ARCTIC WOLF LABS

ARCTIC WOLF LABS

THREAT REPORT 2023

TABLE OF CONTENTS

01

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

/// This edition of the Arctic Wolf® Labs Threat Report comes just as IT decision makers and security professionals worldwide prepare for this year's infosec conference season.

Whether it's RSAC in San Francisco, InfoSec Europe in London, Black Hat Asia, or Security & Risk conferences in Sydney, the subsequent bombardment of vendor claims, new acronyms, and misused statistics and phrases distract security professionals from their tactical goals in 2023 and risks the delay or shift of strategic projects planned for next year and beyond.

As one of the largest security operations centers in the world, our insights into recent trends will help you cut through the noise, understand the current and potential threats to your organization, and keep your focus on delivering the critical tasks that protect your organization 24x7.

2022 was overshadowed by Russia's brutal invasion of Ukraine, with many predicting a huge blowback in cyber attacks and cybercrime. Instead, we saw signs of significantly disrupted activity across threat actor groups in those two countries — the 26% year-over-year decline in observed ransomware cases may point to the repurposing of state actors or recruitment of threat groups as state actors-for-hire. This decline does not, however, mean that the risk of ransomware should fall from your defender's line of sight. Ransomware continues to be the number one risk for organizations of all sizes and all nations.

But for all that, the reduction in known ransomware events corresponds with a rise in attacks where the barrier to entry is lower but detection is harder. For example, we saw business email compromise (BEC) attacks account for over a quarter (29%) of Arctic Wolf® Incident Response cases. Despite what feels like decades of trying to communicate the importance of strong credential hygiene and account security best practices, there is still much work for the cybersecurity industry to do — the majority (58%) of BEC victim organizations did not have multi-factor authentication (MFA) enabled on the compromised accounts.

The economics of cybercrime took a real hit, too, as the average loss from a successfully executed BEC attack was 'only' $79,000 USD, significantly less than the typical demands for ransomware.

As crucial as these insights are, applying them is often left for the practitioner to figure out on their own. This report aims to help you plan for:

- The major threat landscape shifts powered by AI and economic instability
- The long, long tail of the vulnerability lifecycle, starring the seemingly immortal Log4Shell and ProxyShell from 2021
- The growth of as-a-service-driven ransomware
- The five most successful tactics, techniques, and procedures (TTPs) in 2022 and what that means for you in 2023

Cybersecurity is a team game that aims to reduce risk and increase resilience. Protecting yourself in isolation, without sharing, learning, and helping others will prove hard, if not impossible. This is why we are proud to demonstrate the wolf pack mentality, working with our customers and friends in the cybersecurity community, doing what it takes to secure organizations and ensure they survive the ever-increasing incident count.

Ian McShane
VP, Strategy

Daniel Thanos
VP, Arctic Wolf Labs

02 INTRODUCTION

INTRODUCTION

/// The 2023 Arctic Wolf Labs Threat Report aims to combine our security researchers', data scientists', and security developers' most forward-thinking ideas with practical guidance you can apply to protect your organization.

The Arctic Wolf Security Operations Cloud, with its open XDR architecture fuels this report, processing 3+ trillion security events weekly and generating 4.8+ petabytes of data from endpoints, networks, cloud, identity, human sources, and more. We aim to provide insights that transcend any technology or attack surface by combining this vast dataset with Arctic Wolf's threat and malware intelligence data and findings from our digital forensics and incident response work.

Our predictions and insights on the year ahead focus on the macro and micro changes to the threat landscape, including incident response, investigations, insights, and trends. Though the threat landscape is constantly evolving, and the threat actors regularly change their tactics, techniques, and procedures (TTPs), the unfortunate victims of cybercrime give everyone in the security community the opportunity to learn from and react to the shifting waves of threat types and attacks.

We believe sharing intelligence and insights like those in this report is a critical responsibility for those of us in the cybersecurity industry and is vital in helping organizations of all types end cyber risk.

ARCTIC WOLF LABS

Arctic Wolf Labs is a group of elite security researchers, data scientists, and security development engineers who explore security topics to deliver cutting-edge threat research on new and emerging adversaries, develop advanced threat detection models with machine learning and artificial intelligence, and drive continuous improvement in the speed, scale, and detection efficacy of Arctic Wolf's solution offerings.

With their deep domain knowledge, Arctic Wolf Labs brings world-class security innovations to not only Arctic Wolf's customer base, but the security community-at-large.

INCIDENT RESPONSE

Arctic Wolf Incident Response is a trusted leader in incident response (IR), leveraging an elastic framework that enables rapid remediation to any cyber emergency at scale.

A dedicated Incident Director orchestrates every response effort and coordinates team members based on the attack type, scope of the incident, and phase of response.

Team members work in parallel through the response to minimize downtime and costs while the Incident Director ensures clear communication with the organization to ensure everyone remains informed on forward progress.

03

CYBERSECURITY PREDICTIONS

CYBERSECURITY PREDICTIONS

After thorough observation and analysis of the cybercrime landscape of 2022, it's safe to say that cybercrime is only increasing — a trend that is likely to continue through 2023.

Ransomware-as-a-service (RaaS) has opened new attack avenues to cybercriminals who lack the technical expertise of seasoned professionals. Organizations are turning more and more to digital services and the cloud, exposing themselves to new risks. And external factors, such as ongoing geopolitical conflict and the adoption of new technologies, are changing the threat landscape in startling ways.

We predict an increase in the volume and complexity of cybercrime over 2023, meaning organizations need to stay informed and create incident response action plans now to ensure that they are prepared to defend against these looming threats.

01 Geopolitical Instability and Economic Stress Will Drive Cybercrime Increases

During times of economic strife and political instability, new opportunities and incentives are created for cybercriminals.

With the long tail of the COVID-19 pandemic, high rates of inflation, and major conflicts such as the ongoing war between Russia and Ukraine, we predict that more individuals with technical skills will be incentivized to resort to cybercrime. These individuals will seek to reap the profits of illicit activity such as BEC, phishing, ransomware, extortionware, and other tactics.

Research for the Arctic Wolf State of Cybersecurity: 2023 Trends Report showed that small and midsize businesses (SMBs) are more severely impacted by cybercrime in the current economic climate because their budgets tend to either stay the same or decrease, making the payment of ransom demands more costly. On the other hand, enterprise scale organizations tend to increase spending on their cybersecurity efforts.

What it looks like in the real world

In addition to these external threats, we expect to see a rise in insider threats as economic uncertainty continues in the U.S. and abroad.

While individual employees are struggling to make ends meet, threat actors may take advantage of their financial desperation with phishing and social engineering campaigns. Ponemon Institute's 2022 Cost of Insider Threats: Global Report[1] reveals insider threat incidents have increased 44% over the last two years, with costs per incident up more than a third at $15.38 million USD.

02 AI-Driven Information Warfare and Cybercrime Will Increase

The release and rise of ChatGPT, and now GPT-4, by OpenAI has been greeted with much fanfare and mainstream press, but the real implications of its potential are not yet fully known.

ChatGPT and GPT-4 are OpenAI's fourth-generation Generative Pre-Trained Transformers, which are based on natural language techniques that provide answers in a conversational way and have been noted for its extensive capabilities.

With the broader public awareness of, and access to, AI of this nature, we expect to see more bots and automation spread disinformation across the web. We expect to see AI-generated imagery and videos used by threat actors to spread propaganda, influence public opinion, and launch advanced social engineering campaigns.

We predict that threat actors will harness AI technologies, such as ChatGPT and other AI tools to create malware. Early reports on OpenAI's generative AI applications have supported this prediction, demonstrating that the barrier to entry in programming has been lowered for threat actors.

This trend will only increase as the technology becomes further integrated into typical software development workflows.

What it looks like in the real world

As a result of AI-driven enhancements in software development, the sheer number of threat actors is expected to increase. More entry-level developers (also referred to as "script kiddies") under financial pressure will be motivated to pursue cybercrime, and advanced threat actors will become more specialized and sophisticated.

ChatGPT and other generative AI tools can be utilized for social engineering attacks where threat actors create convincing phishing emails or text messages to trick people into disclosing sensitive information or downloading malware.

03 Disruptive Technologies Will Create New Opportunities and Threats

AI is not the only disruptive technology that will change the cybercrime landscape.

Decentralized finance (DeFi), which leverages public blockchain ledgers to process financial transactions via smart contracts, offers an alternative to centralized financial (CeFi) systems.

While DeFi isn't inherently a new technology, 2022 has been the year that's brought DeFi to the mainstream — and there's a lot more to DeFi than just cryptocurrency. This includes non-fungible tokens (NFTs), smart contracts, tokenization, and potential token-based peer-to-peer exchanges that allow individuals to bypass centralized institutions to swap collateralized tokens.

DeFi offers threat actors a means by which they can exchange illicitly obtained crypto funds (either washed or mixed funds, or services to be rendered later via smart contracts). Beyond the exploitation of this technology also lies the potential compromise of it.

Smart contracts, for example, are just programs stored on a blockchain that run when predetermined conditions are met, and like any program, they are susceptible to vulnerabilities. New types of vulnerabilities found in smart contracts or DeFi platforms could cause users to lose their money or could contain embedded strings of code that obfuscate the full scope of a contract's terms and conditions.

A smart contract is a function of Web3, and Web3 offers users even more control over their digital assets.

What it looks like in the real world

DeFi effectively creates the conditions incentivizing new social engineering strategies and advanced techniques to effectively perpetrate crypto-heists and token-heists.

As the adoption of DeFi increases, we will see DeFi platforms pitched to investors as the safer alternative to CeFi. Threat actors, however, could take advantage of the departure to build malicious smart contracts for unwitting investors to connect their wallets to, in turn causing their wallets to be drained under the guise of Web3 DeFi trading platforms and minting new non-fungible tokens (NFTs).

03 Disruptive Technologies Will Create New Opportunities and Threats (cont.)

Web3 allows for new social engineering tactics.

Other emerging cyber environments that have increased potential for exploitation are organizations hosting virtual reality (VR) and augmented reality (AR) data.

As more data is collected through VR/AR devices, sensors, cameras, etc., and stored on servers and databases connected to the internet, these become rich targets of potentially large amounts of personal data on the user such as eye tracking data for ads and many other examples.

There is an emerging opportunity for new social engineering attacks in VR applications in Web3 applications, providing even more incentive to support DeFi services.

What it looks like in the real world

Web3 technology develops, and threat actors leverage emerging AI technologies to enhance their attack capabilities, we anticipate that demand for DeFi to continue to gain traction, so long as the economic incentives continue to grow while the barrier to entry continues to drop. These overall trends could also push the broader crypto community towards DeFi trading platforms at the expense of CeFi.

04 Ransomware- and Extortionware-as-a-Service will Advance

With the cybercrime industry raking in $1.5 trillion USD in revenue annually, criminal groups and organizations are only gaining strength and growing in sophistication.

We expect RaaS to continue to prove to be an attractive business model through 2023, as it isolates the ransomware infrastructure and tooling from the threat actors performing the breach and demanding payment.

Threat actors now commonly build, market, and lease ransomware infrastructure to other entities skilled in penetration testing, allowing the infrastructure operators to take a 20-30% cut of the proceeds from the ransom and extortion while reducing risk on their part.

Many modern ransomware organizations operate like legitimate businesses, with their own organizational structure and departments. Some even offer their victims robust customer service and vacation days for their 'employees,' and invest in their talent through skills development opportunities.

In addition to structural changes, we expect ransomware groups to increasingly rely on double-extortion or triple-extortion without encryption to simplify future ransomware attacks. Traditionally, a ransomware attack meant that a threat actor that infiltrated a network would encrypt a company's data, making it inaccessible. Only after paying a ransom would the victim receive the decryption key.

What it looks like in the real world

In 2019, ransomware groups found another way to put pressure on victims — a double-extortion ransomware attack.

This style of attack is where the threat actor makes a copy of some or all the data before encrypting it. If the victim refuses to pay a ransom, the sensitive data stolen from the network will be made public or sold on the black market.

Since this discovery, ransomware groups have become even more creative, adding one more layer to their attacks — a triple-extortion ransomware attack —where a victim's associates (such as partners, customers, or patients) are threatened with data leaks if the original victim refuses to pay a ransom.

These kinds of attacks increase the likelihood that an organization will pay and offer cybercriminals another route if the business doesn't play along.

05 Initial Access Techniques Will Evolve, Allowing for More Exploitation

Threat actors will continue to identify new ways of gaining initial access to vulnerable organizations.

Here we review several relevant techniques that we expect to see more of in 2023:

IoT/ICS being used for initial access

Threat actors may try to take advantage of appliances not supported by endpoint detection response (EDR) products, such as VoIP gateways, firewalls, or Internet of Things (IoT) devices.

In 2022, Cybersecurity and Infrastructure Security Agency (CISA) saw advanced persistent threat (APT) actors developing custom-made tools for the targeting of ICS/SCADA (supervisory control and data acquisition) devices.

We expect this type of threat actor activity to continue and increase as nation-states look to target critical infrastructure.

> **What it looks like in the real world**
>
> Attacks targeting ICS/SCADA devices have recently been observed in Russia, Ukraine, and the US, for example. IoT devices are often left unsecure on the network, as digitization outpaces security implementations, and are therefore targeted to gain initial footholds. We expect this type of behavior to increase with the increased adoption of IoT in network environments across manufacturing, healthcare, and other industries.

SEO poisoning

SEO poisoning, a tactic in which threat actors create malicious websites and use keywords to increase their rankings and display as a top search result, will increase.

> **What it looks like in the real world**
>
> Malicious websites use various tactics to manipulate their search engine rankings and get shown as a top search result. By posing as websites hosting legitimate software and increasing their search engine rankings, threat actors can trick unsuspecting users into downloading malware. In some instances, Google Ads are purchased by threat actors to elevate their appearance of legitimacy. We predict that ransomware groups and other threat actors will continue to exploit this technique as an initial access vector.

05 Initial Access Techniques Will Evolve, Allowing for More Exploitation (cont.)

Remote monitoring and management tool abuse will continue.

Remote monitoring and management (RMM) tools such as Microsoft Remote Desktop Protocol, ConnectWise Automate, and others have been a mainstay for threat actors, and we don't expect that to change any time soon.

We've also observed incidents where threat actors abused native ConnectWise functionality in social engineering campaigns against unsuspecting victims.

These types of attacks are particularly effective in environments where users expect to see ConnectWise Automate activity from their network administrators, leaving them less suspicious when confronted with an illegitimate activity that looks similar.

We expect threat actors to get more creative in the abuse of RMM solutions.

What it looks like in the real world

RMM solutions allow threat actors to easily blend into normal enterprise network traffic. It can be challenging for organizations to restrict RMM tool traffic unless they are very well tuned into what RMM tool uses are expected in their networks, furthering threat actors' success.

06 Increased Business Email Compromise Activity

Sophisticated attacks may garner most of the attention, but more familiar email-based attacks will also continue to evolve.

BEC, already a go-to attack method for cybercriminals, will increase in frequency and cumulative financial costs, as it continues to deliver lucrative payouts for threat actors.

In fact, the FBI Internet Crime Complaint Center (IC3) [2] lists BEC as one of the most financially damaging forms of cybercrime. In 2021, reported BEC and EAC (email account compromise) attacks increased by 30% from the year prior, resulting in roughly $2.4 billion USD in global cyber losses.

For perspective, compare this to the $49.2 million USD in losses caused by ransomware attacks for the same period, as reported by the FBI.

Even as financial damages mount, organizations struggle to eliminate the threat posed by BEC, as the text-based attacks prove difficult to detect. Lacking links and attachments, these messages often bypass existing email security filters on the way to users' inboxes.

The arrival of new AI-based tools and the evolution of deepfake video and audio will only further aid social engineers, who are already adept at updating their tactics to circumvent existing security controls.

What it looks like in the real world

Organizations in industries such as finance, insurance, and business services regularly rely on email correspondence for invoicing and payment. These industries will continue to be a prime target for BEC attacks, as the volume of payments and wire transfers commonly conducted via email in these sectors occurs at a higher rate, presenting more opportunities for bad actors to insert themselves in these transactions.

07 High Impact Software Vulnerabilities Will Continue to be Exploited

In 2022, only a handful of vulnerabilities were harnessed by ransomware threat actors for initial access, but the sheer volume of vulnerabilities has grown significantly year over year.

While this trend will continue in 2023, even several years old vulnerabilities have been, and will continue to be exploited by threat actors if there's a large enough unpatched installation base. Software hosted on-premises will continue to present challenges for organizations as they struggle to stay on top of patching the most impactful vulnerabilities. It's important to note that a CVSS score alone does not serve as a definitive measure of how attractive an exploit is to threat actors; a large unpatched base may be more lucrative than a singular critical vulnerability.

Supply chain exploits are expected to grow in volume as new vulnerabilities continue to be found by security researchers and threat actors. These kinds of attacks are attractive due to their centralization and large blast radius. A single vulnerable entry point in the supply chain can expose hundreds or thousands of customers and subsequent organizations to an attack.

What it looks like in the real world

High-impact vulnerabilities such as Log4Shell (CVE-2021-44228), the on-premises Exchange vulnerability ProxyLogon (CVE-2021-26855), ProxyShell (CVE-2021-34473), and others will continue to be widely exploited.

08 Living Off the Land Techniques Will Continue to Increase

We expect to see threat actors continue to use built-in tools in the operating system (especially for Windows).

This approach is known as “living off the land” (LOTL), which is a deliberate effort to evade detections by legacy products by finding creative ways to weaponize them to establish persistence or perform other malicious actions. With hundreds of binaries built into Windows, numerous opportunities exist for abuse and evasion of EDR defenses. Additionally, native scripting languages in Windows, such as PowerShell, VBScript, and JScript will offer many opportunities for obfuscation and tricking users into running these specially crafted malicious commands.

What it looks like in the real world

Attacks involving these tools will continue to be difficult to detect because the binaries are legitimate and integrated into the operating system. This makes it impossible to block the use of these tools outright, shifting the focus to group policy and overall security configuration.

09 Organizations Will Migrate More On-premise Applications into the Cloud

It’s no secret that organizations are migrating to the cloud.

It’s cost-effective and reduces on-premises risks. However, the same enthusiasm hasn’t manifested when it comes to cloud security. According to our annual The State of Cybersecurity: 2023 Trends report, only 38% of respondents believe they are effectively securing their cloud resources. In addition, 42% of respondents stated that cloud security gaps were their primary area of worry, and in a positive trend, 46% of respondents would like to learn more about cloud security and evolving infrastructures.

What it looks like in the real world

Steps are being taken in the right direction, but that doesn’t mean organizations should let down their guard when it comes to cloud security. Between misconfigurations and the rise of cybercriminals targeting the cloud specifically, we expect this gap to lead to breaches in the future.

10 Cloud-Based Security Controls and Supply Chain Risk

As organizations continue to express significant interest in migration to the cloud, they will need to consider cloud-native approaches to security controls.

Cloud-based Identity and Access Management (IAM) solutions offer a replacement for on-premises IAM for organizations, but every cloud deployment potentially contains hundreds to thousands of human and machine identities, making up a very large attack surface.

We continue to see cross-tenant vulnerabilities—sometimes referred to as side-channel attacks—where other tenants on the same public cloud gain access to the data. We predict that, as more organizations continue to move from on-prem to the cloud in 2023, opportunistic threat actors will continue to hunt for these kinds of vulnerabilities and gain unauthorized access to resources. We also expect to see an increase in cloud-related software supply chain attacks, affecting repositories at GitHub, Docker, NPM, Azure artifacts, and AWS artifacts.

What it looks like in the real world

Cloud misconfigurations by administrators will continue, and the resulting breaches will expose more customer and employee information, causing further disruption.

04 KEY THEMES

KEY THEMES

The predictions and real-world scenarios shared above aim to forecast what is coming next for security teams, while in this section we will look back at the past year to see what can be learned from the thousands of incidents we have responded to. Learning from the experiences of other teams and organizations is where you build resilience, focus tactics, and short-term priorities that can help you avoid becoming a victim of similar incidents.

Leveraging data from the Arctic Wolf Security Operations Cloud, and working in close collaboration with Arctic Wolf's Incident Response and Security Services Teams, Arctic Wolf Labs have compiled these key themes based on threat intelligence gathered from our data set.

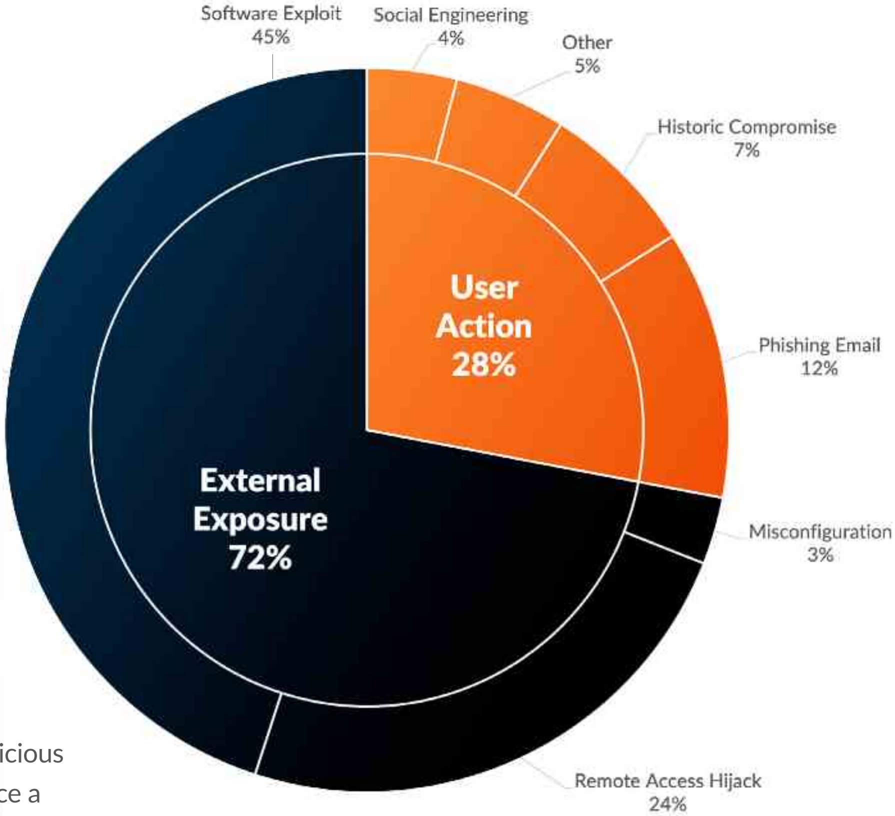
These key themes tell a clear story of a shifting threat landscape. The headline-grabbing dangers of ransomware and BEC attacks remain a top concern, but just as important are how threat actors get their initial foothold in the environment with a simple user action or by leveraging a handful of critical vulnerabilities. While others may have a more device-centric approach to these insights, the open XDR architecture of our platform allows us to span across attack surfaces and focus on a broader set of risks.

Root Point of Compromise (RPOC)

Because our visibility reaches beyond devices alone, we believe it is important to focus on root point of compromise ("RPOC"), the initial entry point method leveraged by a threat actor. Whereas the initial access point describes the device that is first compromised, RPOC focuses on the **methods** used by threat actors to obtain initial access to the victim's systems. RPOC is defined by two main categories:

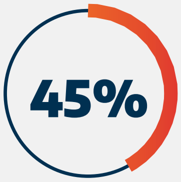
External Exposure: A threat actor targeted a system exposed to the public Internet and gained access to the victim's network or data. This is the easiest method for threat actors to deploy, therefore it is widely used.

User Action: A threat actor gained access due to a user's action, such as opening a malicious website or file. Threat actors need to convince a user to perform an action for the attack to work.



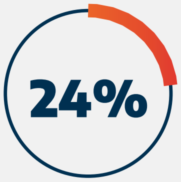
External Exposure

The external exposure RPOC for non-BEC cases is divided into three categories based on an organization's IT environment.



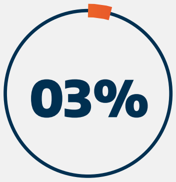
Software Exploit:

45% of incidents this year were caused by vulnerabilities that could have been mitigated through security patches and updates available prior to the incident. In these incidents, a threat actor utilized a known vulnerability (e.g., ProxyShell, Log4Shell) to gain access to the network.



Remote Access Hijack:

24% of incidents were caused by IT practices that allowed remote access from outside of their network (e.g., leaving Remote Desktop Protocol open to the public internet), which we consistently find to be a high-risk practice.



Misconfiguration:

3% of incidents were caused by misconfigurations of IT systems.

Root Point of Compromise – External Exposure Deep Dive

Arctic Wolf Labs has determined that a handful of solutions and vulnerabilities are responsible for a significant portion of incidents responded to by the Arctic Wolf Incident Response. Of the top five vulnerabilities leveraged by threat actors in 2022, four of them were published in 2021:

01 VMWare Horizon (Log4Shell – CVE-2021-44228)

02 Microsoft Exchange (ProxyShell – CVE-2021-34473)

03 WSO2 Multiple (CVE-2022-29464)

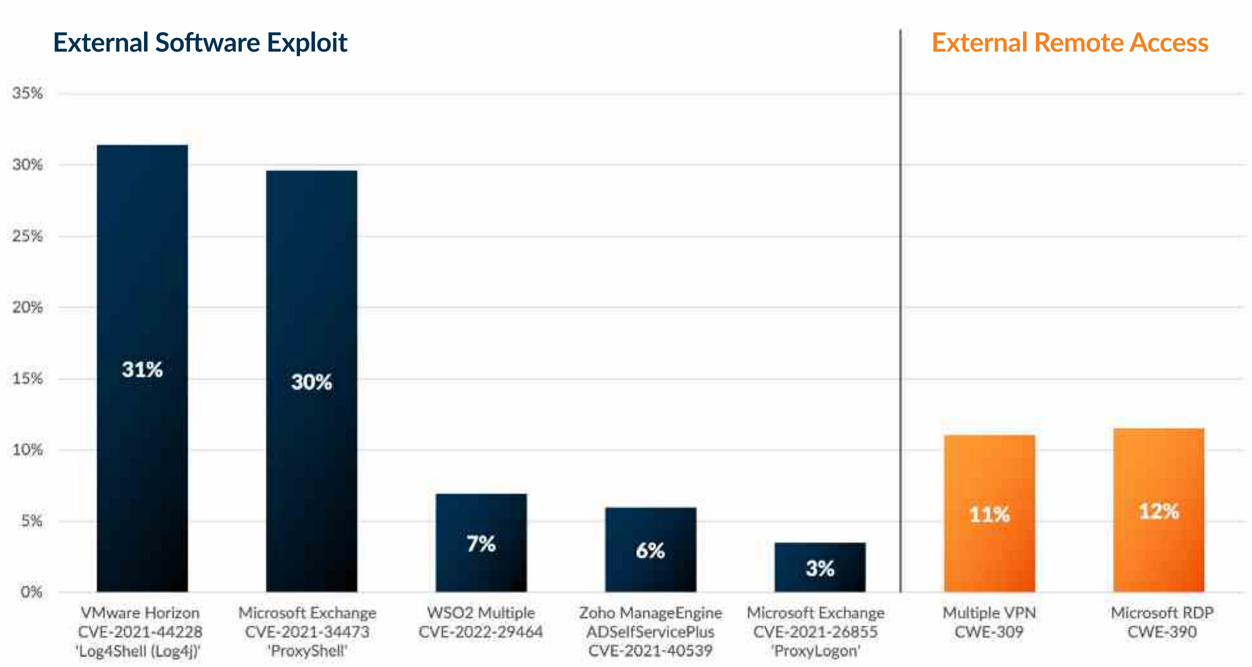
04 Zoho Managed Engine AD Self Service Plus (CVE-2021-40539) and

05 Microsoft Exchange (ProxyLogon – CVE-2021-26855)

Older vulnerabilities can be enticing for threat actors because the vulnerabilities are well researched and public exploits are validated, taking the guess work out of exploitation. Furthermore, exploit modules are developed for penetration software, such as Metasploit, making exploitation easier.

With respect to external remote access tools, Microsoft RDP (CWE-390) and Multiple VPN (CWE-309) continued to be the root point of compromise for a significant number of incidents (23%) in 2022.

Most external exposure RPOCs can be prevented by having a strong security posture, which includes defense in depth, policies and procedures, robust vulnerability management, and regular penetration testing.



User Action

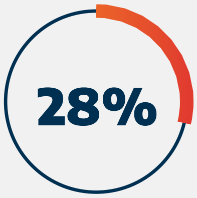
The user action RPOC for non-BEC cases is divided into four categories:

Phishing Email: 12% of incidents were caused by users clicking on malicious links or downloading malicious attachments in an email.

Historic Compromise: 7% of incidents were due to bad password hygiene. These incidents began with threat actors using previously leaked credentials from a data breach.

Social Engineering: 4% of incidents were caused by a threat actor tricking a user into completing a specific action via scam phone calls, text messages, and other deceptive means.

Others: Catch all for infrequent RPOCs, such as drive by attack and malicious software download. 5% of incidents fell into this category.



A TOTAL OF 28% OF NON-BEC CASES INVESTIGATED BY ARCTIC WOLF INCIDENT RESPONSE WERE DUE TO USER ERROR.

Each of these cases could have been prevented by victim organizations hardening their security postures with security awareness training, which prepares employees to recognize and neutralize social engineering attacks and human error.

05 RANSOMWARE

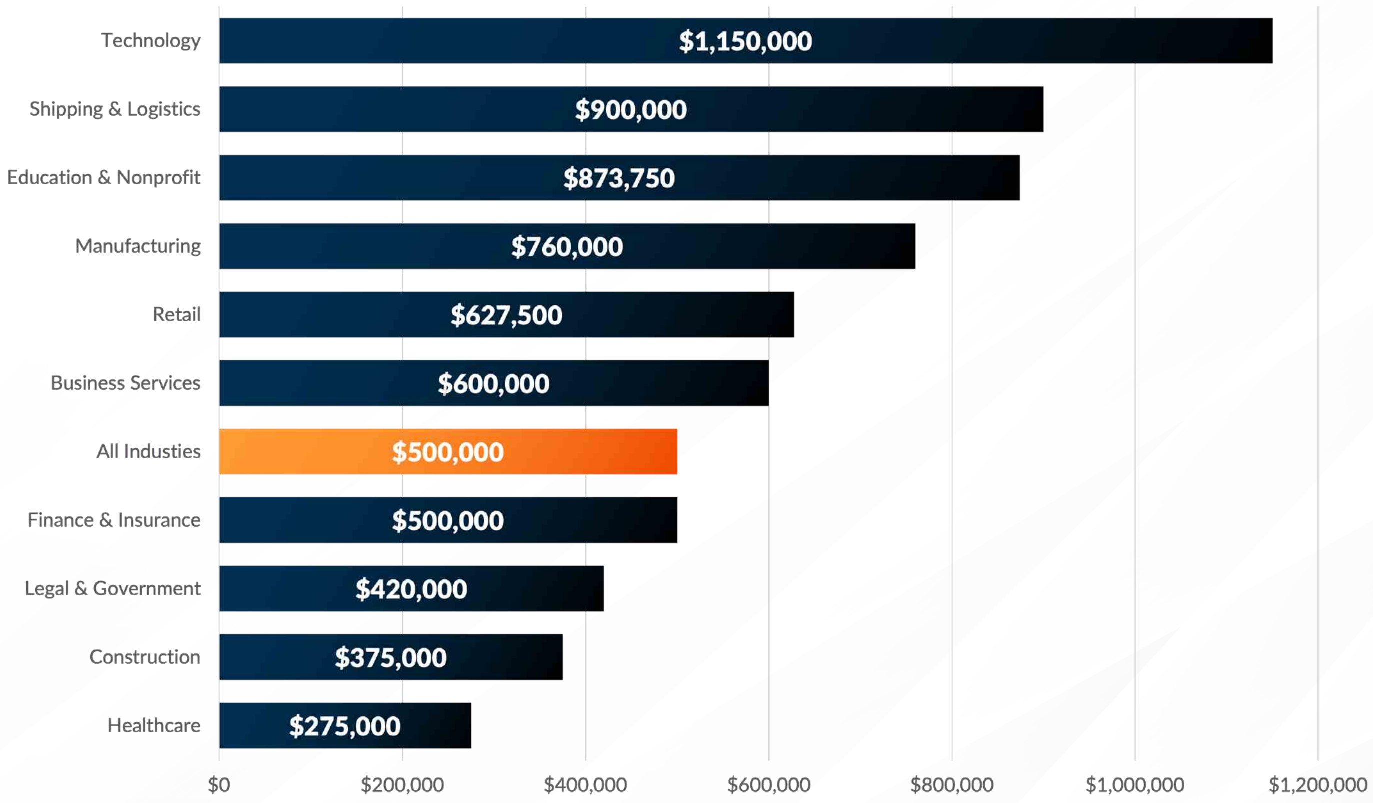
RANSOM DEMANDS BY INDUSTRY

Based on ransomware incidents investigated by the Arctic Wolf Incident Response the median initial ransom demand across all industries was $500,000 USD.

Ransom demands vary across industries due to many factors, including the victim organization's size, revenue, data, and, in some cases, their insurance policy maximums. Some ransomware groups actively seek out cyber insurance policies in a victim's environment to better inform their ransom demands, typically asking up to the maximum the insurance policy will cover.

The industries with the highest median initial ransom demands for 2022 were technology (**$1.2 million USD**), shipping and logistics (**$900,000 USD**), and education and nonprofit (**$874,000 USD**).

Median Initial Ransom Demand



**Note: Median figures are used for comparison purposes because the cost of a ransom demand or incident response activities can vary wildly based on the size of the organizations and the scope of the incident. Median figures provide the best approximation of what a "typical" event looks like because very large and very small outlier incidents can have a significant impact when reporting averages.*

Ransomware-as-a-Service Dominates with LockBit Ahead of Other Variants

In 2022, ransomware threat actors demonstrated an increased adoption of the RaaS model.

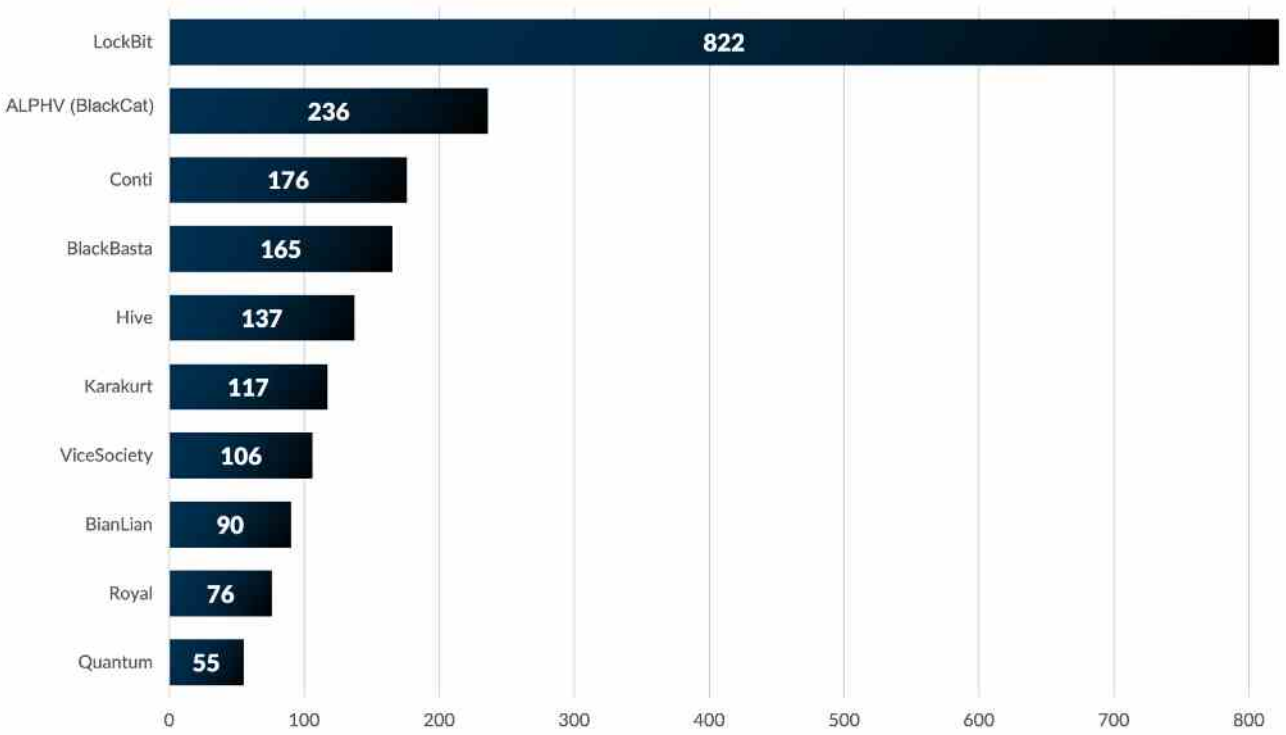
In this model, RaaS operators offer technical resources (e.g., encryption software, leak site) and branding to independent affiliates who perform the work of comprising and extorting victims. The proceeds of these attacks are commonly split between affiliates and the operators.

While RaaS was previously limited to highly skilled actors, the model has proven attractive as a way for less technically proficient cybercriminals to execute ransomware attacks, while shielding the identities of the threat actors.

Based on known victimology from monitoring dark web ransomware leak sites, five ransomware variants, all falling under the RaaS paradigm, have dominated with the highest number of known victims in 2022. Complicating matters further, independent affiliates have been shown to utilize multiple ransomware variants at once, sometimes jumping between them as they test the waters and look for more attractive packages.

OF ALL TRACKED RANSOMWARE VARIANTS IN 2022, LOCKBIT SHOWED THE MOST ACTIVITY, WITH 822 VICTIM ORGANIZATIONS DISCLOSED.

Number of Organizations Listed on the Ransomware Leak Sites



LockBit

LockBit ransomware was first observed in mid-2019 as ABCD ransomware, due to the encrypted ".abcd" file extension the threat actors used before changing to ".lockbit."

The group is known for its self-propagating ransomware and short dwell times. While other ransomware groups may spend days or weeks manually conducting reconnaissance after gaining initial access to a network, LockBit has automated these tasks and has been observed dwelling in the network for as little as a matter of hours. This helps explain why they have 3.5 times more activity than the second-most-prevalent ransomware variant on our list — ALPHV (BlackCat).

ALPHV (BlackCat)

The ALPHV (BlackCat) ransomware variant was first identified in November 2021.

The name and imagery used in the ransomware variant's branding stem from Russian folklore around a similarly named street gang[3] dating back to the Soviet era. Attacks observed thus far have employed the "double extortion" method to both encrypt victims' systems and exfiltrate their data, as well as reports of DDoS threats in some cases — a tactic known as "triple extortion."

Conti

Conti was first observed in mid-2020.

While Conti was a dominant ransomware variant in 2021, the associated group disbanded in 2022, with some involved members splintering off into other ransomware groups. The group was first observed using double extortion by encrypting files and threatening to leak them publicly if ransom demands aren't met.

BlackBasta

BlackBasta is a relatively new ransomware variant, emerging in April 2022.

Files are encrypted with the ".basta" extension. They primarily rely on phishing emails and social engineering as a root point of compromise and then move laterally within victim networks. One noteworthy aspect of their encryptor malware is that it only partially encrypts larger files to increase the speed of encryption.

Hive

Hive ransomware was first observed in June 2021, and in just two months it became one of the most active ransomware groups operating.

According to the U.S. Department of Justice [4], Hive ransomware group has targeted more than 1,500 victims in over 80 countries, including hospitals, school districts, financial firms, and critical infrastructure. The FBI has stated that Hive's total ransomware demands to date have exceeded $130 million USD.

Strategic and Technical Insights into Ransomware Groups

In 2022, Arctic Wolf Labs conducted extensive research into TTPs leveraged by ransomware and extortion threat groups.

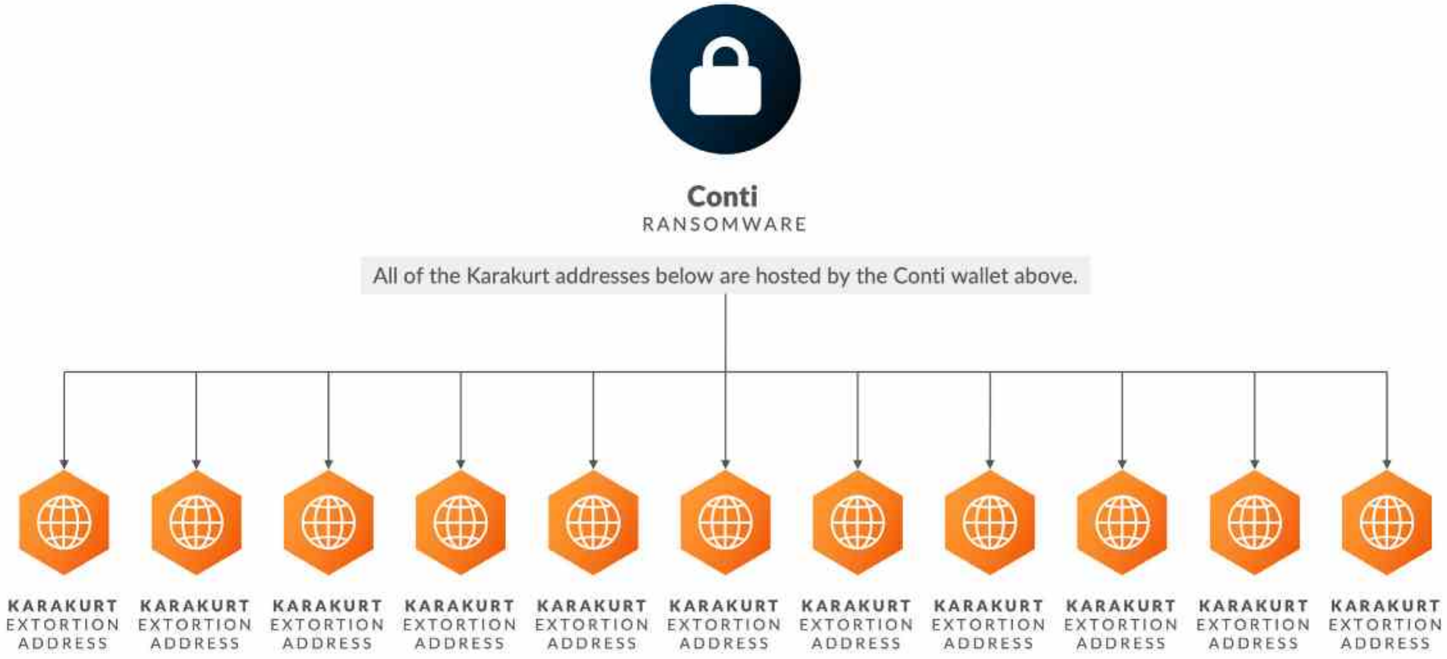
The research allowed us to provide customers and the security community with strategic and technical insights into their operations.

By applying these insights to an organization's environment, IT and security leaders could reduce risk, prevent or minimize disruption to business operations, and increase understanding of specific threats to help prevent future attacks.

In addition, these insights would help organizations prevent financial loss by making timely, informed decisions to prevent system downtime.

The Karakurt Web: Threat Intel and Blockchain Analysis Reveals Extension of Conti Business Model

In early 2022, the Arctic Wolf Incident Response partnered with Chainalysis to use digital forensics and blockchain analysis to reveal clear connections between the extortion group Karakurt and the ransomware groups Conti, Ryuk, and Diavol.


Conti
RANSOMWARE
All of the Karakurt addresses below are hosted by the Conti wallet above.
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS
KARAKURT EXTORTION ADDRESS

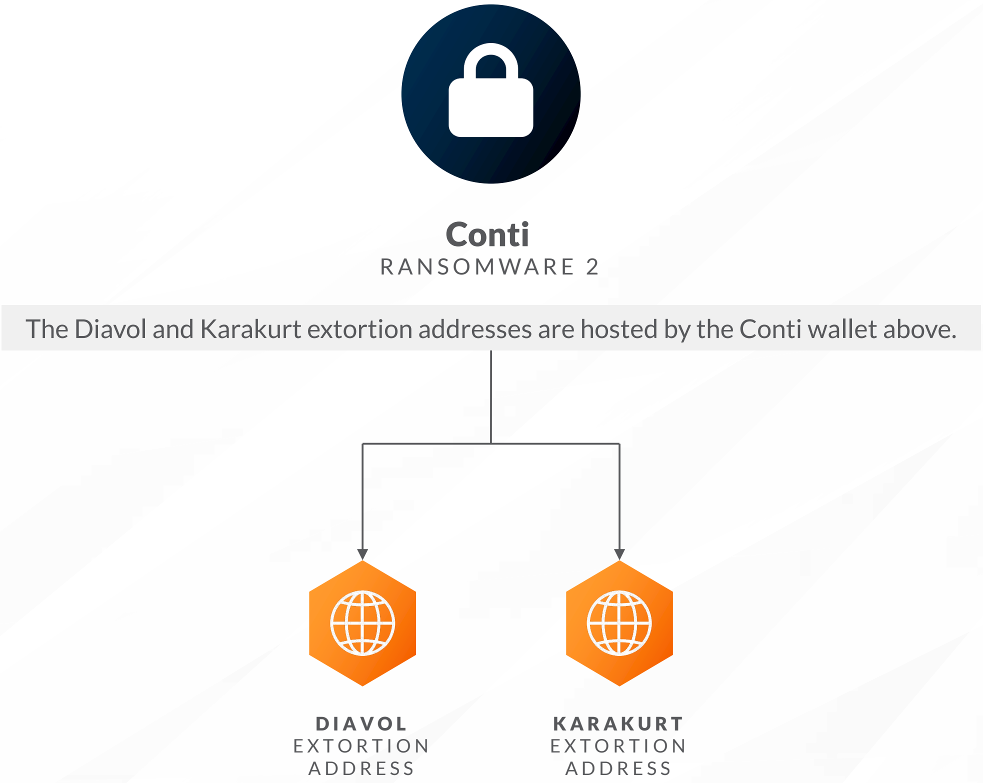
Conti Connections: Having worked on over a dozen Conti re-extortion cases, the Arctic Wolf Incident Response team recognized that Conti relied primarily on Fortinet SSL VPNs as the root point of compromise in re-extortion cases. This same technique was also found to be commonly used by Karakurt.

There are other overlaps seen between Conti-related re-extortion attacks and Karakurt intrusions, including the use of the same tools for data exfiltration, the creation of a file listing of exfiltrated data, and the use of the same hostname when remotely accessing victims' networks. Arctic Wolf Incident Response also identified connections between Karakurt attacks and the Ryuk ransomware variant.

To further support these connections, Chainalysis, in partnership with Arctic Wolf, identified evidence of Karakurt wallets sending significant sums of cryptocurrency to wallets owned by Conti, indicating a financial connection between the two groups.

Diavol Connections: The Arctic Wolf Incident Response discovered operational security errors made by Karakurt operatives which revealed a connection to Diavol ransomware, another group which emerged around the same time as Conti (July 2021) and has been associated with the use of Trickbot malware.

Our responders observed adversary actions across multiple cases which proved shared use of tools and infrastructure between Diavol, Conti, and Karakurt. Through blockchain analysis, it was also revealed that a cryptocurrency wallet used by Diavol was utilized by Karakurt and Conti in all three attacks, further linking the three groups.



Conti
RANSOMWARE 2

The Diavol and Karakurt extortion addresses are hosted by the Conti wallet above.

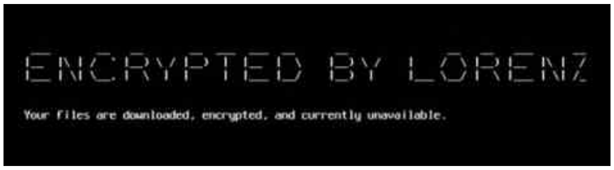
DIAVOL
EXTORTION
ADDRESS

KARAKURT
EXTORTION
ADDRESS

Chiseling In: Lorenz Ransomware Group Cracks MiVoice

In September 2022, Arctic Wolf Labs **published findings of an investigation into the Lorenz ransomware group**, who had exploited a vulnerability in Mitel MiVoice Connect to gain initial access to a victim organization as part of a ransomware attack.

This group has been active since at least 2021 and has been engaging in double extortion activities primarily in the US, with outlier attacks in China and Mexico.



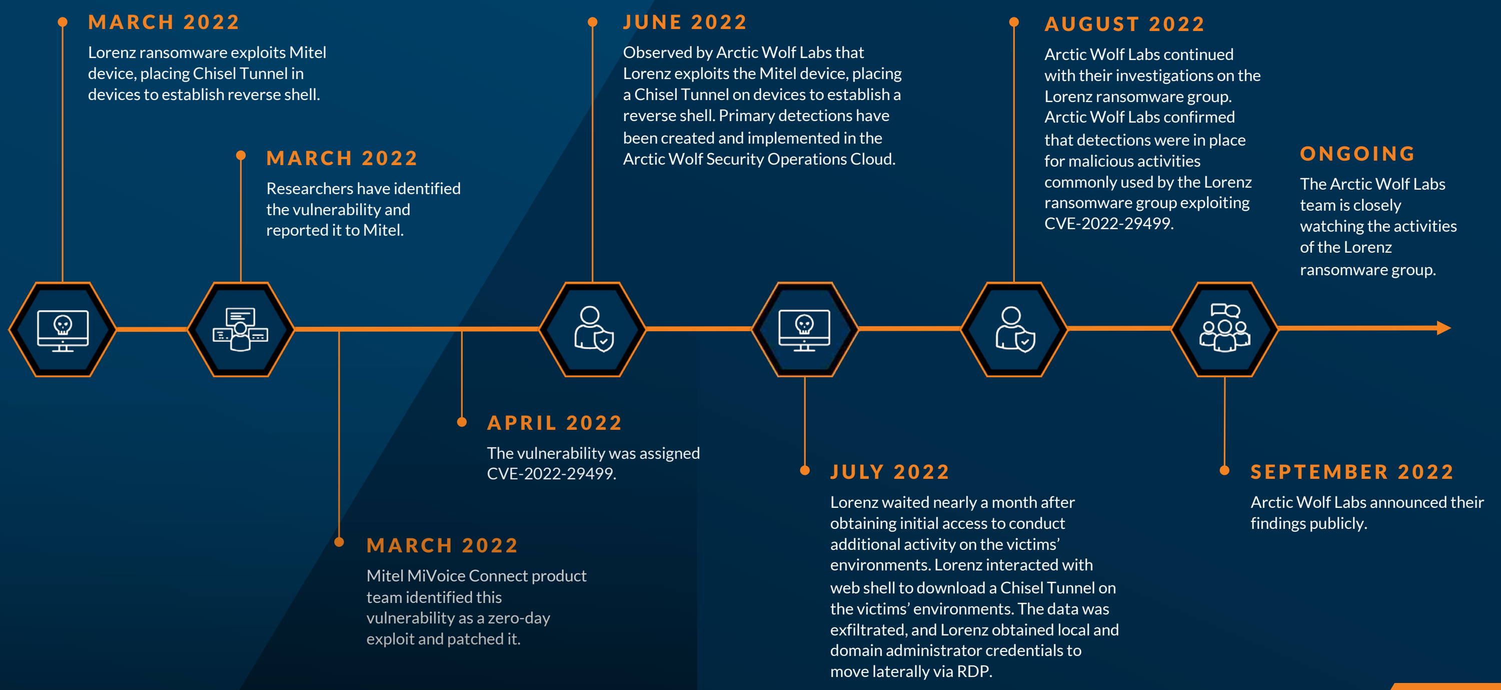
```
ENCRYPTED BY LORENZ

Your files are downloaded, encrypted, and currently unavailable.
```

In this attack, the Lorenz threat actor demonstrated good operational security awareness by changing infrastructure regularly and tunneling into compromised VoIP devices using Chisel, which acted as a SOCKS proxy.

Lorenz exfiltrated data via Filezilla and was seen using BitLocker for encryption as well as Lorenz ransomware on ESXi.

Lorenz exploited CVE-2022-29499, a remote code execution (RCE) vulnerability in the MiVoice Connect, to gain initial access to vulnerable VoIP devices in the victim's environment. To deploy a tunneling tool to those devices, Lorenz interacted with a web shell that had been deployed using the RCE vulnerability. Lorenz then obtained domain administrator credentials and used them to move laterally via Remote Desktop Protocol (RDP). Finally, data was ultimately exfiltrated, followed by BitLocker encryption via PowerShell.

One of the key insights stemming from this security research is that highly sophisticated threat actors continue to rely on "living off the land" (LOTL) techniques to evade detection, and that PowerShell logging can significantly aid in the detection of these activities.



MARCH 2022

Lorenz ransomware exploits Mitel device, placing Chisel Tunnel in devices to establish reverse shell.

MARCH 2022

Researchers have identified the vulnerability and reported it to Mitel.

MARCH 2022

Mitel MiVoice Connect product team identified this vulnerability as a zero-day exploit and patched it.

APRIL 2022

The vulnerability was assigned CVE-2022-29499.

JUNE 2022

Observed by Arctic Wolf Labs that Lorenz exploits the Mitel device, placing a Chisel Tunnel on devices to establish a reverse shell. Primary detections have been created and implemented in the Arctic Wolf Security Operations Cloud.

JULY 2022

Lorenz waited nearly a month after obtaining initial access to conduct additional activity on the victims' environments. Lorenz interacted with web shell to download a Chisel Tunnel on the victims' environments. The data was exfiltrated, and Lorenz obtained local and domain administrator credentials to move laterally via RDP.

AUGUST 2022

Arctic Wolf Labs continued with their investigations on the Lorenz ransomware group. Arctic Wolf Labs confirmed that detections were in place for malicious activities commonly used by the Lorenz ransomware group exploiting CVE-2022-29499.

SEPTEMBER 2022

Arctic Wolf Labs announced their findings publicly.

ONGOING

The Arctic Wolf Labs team is closely watching the activities of the Lorenz ransomware group.

06

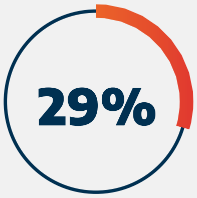
THE CONTINUED SCOURGE OF BUSINESS EMAIL COMPROMISE

THE CONTINUED SCOURGE OF BUSINESS EMAIL COMPROMISE

One of the most notable trends in the threat landscape was a significant uptick in the number of successful business email compromise (BEC) attacks observed in 2022 compared to 2021.

Business email compromise attacks continue to be endemic in the industry, and the large payouts threat actors can steal continues to motivate them to conduct this type of attack.

Business email compromise — also known as email account compromise (EAC) — is a type of email cybercrime scam in which an attacker impersonates a trusted contact then deceives victims into transferring funds or revealing confidential information.



BUSINESS EMAIL COMPROMISE ACCOUNTED FOR OVER A QUARTER (29%) OF INCIDENT RESPONSE CASES LAST YEAR.

As a prerequisite to conducting a BEC attack, threat actors gain access to a victim's inbox.

This can be done via phishing or social engineering.

If the account compromise goes undetected, the threat actor has a window of opportunity to conduct their attack using the compromised account.

Business email compromise attacks that aren't thwarted upon initial account compromise can be difficult to detect because they don't always use malware or malicious URLs that can be analyzed with standard cyber defenses. Instead, BEC attacks rely on impersonation and other social engineering techniques to trick people into interacting on the attacker's behalf.

There are several common social engineering techniques used in BEC attacks:

CEO (Executive-level) Fraud

Attackers position themselves as the CEO or another high-level executive. They typically target an individual within the finance department, requesting that funds be transferred to an account controlled by the threat actor.

Vendor Impersonation

Vendor payment is a pretense that is often used to trick victims with access to company finances.

In these BEC attacks, threat actors pose as legitimate vendors requesting fraudulent payments. Employees should be on guard to question and double-check unusual or unexpected financial requests.

Data Theft

These types of attacks often target HR departments, given their access to sensitive data.

Threat actors attempt to obtain personal or sensitive information about individuals within the company, such as CEOs and executives. Gathered data can then be leveraged for future attacks. In some instances, threat actors may attempt to extort victims into paying to keep sensitive information from being revealed publicly.

Attorney Impersonation

Lower-level employees are commonly targeted through these types of BEC attacks, where attackers impersonate a lawyer or legal representative.

The goal of these types of attacks is often to elicit the transfer of funds to a bank account controlled by a threat actor.

While threat actors often launch BEC attacks against many industries at once, industries such as finance, insurance, and business services were particularly impacted in 2022.

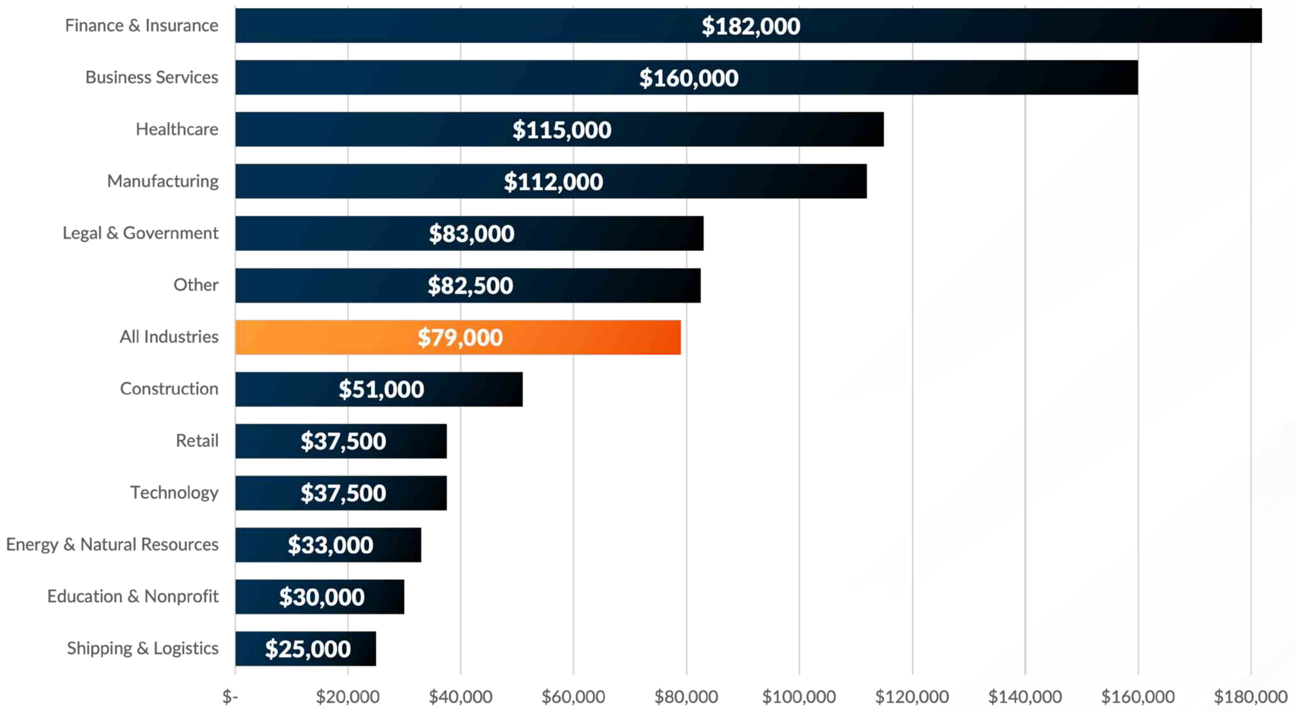
Organizations in these sectors often rely heavily on email to facilitate payments and perform wire transfers. Therefore, individuals working in these sectors tend to fall victim to BEC attacks at higher rates than those in other industries.

The healthcare industry, in particular, saw an uptick in BEC attacks.

In these industry attacks, threat actors typically target employees with transactional authority (e.g., accounts payable, check signers, authorized individuals), but they could also target accessing systems managing personal identifiable information (PII), protected health information (PHI), or other sensitive tax documents.

OF SIGNIFICANT NOTE IN THESE BEC CASES, 58% OF THE IMPACTED ORGANIZATIONS DID NOT HAVE MULTI-FACTOR AUTHENTICATION (MFA) IN PLACE.

Cost of Business Email Compromise by Industry



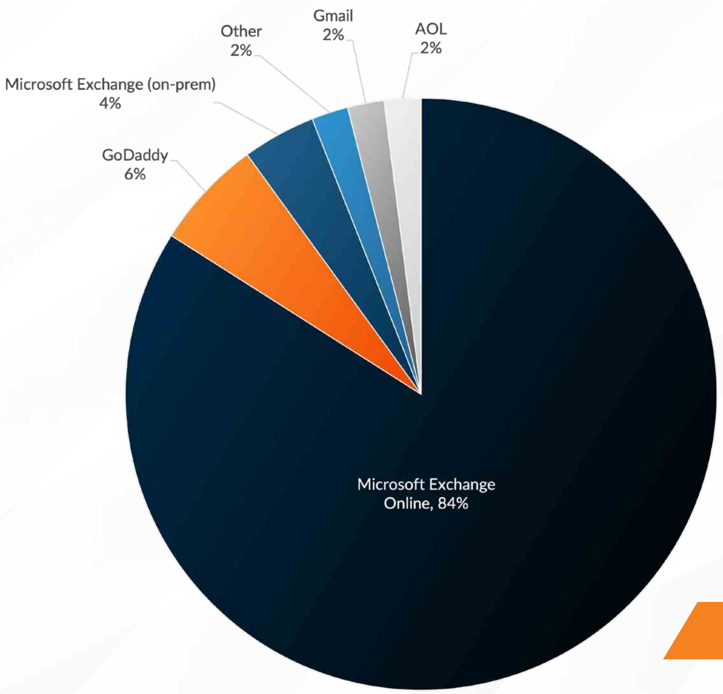
The ongoing exploitation of compromised credentials in BEC attacks highlights the importance that MFA and dark web monitoring play in securing organizations.

With MFA in place, exploitation of compromised credentials becomes more challenging.

Even if a threat actor has a known username and password pair, the account remains inaccessible without a second factor of authentication such as an app push notification, text message, or security token. As a next layer of defense, dark web monitoring can alert organizations if credentials have been exposed.

In addition to the need for MFA, the ongoing exploitation of compromised credentials in BEC attacks underscores the need for organizations to have robust security awareness training programs, focused on increasing user vigilance of fraudulent credential requests, in addition to 24x7 monitoring. This user vigilance training is critical due to the increasing number of phishing toolkits that prompt users to enter MFA tokens.

Email Providers Used by BEC Victims



Interactive Incident Timeline:

Arctic Wolf Security Operations Cloud detected a business email compromise attack in only 19 minutes with a dedicated team of security experts investigating and alerting the customer in less than 10 minutes.

07

FIVE NOTABLE EMERGING THREAT ACTOR TTPs

FIVE NOTABLE EMERGING THREAT ACTOR TTPs

Threat actors are constantly adapting their tactics, techniques, and procedures (TTPs) to evade defenses and exploit novel initial access vectors.

We reviewed threat intelligence from various sources to identify several key TTPs over the course of 2022. Data sources included threat intelligence data resulting from incident response activities and digital forensics, as well as from our Managed Detection and Response solution.

Initial Access 2 TECHNIQUES	Execution 1 TECHNIQUE	Persistence 1 TECHNIQUE	Credential Access 1 TECHNIQUE	Lateral Movement 1 TECHNIQUE	Command and Control 2 TECHNIQUES
Exploit Public-Facing Application	Command and Scripting Interpreter	External Remote Services	Multi-Factor Authentication Request Generation	Remote Services	Ingress Tool Transfer
External Remote Services					Multi-Stage Channels

01 T1059.001 – Command and Scripting Interpreter – PowerShell

PowerShell remained a favorite of threat actors in 2022.

Numerous other ATT&CK TTPs depend on PowerShell, which provides several features that are attractive to threat actors:

1. PowerShell comes preinstalled on most Microsoft Windows systems targeted by threat actors, including across desktop and server devices.
2. PowerShell provides a means for obfuscation, serving as an evasion against detection by endpoint protection and monitoring solutions.
3. PowerShell can be downgraded, with some effort, to an older version with reduced logging capabilities. This makes it harder for security solutions to detect anomalous activity, especially when process creation and other critical events on endpoints are not externally monitored.

02 T1104 – Multi-Stage Channels and T1105 – Ingress Tool Transfer

Throughout 2022, attackers have continued to show a preference for the use of stagers.

This may take the form of a small binary or script that deploys a more sophisticated malware payload. Scripting languages such as PowerShell and VBScript have also been shown to be attractive methods of staging malicious payloads. These runtime environments tend to be pre-installed in Microsoft Windows.

By using lightweight stagers through off-the-shelf runtime environments, threat actors are able to quickly adapt their malware and evade detection by endpoint protection solutions.

03 T1190 - Exploit Public-Facing Application

In 2022, remote code execution vulnerabilities in major web applications have continued to serve as a potent initial access vector for threat actors.

This list includes a diverse variety of products, such as Microsoft Exchange, Fortinet firewalls, and Meraki VoIP devices.

Due to the wide variety of affected products, organizations find it challenging to prioritize patching of the most urgent affected applications and prevent these kinds of attacks. In many instances, major vulnerabilities that had been disclosed years ago continue to be exploited.

04 T1133 - External Remote Services, T1021 - Remote Services and T1021.001 - Remote Services: Remote Desktop Protocol

Threat actors have continued to show a tendency to rely on remote access solutions such as Microsoft Remote Desktop Services, AnyDesk, ConnectWise Control (formerly known as ScreenConnect), and many others.

The continued advantage of this approach for threat actors is that legitimate software is more likely to fly under the radar when compared to remote access trojans, which are readily blocked by endpoint protection solutions.

05 T1621 - Multi-factor Authentication (MFA) Request Generation

One technique that has become more prevalent in 2022 is excessive use of MFA requests with the goal of convincing users to unintentionally grant access to privileged services.

Threat actors have especially demonstrated the potency of this attack when combined with social engineering techniques, which create more plausible scenarios for users to accept a MFA request. This attack methodology was employed in the Uber compromise, which serves as a cautionary tale in credential management.

This type of attack is made possible when user credentials are compromised through a prior attack, typically leaked onto the dark web. Initial vectors of compromise may include brute force attacks or the exploitation of vulnerable web services.

08

THE LONG TAIL OF LOG4SHELL

THE LONG TAIL OF LOG4SHELL (LOG4J) BACKGROUND

Log4j is a Java-based logging library maintained by the Apache software foundation. Software developers use the Log4j framework to record user activity and review application behavior.

This library is one of the most used libraries for logging and is likely present in millions of java applications. The vulnerability is especially dangerous because Log4j is used as a backend dependency in many cloud-based services.

In early December 2021, Log4Shell (CVE-2021-44228 and CVE-2021-45046) was first identified as a zero-day remote code execution (RCE) vulnerability in Apache Log4j 2. An unauthenticated, remote threat actor can exploit this flaw by sending a specially crafted request to a server running a vulnerable version of Log4j.

Arctic Wolf's Response

After this vulnerability was discovered, Arctic Wolf Labs built the Log4Shell Deep Scan Tool to detect this vulnerability at the source.

The tool enables the detection of both CVE-2021-45046 and CVE-2021-44228 within nested JAR, WAR, and EAR files. Arctic Wolf Labs released this tool first to Arctic Wolf customers and then made it publicly available as open-source software on GitHub within days of authoring it.

Traditional vulnerability scanning solutions are often limited to vulnerabilities that can be detected through network traffic. For vulnerabilities such as Log4Shell that involve software dependencies buried deep within applications, network-based scanning is not exhaustive enough to identify exposure. The Arctic Wolf standalone deep scanning tool goes deeper than network-based scans to detect vulnerable instances of the Log4j dependency at the filesystem level.

As a result of this contribution, Arctic Wolf was named Open-Source Tool Creator of the Year[5] by the SANS Institute for our work on the Log4Shell Deep Scan Tool.

Retrospective

Arctic Wolf Labs observed one in four organizations in our Arctic Wolf customer base have been targeted with Log4Shell exploitation attempts since January 2022. Log4Shell exploitation was the root point of compromise in 11% of all Arctic Wolf Incident Response cases in 2022 for customers where incident response services were the customer's first engagement with Arctic Wolf.

APPROXIMATELY 60% OF ALL INVESTIGATED INCIDENT RESPONSE CASES INVOLVING LOG4SHELL WERE ATTRIBUTED TO THREE RANSOMWARE VARIANTS:

LockBit (26.9%), Conti (19.2%), and ALPHV (BlackCat) (11.5%). The average incident response cost of an incident involving Log4Shell exceeded $90,000 USD.

09

RECOMMENDATIONS FOR A STRONGER SECURITY POSTURE

RECOMMENDATIONS FOR A STRONGER SECURITY POSTURE

Though the cybercrime landscape is continuously evolving, that doesn't mean organizations are on their own when it comes to protection.

Cybersecurity continues to evolve as well, and there's a myriad of ways organizations can better their own security posture and put themselves in a strong position to fight off immediate or future threats.

A robust cybersecurity strategy is one that is not only unique to the organization's needs but focuses on proactive and reactive strategies that work before and after an incident occurs. This strategy should also be scalable and comprehensive, relying on more than just an abundance of software tools. Regardless of an organization's maturity level or security needs, the following recommendations would help address the troublesome trends seen over the last year and strengthen cybersecurity postures going into 2023.

01 Have a Solid Understanding of Your Overall Attack Surface

One of the most important pillars of an organization's security posture is understanding the breadth of the attack surface.

How many devices are exposed to the perimeter? How many workstations are running outdated operating systems? How many servers are being hosted on-premises? These types of questions illustrate the importance of inventory management in an organization's overall security posture.

By creating a full inventory of assets in the environment, organizations are able to gain a better understanding of the overall attack surface while determining which assets are exposed to the perimeter.

This data enables organizations to prioritize and refine their security program with precision, as well as developing a stronger vulnerability and security posture management program.

In addition to creating an inventory of assets, implementing endpoint monitoring across the environment will help organizations review public ports, disable unnecessary ports, and restrict port destinations. This type of monitoring is crucial to provide visibility into actions taken by potential threat actors. While other types of log sources can complement this type of visibility, they cannot replace it.

02 Monitor Critical Log Sources for Security Threats

Arctic Wolf has consistently recognized that a lack of visibility allows security threats to go unnoticed and cause significant damage to organizations.

Log monitoring is critical to detect major threats. This includes logs from intrusion detection systems (IDS)/ network detection response (NDR) systems, firewalls, EDR solutions, IAM systems, and the cloud-hosted services used in your environment.

Expanding environmental visibility to these types of log sources increases the likelihood of detecting potential threats at an early stage, allowing for those threats to be stopped before they have a chance to incur significant damage.

Log monitoring also allows organizations to utilize the full potential of their cyber threat intelligence. Insight gained from the logs can illustrate which TTPs threat actors are using against their targets. That intelligence is critical for identifying Indicators of Compromise (IOCs) and mapping out the adversary's kill chain, ultimately helping analysts understand the motives and goals of threat actors which can assist in decision-making about how to best respond to an incident.

03 Implement Multi-factor Authentication (MFA) Across Applications Used in the Environment

By requiring multiple forms of authentication, it becomes much more difficult for unauthorized individuals to gain access to sensitive systems and data within a network or system.

One trend we've seen in 2022 is the **growing risk of MFA fatigue attacks**, where a threat actor spams a target with MFA authentication prompts to the point of exhaustion, increasing the odds that the target will acquiesce and accept the prompt.

Organizations should consider their overall MFA configuration against these types of threats, implementing countermeasures against MFA fatigue.

These countermeasures include rate limiting of authentication requests, adding a step after the authentication prompt, and end-user security awareness training. Additionally, organizations should consider emerging standards such as WebAuthn which include safeguards against MFA fatigue.

04 Employ a Zero Trust Security Strategy

As organizations continue to migrate to the cloud by the masses and implement remote or hybrid work, implementing Zero Trust strategies becomes an important consideration.

Zero Trust focuses on the user, not the perimeter, and limits all access unless it can be verified. This tactic — which includes strong identity and access management strategies — can reduce the attack surface and prevent an attacker's ability to move laterally through an organization's network.

There are multiple ways to implement Zero Trust strategies, including implementing multi-factor authentication and other identity management tools like Zscaler or Okta.

Utilizing a Zero Trust strategy, and relevant solutions will reduce the risk of account takeovers and will provide additional security for organizations.

05 Understand the Shared Responsibility Model and Eliminate Misconfiguration

It's important to recognize where a cloud provider's security responsibilities end, and an organization's security responsibilities begin.

This is sometimes referred to as the shared responsibility model. In this model, the cloud provider is responsible for the security of the cloud, while the customer is responsible for the security within the cloud. The specifics of this responsibility can vary depending on the cloud service model an organization is using, such as IaaS, PaaS, or SaaS.

Without having a clear understanding of these principles, cloud security configuration can be complex, confusing, and lead to misconfigurations or a lack of proper cloud security for organizations.

It's also important for organizations, as they're moving data to the cloud (and once it's in the cloud), to ensure secure protocols and encryption is always used. These protocols should include a knowledge of, and restrictions to, who can access the data and applications within the cloud environment.

06 Establish a Comprehensive Security Awareness Program/Cybersecurity-Minded Culture

A comprehensive security awareness program can help users understand how they can be targeted and how they can act as a critical line of defense against threat actors and breach attempts.

A strong program includes regular training on current trends and topics — such as password management, browsing habits, social engineering tactics, and how to report and respond to suspicious activity.

Creating an industry-specific program can help users be well prepared to encounter threats and help the organization's overall security posture.

10 CONCLUSION

CONCLUSION AND HOW ARCTIC WOLF CAN HELP

/// **Cybersecurity is a team sport, and we hope the insights and recommendations in this report can help you practically reduce risk and increase resilience for your organization.**

But if you feel overwhelmed by the sheer volume of priorities your security team already had before this report, you are not alone.

No organization can protect itself in isolation. We, as a community, rely on each other for sharing, learning, and providing expertise. It's impossible to go it alone in today's threat landscape. We believe we are all stronger together. We believe in having each other's backs — that everyone is safer when running as a pack.

Our customers rely on us every day to secure their organization against threats. We help level the playing field against attackers — ensuring that every organization of every size has the technology, tools, and processes needed to defend itself. If you aren't getting the outcomes you're looking for from the solutions you have today, or if you just need some support in putting your existing investments to work, we would love to help.

This is why we are proud to bring and demonstrate the wolf pack mentality, working with our customers and peers in the cybersecurity community, doing what it takes to secure organizations and ensure they survive the ever-increasing incident count.

For more information about Arctic Wolf, visit arcticwolf.com

CONTACT US

References:

1. https://securityboulevard.com/2022/03/by-the-numbers-the-cost-of-insider-data-breach-vs-the-cost-of-protection/
2. https://hsdl.org/c/2021-internet-crime-report/
3. https://researchgate.net/publication/332870814_Legends_of_the_Black_Cat_Gang_as_a_Reflection_on_the_Phenomenon_of_Criminal_Myths_in_Russian_Public_Consciousness
4. https://justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
5. https://sans.org/about/awards/difference-makers/

ARCTIC WOLF