blackpoint

2024 ANNUAL THREAT REPORT

PRESENTED BY THE

ADVERSARY PURSUIT GROUP

Table of Contents

Executive Summary

REPORTING PERIOD: DECEMBER 2022-NOVEMBER 2023

2023 marked a year of intensified cyberthreats, with small- and medium-sized businesses (SMBs) finding themselves increasingly in the crosshairs of sophisticated cybercriminal operations. Blackpoint witnessed evolving ransomware and phishing attempts, advantageous Initial Access Brokers (IABs), an influx of Business Email Compromise (BEC) attempts, and the ongoing exploitation of legitimate applications. All of which created a challenging environment for organizations working hard to actively safeguard their hybrid environments.

Ransomware Attacks

Ransomware attacks continued prominently with the existence of double extortion schemes, even triple at times, schemes adding a complex layer to the already daunting threat. Cybercriminals not only encrypt victim data but also threaten public release or deletion of sensitive information unless they receive the ransom. This tactic compounded the dilemma for businesses, forcing them to consider the dire consequences of data exposure, in addition to the operational paralysis caused by data encryption.

Inital Access Brokers

In 2023, IABs, who specialize in breaching systems and selling unauthorized access to the highest bidder, significantly increased their activities. The commoditization of access turned into a booming business, fueling subsequent attacks, including ransomware and data theft.

Phishing Attacks

While the year began with the dominance of access attempts, it gradually diversified to include credential access, Command and Control (C2), and phishing. We witnessed a noticeable sophistication of phishing attacks. Cybercriminals fine-tuned their social engineering (SE) tactics to craft highly convincing and personalized emails, websites, and messages. These phishing campaigns, often initiating multi-stage attacks, no longer aim solely at indiscriminate credential theft. Instead, they have become tools for installing malware, initiating lateral movement within networks, and setting the stage for more devastating attacks.

Supply Chain Attacks

Supply chain attacks emerged as a critical vector, exploiting the interconnected nature of business operations. Attackers capitalized on the potential to breach one entity and infiltrate several others, exploiting the trust and relationships between businesses, their vendors, and Managed Service Providers (MSPs). These attacks had far-reaching ramifications, affecting multiple organizations through a single breach.

Business Email Compromise

Amidst these evolving threats, the ongoing threat of BEC persisted, often targeting SMBs with perceived lower defenses. In these schemes, attackers often impersonate company executives or partners to authorize fraudulent transactions, leading to significant financial losses and eroding trust in business communications.

The Exploitation of Public-Facing Applications

Lastly, threat actors increasingly exploited public-facing applications, capitalizing on common vulnerabilities and misconfigurations. Web servers, content management systems, and remote management interfaces, such as Remote Monitoring and Management (RMM) and Remote Desktop Protocol (RDP), were among the frequently targeted assets.

In Summary

The 2023 landscape served as a stark reminder of the escalating sophistication and interconnectedness of cyberthreats. **For SMBs, the year was a stark reminder to fortify their security defenses by:**

- Prioritizing cybersecurity training
- Monitoring their networks with vigilance
- Having regular vulnerability assessments
- Patching vulnerabilities promptly
- Adhering to strict email security measures
- Proactively addressing emerging threats
- Monitoring the security practices of those they are partnered with
- Adopting the Defense in Depth (DiD) approach

In the face of these multifaceted threats, the importance of resilience, vigilance, and proactive threat mitigation strategies cannot be overstated, as we all navigate the intricacies of modern cyber-risks.

What is Defense in Depth?

A cybersecurity strategy that involves the implementation of multiple layers of security, each layer protecting against different types of security threats.

The 2023 Cyberthreat Landscape

Understanding Initial Access in Cybersecurity

A common thread you will find throughout our threat report is the subject of initial access. Initial access covers the various methods a threat actor may use to gain unauthorized entry into a computer network or system. It is where a threat actor begins, and, when up against Blackpoint's 24/7 Security Operations Center (SOC), is detained.

The Speed of Cyberthreats & Blackpoint's Response

83 minutes
The average time between initial access and lateral movement for threat actors.

15 minutes
The average time Blackpoint SOC takes to respond to initial access attempts.

95%
of endpoint device incidents were initial access attempts.

Experts often discuss cybercriminals' dwell time in terms of days, but the initial stages of the attack chain occur in a much shorter timeframe. According to the SOC's 2023 data, the average time between initial access and lateral movement for a threat actor was 83 minutes. With that in mind, CrowdStrike's recommended response framework seems sufficient. The 1/10/60 rule suggests one minute to detect the intrusion, 10 minutes to understand what the threat actor is trying to do, and one hour to contain the threat. At Blackpoint though, we see firsthand the critical nature of stopping initial access attempts, responding to discovered breaches within 15 minutes.

In fact, Blackpoint observed that attempts to gain initial access and move laterally through an organization, specifically targeting endpoint devices, constituted 95% of the threat landscape seen on these devices. This marks an increase from 2022's already high percentage of 86%. The growth in this space can be attributed to several factors, such as:

- Implicit trust on binaries that support live-off-the-land (LotL)
- Easy access to trusted enterprise-level software such as RMM tools
- The rise of Software-as-a-Service (SaaS) that operates in the cloud and unifies entire organizations using just an email address

These factors and more, have led to a growing market for various threat actors acting as IABs for other groups.

Diverse Tactics for Initial Access

To gain initial access, threat actors have an arsenal of methods to pull from. Phishing and spear-phishing attacks, of course, continued to be prevalent methods. In 2023, a series of severe software vulnerabilities exposed organizations to the risk of remote code execution (RCE). The MSPs we partner with encountered a continual increase in attempts to compromise business email accounts through brute force and stolen credentials. With unfettered access into various industries, MSPs are highly desirable targets for supply chain attacks due to the implicit trust placed upon them by their customers and the powerful tools embedded in their environments, such as RMMs.

The Growing Trend of RMM Tool Exploitation

With that in mind, threat actors frequently exploited RMM tools to gain initial access. Blackpoint observed this trend back in the spring of 2022, when threat actors were using these tools to deploy malicious payloads. Then, at the start of 2023, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory (CSA) warning of the dangers presented by RMMs. Throughout 2023, we continued to see threat actors use these legitimate enterprise tools to gain initial access and propagate through organizations. In each case, the RMM being used was available through trial versions that lack human verification.

1,000+ incidents

of threat actors using the LotL strategy were observed in 2023.

The Role of Live-off-the-Land in Cyberattacks

The increased use of enterprise software such as RMM tools is one of the primary reasons threat actors can work so quickly within an environment. These tools often use native binaries and libraries that support the LotL strategy, which enable a threat actor to remain undetected, avoid dependency on external tools, facilitate lateral movement, and more. In 2023, we observed over 1,000 instances of threat actors using the LotL strategy against our partners, with software such as PowerShell, Wscript, and Mshta amongst the most common native binaries. By doing so, IABs ensure wide-spread access before selling to other groups.

The Threat of Initial Access Brokers

IABs employ a variety of techniques, not limited to living off the land. They also use phishing attacks, stolen credentials, and exploitable vulnerabilities to gain initial access to systems. The increased demand for access has led to the growth of this offering with prices ranging from $500 to upwards of $20k. In late 2023, the takedown operation of Qakbot saw the seizure of over $8.6 million in cryptocurrencies, demonstrating how much revenue is generated by IAB groups.

64% increase

in ransomware attacks employing double extortion tactics from 2022 to 2023.

The Ongoing Threat of Ransomware

Initial Access Brokers' increased activity and profitability has aided groups specializing in ransomware. Over 2023, ransomware continued to take center stage with notable attacks against a plethora of organizations and industries, with the most damaging and publicly reviewed being those that adopt double extortion tactics. Notable instances throughout 2023 include LockBit's attack against the Royal Mail in the United Kingdom, BlackCat's attack on Leigh Valley Health Network that led to follow-on lawsuits against the company, and Royal's attack on the City of Dallas that resulted in over $8.5 million dollars in restoration services.

Thankfully, our SOC has effectively prevented ransomware threat actors from infiltrating our systems yet again in 2023. As a result, the Adversary Pursuit Group (APG) utilized various open-source intelligence (OSINT) methods at the end of 2023 to evaluate the threat landscape. This approach led us to significant findings:

- We observed an approximate 64% increase in ransomware attacks employing double extortion tactics from 2022 to 2023.
- Almost 50% of ransomware attacks in 2023 were carried out by LockBit, a notorious Ransomware-as-a-Service (RaaS) known for its 'StealBit' tool, which facilitates efficient data exfiltration.

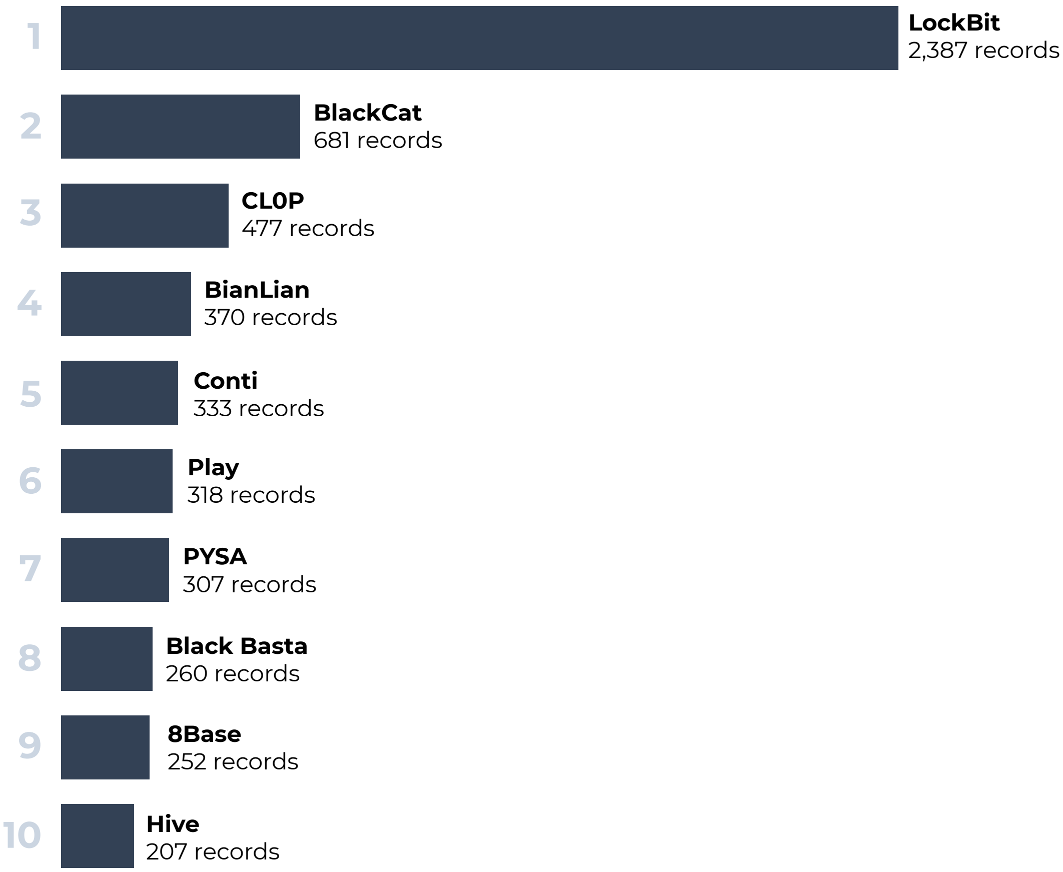
Top 10 Ransomware Threat Actors in 2023

Almost 50%

of attacks committed in 2023 were by LockBit.

LockBit 3.0: 1,381 records

LockBit 2.0: 1,006 records



In Summary

Due to the nature of our services, initial access accounts for 95% of our view of the cyberthreat landscape involving endpoint devices. Before threat actors can get any further, we have halted their steps. Whether a threat actor plans to exploit an RMM tool in a supply chain attack, deploy ransomware, or is an IAB looking to profit off access, time is of the essence. Advanced security services are required to go up against, and defeat, threat actors such as LockBit, BlackCat, and CL0P.

MDR-Powered SOC Combats Citrix Bleed Vulnerability Exploitation

One effective way to withstand advanced threats is through a SOC powered by Managed Detection, Response and Remediation (MDR+R). With our people and technology, we can respond to new threats and exploits in real time, such as the exploitation of RMM tools in 2022 and public-facing applications in 2023.

In October 2023, when the SOC was made aware of the critical 'Citrix Bleed' vulnerability (CVE-2023-4966), the team immediately familiarized itself with the indicators of compromise (IoCs) as well as how to identify and respond to the threats associated. Two months later, their preparation paid off and they encountered the exploitation firsthand. Blackpoint's MDR+R alerted to multiple successful share mounts in one of our MSP's end client environments.

Our Technical Director of Threat Operations, Jason Rathbun, triaged the environment and within one minute of initial triage, began containing the incident. Jason identified malicious activities, including scheduled tasks and suspicious remote executions, which are often signs of an ongoing cyberattack. The threat actors used advanced tactics and tried various methods to establish persistence in the environment, including:

Citrix Bleed Vulnerability Exploitation

- Based on the overall technical investigation, the SOC concluded the threat actors exploited the 'Citrix Bleed' vulnerability to gain initial access to the end client's NetScaler Gateway. This appliance is pivotal for streamlining remote access infrastructure, as it enables single sign-on (SSO) capabilities for a variety of applications. This vulnerability, if left unpatched, can allow threat actors to execute arbitrary code remotely.

Domain Admin Session Theft

- From there, they stole a domain admin session, giving them high-level access privileges within the network, and set up two separate scheduled tasks in the environment to maintain persistence.

Persistence Setup

- Both scheduled tasks were designed to set up Go Simple Tunnel (1), an OSINT resource used in this instance to help create SOCKS5 proxies (2) to establish a backdoor connection.

Lateral Movement

- The threat actors then switched to the default domain administrator account and began using Impacket, a suite of tools for network protocols, to move laterally to a Domain Controller (DC) in the environment.
- Next, they switched accounts again and used Windows Remote Management (WinRM) to get to the Veeam server.

Data Access

- The threat actors also tried to conduct remote executions using PowerShell to expose the Structured Query Language (SQL) database of the Veeam servers and establish a Go Simple Tunnel connection from the DC to their Command and Control (C2), with the possible goal of accessing, modifying, deleting, or extracting data, as one would for double extortion.

Throughout the investigation, the SOC found numerous locations where the threat actors had set up persistence mechanisms, the most prevalent being scheduled tasks. The threat actors moved quickly and showed multiple defense evasion techniques such as rotating through valid accounts. They were methodical and blended in, using general windows management instrumentation (WMI) to evade antivirus (AV) and Endpoint Detection and Response (EDR) detection.

The SOC successfully contained the incident, which could have led to extensive data exfiltration and ransomware deployment. They then contacted the MSP, providing them with key details, time stamps, and remediation steps, such as blocking IoCs in their firewalls, to help eradicate the threat actors and prevent further malicious activity.

blackpoint
The EDR Gap
Real Cases of EDR Blind Spots, and How MDR Stepped in for the Save

The EDR Gap

Hear about real cases of EDR blind spots, and how MDR stepped in for the save.

READ NOW

1. So Simple Tunnel is a tool used to create secure, encrypted communication channels. This connection would allow for data exfiltration and remote control of compromised systems.

2. Go Simple Tunnel is a tool used to create secure, encrypted communication channels. This connection would allow for data exfiltration and remote control of compromised systems.

Cloud Security Trends and Insights

Immense Increase in Cloud Security Incidents

While we continued to combat on-premises threats, such as the ‘Citrix Bleed’ vulnerability, cloud security incidents have escalated significantly over the last year. We introduced the first-ever cloud MDR for Microsoft 365 in the spring of 2022, followed by Google Workspace protection in the fall of 2023. Due to the increasing reliance on cloud services and broadening threat landscape, along with our unmatched visibility, cloud-related incidents rose drastically in the last year. What accounted for 56.91% of Blackpoint’s incidents in December 2022 took up 88.46% in September 2023.

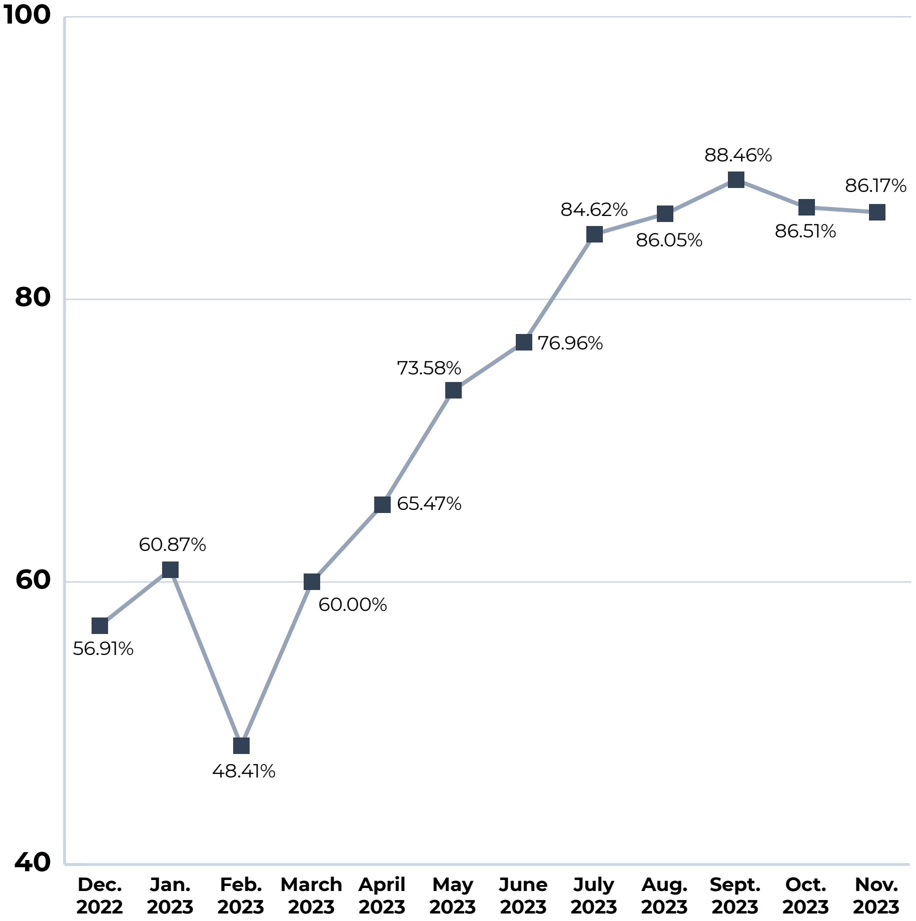
31.55% increase

in cloud-related incidents from December 2022 to September 2023.

78.78%

of all incidents from December 2022 to November 2023 were cloud related.

Percentage of Cloud Incidents Encountered Each Month:



Dominance of VPN-Related Incidents

Over 99%
of all cloud incidents include the presence of VPN usage.

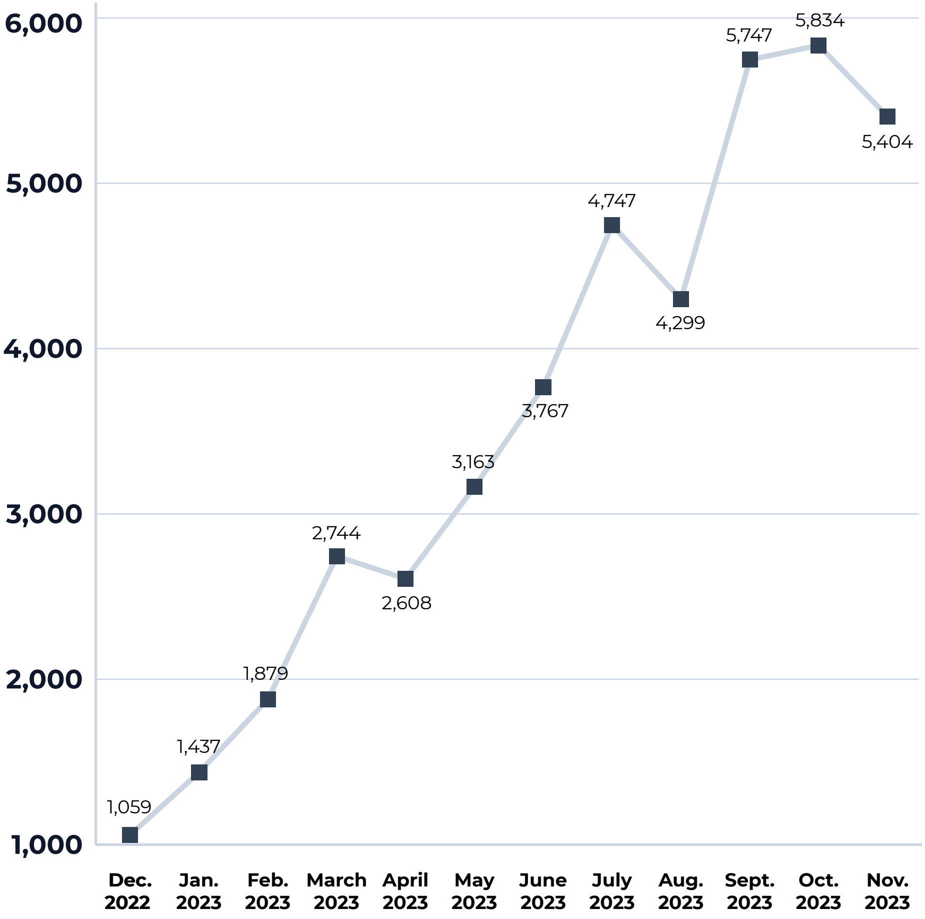
A striking aspect of the year's cloud security landscape was the dominant role of virtual private networks (VPNs) in these incidents. We have observed consistently high VPN usage, present in over 99% of cloud incidents, suggesting they are heavily abused in cyberattacks. This trend emphasizes the criticality of secure and well-managed VPN solutions as part of the broader cloud security framework.

Shift in Attack Vectors: Initial Access and Diversification of Threats

214 attempts
of password spraying attacks were seen in August 2023.

As previously discussed, initial access formed a significant portion of the incident response activities performed by our SOC, accounting for over half of the cloud incidents at certain points during the year. It drastically increased in May 2023 and peaked in August 2023 at 214 attempts. Password spraying attacks, where threat actors use brute force to perform BEC, emerged as one of the largest perpetrators of gaining initial access. In the past year, BEC attempts rose by an average of 210%, reaching a total number of 42,688 incidents, with the highest number recorded in October.

Business Email Compromise Attempts



210% increase
in BEC attempts over the last year, reaching a total number of 42,688 incidents.

In Summary

Our analysis of data from December 2022 to November 2023 reveals the growing complexities and evolving challenges in cloud security. Cloud security incidents significantly increased during this period, reflecting the increased dependence on cloud services and ever-expanding threat landscape. The data shows attackers making concentrated efforts to breach cloud defenses, likely driven by the valuable data within these environments. VPN-related incidents dominated this period, highlighting the critical need for secure and effectively managed VPN solutions.

Furthermore, there was a noticeable shift in attack vectors, initially dominated by access attempts but gradually diversifying to include credential access, C2, and phishing in the latter half of the year. These trends demonstrate the need for robust, adaptive, and comprehensive security strategies to combat the evolving cyberthreats and ensure the protection of cloud environments.

Threat Actor Profiles

As the cybersecurity landscape continues to evolve, being able to recognize significant threat actors behind the threats we have discussed will be essential. While attribution is not always possible due to the speed at which our SOC operates, we encountered five particularly dominant cyber adversaries this year. BlackCat, LockBit, QakBot, RedLine Stealer, and Akira have established themselves in the cyberthreat landscape as frontrunners due to their advanced tactics, techniques, and procedures (TTPs), specific targets, and unique business approaches.

BlackCat

ALIASES:

ALPHV, AlphaV,
Noberus

EMERGENCE:

Mid-November 2021

BlackCat, a RaaS operation, is a possible rebranding of the group DarkSide. They were the first ransomware group to create a public data leaks site and target large enterprises, such as MGM Resorts in September 2023. BlackCat is written in Rust, enabling them to target Windows and Linux devices. Most recently, they escalated their tactics by filing an SEC complaint against a victim who did not disclose a cyberattack. Despite government interference, BlackCat continues to reemerge.

BlackCat TTPs

Reconnaissance	
T1598 Phishing for Information	
Resource Development	
T1586 Compromise Accounts	
Initial Access	
T1190 Exploit Public-Facing Application	
T1078 Valid Accounts	
Execution	
T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell
T1047 Windows Management Instrumentation	
Persistence	
T1078 Valid Accounts	
Privilege Escalation	
T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control
T1134 Access Token Manipulation	
T1078 Valid Accounts	
Defense Evasion	
T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control
T1134 Access Token Manipulation	
T1562 Impair Defenses	T1562.001 Disable or Modify Tools T1562.009 Safe Mode Boot
T1112 Modify Registry	
T1078 Valid Accounts	
Credential Access	
T1557 Adversary-in-the-Middle	
T1555 Credentials from Password Stores	

BlackCat TTPs

Discovery	
T1087 Account Discovery	T1087.002 Domain Account
T1083 File and Directory Discovery	
T1135 Network Share Discovery	
T1069 Permission Groups Discovery	T1069.002 Domain Groups
T1057 Process Discovery	
T1018 Remote System Discovery	
T1082 System Information Discovery	
T1016 NetworkConfiguration Discovery	
T1033 System Owner / User Discovery	
Lateral Movement	
T1570 Lateral Tool Transfer	
Collection	
T1557 Adversary-in-the-Middle	
Command and Control	
T1071 Application Layer Protocol	
T1219 Remote Access Software	
Exfiltration	
T1048 Exfiltration Over Alternative Protocol	
T1041 Exfiltration Over C2 Channel	
T1567 Exfiltration Over Web Service	
Impact	
T1486 Data Encrypted for Impact	
T1491 Defacement	T1491.002 External Defacement
T1561 Disk Wipe	T1561.001 Disk Content Wipe
T1490 Inhibit System Recovery	
T1489 Service Stop	

EVOLUTION:

BlackCat represents a new wave of ransomware threats, evolving from previous groups like DarkSide and BlackMatter. BlackCat is written in Rust, which indicates sophistication on the part of their developers. It enables them to target both Windows and Linux devices, and often evade detection by traditional security tools.

BUSINESS MODEL:

BlackCat operates under a RaaS model, where developers offer malware to affiliates in exchange for a percentage of the ransom payments. They have gained recognition for their sophisticated double and sometimes triple extortion tactics. Recently, they escalated their tactics by including the filing of an SEC complaint against a victim for not disclosing a cyberattack.

INNOVATIVE TECHNIQUES:

BlackCat is notable for being the first ransomware group to create a public data leaks site on the open internet and for employing typo-squatted replicas of victim websites to post stolen data, enhancing the pressure on victims.

TARGET PROFILE:

They target a broad range of global entities including universities, government agencies, and companies in the energy, technology, manufacturing, and transportation sectors.

Recent highly impacted targets include MGM Resorts International and Caesars Entertainment.

ASSOCIATED GROUPS:

They are linked to discontinued RaaS groups like DarkSide and BlackMatter. Some speculate that it may be a rebranding of DarkSide or a successor to REvil.

Typical Attack Chain:

Initial Access:

BlackCat is known to use OSINT (`T1598`) and advanced SE tactics, often pretending to be legitimate IT staff. They do so to trick users into providing additional information. This is done with the aim of social engineering other individuals or acquiring credentials (`T1586`), which can then be used to gain access to the system.

Follow-On Activities:

- Deploy legitimate software (e.g., AnyDesk, Splashtop, Mega Sync, Plink, and Ngrok) for remote access and to prepare for data exfiltration (`T1041`)
- Create a connection to C2 servers such as Brute Ratel C4 or Cobalt Strike (`T1071`)
- Deploy attack frameworks such as Evilginx2 to capture multifactor authentication (MFA), login credentials, and session cookies (`T1557`)
- Use access token manipulation (`T1134`), or credentials from the DC, local networks, and backups (`T1555`) to gain elevated credentials that will enable enumeration and lateral movement
- Exfiltrate system data through the C2 channel (`T1041`), web services (`T1567`), or alternative protocol (`T1048`)

Impact:

- BlackCat often extorts victims with the threat of releasing their exfiltrated sensitive data to other threat actors.
- They are known to encrypt all systems and files (`T1486`) and/or completely erase content (`T1561`).
- They may deface (`T1491`) and inhibit system recovery (`T1490`).

Other Tools Seen:

Mega.nz, Dropbox, Metasploit, POORTRY, STONESTOP, The Onion Router (Tor), sragent.exe, psexec32.exe, version.dll

LockBit

ALIASES:

ABCD Ransomware

EMERGENCE:

September 2019

LockBit is well known for its continuous evolution through versions 2.0 and 3.0. They operate as a RaaS and have been known to recruit insiders from the companies they target. They tend to target healthcare facilities and schools, particularly those with Linux devices.

LockBit TTPs

Initial Access	
T1189 Drive-by Compromise	
T1190 Exploit Public-Facing Application	
T1133 External Remote Services	
T1566 Phishing	
T1078 Valid Accounts	
Execution	
T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell
T1053 Scheduled Task/Job	
T1072 Software Deployment Tools	
T1204 User Execution	
Persistence	
T1547 Boot or Logon Autostart Execution	
T1133 External Remote Services	
T1574 Hijack Execution Flow	
T1053 Scheduled Task/Job	
T1078 Valid Accounts	
Privilege Escalation	
T1548 Abuse Elevation Control Mechanism	
T1134 Access Token Manipulation	
T1547 Boot or Logon Autostart Execution	
T1484 Domain Policy Modification	T1484.001 Group Policy Modification
T1574 Hijack Execution Flow	
T1053 Scheduled Task/Job	T1053.005 Scheduled Task
T1078 Valid Accounts	
Defense Evasion	
T1548 Abuse Elevation Control Mechanism	
T1134 Access Token Manipulation	
T1140 Deobfuscate/Decode Files or Information	
T1484 Domain Policy Modification	
T1574 Hijack Execution Flow	
T1562 Impair Defenses	T1562.001 Disable or Modify Tools

LockBit TTPs

T1070 Indicator Removal	T1070.001 Clear Windows Event Logs T1070.004 File Deletion
T1027 Obfuscated Files or Information	T1027.002 Software Packing
T1127 Trusted Developer Utilities Proxy Execution	
T1078 Valid Accounts	
Credential Access	
T1110 Brute Force	
T1003 OS Credential Dumping	T1003.001 LSASS Memory
Discovery	
T1083 File and Directory Discovery	
T1046 Network Service Discovery	
T1135 Network Share Discovery	
T1057 Process Discovery	
T1018 Remote System Discovery	
T1082 System Information Discovery	
Lateral Movement	
T1570 Lateral Tool Transfer	
T1021 Remote Services	T1021.001 Remote Desktop Protocol T1021.002 SMB/Windows Admin Shares
T1072 Software Deployment Tools	
Command and Control	
T1095 Non-Application Layer Protocol	
T1572 Protocol Tunneling	
T1219 Remote Access Software	
Exfiltration	
T1041 Exfiltration Over C2 Channel	
T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage
Impact	
T1485 Data Destruction	
T1486 Data Encrypted for Impact	
T1491 Defacement	T1491.001 Internal Defacement
T1490 Inhibit System Recovery	
T1489 Service Stop	

EVOLUTION:

LockBit has evolved significantly since its inception, with notable advancements seen in their 2.0 and 3.0 versions. LockBit 2.0 surfaced in June 2021, followed by 3.0 in March 2022. These evolutions include improved encryption methods, targeting strategies, and the introduction of innovative tools like "StealBit" for data exfiltration.

BUSINESS MODEL:

LockBit operates as a RaaS group using double extortion tactics and offers ransomware to affiliates, sharing profits from the ransom payments.

INNOVATIVE TECHNIQUES:

They developed “StealBit” for efficient data exfiltration, and target Linux devices, focusing on ESXi servers, showcasing their adaptability and technical sophistication.

TARGET PROFILE:

They predominantly target the healthcare and education sectors, with significant attacks in Brazil, India, and the United States.

ASSOCIATED GROUPS:

They collaborate with various criminal groups and network access brokers, even recruiting insiders from targeted companies.

Typical Attack Chain:

Initial Access:

LockBit affiliates typically use compromised servers (`T1189`) or exploit external services (`T1133`) such as RDP. LockBit has also been seen gaining access through phishing attempts (`T1566`) and valid accounts (`T1078`).

Follow-On Activities:

- Execute batch scripts (`T1059`) or Chocolatey package manager (`T1072`) to begin attack deployment
- Use compromised user accounts (`T1078`) and find additional accounts with tools such as Mimikatz (`T1003`) to gain privilege escalation with which persistence can be established via scheduled tasks (`T1053`) and autostart execution (`T1574`)
- Evade detection and impair defenses (`T1562`) by attempting to disable EDR processes using tools such as Backstab, Defender Control, GMER, PCHunter, PowerTool, Process Hacker, or TDSSKiller
- Use Splashtop Remote Desktop, Cobalt Strike (`T1570`), and remote services (`T1021`) for lateral movement throughout the network
- Conduct C2 using tools such as FileZilla, SOCKS5 TCP tunnels, and AnyDesk (`T1219`)
- Exfiltrate data using tools like Rclone, FreeFileSync, or Mega (`T1567`)

Impact:

- LockBit encrypts Windows, Linux, and VMware instances, using Advanced Encryption Standard (AES) with randomly generated keys to hold for ransom (`T1486`).
- They change wallpapers and icons to custom LockBit 3.0 ones (`T1491`).
- They delete volume shadow copies (`T1485`) and terminate processes and services (`T1489`) to reduce the likelihood of recovery.

Other Tools Seen:

Blister Loader, ExtPassword, LostMyPassword, SystInternals Prodump, ThunderShell, Plink, Atera RMM, ScreenConnect, TeamViewer

QakBot

ALIASES:

Qbot, Quackbot, Pinkslipbot, TA570

EMERGENCE:

2008. They are one of the longest-standing threats in the cyber landscape.

QakBot is a versatile botnet that offers a suite of tools, often setting the stage for Conti, Egregor, and others' ransomware deployments. Despite government interference, QakBot continues to return with new, innovative tactics.

QakBot TTPs

Execution	
T1106 Native API	
T1047 Windows Management Instrumentation	
Defense Evasion	
T1140 Deobfuscate/Decode Files or Information	
T1112 Modify Registry	
T1027 Obfuscated Files or Information	T1027.001 Binary Padding T1027.010 Command Obfuscation T1027.011 Fileless Storage T1027.006 HTML Smuggling T1027.005 Indicator Removal from Tools T1027.002 Software Packing
Credential Access	
T1110 Brute Force	
T1539 Steal Web Session Cookie	
Discovery	
T1010 Application Window Discovery	
T1482 Domain Trust Discovery	
T1083 File and Directory Discovery	
T1135 Network Share Discovery	
T1120 Peripheral Device Discovery	
T1057 Process Discovery	
T1018 Remote System Discovery	
T1518 Software Discovery	T1518.001 Security Software Discovery
T1082 System Information Discovery	
T1016 System Network Configuration Discovery	T1016.001 Internet Connection Discovery
T1049 System Network Connections Discovery	
T1033 System Owner/User Discovery	
T1124 System Time Discovery	

QakBot TTPs

Lateral Movement	
T1210 Exploitation of Remote Services	
Collection	
T1185 Browser Session Hijacking	
T1005 Data from Local System	
Command and Control	
T1105 Ingress Tool Transfer	
T1095 Non-Application Layer Protocol	
T1572 Protocol Tunneling	
Exfiltration	
T1041 Exfiltration Over C2 Channel	

EVOLUTION:

Initially a banking trojan, QakBot has transformed into a versatile botnet, constantly updating to include more sophisticated functionalities. In August 2023, a government operation took down their infrastructure. By November, DarkGate and PikaBot appeared to be spinoffs. A month later, QakBot was back with novel tactics.

BUSINESS MODEL:

QakBot is not limited to a single type of cybercrime. They offer a suite of tools for reconnaissance, lateral movement, data gathering, and exfiltration. They serve as a vector for delivering various malicious payloads.

TARGET PROFILE:

QakBot focuses on global infrastructures with an emphasis on sectors like finance, emergency services, commercial facilities, and election infrastructure subsectors. Most recently, they targeted the hospitality industry.

ASSOCIATED GROUPS:

They often set the stage for the deployment of human-operated ransomware like Conti, ProLock, and Egregor, among others.

blackpoint

CASE STUDY

Blackpoint Cyber Detains Qakbot Information-Stealing Malware

Blackpoint Cyber Detains Qakbot Information-Stealing Malware

See how our Managed EDR solution detained Qakbot in under two minutes.

READ NOW

Typical Attack Chain:

Initial Access:

QakBot has been known to be used by IABs to sell network access to other threat actors. Their preferred method is spear-phishing with links or attachments (**`T1566`**), which tends to be more time consuming than phishing attacks but has a better success rate.

Follow-On Activities:

- Gain a foothold using native tools such as JavaScript (**`T1059.007`**), PowerShell (**`T1059.001`**), Windows Command Prompt (**`T1059.003`**), scheduled tasks (**`T1053.005`**), and process injection (**`T1055`**)
- Discover and move laterally to as many systems it can get access to through Network Share Discovery (**`T1135`**), Network Connections Discovery (**`T1049`**), exploitation of remote services (**`T1210`**), and replicating throughout discovered systems
- Collect additional information such as Local Emails (**`T1114.001`**), Data from Local Systems (**`T1005`**), and Browser Session information (**`T1185`**), allowing for further targeting and exploitation
- Establish C2 connections via Ingress Tools (**`T1105`**), Protocol Tunnelling (**`T1572`**), and External Proxies (**`T1090.002`**)

Impact:

- Known for its initial access capabilities, QakBot often hands off its control to other threat actors before detonating at the impact stage. That being said, they are known to deliver ransomware deployments including Conti, Egregor, ProLock, REvil, MegaCortex, and Black Basta.

Other Tools Seen:

Visual Basic, Base64, Server Message Block, Dynamic Link Library (DLL) Side-Loading, masquerading file types, Microsoft Excel, Mobsync.exe, wermgr.exe, SOCKS5 protocol, ISO Files, MSIExec, Regsvr32, Brute Ratel C4, WMI

RedLine Stealer

ALIASES:

No known aliases

EMERGENCE:

March 2020

RedLine Stealer has gained a reputation for its extensive information gathering and data exfiltration capabilities. It operates as a Malware-as-a-Service (MaaS) and is used by a wide range of cybercriminals. RedLine attacks often target industries such as healthcare and manufacturing.

RedLine Stealer TTPs

Initial Access	
T1659 Content Injection	
T1189 Drive-by Compromise	
T1566 Phishing	
Execution	
T1053 Scheduled Task/Job	
T1204 User Execution	
Persistence	
T1053 Scheduled Task/Job	
Privilege Escalation	
T1053 Scheduled Task/Job	
Credential Access	
T1555 Credentials from Password Stores	
T1056 Input Capture	
T1003 OS Credential Dumping	
T1539 Steal Web Session Cookie	
T1552 Unsecured Credentials	T1552.008 Chat Messages
Discovery	
T1087 Account Discovery	
T1217 Browser Information Discovery	
T1526 Cloud Service Discovery	
T1652 Device Driver Discovery	
T1083 File and Directory Discovery	
T1654 Log Enumeration	
T1057 Process Discovery	
T1518 Software Discovery	
T1614 System Location Discovery	
T1016 System Network Configuration Discovery	

RedLine Stealer TTPs

`T1033` System Owner/User Discovery	
`T1007` System Service Discovery	
Collection	
`T1119` Automated Collection	
`T1005` Data from Local System	
`T1039` Data from Network Shared Drive	
`T1056` Input Capture	
Command and Control	
`T1659` Content Injection	
`T1105` Ingress Tool Transfer	
Exfiltration	
`T1020` Automated Exfiltration	
`T1041` Exfiltration Over C2 Channel	
Impact	
`T1657` Financial Theft	

EVOLUTION:

Since 2020, RedLine Stealer has continually updated. They have extensive information gathering and data exfiltration features, including the ability to load remote payloads.

BUSINESS MODEL:

They operate as a MaaS, available on underground forums with different pricing tiers, paid for with cryptocurrencies.

INNOVATIVE TECHNIQUES:

They collect an array of data from users' browsers, including login information, auto-fill form fields, and browser history. They use Simple Object Access Protocol (SOAP) Application Programming Interface (API) for C2 communication and leverage Telegram API for real-time infection notifications.

TARGET PROFILE:

They target a wide range of sectors, notably healthcare and manufacturing.

ASSOCIATED GROUPS:

RedLine Stealer is distributed to a range of cybercriminals on the dark web, indicating a broad base of users rather than specific associated groups.

Typical Attack Chain:

Initial Access:

RedLine got its start with phishing emails (`T1566`) and has since expanded to malvertising (`T1189`), free software, cheat codes, and other methods of tricking users into clicking on or installing software (`T1659`).

Follow-On Activities:

- Steal stored browser information such as credentials, credit cards, and other auto-completed data (`T1217`)
- Steal cryptocurrency wallets (`T1005`)
- Steal baseline system information such as users, locations, operating system (OS) and software versions, hardware configurations, and installed security software (`T1005` & `T1119`)
- Exfiltrate data over C2 connections configured during build with the "RedLine Admin Panel" (`T1020` & `T1041`)

Impact:

- RedLine Stealer has the ability to drop additional payloads (`T1105`).
- They sell sensitive information to other threat actors for additional follow-on exploitation.
- They are responsible for much of the market for stolen credentials.

```
[ AKIRA ]

AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think o
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that
fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is
ur instructions to get back to your daily routine, by cooperating with us you will minimi
ge that might be done.

Those who choose different path will be shamed here publicly. The functionality of this b
emely simple - enter the desired command in the input line and enjoy the juiciest info
orporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and canno
to the place of final storage nor deleted by anyone besides us.

guest@akira:~$ help

List of all commands:

 leaks
```

Akira

ALIASES:

Akira Ransomware

EMERGENCE:

March 2023

Akira is known for its distinctive, retro-style Tor leak site, where their double extortion tactics are played out. They utilize leaked source code of Conti ransomware, suggesting collaboration of some sort. Akira typically targets Linux devices and VMware ESXi virtual machines.

Akira TTPs

Initial Access	
T1190 Exploit Public-Facing Application	
T1133 External Remote Services	
T1566 Phishing	T1566.001 Spearphishing Attachment T1566.002 Spearphishing Link
T1199 Trusted Relationship	
T1078 Valid Accounts	
Execution	
T1059 Command and Scripting Interpreter	
Persistence	
T1136 Create Account	T1136.002 Domain Account
T1133 External Remote Services	
T1078 Valid Accounts	
Privilege Escalation	
T1078 Valid Accounts	
Defense Evasion	
T1006 Direct Volume Access	
T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1078 Valid Accounts	
Credential Access	
T1003 OS Credential Dumping	T1003.001 LSASS Memory

Akira TTPs

Discovery	
T1083 File and Directory Discovery	
T1046 Network Service Discovery	
T1135 Network Share Discovery	
T1018 Remote System Discovery	
T1082 System Information Discovery	
T1016 System Network Configuration Discovery	
T1049 System Network Connections Discovery	
Lateral Movement	
T1210 Exploitation of Remote Services	
T1570 Lateral Tool Transfer	
T1021 Remote Services	T1021.001 Remote Desktop Protocol T1021.002 SMB/Windows Admin Shares
T1080 Taint Shared Content	
Command and Control	
T1219 Remote Access Software	
Exfiltration	
T1048 Exfiltration Over Alternative Protocol	T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol
T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage
Impact	
T1486 Data Encrypted for Impact	
T1490 Inhibit System Recovery	

EVOLUTION:

Although different from the Akira ransomware active in 2017, it uses the same ".akira" extension for encrypted files. Akira uses the leaked source code of Conti ransomware, demonstrating an evolution in its technical capabilities.

BUSINESS MODEL:

Akira operates by performing double extortion with demands typically ranging from $200,000 to over $4 million.

INNOVATIVE TECHNIQUES:

Akira utilizes a unique retro-styled Tor leak site, setting it apart in presentation and style. In September 2023, they exploited a zero-day vulnerability (CVE-2023-20269) in Cisco products to establish unauthorized VPN sessions, indicating an elevated level of technical sophistication.

TARGET PROFILE:

Akira has expanded their targets to include Linux devices and VMware ESXi virtual machines. Initially, they heavily impacted the healthcare industry. They are present predominantly in Canada and the United States.

ASSOCIATED GROUPS:

Code similarities with Conti ransomware actors suggest Akira's collaboration or shared knowledge with these cybercriminal groups.

Typical Attack Chain:

Initial Access:

Akira is a ransomware group that typically focuses on the follow-on attack using credentials or access from affiliates or other threat actors. They seem to prefer utilizing VPN credentials but have also used phishing attacks (**T1566**) and the exploitation of zero-day vulnerabilities (**T1190** & **T1133**).

Follow-On Activities:

- Create a backdoor domain account for persistent access (**T1136**)
- Attempt to terminate any known running AV software (**T1562**)
- Collect system (**T1018**) and network information (**T1016** & **T1049**)
- Use tools such as Mimikatz to gather additional credentials (**T1003**) that may be useful for lateral movement with Living Off the Land Binaries (LoLBins) tools like RDP (**T1021**)
- Use legitimate tools such as AnyDesk, Radmin, RustDesk, RClone, and FileZilla for C2 and exfiltration (**T1219**)

Impact:

- Akira uses a hybrid encryption algorithm for heightened impact (**T1486**).
- They employ selective encryption to avoid directories and files that may affect its operation.
- They inhibit system recovery by deleting shadow copies (**T1490**).

Other Tools Seen:

PowerTool, KillAV, PCHunter, SharpHound, AdFind, Advanced IP Scanner, MASSCAN, Cloudflare Tunnel, MobaXterm, Ngrok, WinSCP

In Summary

Understanding the key players and their methods is essential for proactive, effective cybersecurity. The distinct approaches of dominant threat actors, including BlackCat, LockBit, QakBot, RedLine Stealer, and Akira, highlight the need for targeted defensive strategies. With awareness of top tactics and dominant malicious actors under our belt, we can now look ahead to how to protect the most vulnerable industries and businesses. This full view of the cyberthreat landscape will help create a comprehensive security strategy for you to implement the rest of 2024.

Industry-Specific Threat Analysis

The threat actor groups we have just reviewed target a plethora of industries including education, hospitality, government, healthcare, and manufacturing. At Blackpoint specifically, we have seen certain industries get targeted with initial access attempts more than others. Why initial access, specifically? We encounter this tactic the most, as our SOC's job is to halt malicious actors before they gain entry.

The most common methods for initial access include:

- **Phishing attacks**
- **Exploited vulnerabilities**
- **Email compromise**
- **The use of stolen credentials**

These attempts often couple with the use of VPNs, which obscure crucial information like malicious locations and infrastructure, complicating detection and response. As we examine our top attacked industry verticals, you will see that a heavy percentage of the incidents center on initial access. We will break down other tactics, as well as initial access methods used. Awareness of who could be targeting you or your customers, as well as how they may do so, is crucial to fortifying your defenses accordingly.

99%

VPNs were used in over 99% of our cloud-related incidents.

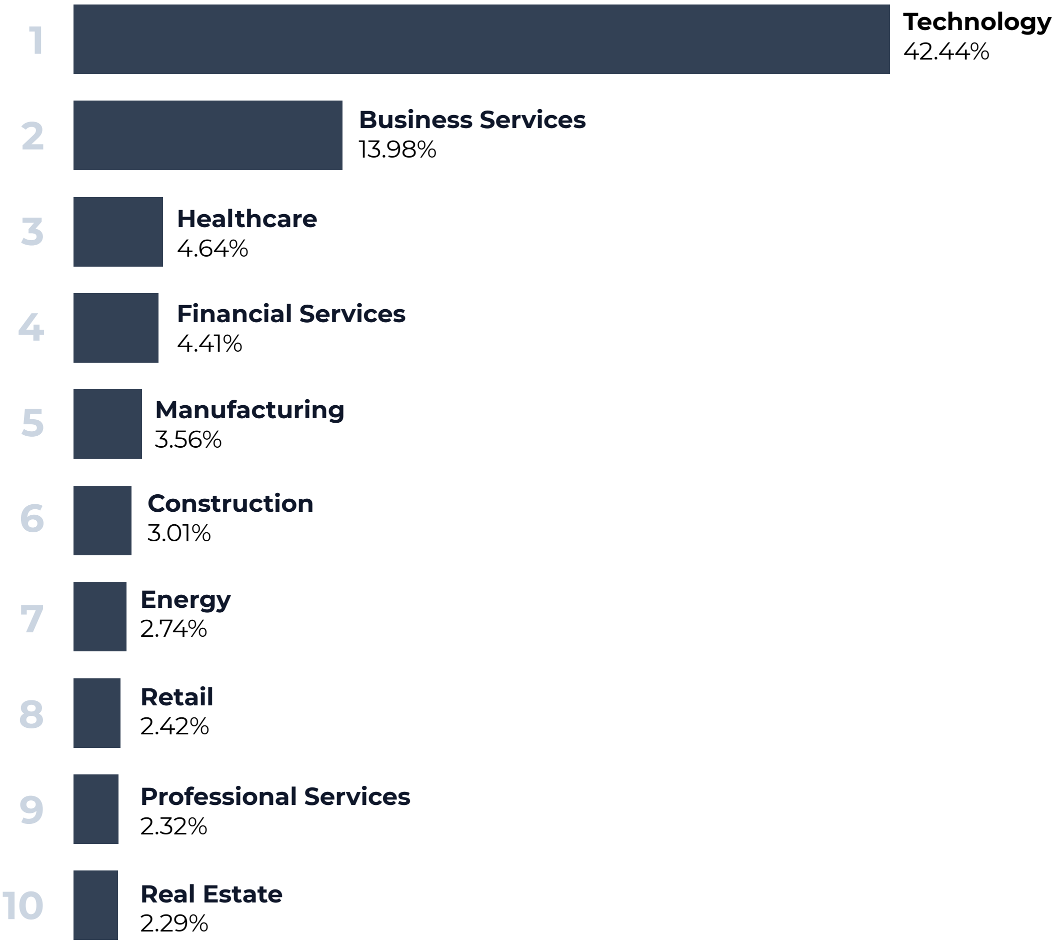
Key Trends Observed

In the following sections, you will note several trends:

- The technology sector is the most represented industry in our observations.
- VPNs are a common factor in most incidents across our top five industries.
- Initial access is the foremost tactic employed against these industries.
- Logins from high-risk countries are the primary method of initial access in these cases.

A few factors explain these trends. One, our partner base consists mostly of MSPs. Two, our SOC is adept at countering initial access tactics, often neutralizing cyberthreats at this stage. Three, the frequent occurrence of logins from risky countries as a key initial access tactic is linked to the fact that VPNs often originate from these locations, where regulations and laws are less stringent.

Percentage of Incidents by Industry



Top Threats for the Top 5 Industries

#1 INDUSTRY

Technology

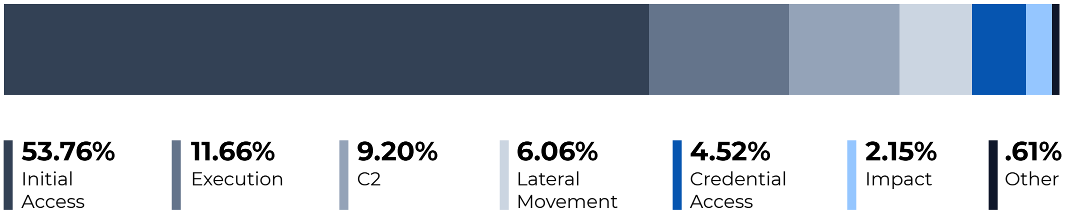
78.76%
VPN Usage
Within Incidents

Due to our partners primarily being MSPs and their customers, the technology sector is our largest and most active industry, accounting for over 40% of our total incidents. They faced more execution, C2, lateral movement, impact, and exploit threats than any other featured sector in this report. Regarding initial access tactics, they experienced the highest instances of RDP exploitation, email compromise, and phishing attempts. It is worth noting that compared to the other industries, they dealt with the smallest percentage of initial access attempts and logins from high-risk countries.

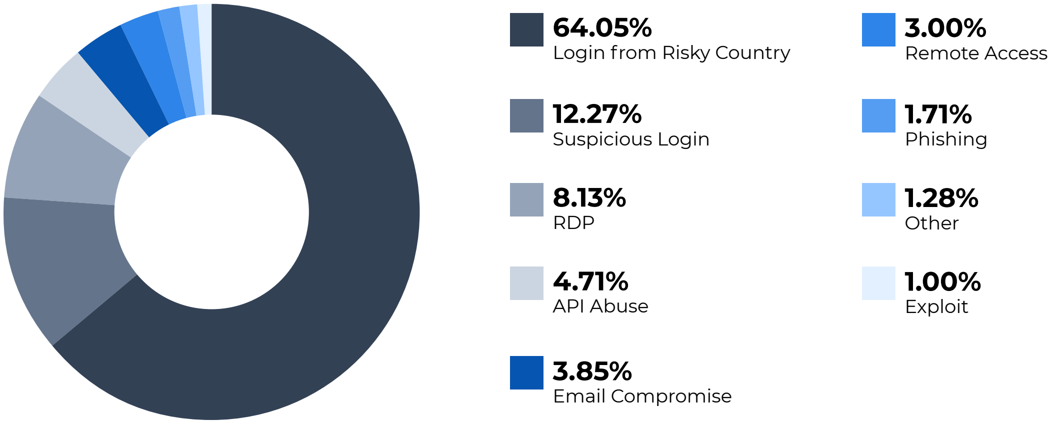
What makes them a desirable target?

- They are rich in intellectual property and cutting-edge technologies.
- They have extensive user data and proprietary information.
- They integrate networks, increasing vulnerability to systemic attacks.

Targeted Tactics



Initial Access Tactics



#2 INDUSTRY

Business Services

84.07%

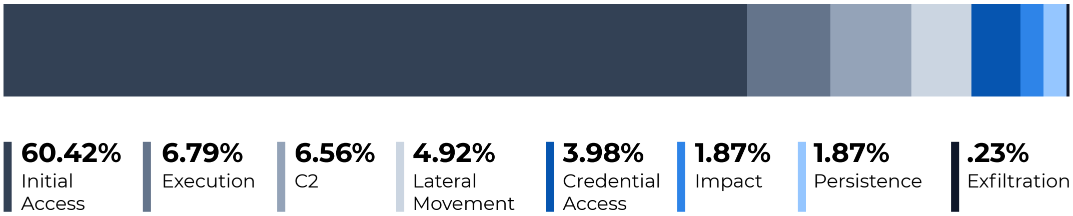
VPN Usage
Within Incidents

Business services, responsible for about 14% of incidents, encountered more initial access attempts and exfiltration attempts than technology, healthcare, financial services, or manufacturing. They also faced the most logins from high-risk countries, but the least percentage of API abuse and email compromise, compared to the other sectors.

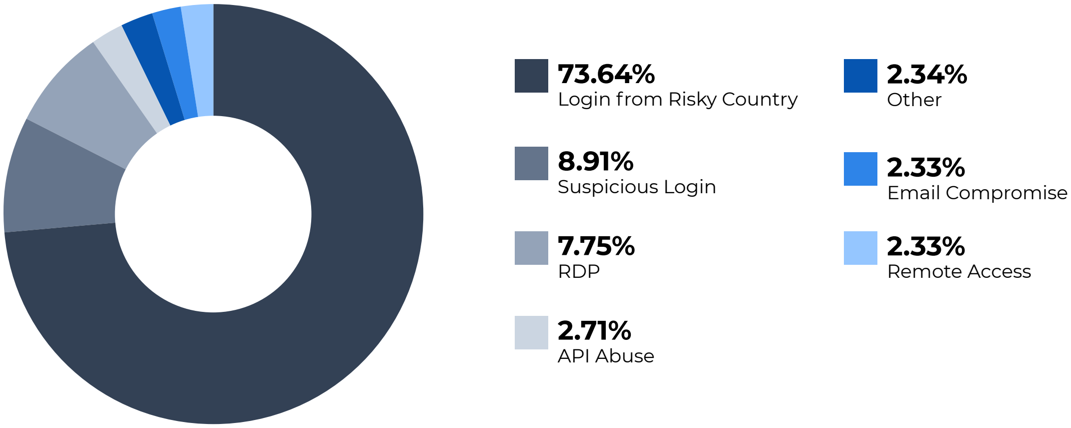
What makes them a desirable target?

- They have access to a wide range of corporate and customer data.
- They are connected to various sectors, offering broad attack surfaces.
- They house financial transactions and sensitive business information.

Targeted Tactics



Initial Access Tactics



#3 INDUSTRY

Healthcare

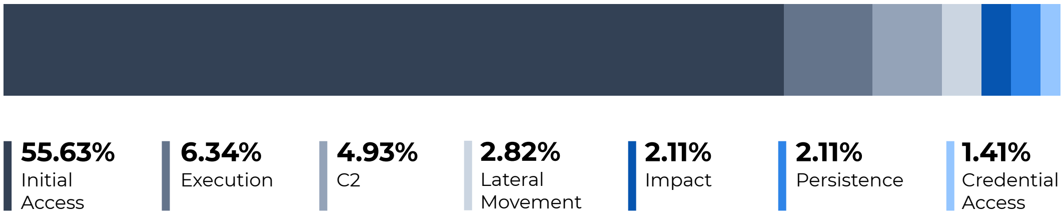
87.32%
VPN Usage
Within Incidents

Healthcare faced more persistence threats than the other four industries, but the least amount of C2 and credential access threats. Compared to the other sectors, they did not face as many phishing or exploitation attempts.

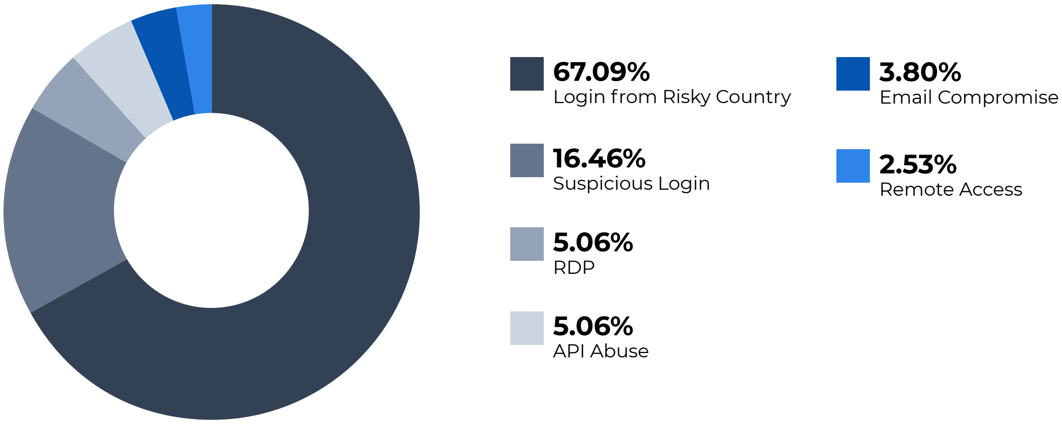
What makes them a desirable target?

- They hold sensitive personal health information.
- They are critical infrastructure yet are often under-prepared for cyberthreats.
- They house high volumes of patient data and healthcare research.

Targeted Tactics



Initial Access Tactics



#4 INDUSTRY

Financial Services

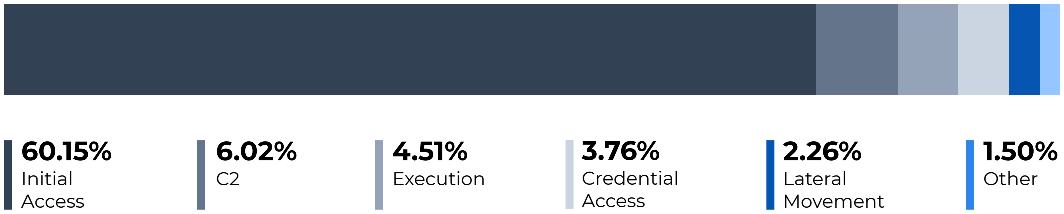
88.72%
VPN Usage
Within Incidents

The financial services industry encountered more API abuse than technology, business services, healthcare, or manufacturing. For the other sectors, it was the #4 initial access threat, but for finance, it was #2. That said, it dealt with the least amount of suspicious logins, remote access attempts, and execution attempts. In fact, C2 was a more prominent threat to them than execution, which is unique to this sector.

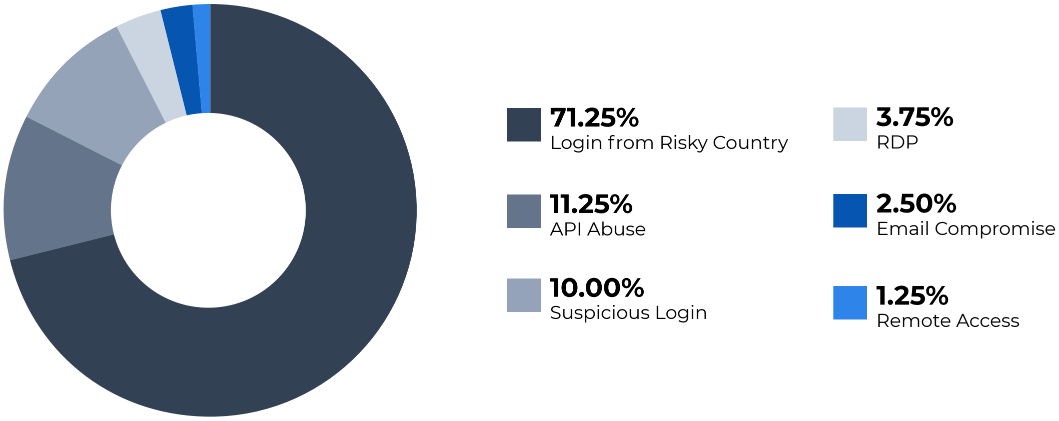
What makes them a desirable target?

- They have direct access to financial assets and transactional data.
- They house sensitive customer information.
- They are highly reliant on digital platforms, increasing cyber-risk exposure.

Targeted Tactics



Initial Access Tactics



#5 INDUSTRY

Manufacturing

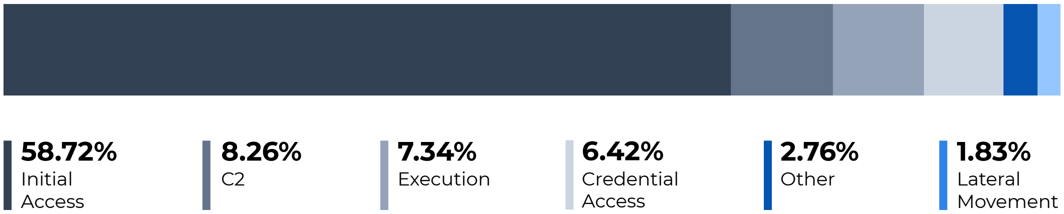
83.49%
VPN Usage
Within Incidents

Manufacturing also uniquely faced more execution threats than C2 threats. They encountered the least amount of credential access attempts, but the most threats of impact. Within initial access, they had the highest number of suspicious login and remote access attempts, but the least amount of RDP abuse. For the other four industries, remote access did not make the top three initial access tactics, but for Manufacturing, it came in third.

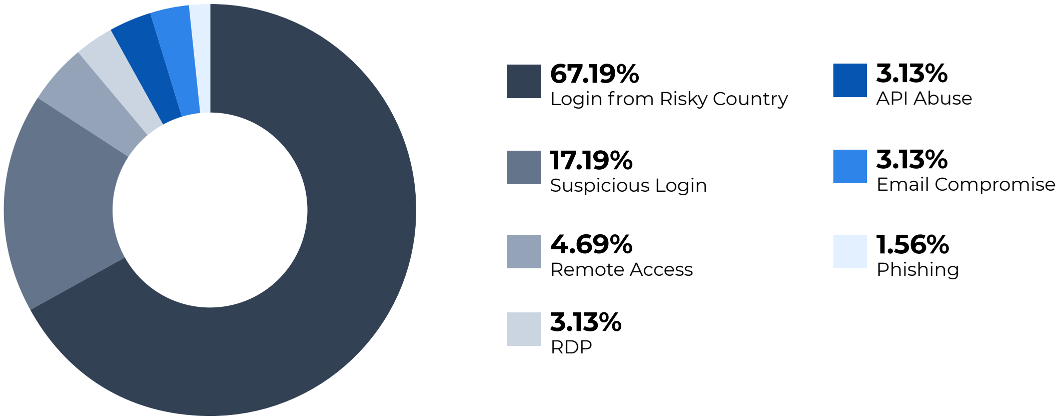
What makes them a desirable target?

- They house industrial control systems and proprietary manufacturing processes.
- They integrate with supply chains, providing multiple entry points.
- They house valuable trade secrets and operational data.

Targeted Tactics



Initial Access Tactics



In Summary

Technology, with a leading 42.44% of incidents, was the most targeted industry, reflecting the extensive digital infrastructure and valuable data that MSPs house and protect. Following technology was business services and healthcare, indicating a significant cyberthreat presence in service-oriented sectors. A notable pattern across industries is the predominance of initial access threats, underscoring the importance attackers place on gaining entry points.

Following initial access, the second and third most common threats across all five industries were execution and C2. Within initial access attempts, logins from high-risk countries were the top threat across the board. These threats are often linked with VPN abuse, which we encountered in most incidents across all five industries.

The diversity in threats thereafter highlights the customized tactics used by cybercriminals, adapting to the unique vulnerabilities of each sector. While threat actors do not discriminate, each industry must instill sector-specific cybersecurity strategies. In order to detain these common threats, all businesses must adhere to best practices, educate their users on email threats, and instill advanced detection capabilities to stop threat actors immediately.

Predictions and Preparations for 2024

Now that we have reflected on the past year's data, it is time to arm ourselves with lessons learned and prepare for the remainder of the year. In 2023, we witnessed a notable increase in cyber incidents overall, significantly focusing on initial access tactics, as well as cloud security threats. The growing number of incidents, especially from mid-year onwards, indicates cyberthreats are becoming more complex. This pattern suggests that in 2024, we may see a continued rise in advanced attacks, targeting credentials and exploiting various vulnerabilities, moving beyond VPN-related incidents. This shift underscores the evolving nature of cyberthreats and the need for adaptive defense strategies across your hybrid work environments.

In 2024, we predict to see...

Learn why Blackpoint Cyber is focusing on catching lateral movement, rather than malware, with our CEO, Jon Murchison.

TUNE IN

The Abuse of Artificial Intelligence (AI):

- Used to enhance SE attacks
- Used to create sophisticated, convincing phishing attacks and deepfake videos
- Used to make BEC appear more legitimate
- Used to build more complex, automated attacks
- Used in malware to adapt to defenses
- Used to identify and target high-value targets or exploitable vulnerabilities

The first three months of 2023 showed malware used 23.8% of the time, whereas in the last three months, it was only present in 9.7% of incidents.

An Increase in Infostealers and Malvertising:

- To increase search engine optimization (SEO) poisoning
- To disguise malware as legitimate downloads in search results

An Increase in Sophisticated Tactics:

- To deploy more covert operations using LoLBins and RMM tools
- To depend less on malware
- To increase the difficulty in detecting threat actors within IT environments

78.78%

of all incidents from December 2022 to November 2023 were cloud related.

An Upward Trend in Ransomware Operations:

- To conduct more targeted and damaging ransomware attacks
- To target a range of companies, from SMBs to Fortune 500 companies
- To deploy low-effort attacks on high-payoff targets
- To target high-risk sectors including education, healthcare, financial services, and government

Cloud and Supply Chain Attacks

- To exploit interconnected systems such MSPs with customers or cloud infrastructure
- To exploit the subsystems that complex systems depend on

In Summary

The cyberthreat landscape this year is predicted to be increasingly complex and sophisticated. AI is expected to play a pivotal role, enhancing SE attacks, creating more convincing phishing attempts, and facilitating BEC attacks. Infostealers and malvertising are likely to rise, exploiting SEO poisoning and masquerading malware in search results. The use of sophisticated tactics, like LoLBins and RMM tools, will make threat detection more challenging. Ransomware attacks are anticipated to become more targeted and damaging, potentially leveraging AI for vulnerability exploitation. We foresee a significant rise in cloud and supply chain attacks, due to their interconnected nature. This evolving threat environment underscores the need for adaptable defenses, a layered security approach, and a dedication to educating your user base.

Cybersecurity Best Practices

To properly defend against the threat actors and cyberthreats we have covered in this report, you must empower your team members and customers to adhere to cybersecurity best practices. Much of the time, cyberattacks can be stopped through simple steps, such as using unique passwords, reviewing email links, and patching for vulnerabilities as soon as possible. Below you will find our suggested best practices.

Cybersecurity Best Practices

Email and Online Security

- Raise awareness of phishing or spear-phishing attacks, which involve links or attachments.
- Raise awareness of malware incorporated into online advertisements, known as malvertising.
- Be cautious about what you share on social media platforms, especially personal information and current locations.

Data Protection

- Avoid storing passwords in web browsers.
- Enforce password complexity requirements.
- Encourage regular password changes.
- Avoid reusing passwords across accounts.
- Utilize MFA with authenticator apps, hardware tokens, or biometrics.
- Always use secure Wi-Fi connections. If in public, use a VPN or your phone's Hotspot.
- Use secure payment methods, such as a credit card or reliable third-party service.

Insider Threat Management

- Be mindful of potential insider threats.
- Manage application control and access.
- Adhere to the Principle of Least Privilege.
- Adhere to data handling best practices.

Network and System Security

- Enable automatic updates where possible.
- Implement a continuous and frequent patch plan.
- Review current configurations for misconfigurations or unauthorized changes.
- Prioritize patching once vulnerabilities are disclosed.
- Phase out older, less secure authentication methods.
- Monitor logins over proxy and VPN to bypass conditional access geoblocking.
- Maintain regular vulnerability assessments.
- Monitor logins from suspicious user agents.
- Implement Zero Trust principles.
- Enforce identity and access control.

Backup and Insurance

- Ensure critical data is backed up regularly.
- Consider obtaining cyber liability insurance for added protection.

Security Guidance

- Adhere to industry-specific compliance requirements.
- Abide by the DiD security framework.
- Follow the guidance of at least one widely recognized security frameworks.

Conclusion

The cyberthreat landscape of the past year has undeniably reinforced the critical need for vigilant, proactive, and adaptive defense strategies to combat the sophisticated and interconnected array of threats targeting organizations, including SMBs. Amidst this landscape, the role of an MDR serves as an essential ally, offering the expertise, technology, and readiness needed to protect businesses' assets and their people.

Blackpoint prides itself on our ability to provide 24/7 monitoring, advanced analytics, and threat intelligence to ensure an ever-watchful eye over the businesses you work for and protect. We reduce the window of opportunity for attackers by detecting and responding to threats swiftly and effectively, all on your behalf. This is particularly crucial in an era where the cost and scale of cyberattacks continue to escalate, and where the time to detect and respond can be the difference between a minor security incident and a significant impact to revenue, reputation, and employees' livelihood.

Moreover, the expertise and resources that Blackpoint services provide alleviates the burden on internal IT teams, allowing businesses to focus on growth and innovation while ensuring their security posture is robust, dynamic, and aligned with the latest threat landscape. The path forward is one of partnership, with MDR+R services at the helm, guiding organizations through the complexities of the modern cybersecurity landscape.

This crucial integration into your organization's cybersecurity strategy is more than a protective measure, it is a strategic decision that empowers you to navigate the digital realm with confidence and resilience.

NEXT STEPS

It's time for advanced security, informed by security experts. Keep the conversation going with the researchers behind the report. **Register for the webinar here**.

Or see how Blackpoint's comprehensive ecosystem can arm your business and customers for success.

GET STARTED

Glossary

AES: Advanced Encryption Standard

AI: Artificial intelligence

APG: Adversary Pursuit Group

API: Application Programming Interface

AV: Antivirus

BEC: Business Email Compromise

CISA: Cybersecurity and Infrastructure Security Agency

CSA: Cybersecurity Advisory

C2: Command and control

DC: Domain Controller

DiD: Defense in Depth

DLL: Dynamic Link Library

EDR: Endpoint Detection and Response

IAB: Initial Access Broker

IoC: Indicator of compromise

LotL: live-off-the-land

LoLBins: Living off the Land Binaries

MaaS: Malware-as-a-Service

MDR: Managed Detection and Response

MDR+R: Managed Detection, Response and Remediation

MFA: Multifactor authentication

MS-ISAC: Multi-State Information Sharing and Analysis Center

MSP: Managed Service Provider

NSA: National Security Agency

OS: Operating system

OSINT: Open-source intelligence

RaaS: Ransomware-as-a-Service

RCE: Remote code execution

RDP: Remote Desktop Protocol

RMM: Remote Monitoring and Management

SaaS: Software-as-a-Service

SE: Social engineering

SEO: Search engine optimization

SOAP: Simple Object Access Protocol

SSO: Single sign-on

SMBs: Small- and medium-sized businesses

SOC: Security Operations Center

TTPs: Tactics, techniques, and procedures

VPN: Virtual private network

WMI: Windows management instrumentation

Contributors

David Rushmer, Director of Threat Research

CONNECT WITH DAVID ON LINKEDIN.

Derick Peterson, Threat Analyst

CONNECT WITH DERICK ON LINKEDIN.

Robert Russell, Senior Director of Threat Operations

CONNECT WITH ROBERT ON LINKEDIN.

Alyssa Reed, Senior Content Writer

CONNECT WITH ALYSSA ON LINKEDIN.