ANNUAL

Threat Hunting Report

24

SentinelOne

Table of Contents

Letter From The Editor

Another year of unrelenting activity on the cyber front has ended. In 2024, we witnessed major events—the Paris Olympics, the reverberations of the July 19th Crowd2K outage, high-profile global elections—and with those came a surge in attacks from both state-sponsored and criminal actors. These adversaries challenged organizations worldwide, targeting critical infrastructure, intellectual property, and personal data. Despite the unending nature of these threats, SentinelOne's Threat Discovery and Response services remain committed to providing 24/7 real-time threat hunting, risk assessments, and immediate response.

In this annual threat hunting report, we highlight the most impactful trends observed in 2024:

A New Paradigm in Chinese State-Sponsored Activity: While "Volt Typhoon" initially drew attention, the broader shift toward operational relay box (ORB) networks and living-off-the-land techniques has reshaped our understanding of Chinese threat actors. Groups such as Salt Typhoon, Gallium, HAFNIUM, and APT41 now rely on stealthier methods— targeting internet-facing appliances (Cisco, Fortinet, Citrix, Ivanti) and blending into legitimate network traffic.

The Com Rises to the Top Among Cybercriminals: Loosely affiliated hackers under "The Com" banner superseded many traditional ransomware crews by using SIM-swaps, social engineering (vishing, smishing), and compromised cloud credentials to infiltrate victims. They also collaborated with ransomware operators, enriching their capabilities and impact.

Evolving Ransomware Landscape: While LockBit dominated 2023, Akira emerged as this year's most prolific ransomware group, followed by Play and BlackSuit. Our "Ransomware Group Risk Matrix" tracks the rise of new families like Orca and RansomHub, as well as the decline of formerly dominant actors.

For the first time, we are excited to include insights from our sister teams for added perspective on how to respond to this evolving threat landscape:

The SentinelOne Incident Response team provides in-depth case studies illustrating real-world breaches—from VPN appliance zero-days to data theft via JIRA plugins—and highlights common pitfalls, including missed detections and lax network segmentation.

PinnacleOne offers a snapshot of key geopolitical risks, explaining how state conflict, critical infrastructure sabotage, and disinformation campaigns shaped the cyber environment of 2024.

We also underscore the top recurring concerns for CISOs: asset inventory, identity and access management, SOC burnout, secure product development, and detection engineering.

In 2024, WatchTower published 188 Flash reports, covering more than 1,000 queries spanning new ransomware families, infostealers, and recurring vulnerabilities—effectively keeping our clients ahead of the evolving threat landscape. We hope this report provides deeper insight into 2024's most significant cyber events and empowers you to fortify your defenses for the challenges ahead.

We look forward to defeating new threats and challenges alongside our customers in 2025.

The WatchTower Threat Hunting Team

WatchTower

2024 WatchTower Recap

Throughout 2024, WatchTower maintained its relentless pursuit of adversaries, publishing 188 Flash reports—an average of more than one every two days—and sharing over 1000 enriched hunting queries with our customers. Our most frequently reported threats were emerging ransomware families and new infostealer activity across Windows, macOS and Linux platforms. We expand on this in the sections below.

WatchTower threat hunters also encountered and reported on the abuse of legitimate software by threat actors over a dozen times in the last 12 months. In addition, we reported on multiple vulnerabilities and exploits throughout the year, keeping our customers appraised of known exploited vulnerabilities including:

CVE-2024-21591	Akira Abuses Juniper VPN without MFA For Intrusion
CVE-2024-27199	JetBrains TeamCity Security
CVE-2024-29847	Ivanti EPM Deserialization RCE CVE-2024-29847
CVE-2024-3094	Backdoored XZ Utils
CVE-2024-38112	Zero-Day Exploits Targeting Internet Explorer
CVE-2024-4978	Backdoored Justice AV Solutions Viewer Software Supply Chain
CVE-2024-6368	OpenSSH regreSSHion Vulnerability

Most Impactful Threat Actors of 2024

A New Paradigm for Chinese State Sponsored Threat Actors

Multiple Chinese threat actors have embraced a new paradigm for conducting their operations in a way that's baffling defenders of all calibers. Their tradecraft now more closely resembles the old-school style of 'hands-on-keyboard' operations, leveraging Living-off-the-Land (LotL) techniques, and relying on non-attribution networks to remain ephemeral.

Notable examples include Volt Typhoon/BRONZE SILHOUTTE, Salt Typhoon, Gallium (Operation Tainted Love), HAFNIUM, and APT41. These threat actors systematically target critical infrastructure sectors across the United States, Europe, Africa, and Asia to further Chinese strategic military and intelligence objectives.

ORB (Operational Relay Boxes) networks are also heavily utilized by these threat actors. These networks are often composed of a blend of servers across different cloud service providers and hacked Small Office/Home Office (SOHO) routers. The latter allow the operators to exit these covert networks through a residential proxy located in the target country –avoiding immediate suspicion based on regional source or known infrastructure blocking– and the changing composition of the network means that they can change their egress node frequently to further avoid identification.

An additional crucial component enabling their operations is the abuse of vulnerable internet-facing appliances. By exploiting a steady stream of unknown (or known and unpatched) vulnerabilities across Cisco, Fortinet, Citrix, and Ivanti devices, these threat actors establish an initial foothold into target networks with little chance of detection.

Putting all of these elements together, high end Chinese-aligned threat actors have established a nightmarish operational playbook whereby they can traverse a practically untraceable relay network, egress from a reputation-neutral residential node within the target country, hack an internet-facing appliance to establish an unmonitored beachhead in the target network, and from there execute 'hands-on-keyboard' commands to orchestrate existing (LotL) resources to conduct espionage and even enable military objectives for wartime prepositioning.

The Com (UNC3944) | Loosely-Affiliated Hacker Group Rises to the Top Tier of Cybercrime

'The Com' is a large, loosely affiliated group of cyber criminals linked to numerous high-profile breaches and a variety of illicit activities.

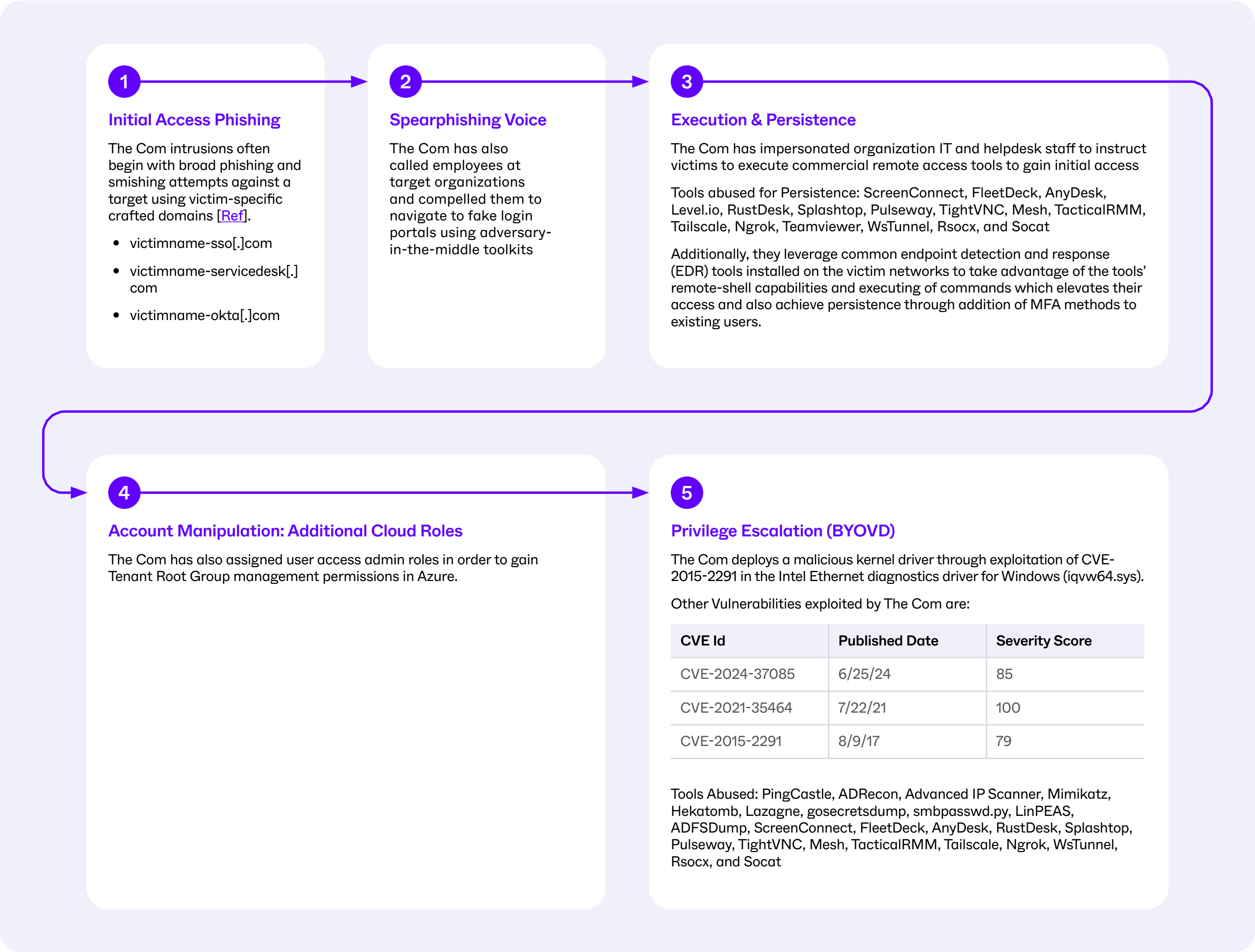
The group's tactics are far from sophisticated, often involving social engineering techniques like vishing and smishing to trick IT service desks into unwittingly facilitating access to enterprise resources. By impersonating legitimate employees, members of The Com manage to bypass Multi-Factor Authentication (MFA), modify settings, and direct victims to fraudulent login portals.

The group exploits stolen credentials obtained from underground markets, carries out SIM swap attacks, and uses hardcoded cloud authentication tokens leaked from repositories like GitHub to infiltrate cloud systems with the help of automated tools.

The Com also utilizes legitimate cloud-native tools to maintain persistence, making their activities harder to detect. Recently, they added Qilin ransomware to their arsenal and partnered with the RansomHub ransomware group. This cybercrime group serves as an umbrella term for associated groups like Oktapus, StarFraud, and the earlier Lapsus$.

Com-associated threat actors were behind the Snowflake attack campaign which came to light in 2024. This financially-motivated attack affected nearly 200 companies (customers of Snowflake's services). Attackers leveraged compromised credential sets (harvested from Infostealer logs), paired with aggressive social engineering to carry out the attack.

Actors within The Com strategically exploit both technological and human vulnerabilities, highlighting the critical need for robust defenses, such as hardened authentication mechanisms, cloud security audits, and employee awareness training.



1

Initial Access Phishing

The Com intrusions often begin with broad phishing and smishing attempts against a target using victim-specific crafted domains [Ref].

- victimname-sso[.]com
- victimname-servicedesk[.]com
- victimname-okta[.]com

2

Spearphishing Voice

The Com has also called employees at target organizations and compelled them to navigate to fake login portals using adversary-in-the-middle toolkits

3

Execution & Persistence

The Com has impersonated organization IT and helpdesk staff to instruct victims to execute commercial remote access tools to gain initial access

Tools abused for Persistence: ScreenConnect, FleetDeck, AnyDesk, Level.io, RustDesk, Splashtop, Pulseway, TightVNC, Mesh, TacticalRMM, Tailscale, Ngrok, Teamviewer, WsTunnel, Rsocx, and Socat

Additionally, they leverage common endpoint detection and response (EDR) tools installed on the victim networks to take advantage of the tools' remote-shell capabilities and executing of commands which elevates their access and also achieve persistence through addition of MFA methods to existing users.

4

Account Manipulation: Additional Cloud Roles

The Com has also assigned user access admin roles in order to gain Tenant Root Group management permissions in Azure.

5

Privilege Escalation (BYOVD)

The Com deploys a malicious kernel driver through exploitation of CVE-2015-2291 in the Intel Ethernet diagnostics driver for Windows (iqvw64.sys).

Other Vulnerabilities exploited by The Com are:

CVE Id	Published Date	Severity Score
CVE-2024-37085	6/25/24	85
CVE-2021-35464	7/22/21	100
CVE-2015-2291	8/9/17	79

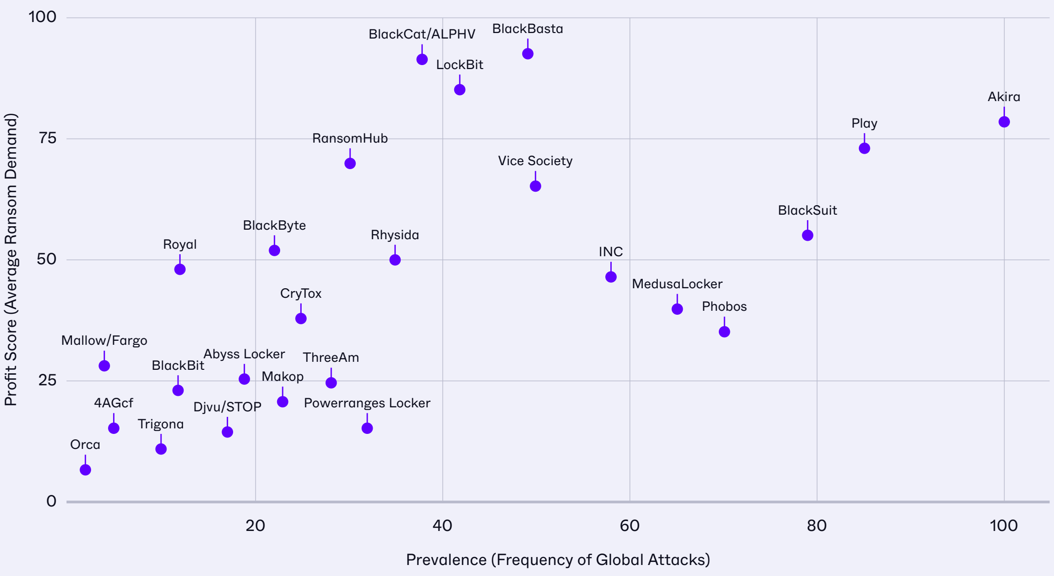
Tools Abused: PingCastle, ADRecon, Advanced IP Scanner, Mimikatz, Hekatomb, Lazagne, gosecretsdump, smbpasswd.py, LinPEAS, ADFSDump, ScreenConnect, FleetDeck, AnyDesk, RustDesk, Splashtop, Pulseway, TightVNC, Mesh, TacticalRMM, Tailscale, Ngrok, WsTunnel, Rsocx, and Socat

Top Ransomware Groups of 2024

WatchTower continued to track threat actors across the ransomware landscape throughout 2024. The Ransomware Threat Matrix below, based on public reporting, shows the prevalence (frequency of global attacks) and the profit score (average ransom demand).

This is the third year we have produced this matrix, and it is interesting to see how dramatically the threat landscape changes year over year. In 2023, LockBit was the most prevalent ransomware, but it was heavily-impacted by an FBI-led international coalition of law enforcement resulting in LockBit being reduced to a mid-level actor in 2024.

2024 Ransomware Group Risk Matrix



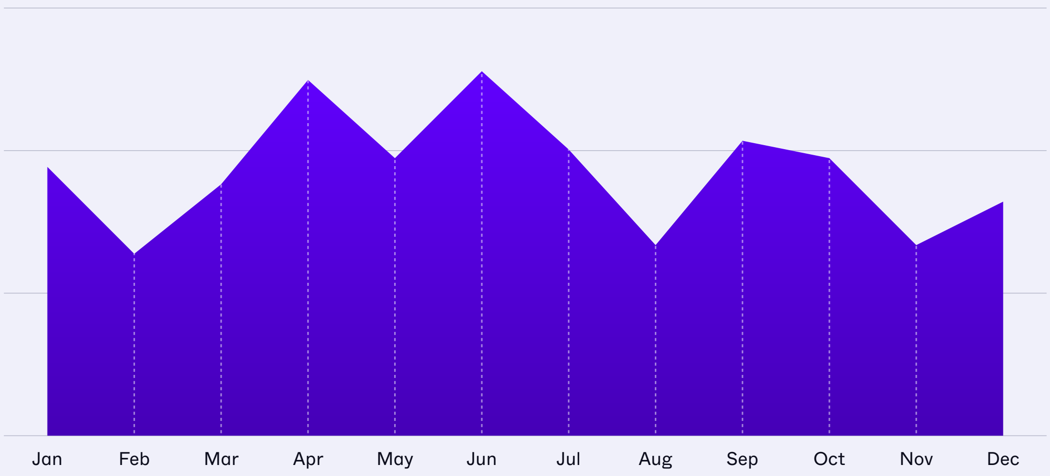
Top groups seen in 2024 in SentinelOne's telemetry were Akira by a significant margin, followed by Play, and then BlackSuit. Several ransomware groups that made the list in the previous year were barely active or entirely missing, while other families, such as Orca and RansomHub, made their first appearance in the matrix this year.

2024 Monthly Ransomware Activity

The intensity of ransomware activity varied throughout the year, with marked peaks and troughs as campaigns gathered or ran out of steam.

April and June were the busiest months for ransomware incidents while February and August were significantly slower. Even so, the data clearly shows that cybercriminals were constantly at work, attacking organizations through every month of year.

2024 Ransomware Monthly Activity (All Threat Actors)

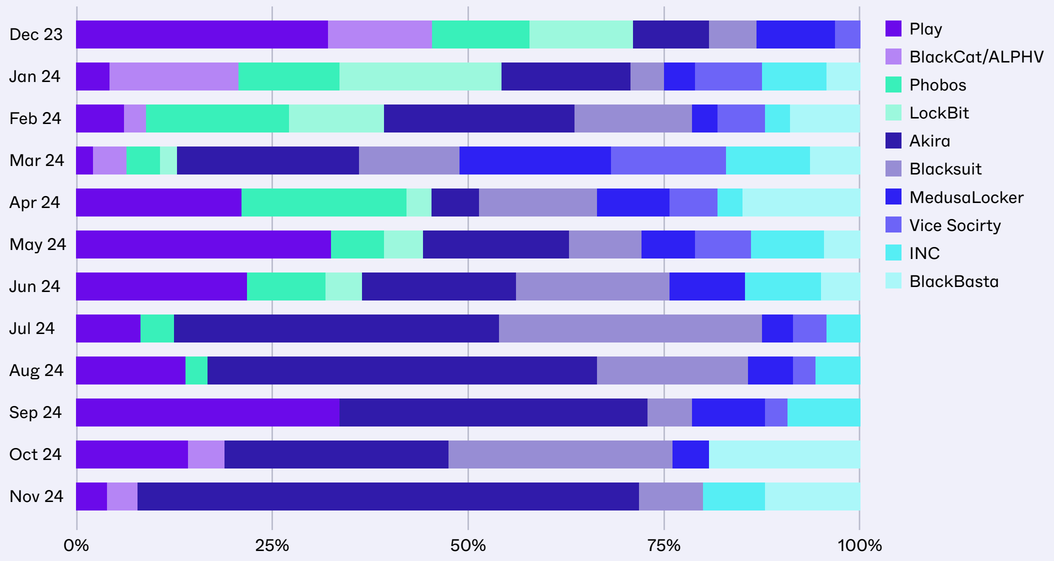


Based on telemetry across the SentinelOne customer base, the following ransomware threats were the most frequently detected in 2024:

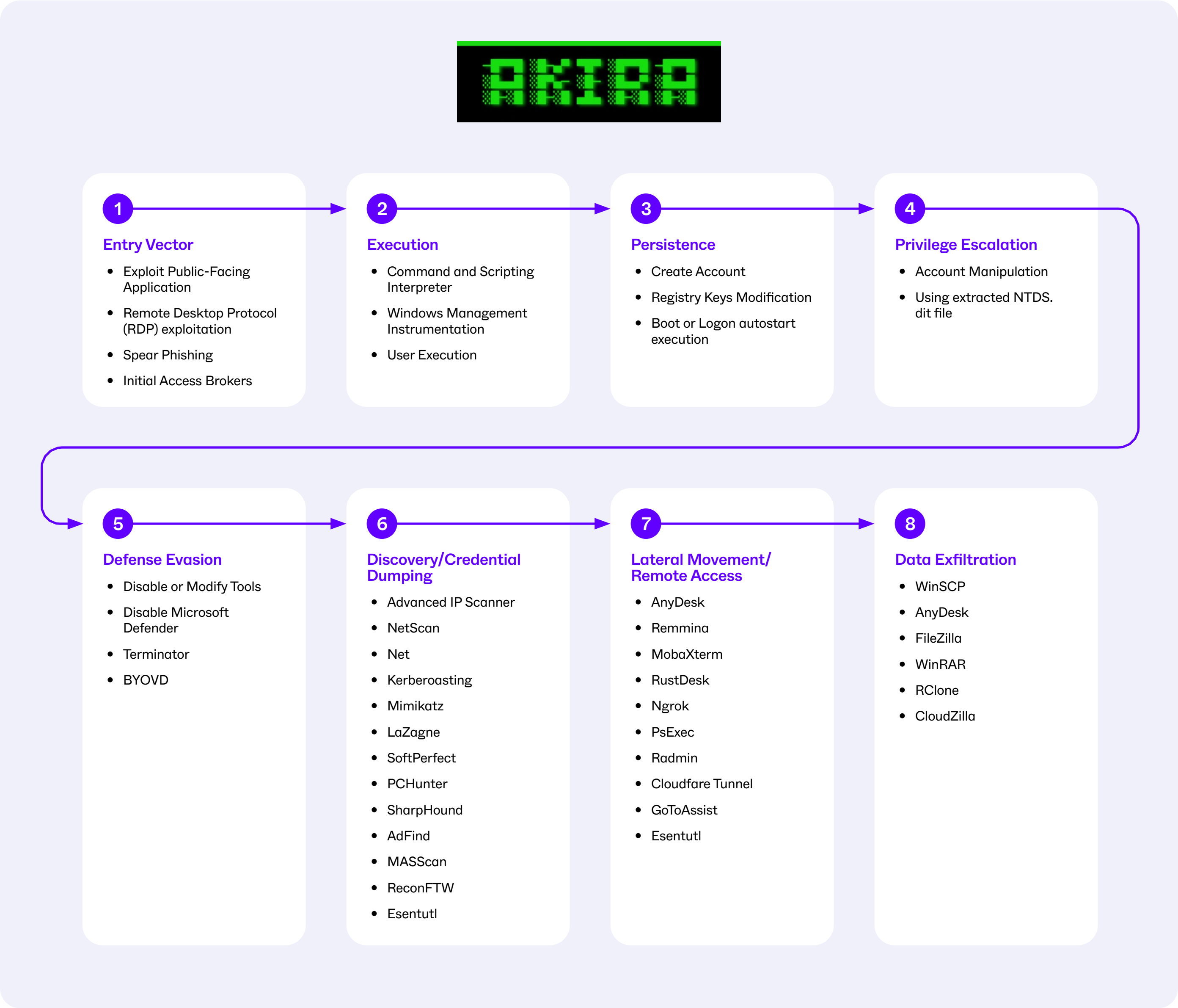
1. Akira
2. Play
3. Blacksuit
4. Phobos/8Base
5. MedusaLocker
6. INC
7. Black Basta
8. Vice Society
9. LockBit
10. BlackCat/AlphV

Examining the monthly activity of the top ten threat actors reveals activity density and sometimes the seasonality of each group. Play, for example, had a light spring but was very active throughout summer and fall. Conversely, BlackCat/AlphV was very active in fall but very dormant in April - this is likely linked to the FBI takedown of their infrastructure in December of 2023. BlackCat/AlphV was one of the most prolific groups of 2023, but their clash with law enforcement likely led to the last vestiges of their operations through the following spring, when we stopped seeing any activity from them, other than a small blip in October of '24.

2024 Ransomware Group Monthly Activity



A Kill Chain View of the Top 3 Active Ransomware Groups



AKIRA

1 Entry Vector

- Exploit Public-Facing Application
- Remote Desktop Protocol (RDP) exploitation
- Spear Phishing
- Initial Access Brokers

2 Execution

- Command and Scripting Interpreter
- Windows Management Instrumentation
- User Execution

3 Persistence

- Create Account
- Registry Keys Modification
- Boot or Logon autostart execution

4 Privilege Escalation

- Account Manipulation
- Using extracted NTDS. dit file

5 Defense Evasion

- Disable or Modify Tools
- Disable Microsoft Defender
- Terminator
- BYOVD

6 Discovery/Credential Dumping

- Advanced IP Scanner
- NetScan
- Net
- Kerberoasting
- Mimikatz
- LaZagne
- SoftPerfect
- PCHunter
- SharpHound
- AdFind
- MASScan
- ReconFTW
- Esentutl

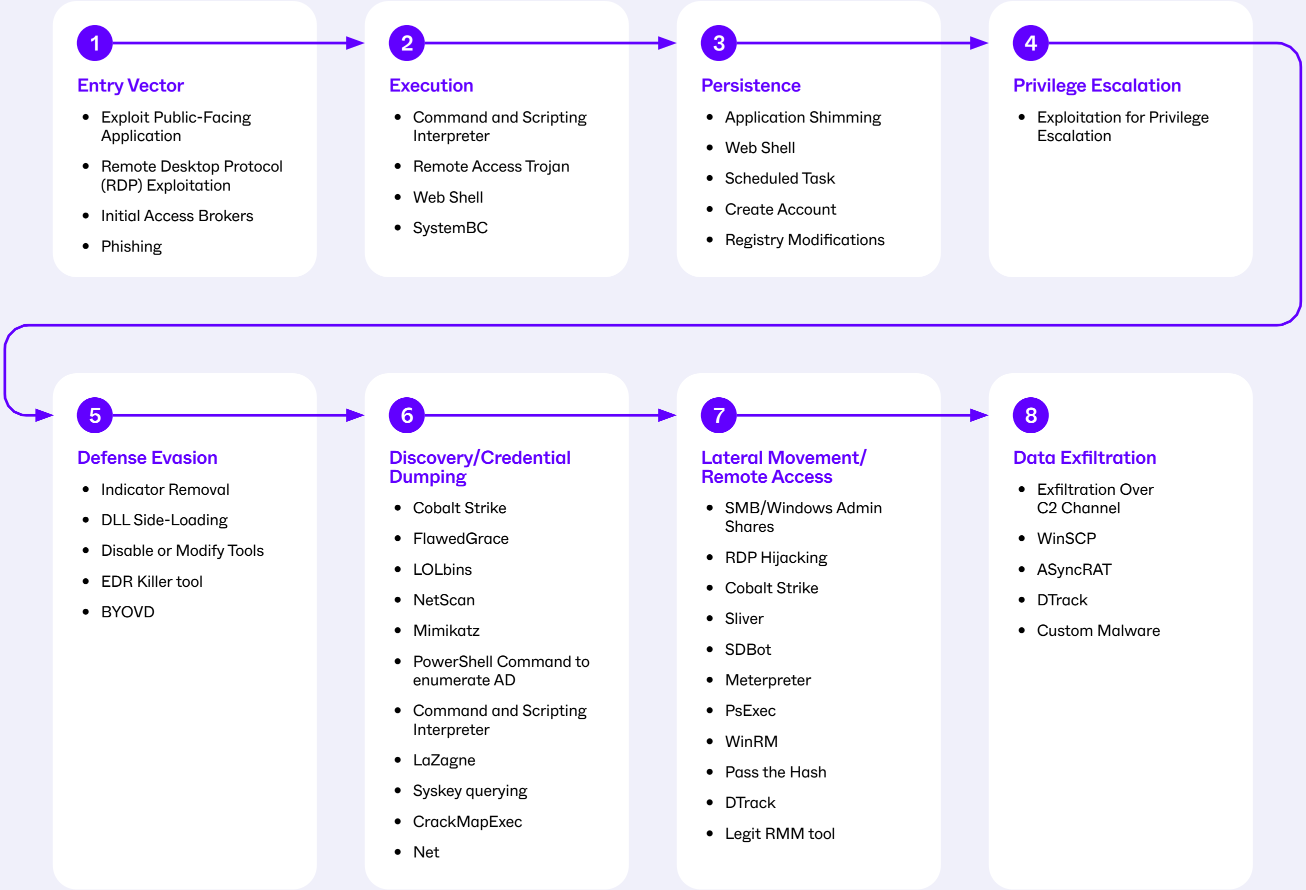
7 Lateral Movement/ Remote Access

- AnyDesk
- Remmina
- MobaXterm
- RustDesk
- Ngrok
- PsExec
- Radmin
- Cloudfare Tunnel
- GoToAssist
- Esentutl

8 Data Exfiltration

- WinSCP
- AnyDesk
- FileZilla
- WinRAR
- RClone
- CloudZilla

PLAY



1 Entry Vector

- Exploit Public-Facing Application
- Remote Desktop Protocol (RDP) Exploitation
- Initial Access Brokers
- Phishing

2 Execution

- Command and Scripting Interpreter
- Remote Access Trojan
- Web Shell
- SystemBC

3 Persistence

- Application Shimming
- Web Shell
- Scheduled Task
- Create Account
- Registry Modifications

4 Privilege Escalation

- Exploitation for Privilege Escalation

5 Defense Evasion

- Indicator Removal
- DLL Side-Loading
- Disable or Modify Tools
- EDR Killer tool
- BYOVD

6 Discovery/Credential Dumping

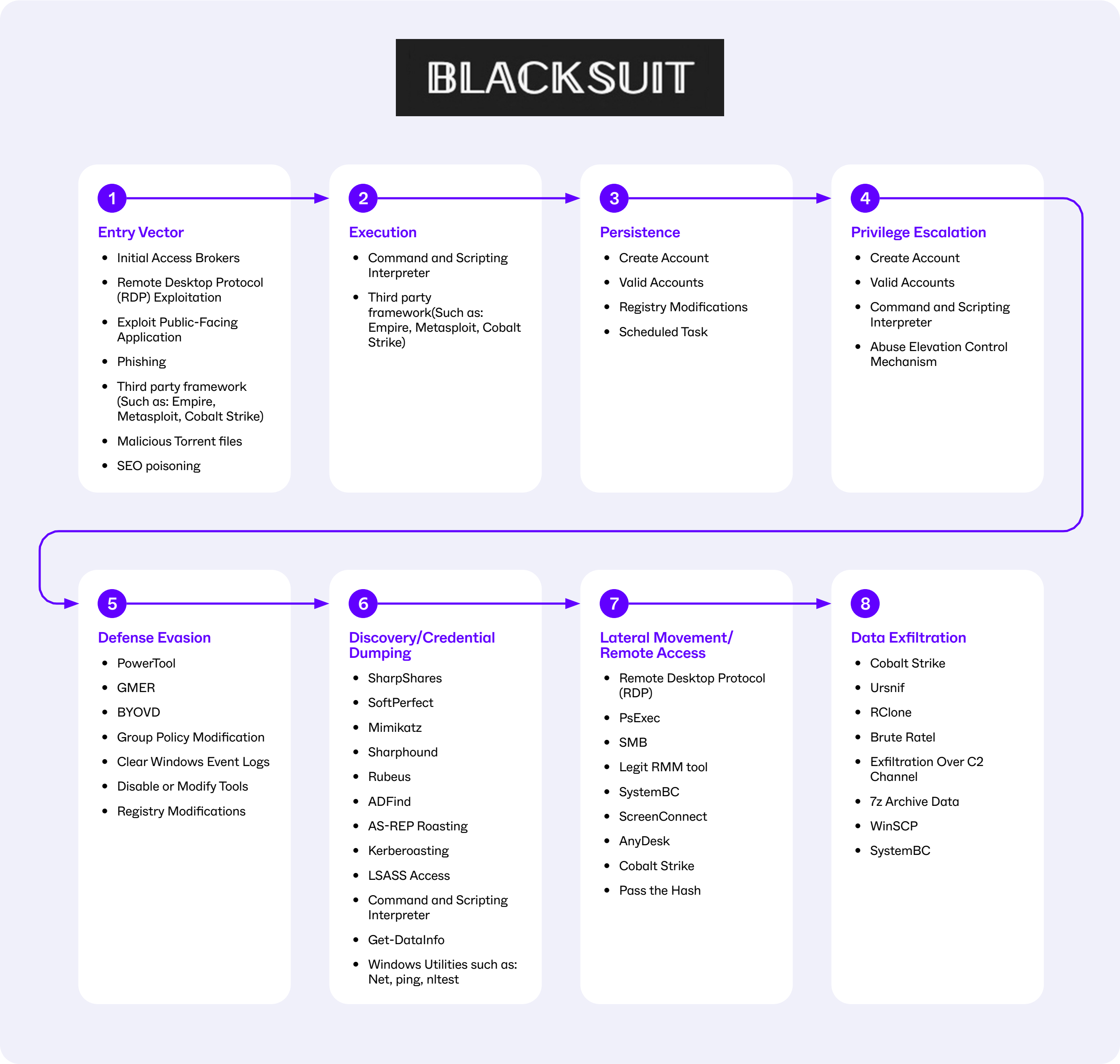
- Cobalt Strike
- FlawedGrace
- LOLbins
- NetScan
- Mimikatz
- PowerShell Command to enumerate AD
- Command and Scripting Interpreter
- LaZagne
- Syskey querying
- CrackMapExec
- Net

7 Lateral Movement/ Remote Access

- SMB/Windows Admin Shares
- RDP Hijacking
- Cobalt Strike
- Sliver
- SDBot
- Meterpreter
- PsExec
- WinRM
- Pass the Hash
- DTrack
- Legit RMM tool

8 Data Exfiltration

- Exfiltration Over C2 Channel
- WinSCP
- ASyncRAT
- DTrack
- Custom Malware



BLACKSUIT

1 **Entry Vector**

- Initial Access Brokers
- Remote Desktop Protocol (RDP) Exploitation
- Exploit Public-Facing Application
- Phishing
- Third party framework (Such as: Empire, Metasploit, Cobalt Strike)
- Malicious Torrent files
- SEO poisoning

2 **Execution**

- Command and Scripting Interpreter
- Third party framework(Such as: Empire, Metasploit, Cobalt Strike)

3 **Persistence**

- Create Account
- Valid Accounts
- Registry Modifications
- Scheduled Task

4 **Privilege Escalation**

- Create Account
- Valid Accounts
- Command and Scripting Interpreter
- Abuse Elevation Control Mechanism

5 **Defense Evasion**

- PowerTool
- GMER
- BYOVD
- Group Policy Modification
- Clear Windows Event Logs
- Disable or Modify Tools
- Registry Modifications

6 **Discovery/Credential Dumping**

- SharpShares
- SoftPerfect
- Mimikatz
- Sharphound
- Rubeus
- ADFind
- AS-REP Roasting
- Kerberoasting
- LSASS Access
- Command and Scripting Interpreter
- Get-DataInfo
- Windows Utilities such as: Net, ping, nltest

7 **Lateral Movement/ Remote Access**

- Remote Desktop Protocol (RDP)
- PsExec
- SMB
- Legit RMM tool
- SystemBC
- ScreenConnect
- AnyDesk
- Cobalt Strike
- Pass the Hash

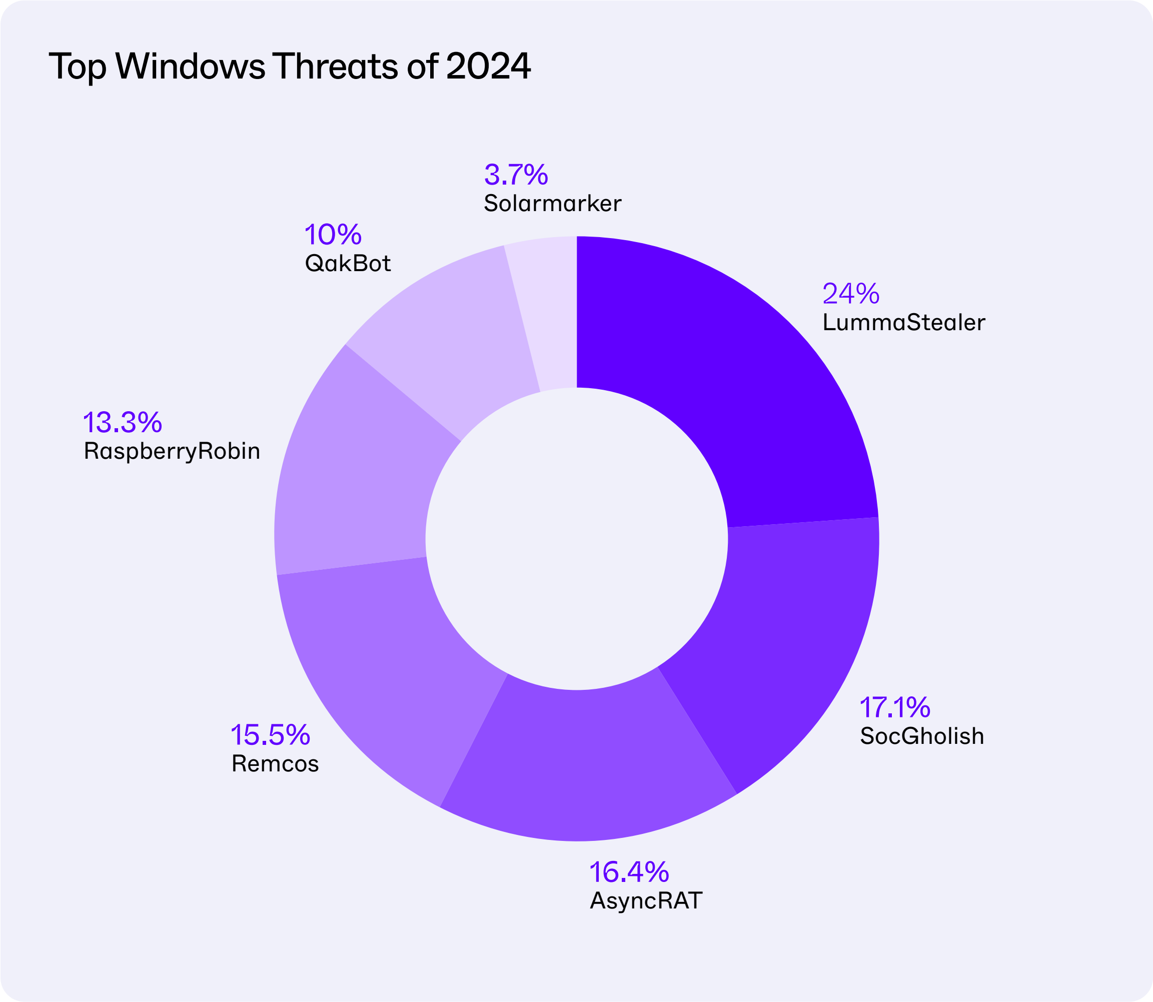
8 **Data Exfiltration**

- Cobalt Strike
- Ursnif
- RClone
- Brute Ratel
- Exfiltration Over C2 Channel
- 7z Archive Data
- WinSCP
- SystemBC

Top Threats of 2024 by Operating System

In this section, we summarize the most active threats seen across our telemetry during 2024 for the three most popular business operating systems, Windows, macOS and Linux.

Windows



1 | LummaStealer

An infostealer sold on dark web forums since 2022, targets cryptocurrency wallets, browser extensions, and 2FA to steal sensitive data. It is distributed via fake websites and malvertising, employs PowerShell and DLL sideloading to compromise legitimate processes through Process Doppelgänging.

2 | SocGholish

A JavaScript-based framework active since 2017, leverages social engineering to deceive users into running malicious JavaScript disguised as critical system updates. A recent SocGholish attack featured Python-based malware, involved a LockBit Green intrusion, and deployed BitRAT by bypassing Mark-of-the-Web controls.

3 | AsyncRAT

An open-source trojan distributed via spear-phishing and malvertising, used to steal credentials, cryptocurrency wallets, and financial data. Recent attacks employed the Screenconnect client to execute malicious scripts and evade detection, with AsyncRAT also being downloaded from AWS.

4 | Remcos RAT

A remote control tool popular since 2018, is sold on underground forums and used in high-profile attacks. It uses malicious VBScript for anti-analysis checks and AMSI bypass, with a C++ crypter embedding the loader. In July 2024, threat actors targeting the LATAM region used the CrowdStrike outage as a social engineering lure, resulting in the widespread deployment of Remcos RAT.

5 | Raspberry Robin

A worm that spreads via external devices and uses the legitimate Windows installer msiexec.exe to download a malicious DLL from a C2 server. Infections occur through ZIP packages executed via DLL sideloading, downloaded from a Discord C2 server.

6 | SolarMarker

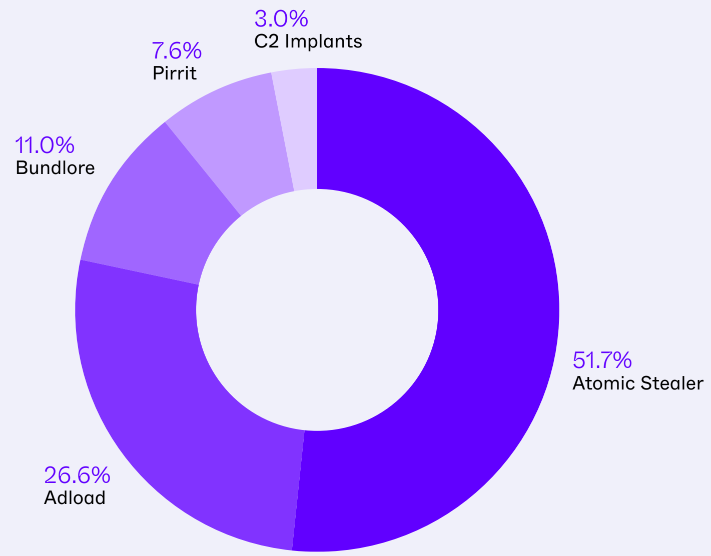
An information stealer and backdoor that spreads via SEO techniques and fake browser updates. It has targeted many U.S. organizations, exfiltrating autofill data, saved passwords, and credit card information. To evade detection, it uses signed files and large installers to impersonate legitimate software while obfuscating its code.

7 | Qakbot

A long-standing global threat that steals financial data and uses C2 servers for payload targeting and downloading. Recent activity includes injecting into curl to download the main loader's configuration file, abusing LOLbins to evade detection, and using JavaScript and Mshta.exe to execute payloads. Qakbot infections have been associated with large-scale ransomware/extortion operations, including Black Basta, and Knight.

macOS

Top macOS Threats of 2024



1 | Atomic Stealer

By far the most common threat seen across our telemetry, Atomic Stealer (aka Amos, SOMA) has a number of variants, variously tracked as Banshee, Cthulu, and Poseidon in public reporting, This infostealer can grab account passwords, browser data, session cookies, and crypto wallets.

2 | AdLoad

AdLoad is one of several adware platforms afflicting macOS users that remains prevalent across the years. It has shown no signs of slowing down throughout 2024.

3 | Bundlore

In a similar vein, Bundlore is a perennial threat that has been around in one form or another since at least 2015. Though categorized as adware, Bundlore has many features associated with more traditional backdoors.

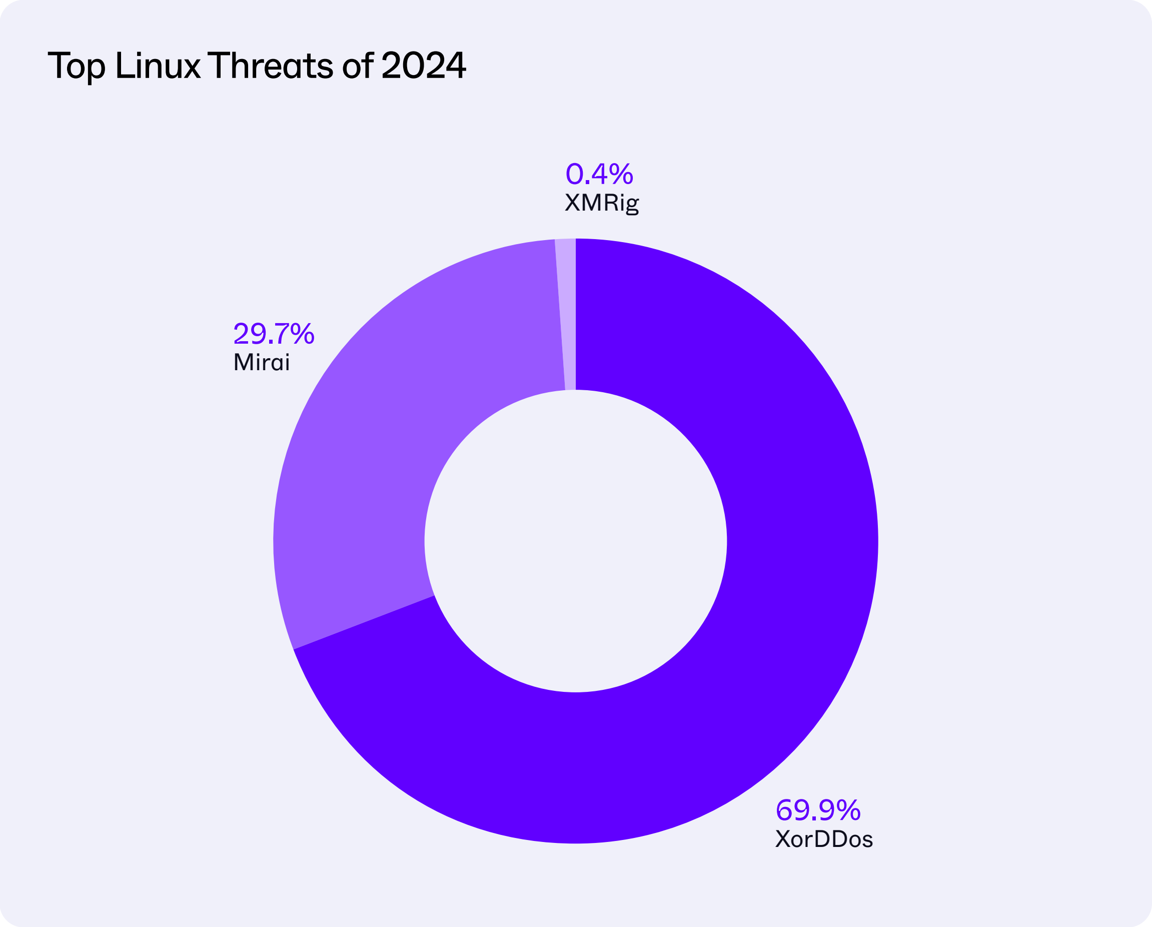
4 | Pirrit

Pirrit is an adware and browser hijacker with the aim of making money through search engine redirections. It remains prevalent in 2024 despite going largely under the radar in public reporting in recent years.

5 | C2 Implants

Increasingly common, and increasingly cross-platform, C2 implants include Command and Control (C2) payloads for popular 'red teaming' and 'offensive security' frameworks like Metasploit, Sliver, Cobalt Strike, and Mythic.

Linux



1 | XorDDos

XORDDoS is a Linux Trojan with rootkit capabilities, designed to execute large-scale distributed denial-of-service (DDoS) attacks. The malware derives its name from its extensive use of XOR encryption to obfuscate both its payload and communication with command-and-control (C&C) servers. It is compatible with multiple Linux architectures, including ARM, x86, and x64.

2 | Mirai

Throughout 2024, Mirai remained one of the most widely observed and dangerous botnets., Mirai initially gained infamy for its role in the massive DDoS attack of 2016, which took down major websites like Twitter, Reddit, and Netflix. Known for exploiting IoT devices to launch large-scale distributed DDoS attacks, Mirai continues to evolve. Researchers in 2024 have reported several variants of Mirai, including Corona, NOSEDIVE, Moobot, and Rimasuta.

3 | XMRig Cryptominer

XMRig is a cryptocurrency mining software that malicious actors can utilize to mine digital currencies. The malware was first observed in 2017, and continues to dominate the malicious-cryptominer space (targeting Linux-based systems). Miner malware can consume a substantial portion of a computer's CPU and GPU power, potentially using up to 80% of these resources. As a result, the affected computer may experience slower performance, freezing, and overheating. In 2024, we identified that threat actors deployed the XMRig cryptominer by exploiting Java, specifically jdk1.8.0_171.

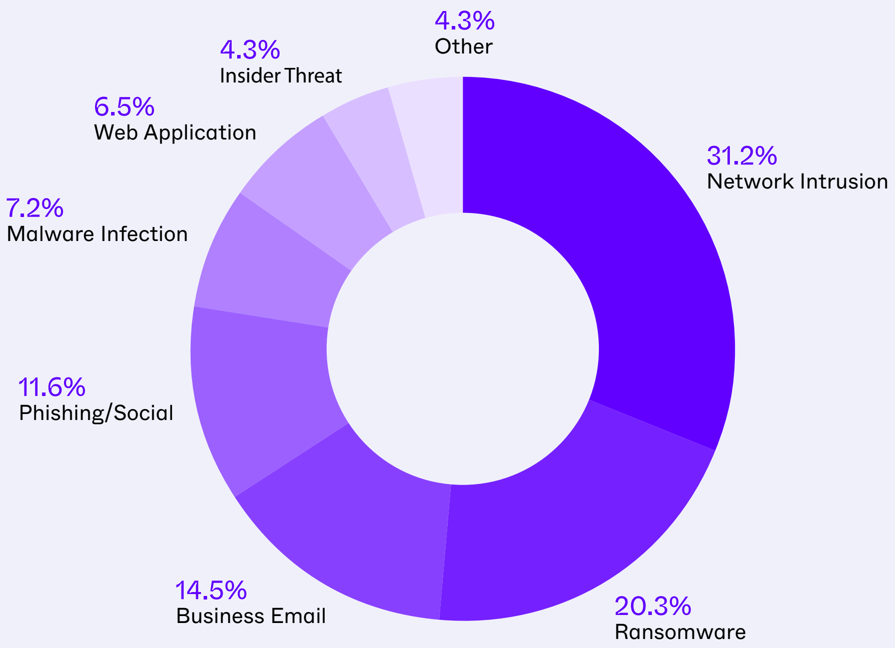
Digital Forensics and Incident Response (DFIR)

A Year of Investigations with SentinelOne DFIR

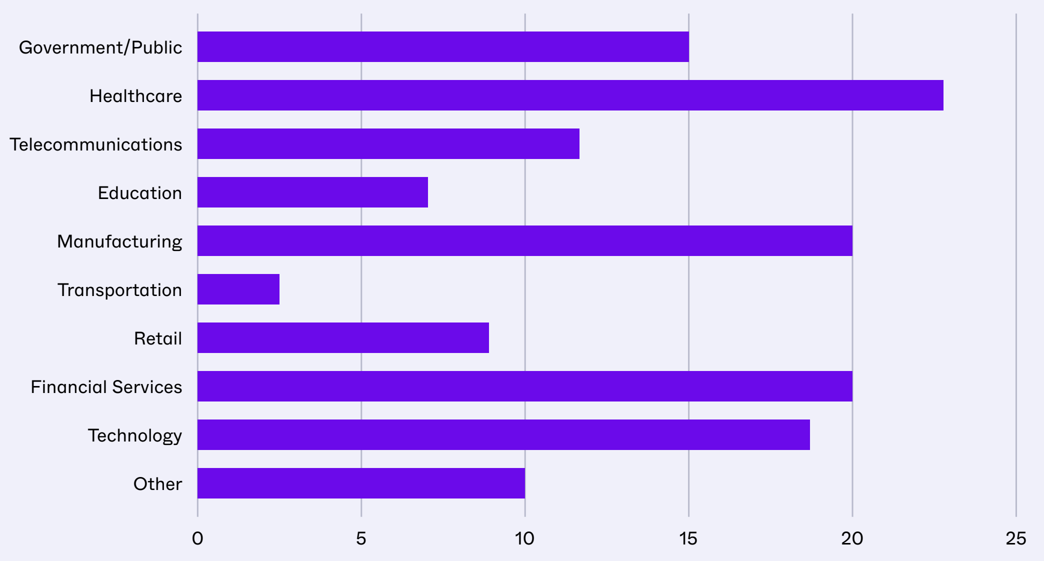
The incident response team at SentinelOne took on nearly 250 cases throughout 2024.

While our incident responders encountered novel tactics and engaged on behalf of customers in unique environments, there were several recurring themes. Data Exfiltration, Lateral Movement, Ransomware and Business Email Compromise were consistently top-of-mind for breach customers. Maintained integrity and availability of services were top priorities for customers in critical sectors, including healthcare and manufacturing. Among cases leading to network compromise, VPN appliance exploitation or authentication with stolen credentials was most prevalent, followed by social engineering and infections from commodity malware strains like Gootloader and SocGholish.

DFIR Cases by Type



Incidents by Victim Industry



The following case studies depict the breadth and depth required to effectively respond to a variety of incidents. Keen eyes from our forensic investigators spotted the difference between opportunistic, short campaigns and targeted, persistent intrusions.

Case Study 1: E-Commerce Platform Compromise

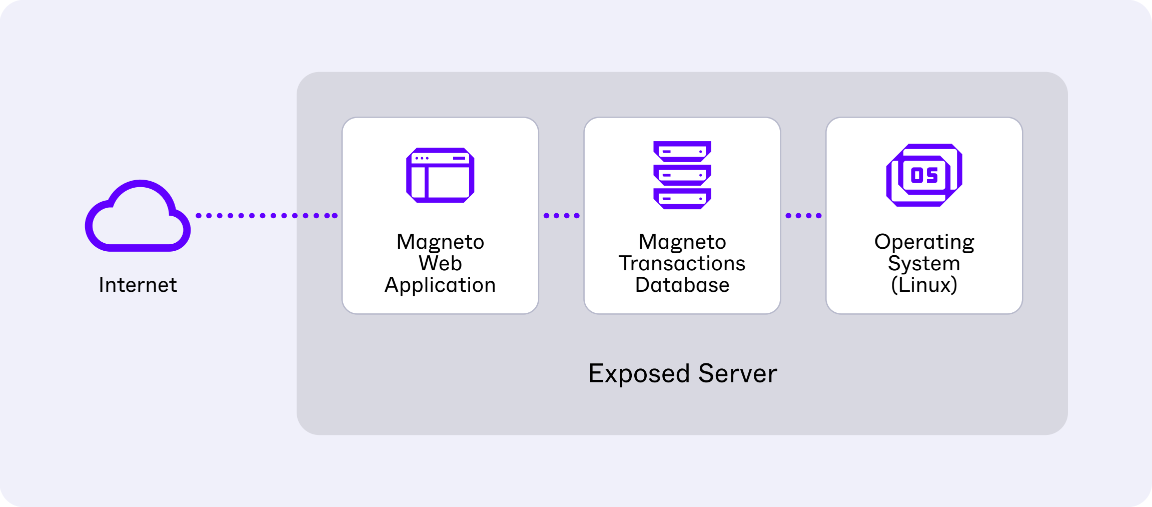
For a global financial services organization, a compromise in their e-commerce platform where sensitive payment data may be stored is a dire scenario. In this incident, a threat actor took advantage of a vulnerability in the Magento platform to drop webshells on an exposed server, which could have led to general network compromise.

The DFIR team used their expertise to confirm web exploitation, analyze implanted malware and search the customer's transaction data for malicious entries.

The investigation began with several SentinelOne Threats triggered by PHP files being downloaded on a public-facing server via curl. Upon analysis, these were found to be webshells cleverly disguised as Magento components. These had the capability to execute encoded commands sent to the server via web request. The IRR Team quickly pivoted to understanding the vulnerability that led to the creation of the webshells. Investigators analyzed logs and collected evidence to understand when the webshells were created and what web applications were being accessed at that time.

After finding overlap with a known Magento CVE, our investigators found that the webshells were likely created by an OS command injection vulnerability in a Magento form. Working with the customer, IR Team was able to confirm that malicious transactions had been submitted to the e-commerce platform, which resulted in commands being executed on the server.

Through analysis of their database, IRR noted several consistent tactics by the threat actor to probe the database and drop the webshells, but the investigation yielded no findings of sensitive data exfiltration. IR Team collaborated with SentinelLABS on searching for other victims of this campaign, hunting for additional mal- ware samples and collating intelligence on this threat actor.

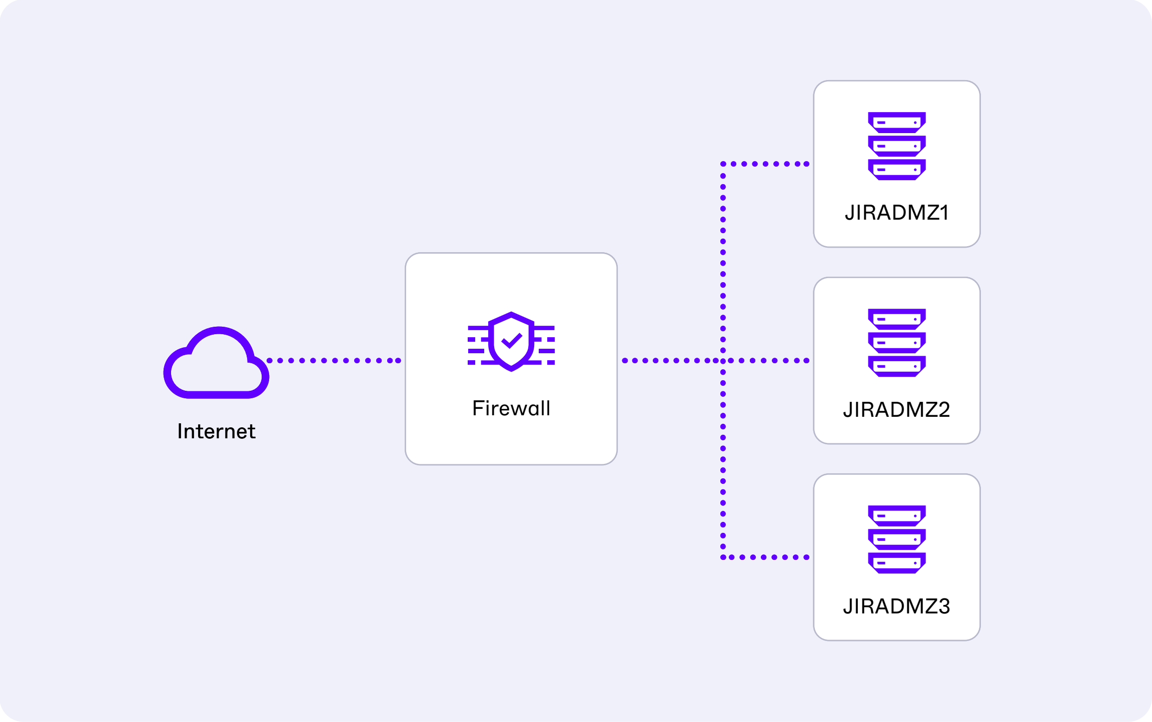


Case Study 2: Data Theft Through JIRA

SentinelOne DFIR was engaged by a global manufacturing and utilities provider to respond to an SSH reverse shell that spawned on one of their JIRA servers. Three webshells, uploaded as JIRA plugins, were found on the three servers in the customer's DMZ. In the end, IR investigators used a variety of tools to confirm methods of data exfiltration, and reverse-engineered the malware written by the threat actors in order to confirm their capabilities.

The incident began with a local administrator account which had its credentials compromised via an infostealer. IR found that the threat actor used these credentials to query the JIRA servers via their REST APIs. The threat actor was able to remotely access sensitive data and attempted to exfiltrate data via SCP and SFTP, but was unsuccessful due to network controls on outbound traffic. Further analysis of the JIRA servers at the operating system level revealed that the threat actor tried again to exfiltrate data via curl and was successful, resulting in data loss for the customer.

The JIRA plugins, written in Java, proved a novel method of persistence to the customer's environment and enabled commands to be executed via web requests.

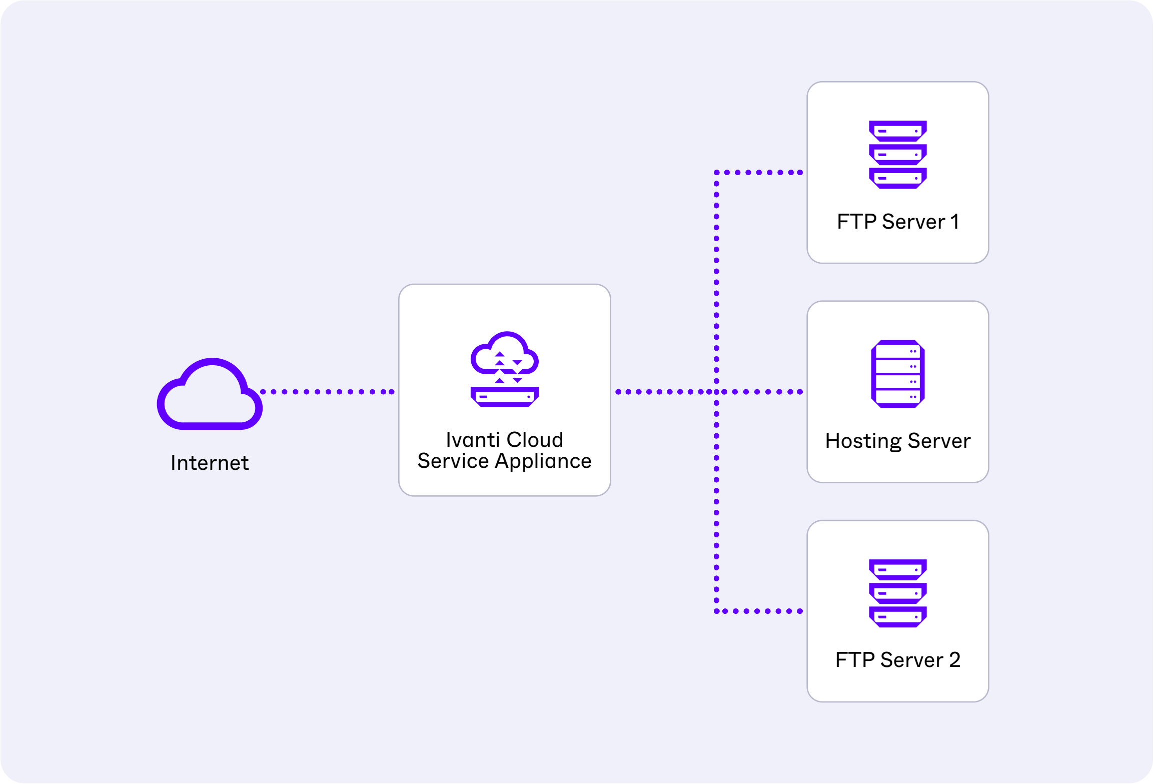


Case Study 3: VPN Appliance Zero-Day Exploitation

A SentinelOne customer in media and communications was victimized by an advanced persistent threat actor, using two zero-day exploits in Ivanti Cloud Service Appliance (CVE-2024-8190 and CVE-2024-8963).

SentinelOne IRR responded to a malicious file alert on one of the customer's FTP servers. The malicious activity was conducted under a user account, later traced to their Ivanti CSA. IRR investigators were able to identify exploitation as the initial access vector. Further investigation revealed brute-force logins and lateral movement from the Ivanti appliance to three internal servers.

On two FTP servers in the environment, IRR found several malicious Golang backdoors (classified as GORE-VERSE) dropped by the threat actor. In addition, the intruders used the privilege escalation exploit CVE-2021-4034 and deployed the post-exploitation toolkit PwnKit as well as Ettercap for man-in-the-middle network capture. The threat actor also accessed certificate and credential stores on servers, which appeared to serve the goal of covert data collection. IRR worked with SentinelLABS and collaborated with government partners to gather and share actionable intelligence about the threat actor. The modus operandi in this incident aligned with a Chinese APT cluster.



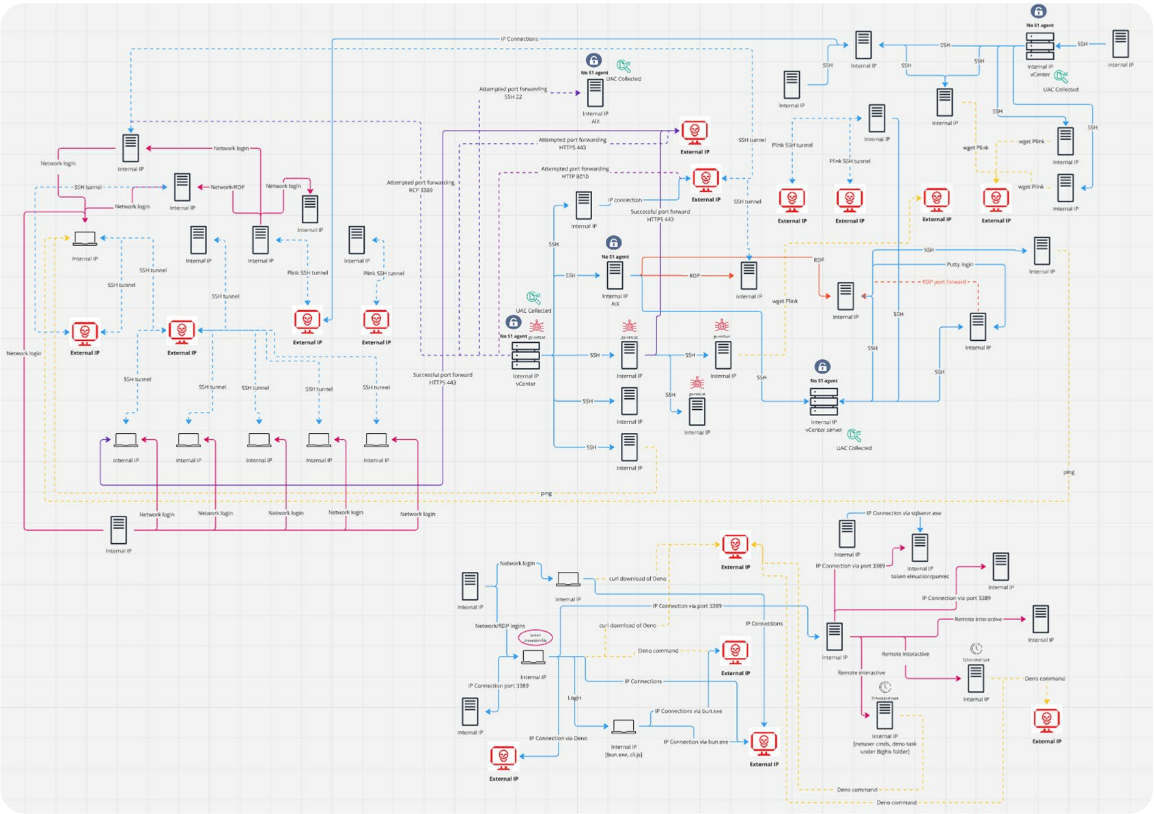
Case Study 4: Re-Intrusion Post Ransomware

One of the largest IRR cases of 2024 came from a manufacturing and distribution customer who engaged another incident response provider when impacted by Akira ransomware. IRR was engaged when the customer noticed continued activity within their network and had many lingering concerns post-incident.

Our investigators began a large-scale investigation focused on identifying persistence and the root cause of the prior incident. As the threat actor was still active, this entailed two investigations in one effort. The threat actor had established many methods of persistence, including Scheduled Tasks, Cron jobs, SSH tunnels and backdoors. Each of these were identified by IRR and studied for their prevalence within the environment.

One unique feature of this incident was the use of JavaScript runtime environments like Deno and Bun to evade detection. The threat actor dropped various JavaScript files along with these interpreters on several systems for persistence and other objectives. IRR was also able to identify systems the threat actor moved laterally to, which did not have SentinelOne agents. These included virtual machine infrastructure which our investigators were able to acquire.

In the course of this incident, SentinelOne IRR identified over 55 affected systems and parsed several months of compromise data. Dealing with a threat actor of such persistence was a challenge, but delivering a comprehensive report to our customer with actions and recommendations was truly a team effort.


IP Connections
No S1 agent
UAC Collected
Attempted port forwarding SSH 22
Internal IP AIX
SSH
Internal IP
Internal IP vCenter
Network login
Network/RDP
SSH tunnel
Attempted port forwarding RCP 3389
Attempted port forwarding HTTPS 443
Attempted port forwarding HTTP 8010
External IP
IP connection
Successful port forward HTTPS 443
Plink SSH tunnel
wget Plink
RDP
RDP port forward
Putty login
gs-netcat
Successful port forward HTTPS 443
Internal IP vCenter server
ping
IP Connection via sqlservr.exe
IP Connection via port 3389
Internal IP token elevation/psexec
Remote interactive
Scheduled task
Internal IP [netuser cmds, deno task under BigFix folder]
Deno command
curl download of Deno
Network/RDP logins
token elevation file
IP Connection port 3389
IP Connections
Login
IP Connections via bun.exe
IP Connection via bun.exe
Internal IP [bun.exe, cli.js]
IP Connection via Deno

PinnacleOne

PinnacleOne 2024 Snapshot

In 2024, the world faced escalating geopolitical tensions and sophisticated cyber campaigns that challenged global security. Events across the calendar year showcased the interconnected risks of great-power competition, regional conflicts, and the weaponization of emerging technologies. Here, we summarize the key geopolitical and cyber events, lessons learned, and implications for future stability.

Top 5 Geopolitical Risks

1 | **U.S.-China Strategic Competition**

The U.S. and China deepened their competition in advanced technologies, economic influence, and military power projection. Taiwan's security, semiconductor supply chains, and the South China Sea remain potential flashpoints for confrontation.

2 | **Regionalization of Trade Networks**

Countries shifted toward localized and regional trade agreements, reducing reliance on global supply chains. This trend, driven by economic nationalism and geopolitical tensions (including in the Red Sea), disrupted global trade flows.

3 | **Escalation in Information Warfare**

State actors expanded their use of disinformation campaigns and cyber-enabled espionage to influence public opinion and undermine political stability. AI-powered tools may amplify the scale and sophistication of these tactics, particularly during elections and geopolitical crises.

4 | **Tensions in the Indo-Pacific**

The Indo-Pacific region faced intensifying military activity, including joint exercises by Western allies and aggressive maneuvers by China. Strategic competition over maritime security and trade routes heightens the risk of localized tensions spilling over into great power conflict with global repercussions.

5 | **Sabotage of Critical Infrastructure**

Subsea cables, pipelines, and other critical infrastructure faced increased risks of sabotage by state and non-state actors. Attacks targeting global communication networks and energy supply routes threaten to undermine economic stability and complicate strategic deterrence, particularly in the Indo-Pacific and Europe.

Top Five Recurring CISO Management Concerns of 2024

1 | Asset Inventory

The first to-do on well-regarded cybersecurity frameworks, such as NIST's CSF, and frequently the thing never completed by defenders. Nothing is more critical to security teams than the ability to answer the questions "should that be on the network?" and "what is the business value of this asset?" Beyond just a list of hardware and devices and MAC addresses, an inventory including current software,SaaS/cloud apps, and third parties are critical to understanding your organization's network, dependencies, and attack surface. Asset inventory is key to accurate risk identification. If you don't know which firewalls your companies deploy and where, how can you know they are vulnerable to the latest round of Chinese hacking efforts? Similarly, data residency laws are pushing businesses to identify the use-cases and location of regulated data–a task also falling to CISOs. The most common cause for not completing asset inventory is technical debt–that it was not done early as the company grew, and so no one has gone backwards to complete it.

2 | Identity and Access Management

IAM is a natural chokepoint in the kill chain that defenders often fail to use. Effective identity and access management stem from coordination between HR policies, employee movements (joiners, leavers, contractors) and IAM rules, in addition to understanding which users should have access to what data. Identity and access management issues commonly stem from technical debt during growth, a failure to understand its value for defense, and competing tool use. All of which are also frequent causes of poorly federated identity and access management policies. Moving towards a well-managed and strategically architected approach to IAM is critical for companies aiming to achieve zero trust.

3 | SOC Burnout

SOC teams overloaded with alerts are often deleting smoke and missing fires. We are at the start of a SIEM replacement cycle where companies are beginning to augment their workforce with AI capabilities. As the technology proves itself valuable, SOCs without AI integration will gradually become "legacy SOCs." The most successful teams observed are investing time and people into automating triage and simple response activities and redirecting excess capacity towards taking action against actual, confirmed threats. Underpinning all this automation and triage are dynamic and usable information architectures (see item #5.) We will soon see automation and AI take over more complex response activities. Those who embrace it now will have an easier time adopting later.

4 | Secure Product Development

CISOs at product companies often play second fiddle to engineering teams, thus creating cyber risks for companies that the CISO is not empowered to mitigate. 2024 was full of product companies whose security teams did not influence the practices of their product engineering teams, leading to losses for the business. Product governance is driven by incentives–who is ensuring the security of your products and who is responsible for implementation? Lack of documentation, accrued expert knowledge among senior staff, and no oversight or enforcement of documented processes jeopardize product development lifecycles. Successful organizations use a standardized set of tools and processes across project teams, and engineers are interchangeable between teams owing to these unified tools. These foundational concepts are critical to enabling secure product delivery.

5 | Detection Engineering

Commonly overlooked among even mature organizations–and often thought of as "turning down the noise" on alerts–detection engineering can help mature teams and organizations identify malicious activity in the environment. Detection engineering teams can codify bespoke intelligence alerts (e.g. from government partners) and fine-tine user behavior alerts that indicate something is amiss. CISOs should aim to coordinate detection engineering with other teams, such as HR, to create alerts for insider risk scenarios, for example. In many cases, CISOs and security teams have access to the most data about an organization and are in a position to act on that information in service of the business itself. Our services teams saw plenty of detection tuning in 2024, but few organizations rose to the challenge of creating bespoke detections for their environment or coordinating with non-security business functions.

About SentinelOne Threat Services

WatchTower is SentinelOne's threat hunting service, provided as a value-added benefit for Managed Detection & Response (MDR) customers.

DFIR is SentinelOne's global digital forensic and incident response team, ready to initiate investigations within moments of initial notification, 24×7.

PinnacleOne is SentinelOne's Strategic Advisory Group, providing tailored strategic advisory services to help organizations succeed faster and enhance their cybersecurity posture.

SentinelOne®

Contact Us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.