LockBit 2.0 is also known for its extensive use of double- and multi-extortion techniques. The group maintains a leak site – a website located on the dark web where names and details about compromised organizations are posted and shared in order to increase the pressure to pay a ransom. In addition, LockBit 2.0 operators have been known to perform distributed denial-of-service (DDoS) attacks against compromised organizations' infrastructure to raise the volume even higher—a technique known as triple extortion.

As of May 25, 2022, LockBit 2.0 accounted for 46% of all ransomware-related breach events shared on leak sites in 2022. The LockBit 2.0 RaaS leak site has published names and information about more than 850 compromised organizations. The site itself typically features information such as victim domains, a time tracker and measures of how much data was compromised.

LockBit 2.0 has been observed changing infected computers' backgrounds to a ransom note, which not only demands payment but also attempts to recruit insiders from targeted organizations. Notes that we've observed claimed that threat actors would pay "millions of dollars" to insiders who provided access to corporate networks or facilitated a ransomware infection by opening a phishing email and/or launching a payload manually. The threat actors also expressed interest in other access methods such as RDP, VPN and corporate email credentials. In exchange, they offer a cut of the paid ransom.

These tactics underscore how organizations must prepare to defend against evolving business models being used by threat actors. LockBit 2.0 is not simply aiming to encrypt data and halt business operations; the group also aims to do reputational harm and to encourage insider threats. Defense against this type of ransomware requires a comprehensive awareness of possible attack vectors and a strong incident response plan for mitigating damage after an initial breach.

Ransomware: Initial Access

Ransomware threat actors appear to favor different means of initial access than we saw in our overall statistics. For ransomware, the suspected means of initial access for 48% of our cases came from software vulnerabilities. This is followed by brute-force credential attacks at 20%, phishing at 12%, and both previously compromised credentials and abuse of trusted relationships or tools at 8%.

The heavy use of software vulnerabilities matches the opportunistic behavior we often see from ransomware actors. They typically scan the internet at scale for vulnerabilities and weak points where they can focus. This approach and brute-force credential attacks (typically focused on RDP) can get them the majority of their business.

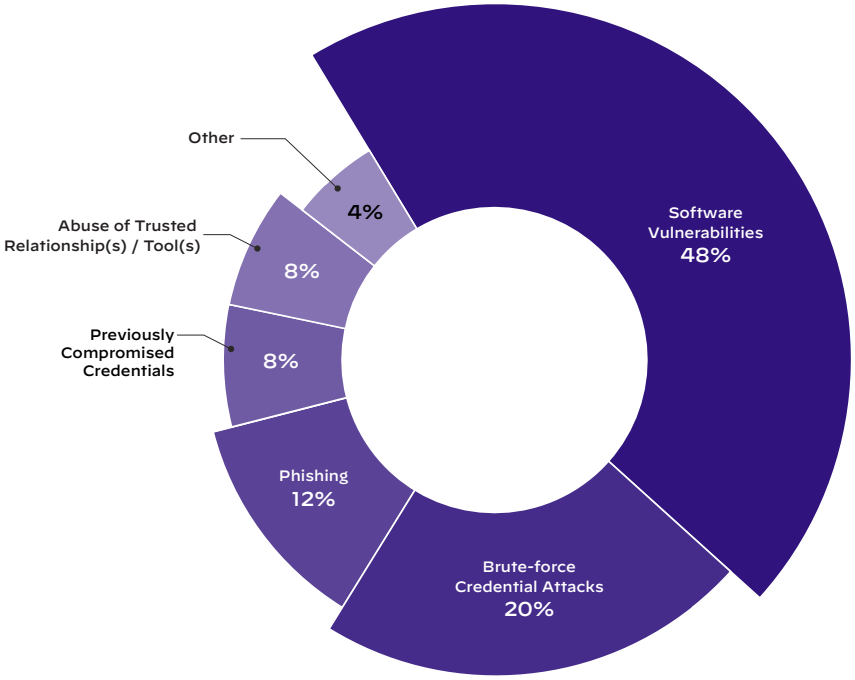


Figure 5: Ransomware – Suspected Means of Initial Access

Ransom Demands and Payments

We have seen ransom *demands* as high as $30 million over the past year, and we have seen instances of clients *paying* ransoms over $8 million.

Threat actors increasingly mention cyber insurance during ransomware negotiations as a reason why a victim organization can afford to pay a ransom. This is sometimes just a negotiation tactic, as we have observed this even with clients who are uninsured. Even so, threat actors do attempt to access financial information when they have unauthorized access to a victim organization and calculate ransom demands based on the (perceived) revenue of the organization being extorted.

News reports often include other examples of large ransom demands or payments.

> "Threat actors will find a way into a network if they want to."
>
> Jessica Ho, Unit 42 Principal Consultant

Ransom Demands and Payments by Industry

When we break our case data by industry, we find the averages and medians shown in Figures 6 and 7. (Note: The median payments shown in Figure 7 are calculated using only cases where a ransom was paid and do not directly relate to the average amount demanded shown in Figure 6.)

Key Insight: Ransomware attacks can happen fast.

The median dwell time we observed for ransomware attacks – meaning the time threat actors spend in a targeted environment before being detected, was 28 days. Our security consultants say that clients most often learn about ransomware attacks the hard way—when they receive a ransom note.

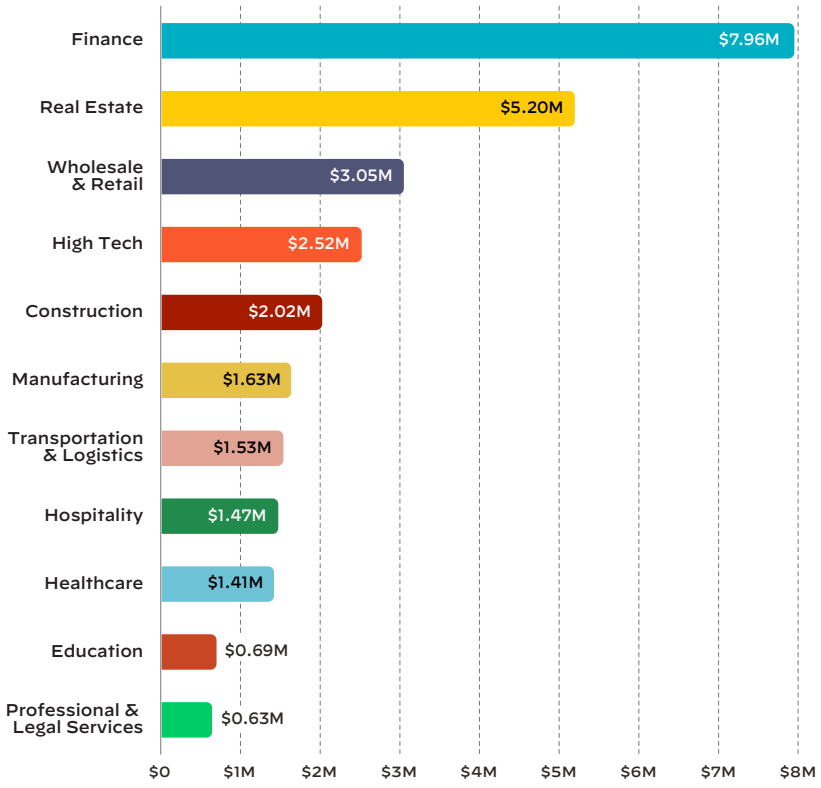


Figure 6: Average Ransom Demand by Industry

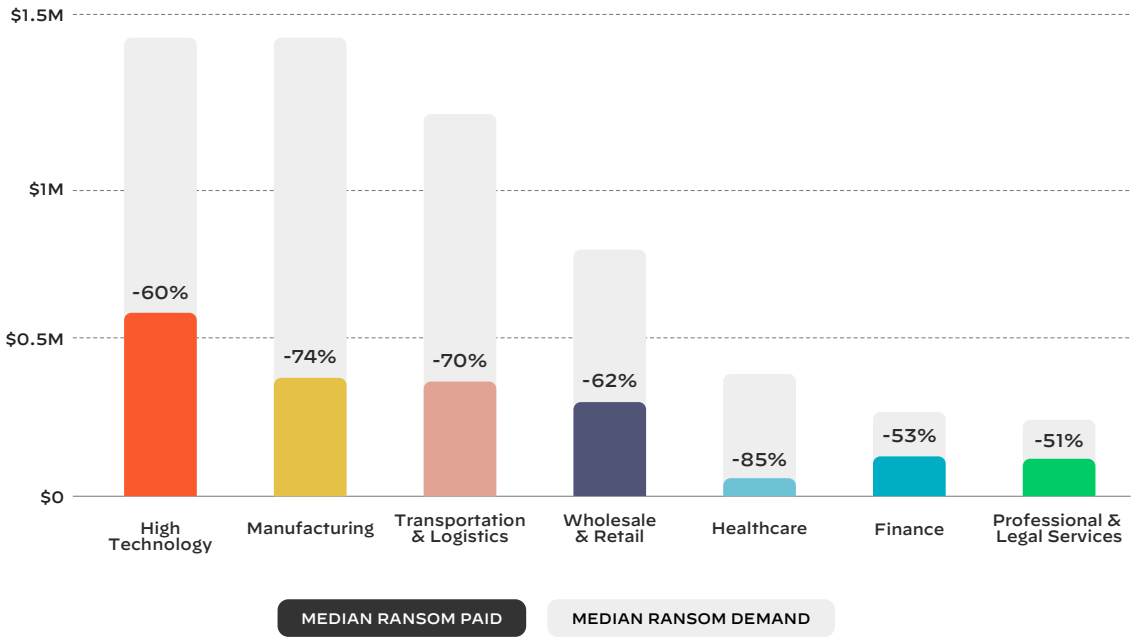


Figure 7: When Ransom is Paid: Median Reduction from Initial Demand by Industry

Most Active Ransomware Groups

Among the cases our incident response consultants handled, certain ransomware groups stood out as particularly active. Ransomware groups are often known for using particular tactics, techniques, and procedures (TTPs), so knowing which groups are most active and dangerous can help your security teams determine where to focus your defense. Be aware, however, that new ransomware groups start up regularly, and existing groups often rebrand for a variety of reasons, including to shift their approach or to avoid attention from law enforcement.

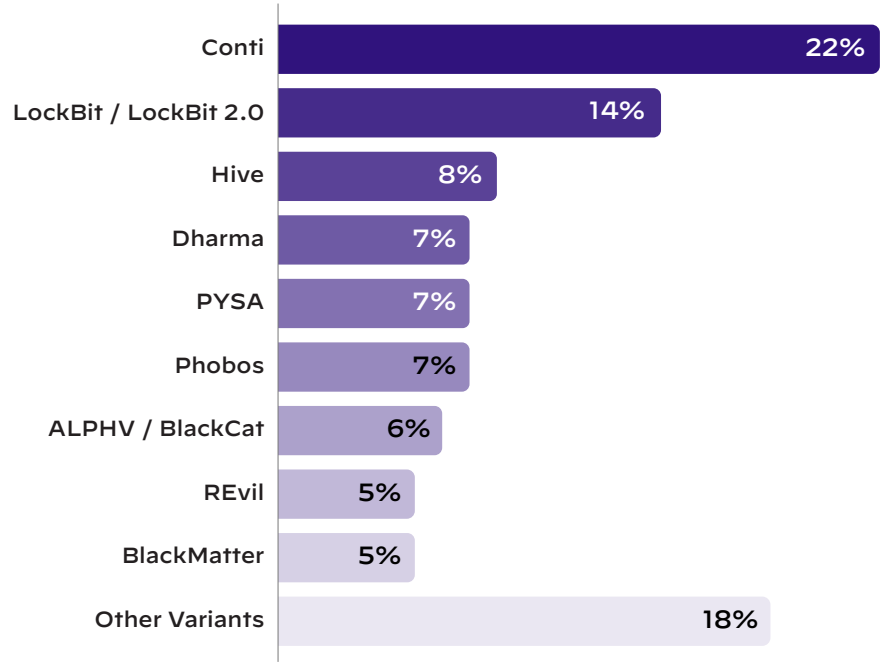


Figure 8: Top Confirmed Ransomware Actors Observed in Unit 42 Cases

Unit 42 regularly releases freely available overviews of active ransomware groups, including TTPs and advice for how to defend against them.

Read our assessments of:

- Conti
- LockBit 2.0
- Phobos
- Dharma
- REvil
- BlackCat

Sign up for notifications on new research about ransomware groups and other threats.

For an in-depth ransomware update and overview of ransomware threat actors and their TTPs, refer to the 2022 Unit 42 Ransomware Threat Report 2022 or our corresponding webinar.

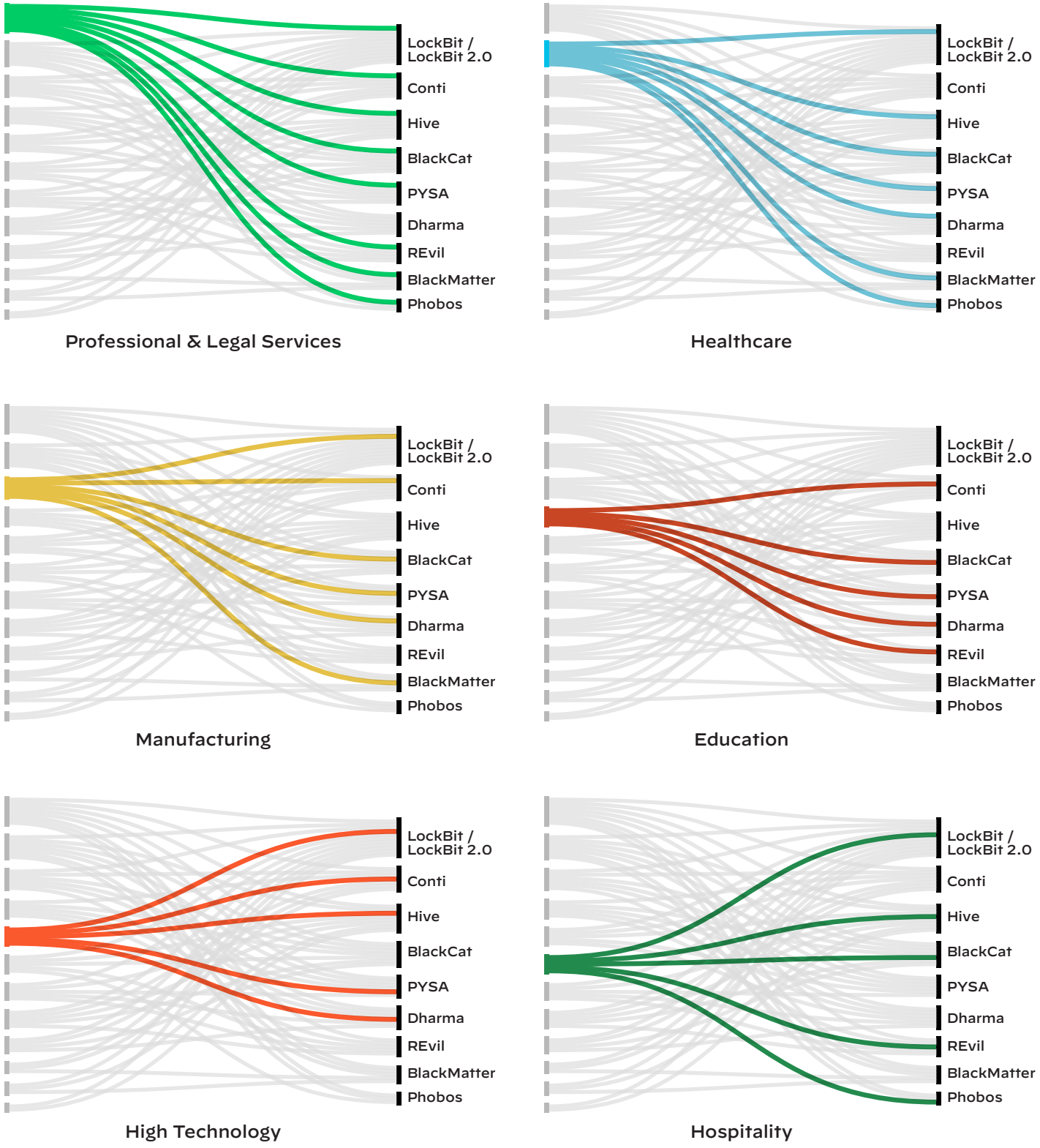


Figure 9A: Industries Affected by Ransomware vs Ransomware Groups

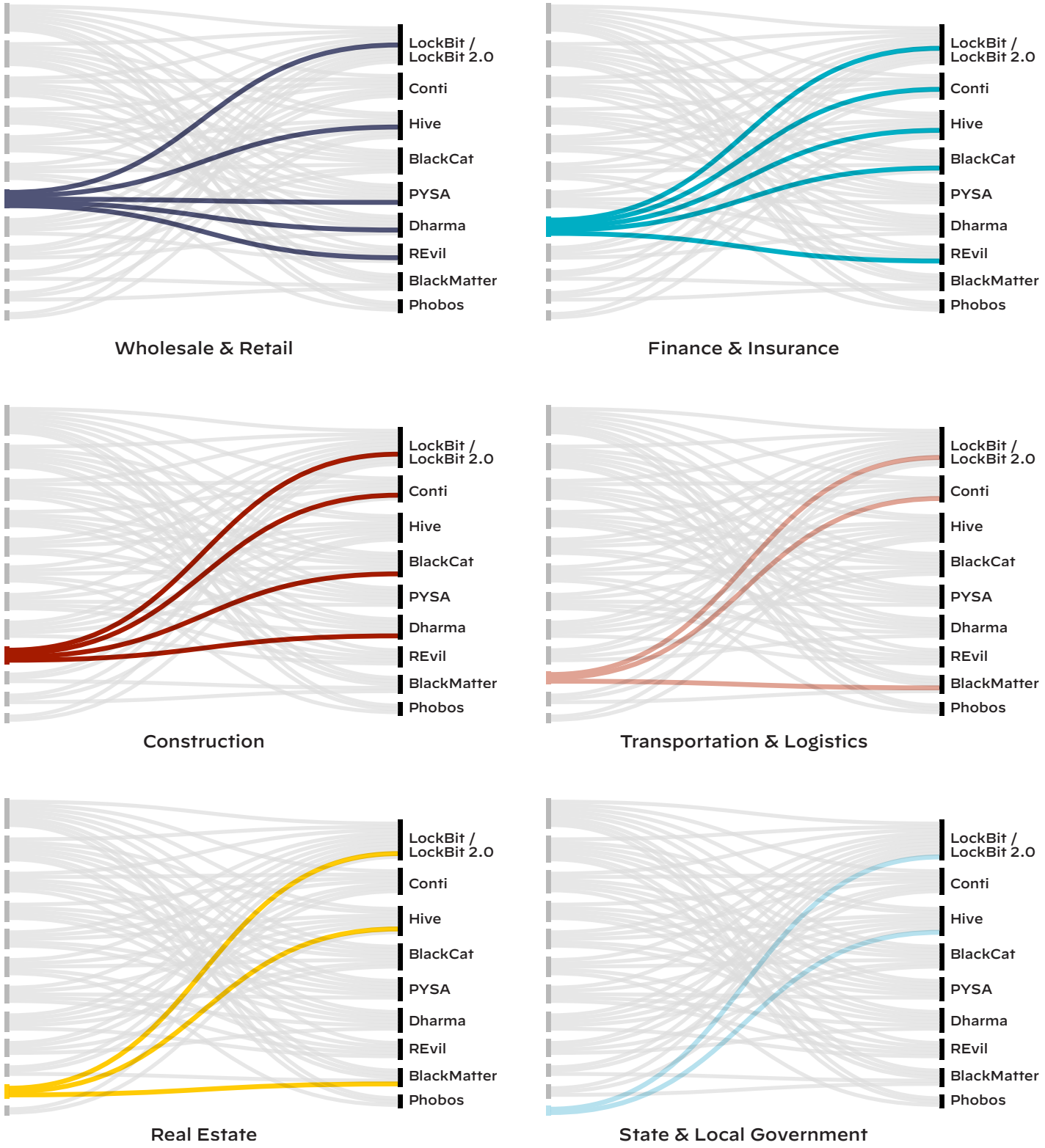


Figure 9B: Industries Affected by Ransomware vs Ransomware Groups

04

Spotlight: Business Email Compromise

UNDER THE RADAR, BUT COSTLY

Case Study

It was a typical day for our client, an executive with a U.S. financial services firm that relies on a widely used MFA mobile app to protect access to email, customer files, and other sensitive data. His iPhone kept pinging him with MFA requests to access his email, interrupting him on a day packed with customer meetings. He was annoyed by the intrusion, figuring it was some kind of system error, and rejected each request so he could focus on work.

He thought it was over when the requests stopped. Months later, however, he learned he had fallen for an MFA fatigue attack. He had mistakenly authorized one of those many requests, unknowingly granting an attacker unfettered access to his email. He learned about the compromise when his bank flagged suspicious wire transfers totaling nearly $1 million. Our investigation uncovered the exposure of data belonging to the company, its employees, and clients.

Fortunately, the company was able to recover the stolen funds, but attacks of this nature can still be costly in terms of reputation—as well as the time and resources spent cleaning up after them.

For more examples of BEC from Unit 42 case files, refer to our blog, "Nightmare Email Attacks (and Tips for Blocking Them)."

Key Business Email Compromise Data Points From Unit 42 Investigations

7-48 DAYS
Typical Dwell Time Prior to Containment

38 DAYS
Median Dwell Time

$286,000
Average Amount of Successful Wire Fraud

SPOTLIGHT: BUSINESS EMAIL COMPROMISE—UNDER THE RADAR, BUT COSTLY

While ransomware attacks tend to dominate the headlines, cybercriminals continue to compromise business emails for financial gain. The U.S. Federal Bureau of Investigation calls BEC the "$43 billion scam," referring to statistics for incidents reported to the Internet Crime Complaint Center from 2016-2021.

Techniques for business email compromise can vary. Some threat groups gain access to targeted accounts through brute-force credential attacks, for example. However, social engineering, including phishing, is often an easy and cost-effective way to gain clandestine access while maintaining a low risk of discovery.

In many cases, cybercriminals are simply asking their unwitting targets to hand over their credentials—and getting them.

SilverTerrier

Over the past half decade, Unit 42 has actively monitored the evolution of business email compromise with a unique focus on threat actors based in Nigeria, which we track under the name "SilverTerrier."

While BEC is a global threat, our focus on Nigerian actors provides insights into one of the largest subcultures of this activity, given the country's consistent ranking as one of the top hotspots for cybercrime. We have compiled one of the most comprehensive data sets across the cybersecurity industry, with over 170,700 samples of malware from over 2.26 million phishing attacks, linked to roughly 540 distinct clusters of BEC activity.

This telemetry enables Unit 42 researchers to proactively share intelligence on cybercriminals with law enforcement agencies. We were recently able to assist with investigations and operations led by INTERPOL, resulting in several high-profile BEC actors being arrested in Operation Falcon II and Operation Delilah.

05

Spotlight: Cloud Incidents

LOW-HANGING FRUIT FOR THREAT ACTORS

Cloud incident response cases deserve a separate discussion because our incident response consultants say there are two key distinctions in the cloud cases we handle:

1. Different technology concepts mean that incident response cases in the cloud often work differently than traditional incident response cases.
2. Right now, cloud threat actors have it easy due to the many unknown facets of the current cloud threat landscape (though organizations have the power to change this).

How the Cloud Landscape Changes Incident Response

Cloud environments are ever-changing. Instances are spun up briefly to handle key workloads, and the next day they no longer exist. Standard incident response procedures, specific to data collection, often aren't as effective in cloud environments because the cloud landscape is both dynamic and ephemeral, and cloud environments can be complex, often using a variety of applications and tools that may even be hosted across several different cloud service providers (CSPs). This can create a challenge in identifying the full scope.

"Right now, threat actors in the cloud don't have to try very hard to be successful at what they do. They may look around and say, 'Okay, there is a door, here are the keys – nobody even knows we found them. Let's see if this works. Oh, it does!' Then they take what they think is worth something, leave a ransom note, and kick over a few flower pots on the way out—just to add a dash of destruction."

Ashlie Blanca, Unit 42 Consulting Director

Case Study

An organization set up a cloud environment for a short-term project. It was left exposed to the internet and misconfigured with a blank root password. A threat actor happened to find the asset and came in, wiped the data, and left a ransom note.

Incident response cases involving cloud breaches call for a different understanding of how to gather evidence. Ephemeral workloads may mean it's not as simple as pulling a standard set of logs, and the amount of data required for review often far exceeds what's seen in a traditional case. Working in the cloud also requires an understanding of the shared responsibility model. Some aspects of security are the responsibility of the CSP's hosting data and applications, but others are the responsibility of the customer.

Many customers appreciate the "plug and play" aspects of operating in the cloud, and they operate trusting in the security controls afforded by major CSPs, but that security breaks down when organizations don't realize that those security controls often need to be activated and properly configured. Organizations are also responsible for identity and access management (IAM)—setting and maintaining proper controls over who can do what in a given cloud environment.

While understanding cloud technologies and configuring them properly is a general issue in cloud security, it can have a specific impact on incident response. For example, if an organization hasn't properly configured data and logs, it's possible not to have access to that information in the event of a breach. In some cases, our consultants report having to subpoena CSPs to obtain key information for an investigation—a time-consuming process at a moment when every second counts.

Why Cloud Threat Actors Have it Easy

Our security consultants say that misconfigurations are a primary root cause of breaches in the cloud—and the problem appears to be growing worse. Properly configured cloud environments ensure that data is preserved and present, turn on security controls provided by CSPs, and manage identity and access to avoid sharing powerful capabilities or sensitive information with people who don't need it.

Improperly configured cloud environments can essentially leave the door unlocked for malicious actors, allowing them to gain initial access without needing to find and exploit a vulnerability or make use of sophisticated techniques. Unfortunately, improperly configured cloud environments are extremely common. Recent Unit 42 research into IAM analyzed more than 680,000 identities across 18,000 cloud accounts from 200 different organizations and found that **nearly all (99%) lacked the proper IAM policy controls to remain secure.** This matters because the same research found that **65% of known cloud security incidents were due to misconfigurations**.

To make matters worse, when Unit 42 researchers have followed changes in misconfigurations over time, they've observed more misconfigurations, not fewer. We've also observed that known cloud incidents have grown at a faster rate than cloud workloads. This essentially means that threat actors targeting cloud environments have plenty of low-hanging fruit to choose from. As a result, our security consultants focused on cloud incident response say they don't typically see the same types of cases that are common for the rest of the organization. Ransomware, for example, is harder to deploy in cloud environments and often calls for more complexity than cloud threat actors need to meet their goals.

Instead, many threat actors targeting cloud environments simply steal credentials—often stored externally in GitHub or other code-sharing instances and not sufficiently secured—and then engage in data theft or destruction. Occasionally, threat actors extort organizations by using their access to drive up resource costs, coercing payment through the threat of an exorbitant bill from a CSP. These tactics allow threat actors to make money by selling sensitive information or extorting organizations without needing to use sophisticated malware.

For an in-depth overview of cloud security findings, with a particular focus on the importance of identity and access management and the TTPs of cloud threat actors, refer to the Unit 42 Cloud Threat Report, Volume 6, or watch Unit 42 researchers discuss these issues in an on-demand video.

How to Make a Cloud Threat Actor's Job Harder

Our consultants say that one of the best things organizations can do to protect against breaches in cloud environments is to ensure that those responsible for those environments are well-trained in how to properly configure them and how to manage access securely. Simply making it harder for threat actors to gain access would prevent a great number of today's cloud incidents. Our clients often notice a breach due to alerts going off or an uptick in resource usage. This means that ensuring that monitoring and logging are properly set up can help identify issues quickly.

As long as the majority of organizations are leaving cloud threat actors easy access points, attackers likely won't mature their techniques. After all, why work harder than necessary? However, our consultants predict that as more organizations learn how to properly safeguard cloud environments, threat actors will likely begin to use more sophisticated techniques.

06

Seven Issues Threat Actors Don't Want You to Address

When breaches happen, one of the most common questions after the fact is: What went wrong? Below are the most common answers from the cases we handled.

Consider this list a reverse-engineered set of recommendations based on our case observations from the past year. If you ensure your organization addresses the issues below before an incident occurs, you can discourage threat actors who are after low-hanging fruit. If threat actors do try to attack your systems, they'll have a harder task ahead. **In other words, here are seven issues threat actors are hoping you won't get around to addressing.**

1 ## Multifactor authentication

In 50% of cases, organizations lacked multifactor authentication on key internet-facing systems such as corporate webmail, virtual private network (VPN) solutions and other remote access solutions.

2 ## EDR/XDR

In 44% of cases, organizations did not have an endpoint detection and response (EDR) or extended detection and response (XDR) security solution or it was not fully deployed on the initially impacted systems to detect and respond to malicious activities.

3 ## Patch management

In 28% of cases, having poor patch management procedures contributed to threat actor success. This refers to any time a non-zero-day vulnerability was exploited by a threat actor in any way and includes situations in which an exploit helped a threat actor at some point after initial access. It does not include cases when threat actors exploited a zero-day vulnerability to gain access.

4 ## Mitigations for brute-force attacks

In 13% of cases, organizations had no mitigations in place to ensure account lockout for brute-force credential attacks.

5 ## Security alerts

In 11% of cases, organizations failed to review/action security alerts.

6 ## Password security

In 7% of cases, weak password security practices contributed to threat actors' ability to further their objectives (e.g., default password, blank or empty password, easily guessed or brute-forced password).

7 ## Misconfigurations

In 7% of cases, system misconfiguration was a contributing factor to the incident.

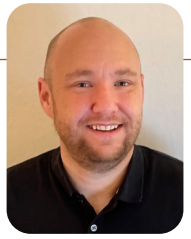
Case Study

Unit 42 incident responders assisted a client with a matter where it was determined that the threat actor was persistently accessing the environment using the client's VPN solution. The company's IT personnel were bewildered as to how this could happen since they required MFA for all accounts. Unit 42 determined that a single IT administrator had been granted an exception and used a web-based SSL VPN portal to support a legacy solution that did not require MFA, and this ended up being the threat actor's entry vector.

In many of these matters, organizations *did* do some of these things in *many* instances. But even *one* gap is all an attacker needs to get a foothold into a victim's environment.

Likewise with EDR/XDR deployment, even in environments with broad coverage, there can be "shadow IT" (unmanaged or unauthorized) systems in the environment with inadequate security controls, or unsupported legacy systems with deficient protections. Often companies are unaware of these systems, and they can end up being contributing factors to a cybersecurity incident.

Therefore, one important step organizations can take to improve defenses is to conduct a thorough inventory of what's on the network and watch out for anomalies, which can be done through an attack surface management solution. If you know the attack surface, you have a better chance of getting ahead of a threat actor.



"If your organization has an EDR or XDR solution, make sure to monitor the alerts.

I have been on multiple engagements where threat actors were eventually able to disable EDR and antivirus to deploy ransomware. The clients sometimes see this as a failure of their security product, when in fact, their security tool has been telling them there are major, obvious problems for weeks or even months before the threat actor was finally able to get to a point where they could disable security tools.

This advice also applies to old school antivirus for organizations that don't have EDR or XDR. Many threat actor tools will be blocked by antivirus. It is important to stay on top of what your security tools are blocking so you can take appropriate action."

John Percival, Unit 42 Consultant

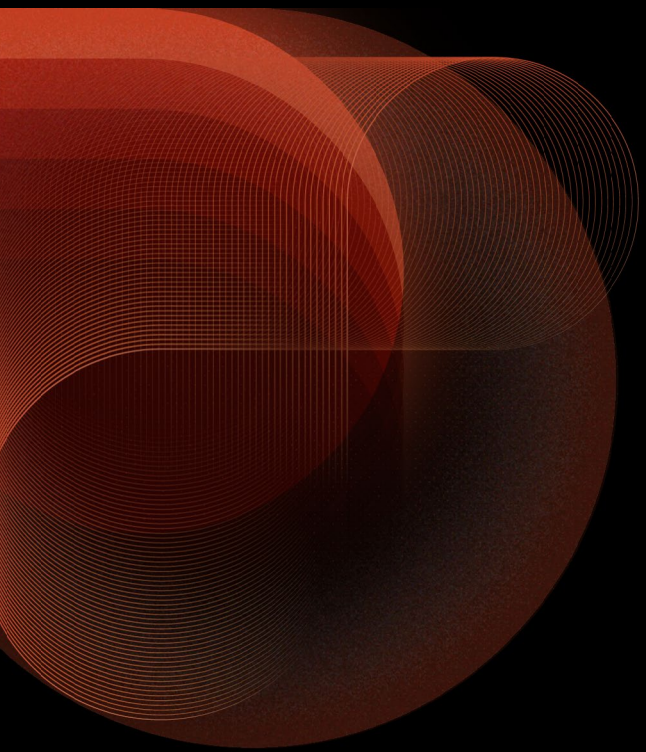
50%

of organizations involved in breaches lacked multifactor authentication on key internet-facing systems.

07

What Threat Actors Do Once They're Inside a Network

Once attackers gain access to a network, they have certain typical goals. For example, they might begin using tactics associated with discovery—gaining knowledge about the system and internal network—in order to decide what to do next.



This section describes the capabilities we most commonly observed threat actors using in our incident response cases after initial compromise of a network. If you work closely with the specifics of your organization's systems, this list can help you see what you most need to watch for. If you safeguard your organization from a higher-level perspective, you can share this list with your security team or use it to help you gain an understanding of how threat actors typically behave once they're inside.

Discovery

This is a step attackers take to figure out what they can do with the access they've gained. They're essentially exploring a system and internal network to see what they can control, what they can steal, what else they can attack, etc.

Capabilities most commonly used for discovery

- Advanced IP Scanner
- Advanced Port Scanner
- AdFind
- Nmap

Command and Control or Beacon

Command and control (C2) covers the techniques that attackers use to communicate between a network they've compromised and a network they control. For example, malware often "phones home" to a C2 server to check for other malware to download or to send exfiltrated data to the threat actor. Attackers typically take steps to make C2 traffic appear "normal" in some way to make it harder for organizations to notice that a breach has occurred.

Capabilities most commonly used for C2/Beacon

- Cobalt Strike
- Metasploit

Lateral Movement

An attacker gains initial access to a specific part of a network. Similar to opening doors to get from a foyer into other parts of a house, lateral movement is the process attackers use to move into and control other systems on a network. Doing this expands the impact an attacker can have in a compromised environment.

Capabilities most commonly used for lateral movement

- AnyDesk
- ConnectWise/ScreenConnect
- TeamViewer
- Splashtop
- Microsoft Remote Desktop
- LogMeIn
- TightVNC
- PuTTY

Key Insight

Our incident responders sometimes find that threat actors have been active in an environment for much longer than initially thought by the client. In some cases, threat actors have been found to have been active and moving laterally through an environment for a period of six months or more.

Credential Harvesting

Credential harvesting is another way for attackers to gain access to more resources or more sensitive information. It refers to methods of stealing names and passwords. Like many other techniques here, this expands access for the threat actor, which in turn expands the potential impact of the breach.

Capabilities most commonly used for credential harvesting

- Mimikatz
- LaZagne
- Impacket secretsdump
- Procdump targeting lsass process
- Multifunctional post-exploitation tools (e.g., Cobalt Strike)

Exfiltration

Exfiltration means stealing data. This is often where attackers make their money. Once they steal data, they can sell it to interested parties or extort the target by threatening to release it publicly.

Capabilities most commonly used for exfiltration

- Applications
  - Rclone
  - MEGASync
  - FileZilla
  - WinSCP
- Compression
  - 7-Zip
  - WinRAR
- Web/cloud storage services
  - MEGA
  - Dropbox
  - Google Drive
  - OneDrive
  - DropMeFiles
  - Sendspace
  - Web Email Services
  - Threat Actor Controlled System

"The quantity of stolen data does not directly correlate to the negative impact of its theft. Unauthorized acquisition of a single spreadsheet containing a list of individuals' personally identifiable information (PII) could result in a large data breach, even though the file size itself may be very small. Companies should avoid storing such repositories of sensitive information in unencrypted files and should be cognizant of where this information is located in their environment."

Dan O'Day, Unit 42 Consulting Director

Classifying Attacker Behavior

One common language for understanding adversary tactics and techniques, used by many organizations globally, is the MITRE ATT&CK framework, which seeks to classify real-world observations of threat actors. This framework provides a way to understand the underlying purpose of the actions attackers take, and it provides a clear way to communicate about these actions across organizations. When Unit 42 publishes about adversary behavior, we typically align what we've seen with this framework, and it can be a useful reference if you're seeking more information about any of the categories of attacker behavior listed here.

08

Predictions: Follow the Money

So far, we've shared key insights into current trends around breaches. We know attackers are often financially motivated and they're looking for the easy way in—and we've shared the specifics of how that appears in the current threat landscape.

But we also asked our security consultants to take a guess at where threat actors are going in the near future. After all, so much of cybersecurity involves the constant attempt to stay ahead of ever-evolving threats – where might defenders get a leg up?

As always, the general advice is to continue to follow the money. Since much of what threat actors do is financially motivated, a good rule of thumb for defenders is to secure any pathway that could allow attackers to make a buck.

However, our on-the-ground view can give us more specific insights. **Here are our incident responders' top predictions for the coming year.**

"One thing is certain: Wherever threat actors can make money is where they're going to spend their time."

Chris Brewer, Unit 42 Consulting Director

Prediction #1: Time to Patch High-Profile Vulnerabilities Will Continue to Shrink

Attackers are making increasing use of high-profile zero days—the kind you read about in the news. For evidence, see our earlier statistics on attackers' use of Apache Log4j vulnerabilities, for example, and highly publicized vulnerabilities in Zoho ManageEngine ADSelfService Plus. Anytime a new vulnerability is publicized, our threat intelligence team observes widespread scanning for vulnerable systems. Our security consultants say they're also seeing threat actors—ranging from the sophisticated to the script kiddies—moving quickly to take advantage of publicly available PoCs to attempt exploits.

While some threat actors continue to rely on older, unpatched vulnerabilities, we're increasingly seeing that the time from vulnerability to exploit is getting shorter. In fact, it can practically coincide with the reveal if the vulnerabilities themselves and the access that can be achieved by exploiting them are significant enough. For example, Palo Alto Networks released a Threat Prevention signature for the F5 BIG-IP Authentication Bypass Vulnerability (CVE-2022-1388), and within just 10 hours, the signature triggered 2,552 times due to vulnerability scanning and active exploitation attempts.

The 2022 Attack Surface Management Threat Report found that attackers typically start scanning for vulnerabilities within 15 minutes of a CVE being announced. Additionally, end-of-life (EoL) systems remain unpatchable and available to an opportunistic attacker for exploitation. For example, the same report found that nearly 32% of exposed organizations are running the EoL version of Apache Web Server, which is open for remote code execution from the vulnerabilities CVE-2021-41773 and CVE-2021-42013. We expect this trend to continue and be augmented by the ongoing increase in internet-exposed attack surface.

> "Asset inventory is a critical part of cybersecurity. You likely won't secure what you aren't aware of, and you have zero visibility into assets you don't manage or know about."
>
> Dan O'Day, Unit 42 Consulting Director

What You Can Do to Get Ahead

Organizations may have previously grown used to taking time between the disclosure of a vulnerability and patching it, but while it's still necessary to perform due diligence on a patch, attackers' ability to scan the internet in search of vulnerable systems means it's more important than ever to shorten the time it takes to patch. Organizations need to ramp up patch management and orchestration to try to close these known holes as soon as possible. An attack surface management solution can help organizations identify vulnerable internet-exposed systems and can often catch systems that organizations may not be aware are running on the network.

Prediction #2: Unskilled Threat Actors Are on the Rise

Our incident responders anticipate a rise in, to put it bluntly, threat actors who don't seem to know what they're doing. Even threat actors who seem to have attack basics down are beginning to resort to the simpler versions of attacks—for example, using extortion without encryption rather than executing a full-blown ransomware attack. Cloud incidents could also rise since threat actors in the current environment often need to discover carelessly guarded credentials rather than demonstrate advanced technical skill.

Several factors could contribute to the phenomenon. High-profile reports of lucrative hacks combined with global economic pressures could push more people to try their hand at becoming cybercriminals—whether or not they have the technical skills. RaaS and similar affiliate programs could cause a flood of wannabes. It's also possible that nation-state recruitment of skilled threat actors could leave spots open for novices wishing to operate more pedestrian scams. Even unskilled attackers, however, could do damage to your organization if they're able to breach your systems.

Case Study

Unit 42 security consultants were attempting to negotiate for a ransomware case, but the threat actors they needed to deal with had a broken chat portal and busted infrastructure. This left no way to communicate with the threat actors—or even to pay the ransom demand should the client have chosen to do so.

What You Can Do to Get Ahead

The good news about unskilled attackers is that they're more likely to be stopped when organizations follow best practices and consistently introduce basic roadblocks. You can see this as an opportunity to reinvest in the fundamentals and ensure that you're using a defense-in-depth strategy.

Educate members of your organization about best practices to avoid social engineering schemes—an approach often favored by less technically skilled threat actors. Solidly covering the foundations of good cyber defense can ensure that rookie cybercriminals looking for a quick payout have a very frustrating day when they encounter your network.

Prediction #3: Changes to Cryptocurrency Could Cause a Rise in Business Email and Website Compromises

One thing that currently contributes to the lucrative nature of ransomware is the prevalence and relative anonymity of cryptocurrency, which gives attackers a way to collect ransoms that avoids banks or institutions that might be able to reveal their true identities. Recently however, law enforcement agencies have had greater success tracing crypto wallets back to their true owners and recovering ransoms. The DOJ, for example, successfully recovered $2.3 million in bitcoin tied to the Colonial Pipeline ransomware attack.

Further, changes in the availability or stability of cryptocurrency undermines its utility as a means of payment. These trends may incentivize threat actors to pivot back to classic fiat currency-based schemes. This could cause a rise in, for example, traditional credit card fraud (often associated with website compromise), and of course, BEC (already popular with threat actors).

What You Can Do to Get Ahead

It's important to prepare against the possibility of ransomware—after all, that's the top incident type that our consultants see. However, don't focus on ransomware to the exclusion of all else. Your organization should institute protections against any popular scheme that could earn threat actors money. In that way, you can be ready if attackers shift to a different favorite attack type.

Prediction #4: Difficult Economic Times Could Lead More People to Leverage Cybercrime

If global economic conditions worsen, more people may be incentivized to try their hand at cybercrime. While this could mean people with some technical skills looking to make a quick buck during a hard time, it could also mean that people within organizations are more likely to explore potential deals with threat actors.

Some threat actor groups have been known to offer to pay insiders who are willing to hand over credentials or assist with other forms of sabotage. When some people are struggling to make ends meet, those offers could be more tempting to some.

These factors may combine with the prevalence of remote and hybrid work—which can make it easier for insiders to steal intellectual property. When working remotely for most organizations, simply disconnecting from the VPN is sufficient for preventing the organization from having insight into your traffic. A company might block personal email and cloud storage sites, but the employee can simply disconnect from the VPN and use their home internet to access these resources from their work computer, then copy company data to these personal locations.

Case Study

Unit 42 has helped organizations respond to multiple Lapsus$ attacks—a group notable for its low emphasis on attacks that require technical skill. The Lapsus$ group doesn't employ malware in breached environments, doesn't encrypt data and in most cases, doesn't actually employ extortion.

Instead, the group focuses on using a combination of stolen credentials and social engineering to gain access to organizations. We've also seen them solicit employees on Telegram for their login credentials at specific companies in industries including telecom, software, gaming, hosting providers, and call centers.

Despite the low-tech approach, the group's attacks and leaking of stolen data can be damaging. We've also seen destructive Lapsus$ attacks where the actors gained access to an organization's cloud environment, wiped systems, and destroyed virtual machines.

Arrests associated with Lapsus$, including that of the apparent ringleader, involved a number of individuals between 16 and 21. Unit 42 researchers assisted law enforcement with information on Lapsus$ threat actors' activities.

What You Can Do to Get Ahead

Follow best practices for remote workers, including deploying robust endpoint detection. Make sure you are practicing the principle of least privilege, limiting access to sensitive data to those who need to have it. Consider a data loss prevention (DLP) solution to monitor, govern, and prevent unsafe transfers of sensitive data and corporate policy violations.

To protect against insider threats from employees who leave your organization, revoke access to accounts promptly upon an employee's departure. Integrating these processes with HR termination processes can help ensure these steps are not overlooked. Analyze data sent to personal email accounts, cloud storage accounts, removable storage devices and so on during the last 30 days prior to an employee submitting their resignation and continue monitoring/restricting until their employment ends.

Prediction #5: Politically Motivated Incidents May Rise

As hot-button political issues intensify around the globe, our incident response consultants believe there may be an increase in hacktivism and politically motivated cybercrime. This could include, for example, data exfiltration, likely with the purpose of sharing it publicly, website defacement, or other ways to make a statement.

In some cases, threat actors may be working with nation-states or on the payroll of politically motivated groups, and in other cases, the threat actors may themselves have political motivations.

What You Can Do to Get Ahead

In addition to following best practices to protect your network—as you would for any cyberthreat—keep a particular eye on alerts from organizations such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Organizations like this one often provide warnings about prominent attack vectors or groups of concern.

09

If You Take Any Action to Protect Your Organization, Start With These Six Things

The cyberthreat landscape can be overwhelming. Every day brings news of more cyberattacks and ever-more-sophisticated attack types. Some organizations may not know where to start, but our security consultants have some suggestions.

Unit 42 security consultants take pride in acting as trusted advisors. We are always looking for opportunities to give back to the cybersecurity community, and we often share key pieces of advice with existing and future clients.

Our security consultants have compiled the list below of the most common recommendations given to clients, based on real-time threat intelligence and experience with hundreds of incident response matters. It is important to note that the provided recommendations are in no way a "silver bullet" for security. However, they are a starting point toward achieving a more robust and resilient cybersecurity program. If you aren't addressing these recommendations, we advise that you try to incorporate them into your organization's strategic roadmap.

If you're further along in the journey toward securing your organization, it's still a good idea to double check to be sure you have these fundamentals in place. For example, in our work with BEC, we found that many organizations believe they've already taken the necessary steps to protect themselves. However, in 2021, Unit 42 found that 89% of organizations that had been subject to BEC attacks had not turned on multifactor authentication (MFA) or followed email security best practices.

Multifactor Authentication (MFA) improves on the traditional password authentication method by requiring two or more pieces of evidence for authentication—helping prevent threat actors from being able to access a system with stolen passwords alone. Additional authentication methods include confirmation messages sent to a smartphone, for example, or the use of an app for additional verification.

"Use multifactor authentication everywhere possible."

Preeti D'Costa,
Unit 42 Principal Consultant

The broad domains and extensive reach of cybersecurity make it easy for potential gaps or deficiencies to fall off the radar. All it takes is one unrecognized gap for an attacker to gain a foothold in an organization's cybersecurity infrastructure.

If You Take Any Action to Protect Your Organization, Start With These Six Things

1. **Conduct phishing prevention and recurring employee and contractor security training.**
2. **Disable any direct external RDP access:** ensure all external remote administration is conducted through an enterprise-grade MFA VPN.
3. **Patch internet-exposed systems** as quickly as possible (given best practices for testing and responsible deployment) to prevent vulnerability exploitation.
4. **Implement MFA** as a technical control and security policy for all users.
5. **Require that all payment verification takes place outside of email** to ensure a multi-step verification process.
6. **Consider a credential breach detection service and/or attack surface management solution** to help track vulnerable systems and potential breaches.

"Work on the basics. Organizations like to follow the news and go after the new 'named' vulnerability while still lacking in the fundamentals such as patch management and multifactor authentication."

Clint Patterson, Unit 42 Principal Consultant

10

Conclusion: Securing Your Organization Is a Journey, Not a Destination

We've aggregated the information gathered during our incident response cases to provide an in-depth view of today's cyberthreat landscape, as well as what tactics threat actors may use in the future.

Now, it's up to you to determine where to focus your defense efforts. We don't believe it's possible to ensure that no breach will ever happen, but we do know it's possible to be well-prepared.

By taking action now, you can ensure that your organization isn't an easy target for threat actors. You can also minimize damage in the event of a cyberattack by limiting attackers' ability to spread through your networks and work out ahead of time what your organization will need to do to remove threats, restore normal operations and recover.

Once you've covered the basics outlined previously, you can turn to the more in-depth recommendations that follow. First, we share a more detailed list of recommendations that can help secure your organization as a whole. Next, we share recommendations geared toward preventing common initial access methods and attack types, which can help you concentrate on mitigating the risks that matter most to your organization.

Initiate Your Response Within Minutes

The clock starts immediately when you've identified a breach. If you don't contain the breach right away and determine the root cause, your adversary will be back in your environment again.

With a Unit 42 Retainer, our experts become an extension of your team on speed dial, helping you respond faster so you can minimize the impact of an attack and get back to business sooner.

"Remember to protect yourself against the hackers—not just the auditors."

Dan O'Day, Unit 42 Consulting Director

Appendix: In-Depth Recommendations to Help Secure Your Organization

Once you've addressed our six essential recommendations, you can turn to the sections below for more comprehensive recommendations and guidance. The recommendations are divided into sections to help you focus your efforts where your organization most needs protection.

Recommendations to Help Make Your Organization as a Whole More Secure

- **Regularly create and test backups**; ensure the backups are stored in a secure off-network location and are appropriately protected via physical or technical controls so threat actors cannot gain access and disable or delete backups to prevent recovery.
- **Adopt account administration best practices across the organization**, including requiring unique and complex passwords that are at least 15 characters in length so they cannot be easily brute forced.
- **Implement a password management solution** to enable employees to manage complex passwords more effectively.
- **Prevent the use of default accounts and passwords**.

Password Tips to Help Prevent Compromise

One of the easiest ways for threat actors to perform unauthorized actions is if they can gain access to authorized credentials. Because of this, strong passwords are of paramount importance. While passwords should be augmented with MFA wherever possible, we recommend the following best practices to strengthen password security:

- Require that default passwords be changed.
- Passwords should be at least 15 characters in length.
- Passwords should include both uppercase and lowercase letters.
- Passwords should include numbers.
- Passwords should include special characters.
- Individuals should be educated about the dangers of reusing passwords in multiple contexts.
- Provide a password management solution to enable employees to manage complex passwords more effectively.

- **Integrate MFA** for all remote access, internet-accessible, and business email accounts to greatly reduce the organization's attack surface. To prevent threat actors from circumventing MFA, disable legacy authentications/protocols and confirm that MFA is not only deployed, but that employees are also using it correctly.
- **Remember to implement MFA internally.** Too often, after authenticating MFA once, a user can bounce around the network without needing to re-verify MFA, even when moving to a system with a different trust level (e.g., from workstation to server).
- **Consider using single-sign-on (SSO) platforms** for web applications.
- **Leverage EDR or XDR solutions,** and ensure your security operations team understands how to utilize this technology in order to maintain full visibility across the network.
- **Patch management is critical** for operating systems and on-premises applications; APT actors will move very quickly to capitalize on vulnerabilities. While it's still necessary to test patches in non-production environments and follow best practices for responsible deployment, organizations must prioritize speed as well. Address new published vulnerabilities as quickly as due diligence allows.
- **Identify your organization's critical and most valuable assets.** This should include conducting an inventory of critical assets to understand where your highest-value targets are and if they require any additional protection.
- **Regularly review Active Directory** for newly created accounts, mailboxes, and unrecognized group policy objects.

"My proudest moments come when the client is able to restore their systems so they can resume business operations."

Danielle Lopez, Unit 42 Senior Consultant

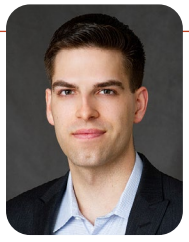
- **Maintain a log retention repository** and regularly review all logs and login attempts for any unusual behavioral patterns. Ensure that logs are stored for the appropriate amount of time to fulfill any legal or regulatory obligations. Our consultants recommend a bare minimum of 90 days, though some we surveyed recommend a year or more—as long as possible.
- **Leverage log aggregation systems**, such as a security information and event management (SIEM) system, to increase log retention, integrity, and availability.
- **Conduct regular security awareness training for all users**, including contractors, on a yearly basis. Also consider utilizing a trusted training platform that allows you to incorporate custom goals and objectives into the training curriculum.
- **Avoid utilizing a flat network**: segregate networks and Active Directories, segmenting sensitive data, and leverage secure virtual local area networks (VLANs).
- **Understand where sensitive data lives** and implement strong access controls to protect that data; monitor and audit access regularly. Limit sensitive data access to only those who need it within your organization and with third parties.

- **Have an incident response and remediation plan**: Incidents may occur despite best efforts, so have a tested, comprehensive plan to ensure fast action should an incident occur. If you have cyber insurance (recommended), be sure to integrate the policy's key processes and contacts into the plan.
- **Follow a defense-in-depth approach**, implementing safeguards at each layer of the web application stack. While the list can be long, it can include, for example, web application firewalls, operating system hardening, application input controls (e.g., parameterization, validation), file integrity monitoring, least-privileged user accounts for database access and industry-standard encryption.
- **When implementing open source code, research it to understand whether it has any published vulnerabilities**; only use code that is vetted and patched. Code scanners may help identify vulnerabilities in open-source software. A recent industry movement to embrace the use of software bills of materials—lists of all the components, libraries and modules that go into building a piece of software—could also make it easier to determine whether vulnerabilities lie within a piece of software your organization is using.
- **Conduct regular web application/code reviews and annual penetration testing** for all public-facing infrastructure to search for vulnerabilities; follow remediation recommendations.
- **Run periodic scans that include configuration checks** and perform regular system audits to detect misconfigurations. Open source scanning tools are available to help. For example, there are open source tools to identify leaked information from misconfigured IAM or find vulnerabilities during build-time in infrastructure as code.
- **Upgrade from Server Message Block Version 1** to limit adversaries from using the inherent file sharing protocol to move laterally within your systems.
- **Implement change control protocols** that require review and sign-off on configuration changes.
- **Disable administrative interfaces and access to debugging tools** for anyone whose job role does not require them.
- **Configure servers to prevent unauthorized access and directory listings**. Enforce strong access controls.
- **Configure security settings in your development environment** according to best practices.
- **Implement full-disk encryption for laptops and removable devices**. Also have a contingency plan to disable lost or stolen devices.
- **Implement and utilize mobile device management applications** that have the capability to locate and/or remotely wipe devices.
- **Give your employees a way to conduct their business legitimately;** simply blocking certain vectors will result in creative workarounds that you'll likely miss.
- **Establish a DLP program** responsible for classifying and tagging data and providing alerts when sensitive or other company-identified relevant information is leaving the organization.
- **Should an employee be terminated, act quickly to revoke their access (e.g., active sessions, tokens, accounts, MFA devices and rotating credentials),** and then verify that access has been revoked. Ensure you preserve their system and data in case an investigation is needed. Coupling account revocation processes with HR processes can help ensure these steps are not overlooked during the termination process.

- **Consider purchasing domains based on common spelling errors or variations of your organization's name.** This can make it harder for threat actors to impersonate your organization.
- **Limit the use of privileged accounts** to only when there is a valid business valid need or a user requires a privileged account in order to complete their job task, and do not reuse local administrator account passwords. This will assist in preventing initial access by attackers, privilege escalation and lateral movement across the network.

Recommendations to Prevent Phishing Attacks

- **Utilize trusted training vendors or platforms** that allow for custom curricula tailored to the organization and employee roles and that takes into account the fast-evolving nature of threat actor methodologies.
- **Create a "security awareness culture."** It is essential that company leaders buy into the importance of cybersecurity, support and promote richer cyber training programs, and emphasize security in company communications.
- **Tailor web-based modules customized to individual groups pertinent to their roles** and how they may be specifically targeted so employees can better spot and avoid tactics that may be used against them.
- **Track leading performance indicators for your phishing tests** so you can adjust phishing content and difficulty based on the needs of the organization.
- **Develop comprehensive training that includes—and goes beyond—phishing and spear phishing.** Include other social engineering concerns that involve physical security, industry best practices against device loss, insider threat indicators, etc.
- **Gamify security training to better engage employees** by setting goals, rules for reaching the goals, rewards or incentives, feedback mechanisms and leaderboards (organizations can compete against each other).
- **Hold across-the-board training annually** and a mid-year "refresh" that builds on specific areas of emphasis, such as advanced techniques for all employees.
- **Adopt advanced phishing protection/machine learning solutions o**r other third-party solutions to detect and deter sophisticated phishing campaigns.
- **Use anti-spoofing and email authentication techniques,** such as Sender Policy Framework (SPF).
- **Consider blocking account logins based on geographic regions** if not needed for normal business operations.
- **Make it easy for users to report suspected phishing email;** promptly review and take action on such messages.
- **Visually alert users concerning attachments from external senders.** This may help identify spoofed domains that appear similar to the company's domain.
- **Leverage email security solutions** that scan attachments and message contents as well as assess sender reputation.



"Organizations should assume that phishing will get through at least some of the time and users will engage. Plan around minimizing the impact."

Clint Patterson, Unit 42 Principal Consultant

- **Many users have an unnecessary volume of unencrypted sensitive information in their email accounts.** Simply not having this information in the account would significantly limit the scope of a potential breach should an unauthorized party obtain access. Encourage users to store information of this type via a file share with role-based access controls rather than simply in email.

Patching Recommendations to Keep Your Organization's Systems Up to Date

- **Inventory all IT assets** (including storage, switches, laptops, etc.) across the entire distributed organization through automated discovery tools to get a clear picture of what you have to manage.
- **Prioritize your patching needs.** Determine which vulnerabilities represent high, medium, or low risk, and their level of priority for the business according to your organizational risk tolerance:
  - Supplement that list by researching vulnerabilities for all operating systems, applications, etc., and add those to your list of priorities to address every month.
  - Any vulnerabilities that have published PoC code should be considered in the "high" risk category to fix.
- **Test your patches in a development QA environment** to ensure they won't "break the system" once deployed into production.
- **Have a schedule for deploying patches regularly.** For some companies, that may only be once a month. However, ensure you are able to deploy high-priority patches out of cycle when necessary (such as those for which PoCs have been published).
- **Once patches are deployed, monitor them for stability.** This may also include monitoring your network for stability.
- **Remove systems that are running on operating systems that are no longer supported.**

Recommendations to Secure Your Cloud Environment

- **Periodically evaluate what data is accessible or exposed on the public-facing internet.**
- **Leverage expertise in cloud security, per platform.** Managing security in the cloud requires expertise catered to the nuances of each platform. The more complex the platform, the more plentiful the opportunities for errors that can inadvertently disclose data.
- **Ensure users with cloud control access are fully trained in each cloud environment.**
- **Evaluate your options for managed security services**, if you do not have the in-house expertise, or your cloud estate is particularly complex and in a continual state of change.
- **Control access to the cloud environment.** Access to cloud controls such as CSP consoles, application programming interfaces (APIs), and command-line interfaces in the cloud should be restricted to only those who need it. Such role-based access control (RBAC) is essential to minimizing risks of configuration and other security errors.
- **Use MFA for authorized users** as well as certificates and digital signatures.
- **Separate administrative and user credentials** and limit everyday users to production environments.
- **Implement allow listing where possible**, to further limit access to known and trusted endpoints.
- **Know what data you have in the cloud and where it is.** Regularly audit your cloud data to know what sensitive data you have and where it's located.
- **Encrypt sensitive data (at a minimum),** segment it, provide access using RBAC and rotate keys regularly. Evaluate whether maintaining keys with the cloud provider or within your organization is the best option for you, but ensure you have a key security policy that limits key access and exposure to risk.

- **Ensure file-level operations are logged.** It's important to have visibility into all historical access and creation/deletion events. Some CSPs don't automatically log these events, and logging must be turned on. We recommend ensuring that appropriate logging tools are activated in cloud environments.

Recommendations to Prevent Business Email Compromise

- **Include training on how to identify and manage fraudulent financial requests,** especially if the request appears to be coming from a valid email address of a colleague—or even a superior.
- **To mitigate the primary method of BEC fraud**, ensure that financial wire transfer verification steps are conducted through non-email communication channels (e.g., text messages, voice phone calls).
- **Limit the number of employees authorized to approve wire transfers** and provide additional training for authorized employees.
- **Implement blocking or alerting for auto-forwarding rules** that forward messages externally.
- **Create custom retention tags for email** that: automatically move older items to archive; delete items older than a certain age (e.g., five years); and permanently delete items no longer needed (e.g., those older than seven years) from both primary and archive mailboxes. Keep in mind, however, that archival policies should align with compliance requirements.
- **Disable legacy authentication** (e.g., single-factor POP, IMAP, or SMTP AUTH).
- **Enable enhanced and granular audit logging** to increase visibility into potentially unauthorized activities.
- **Configure and enable a DLP solution** to prevent users from accidentally (or intentionally) sharing sensitive information.

Want help preparing for an incident? Call in the experts.

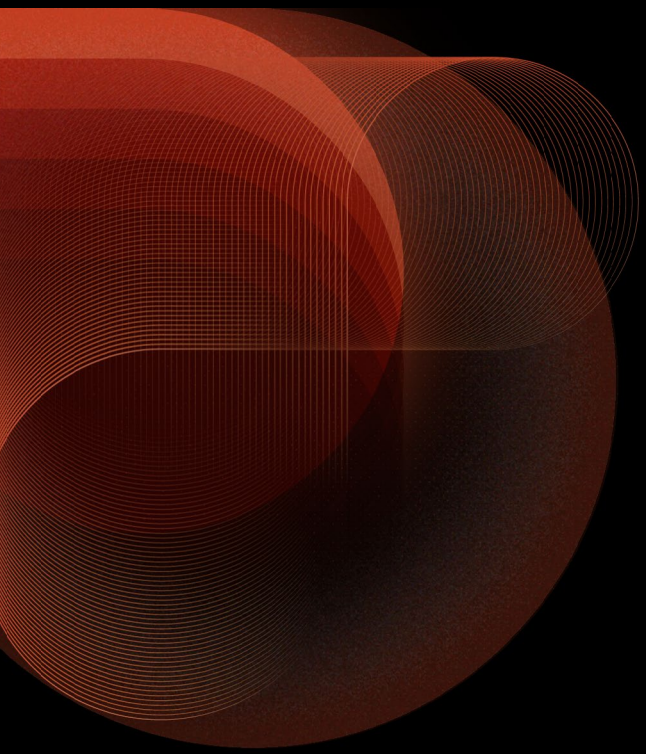
If you have specific concerns about any of the incident types discussed here, believe you may be under attack; or want tailored recommendations for putting together an incident response plan or taking other proactive measures—we'd be happy to help. Please contact us.

The Unit 42 Incident Response team is available 24/7, year-round. If you have cyber insurance, you can request Unit 42 by name. You can also take preventive steps by requesting any of our cyber risk management services.

Methodology

In creating this report, we reviewed the findings from a selection of approximately 600 incident response cases Unit 42 completed between May 2021 and April 2022. These cases included examples of BEC, ransomware, insider threat, nation-state espionage, network intrusions, and inadvertent disclosures. Our clients spanned the range from small businesses and organizations with fewer than 50 personnel to Fortune 500 companies and government organizations with greater than 50,000 employees.

While the majority of cases were located in the U.S., the threat actors conducting attacks were located worldwide, targeting businesses, organizations and IT infrastructure globally. We supplemented our case data with in-depth interviews with experienced security consultants to gather anecdotal and narrative insights from their work with clients in specific areas of expertise. Our recommendations and observations are based on areas where threat actors were largely successful; as such, the lessons themselves have broad applicability regardless of region or industry.



Unit 42 Incident Response Methodology

Every minute an attack remains unresolved costs you money and can damage your reputation. With Unit 42 incident response experts by your side, you will jumpstart your investigation and take advantage of our experience responding to thousands of incidents similar to yours. With our threat intelligence informed approach to incident response and advanced tools across endpoint, network, and cloud, we provide lightning-fast containment to minimize the impact on your business.

Unit 42's average response time—how long it takes us to make initial contact after receiving a request for assistance—is well under 15 minutes. Once called in, we work quickly to understand the full scope of the intrusion, which systems are impacted, and what security actions have already been taken so we can quickly contain the incident.

Learn more about Unit 42 Incident Response services.

We follow a proven methodology:

Scope

For an accurate understanding of the incident, we know it's critical to get the scoping phase right. This allows us to align the right resources and skill sets to get you back on your feet as quickly as possible, and to accurately estimate the level of effort needed to assist you.

Investigate

We then work to fully understand the incident as we investigate what happened, leveraging the available data and working alongside your team.

Secure

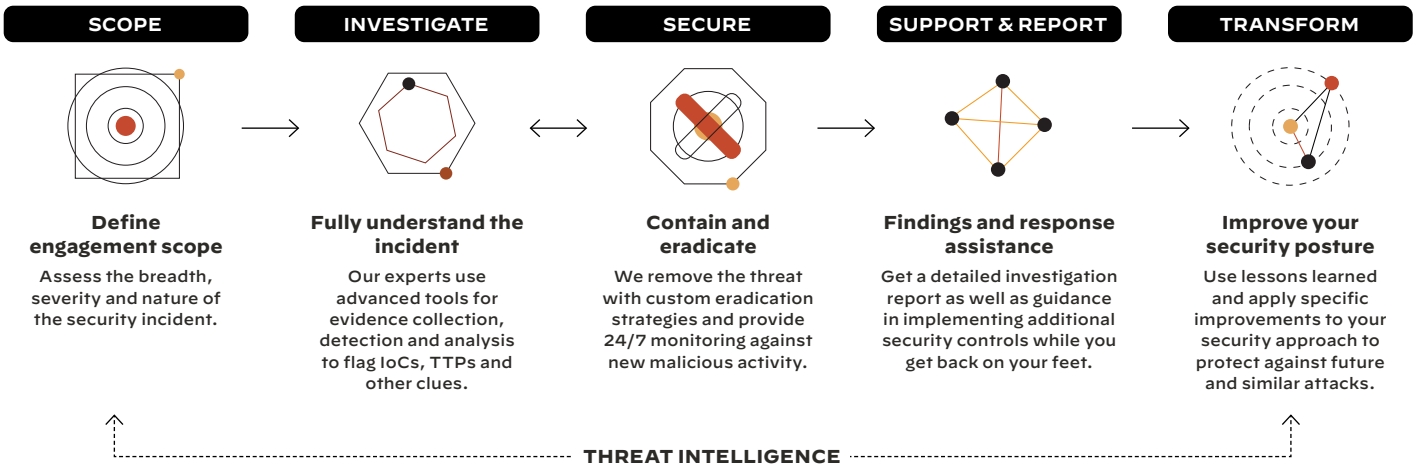
As the incident is contained and the threat actor and their tools are eradicated from your environment, we concurrently assist your organization with rapidly restoring operations.

Support and Report

Unit 42 will also assist you in understanding the root cause and potential impact of the incident, including any unauthorized access or acquisition of sensitive information that may trigger legal obligations.

Transform

We believe a key step in incident response is helping ensure an improved security posture going forward. We work with you to apply specific improvements that will help protect against future and similar attacks.



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 (2021), Comparably Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and systematically disrupt malicious cyber actors. Visit the Cyber Threat Alliance for more information.

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.

Palo Alto Networks Prevent, Detect, and Respond Capabilities

PREVENT

Secure Access and Minimize the Attack Surface

Combine fine-grained, least- privileged access with continuous trust verification and deep, ongoing security inspection to protect all users, devices, apps, and data everywhere. Secure access to implement a system of record to track every asset, system, and service you own that is on the public internet, including RDP—a common initial attack vector.

Recommended products

Cortex Xpanse

ZTNA 2.0

Prevent Known and Unknown Threats

To stay ahead of fast-moving and evasive threats, ML-powered security stops known, unknown and zero-day threats in real time to eliminate the initial victim and any future targets across the attack lifecycle. Seamlessly integrated with Palo Alto Networks' Next-Generation Firewalls, our Cloud-delivered Security Services coordinate intelligence to across all traffic, applications, devices and users to provide best-in-class protection from exploits, malware, ransomware, malicious websites, phishing, spyware, and command and control (C2) and DNS threats.

Recommended products

Advanced Threat Prevention

WildFire

Advanced URL Filtering

DNS Security

SaaS Security

IoT Security

Next-Generation Firewalls

Virtual Firewalls

Cloud NGFW for AWS

Containerized Firewalls

DETECT

Detect Threats in Real Time

To safeguard any enterprise, detecting and blocking exploits and evasive attacks with swift resolution is essential. Cortex XDR® uses machine learning to profile behavior and detect anomalies indicative of attack. WildFire® utilizes near real-time analysis to detect previously unseen, targeted malware and advanced persistent threats, keeping your organization protected.

Recommended products

Cortex XDR

WildFire

Secure Cloud Workloads

Palo Alto Networks helps ensure that all cloud infrastructure, Kubernetes, and container images are securely configured, and steps have been taken to minimize vulnerabilities by:

- Detecting and remediating vulnerabilities and misconfigurations in code repositories, container images, and infrastructure as code from DevOps tools.
- Detecting vulnerabilities and misconfigurations in hosts, containers, and serverless functions from build to deploy to run.
- Segmenting services.

Recommended products

Cloud Workload Protection

Cloud Code Security

Cloud Network Security

RESPOND

Stop Lateral Movement and Data Leakage

Threat actors, including ransomware actors, must establish command-and-control and will then typically move laterally after initial exploitation,. Acting on objectives will often end in sensitive data extraction. Palo Alto Networks:

- Blocks 96% of unknown web-based malleable command and control as well as all known C2
- Stops DNS-based attacks with 40% greater coverage of threats typically used in data exfiltration attempts that specifically exploit the DNS protocol.
- Provides visibility into and segments IoT, OT, IT, and Bluetooth devices.
- Automatically detects and prevents many types of unsafe transfers of sensitive data against corporate policies.

Recommended products

Advanced Threat Prevention

DNS Security

Enterprise Data Loss Prevention

Identity-Based Microsegmentation

Automate Response

Consider implementing tools that support the automated remediation of events that leverage pre-made playbooks to respond and recover from incidents.

Recommended products

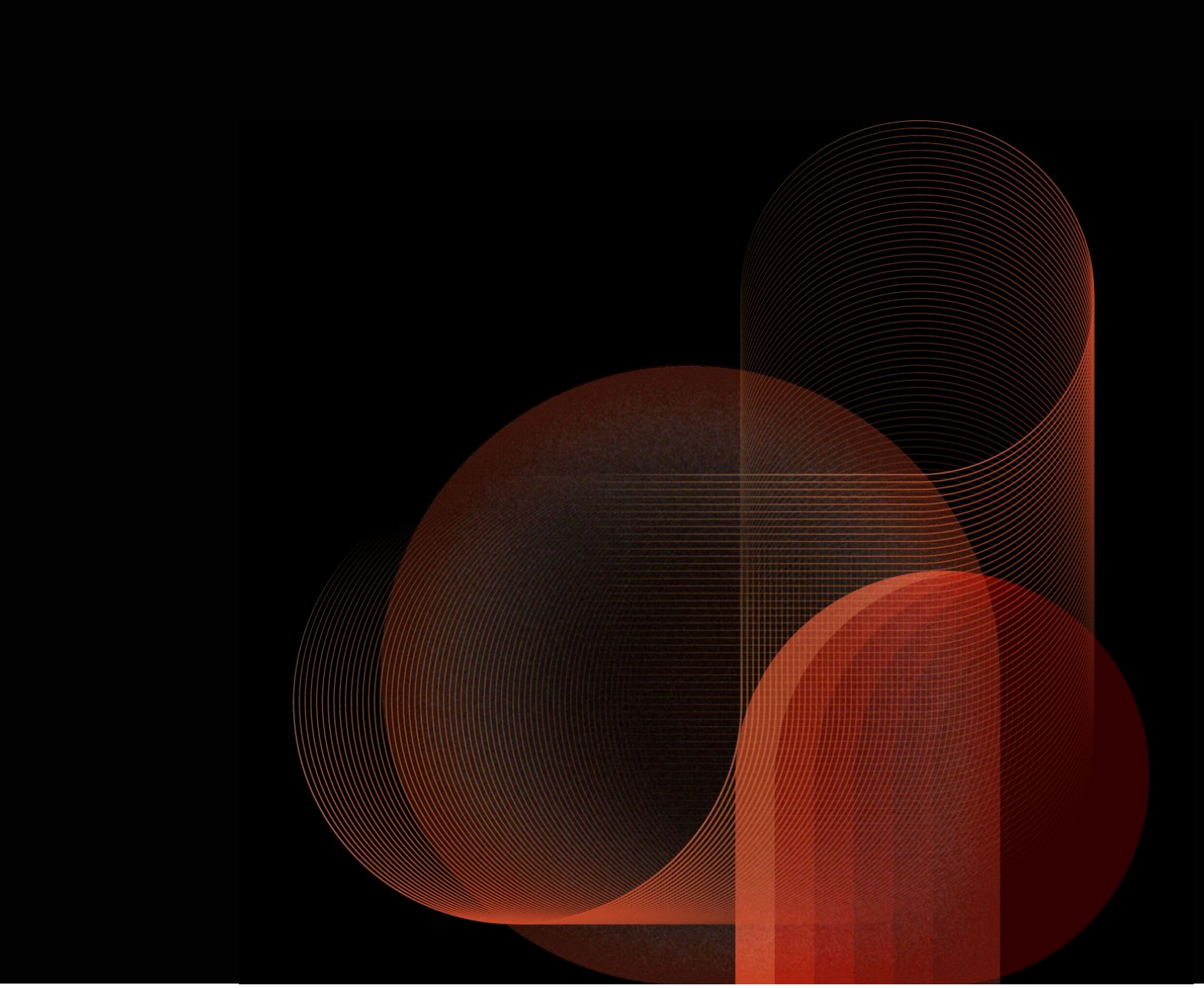
XSOAR Ransomware Playbooks

XSOAR Marketplace contains many other playbooks related to incident types discussed in this report.

Reduce Response Time with Retainers

When an attack occurs, there is a material threat to your business. It is critical to take swift action before the incident escalates. With a Unit 42 retainer in place, you can make our incident response experts extensions of your team on speed dial.

You won't engage in a frantic search for resources either because you will have an assigned point of contact with knowledge of your environment and dedicated communication channels for engaging the team. As a result, you can respond faster and more accurately should an incident occur to minimize the impact and get you back to business sooner.



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