2025 FORTINET

GLOBAL THREAT LANDSCAPE REPORT

A Report by FortiGuard Labs

Table of Contents

For questions related to this report, please contact us.

MITRE ATT&CK

Reconnaissance

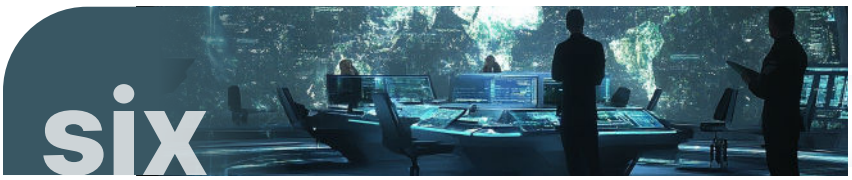
Resource Development

Initial Access

Privilege Escalation

Lateral Movement

Command & Control

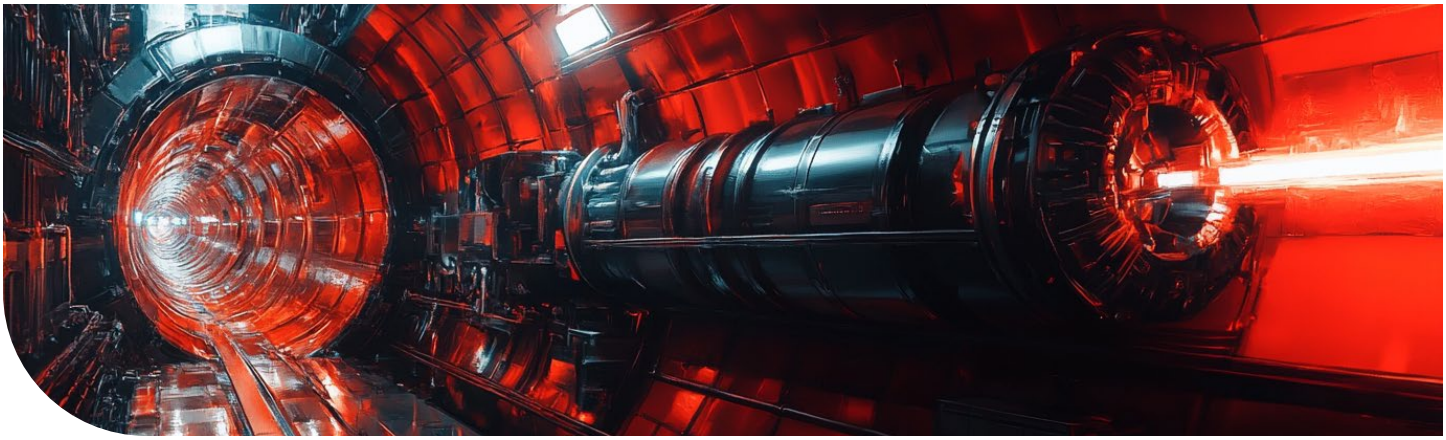


Exfiltration

Impact

Acceleration of the Adversary Advantage

This 2025 Threat Landscape Report reveals a dramatic escalation in both the scale and sophistication of cyberattacks. Data shows adversaries are moving faster than ever, automating reconnaissance, compressing the time between vulnerability disclosure and exploitation, and scaling their operations through the industrialization of cybercrime. Across all attack phases, FortiGuard Labs observed that threat actors are leveraging automation, commoditized tools, and AI to erode the traditional advantages held by defenders systematically.



The challenge is clear: Your adversary's advantage is accelerating. From pre-attack reconnaissance to post-compromise persistence, attackers now operate with unprecedented speed, precision, and reach, challenging organizations to shift from reactive defense to proactive exposure management.

Key findings

- **Reconnaissance is surging.** Cybercriminals are deploying automated scanning at a global scale. Active scanning in cyberspace reached unprecedented levels in 2024, rising by 16.7% worldwide. FortiGuard Labs observed billions of scan attempts each month, equating to 36,000 scans per second, revealing an intensified focus on mapping exposed services, such as SIP and RDP, and OT/IoT protocols like Modbus TCP. Tools like SIPVicious and commercial scanning tools are weaponized to identify soft targets before patches can be applied, signaling a significant "left-of-boom" shift in adversary strategy.
- **AI is supercharging the cybercrime supply chain.** Threat actors leverage AI for phishing, impersonation, extortion, and evasion tactics. Tools like FraudGPT, BlackmailerV3, and ElevenLabs are automating the generation of malware, deepfake videos, phishing websites, and synthetic voices, fueling more scalable, believable, and effective campaigns.

  And as predicted, Cybercrime-as-a-Service (CaaS) groups are using these new tools to embrace specialization, doubling down on specific segments of the attack chain.
- **CaaS is fueling initial access at scale.** The underground economy for stolen credentials and direct corporate access has exploded. FortiGuard Labs observed a 42% increase in compromised credentials for sale and a rise in Initial Access Broker (IAB) activity offering VPNs, RDPs, and admin panels. Infostealers like Redline and Vidar drove a 500% increase in credential logs on darknet forums.
- **Adversaries are fragmented in form and unified in function.** While 13 new ransomware groups entered the Ransomware-as-a-Service (RaaS) market, demonstrating fragmentation, the top four groups still accounted for 37% of observed attacks, indicating concentrated influence. Meanwhile, hacktivists have begun adopting ransomware tactics, and nation-state actors remain active in targeting manufacturing, government, education, and tech sectors. Telegram remains a dominant coordination hub for sharing exploits and infrastructure, offering a layer of operational unity across otherwise disconnected threat groups.

- **Exploitation volumes are soaring as speed remains steady.** While the average time to exploit newly disclosed vulnerabilities held relatively steady in 2024, closely tracking the 5.4-day average observed in 2023, the scale of exploitation attempts surged. FortiGuard Labs recorded over 97 billion exploitation attempts during the year, reflecting increased automation and broader targeting across industries. Attackers prioritized exposed IoT devices, routers, firewalls, and cameras, frequently used for botnet command and control (C2), lateral movement, and persistent access. CVE-2024-21887, a command injection vulnerability in Ivanti products, was exploited just six days after disclosure, underscoring how quickly adversaries can still act when opportunity aligns with impact.
- **Post-exploitation tactics are getting stealthier.** Despite the number of CVEs growing 39% from 2023 to 2024, zero-day attacks only account for a small percentage of observed threats. Cybercriminals increasingly "live off the land," using trusted tools and protocols to escalate privileges and persist undetected. FortiGuard Labs has identified advanced post-compromise behaviors, including Active Directory (AD) manipulation (such as DCShadow and DCSync), RDP-based lateral movement, and encrypted C2 via DNS and SSL.
- **Cloud attacks are evolving, but misconfigurations still reign.** Cloud environments remain a top target, with adversaries exploiting persistent weaknesses, such as open storage buckets, over-permissioned identities, and misconfigured services. Lacework FortiCNAPP telemetry shows a steady rise in cloud compromises, often involving identity abuse, insecure APIs, and privilege escalation. These vectors are frequently combined in multi-stage attacks that leverage automation and legitimate services for stealth and persistence. Reconnaissance remains the most prevalent tactic, with attackers probing APIs, enumerating permissions, and scanning for exposed assets. In 70% of observed incidents, attackers gained access through logins from unfamiliar geographies, highlighting the critical role of identity monitoring in cloud defense.

A call to action: shift left, act fast, reduce exposure

The evidence is clear: Attackers invest heavily in automation, reconnaissance, and scalable operations. Their playbooks emphasize speed, stealth, and scalability, while far too many organizations remain overburdened with reactive patch cycles and static security strategies.

Defenders must shift from traditional threat detection toward Continuous Threat Exposure Management (CTEM) to counter this asymmetry. This proactive approach emphasizes the following:

- Continuous attack surface monitoring
- Real-world emulation of adversary behavior
- Risk-based prioritization of remediation
- Automation of detection and defense responses

The security landscape has radically changed. Staying ahead of attackers now means countering their next move before they make it, which means that traditional security solutions are no longer enough.

1. Cyber Reconnaissance Surge: The Rising Threat of Automated Scanning

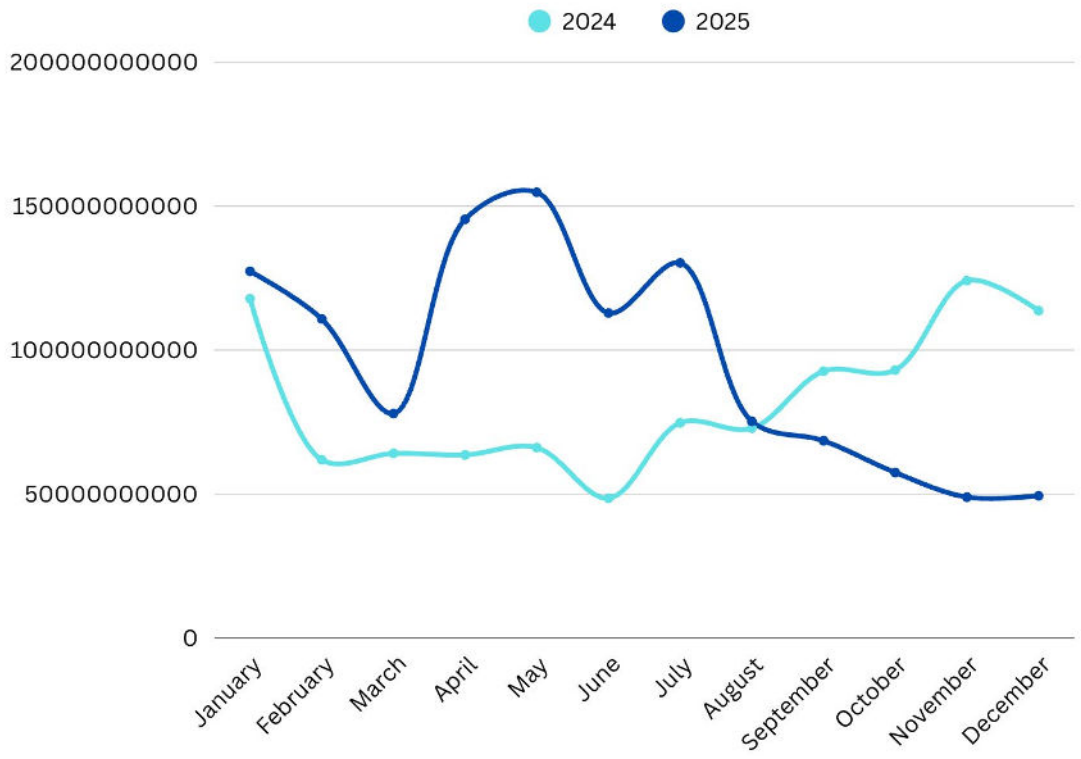
FortiGate

FortiOS

FortiRecon

Active scanning in cyberspace reached unprecedented levels in 2024, rising by 16.7% worldwide, highlighting a sophisticated and massive collection of information on exposed digital infrastructure. Intrusion prevention system (IPS) engines in FortiGate Next-Generation Firewalls (NGFWs) detected an intensification of these scans across all geographies, with attackers leveraging advanced left-of-boom techniques to map attack surfaces before launching targeted offensives.

Behavioral Trend Analysis by Month



Current Detections

1.16 trillion

Detections in 2024

993 billion

Growth year over year

16.71%

This unprecedented volume of automated scans suggests a rise in large-scale reconnaissance campaigns. These scans seek obvious vulnerabilities and explore critical infrastructures to determine which assets can be exploited with minimal effort. As the weaponization phase of attacks becomes smaller, threat actors can now maintain a near-real-time understanding of attack surfaces across many targets. Then, when a vulnerability becomes available, attackers can strike quickly, impacting organizations that have not proactively applied patches.

Millions of active scans: what threat actors are looking for

Millions of scanning attempts are detected worldwide every hour, revealing the persistent effort by cybercriminals to map exposed systems before launching their attacks. This number adds up to billions monthly, demonstrating the sheer scale of automated reconnaissance operations. To effectively protect an organization, defenders must understand what attackers are searching for and how their scans translate into real-world risks.

Attackers are targeting widely used protocols in key sectors, such as telecommunications, industry, OT, industrial control systems (ICS), and financial services, and regularly rely on the following:

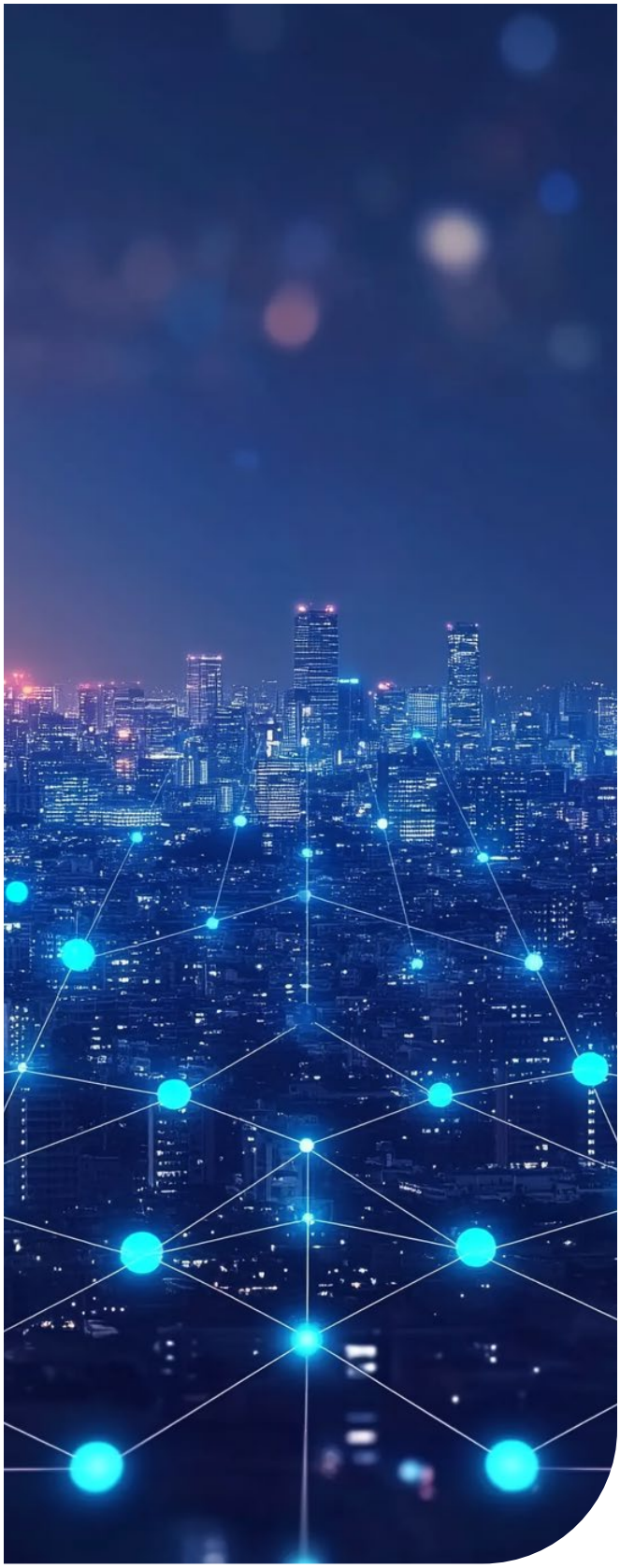
- **SIP (VoIP):** SIP represented over 49% of detected scans. Widely used in telecommunications, SIP vulnerabilities can allow interception attacks and call fraud. For example, APT28 has used legitimate credentials to gain initial access, maintain access, and exfiltrate data from a victim network. The group has also leveraged manufacturers' default passwords to gain initial access to corporate networks via IoT devices, such as VoIP phones, printers, and video decoders.

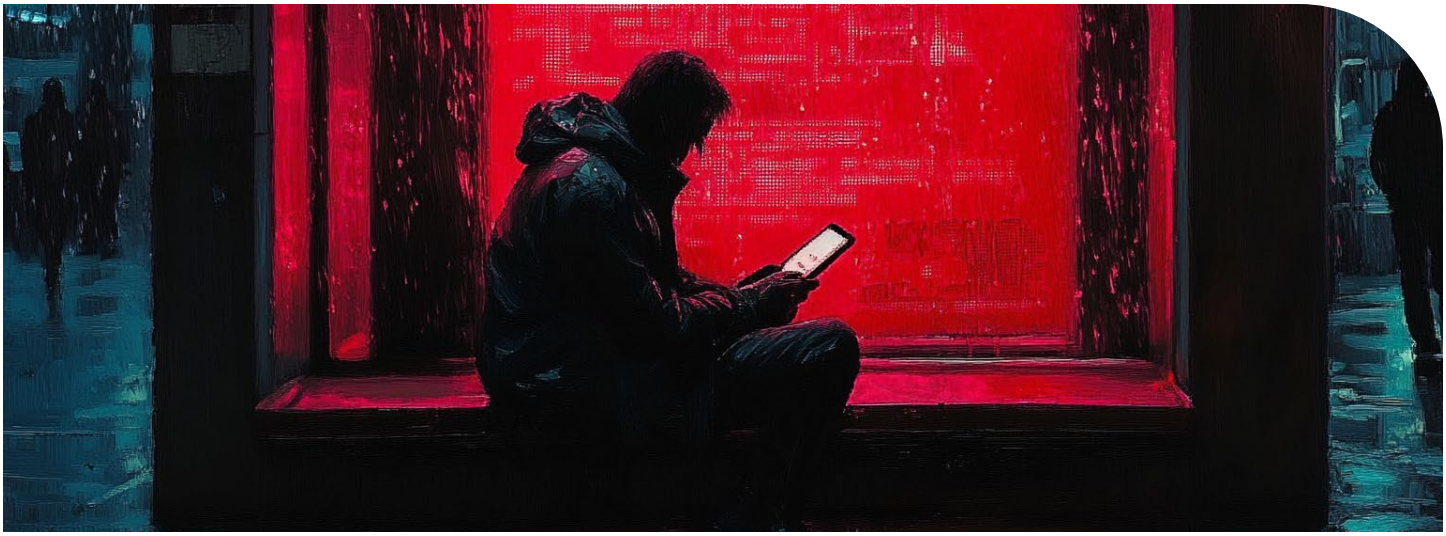
- **Modbus TCP:** Modbus TCP accounted for about 1.6% of scans, highlighting concerns about industrial infrastructure and supervisory control and data acquisition (SCADA) systems. The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple ICS/SCADA devices.

Which scanning tools are cybercriminals using to find system weaknesses?

Threat actors are leveraging sophisticated tools to automate attack surface mapping, hereby optimizing their exploitation campaigns. These tools include:

- **SIPVicious:** SIPVicious is responsible for nearly 50% of detected scanning events. The SIPVicious suite is a set of tools for auditing SIP-based VoIP systems. Malicious actors have adopted this suite to exploit vulnerable SIP servers. This suite contains five tools: swamp, svwar, svcrack, report, and crash.
- **Qualys:** This vulnerability scanner appears in about 2.5% of scans and is used by legitimate security teams and attackers seeking weaknesses in critical infrastructure.
- **Nmap:** Detected in less than 1% of events, Nmap remains a key tool for identifying open ports and vulnerable services. Also known as Network Mapper, this is an open-source tool used for network exploration and security auditing. It was originally designed to scan large networks rapidly.
- **Nessus and OpenVAS:** While representing a smaller percentage of scans, these tools are still widely used to explore vulnerabilities in enterprise systems.





2. Shedding Light on the Darknet: How Adversaries Prepare to Strike

FortiRecon

While much of our telemetry shows what actions attackers have previously taken, darknet intelligence helps us understand what threat actors may do next. Adversaries in the depths of the darknet continue developing, acquiring, and trading resources that enable them to execute large-scale attacks with alarming precision. Security breaches do not begin when an organization detects suspicious activity in its network. By the time an adversary successfully compromises a system, the attacker has already spent significant time planning and testing the attack, with all necessary resources already in place.

The darknet has evolved from a mere refuge for cybercriminals into a supply chain for cyberattacks. The FortiGuard Labs team has identified a rapidly growing underground ecosystem where stolen credentials, corporate access, exploits, and AI-powered tools are bought, sold, and developed to facilitate malicious operations.

This means that attackers no longer need to rely solely on their technical skills. Regardless of technical know-how, any adversary can acquire ready-made resources, significantly lowering the barrier to entry for cybercrime, especially for attackers with lower skills, which ultimately increases the volume, velocity, and sophistication of targeted attacks.

The business of corporate infiltration

Stolen credentials are not the only valuable commodity being sold. In 2024, the darknet saw a sharp increase in IABs, which sell direct access to corporate infrastructures. This service allows adversaries to infiltrate networks without searching for and exploiting vulnerabilities. IABs offer far more than just individual credentials, with some of their most sought-after assets being:

- Corporate VPN credentials (20%)
- RDP access (19%)
- Admin panels (13%)
- Webshells (12%)

IAB groups such as sandocan (26%), F13 (16%), and JefryG (12%) lead this economy, offering pre-compromised internal network access to current and aspiring cybercriminals.

Credentials are the currency of cybercrime

One of the darknet's most active markets is the trade of compromised credentials. In 2024, over 100 billion records were shared in underground forums, a 42% increase from 2023.

This surge is largely driven by combo lists: massive data files containing email addresses, usernames, and passwords obtained from past breaches. More than 50% of darknet posts are related to leaked databases, which, if acquired, can easily allow cybercriminals to automate credential-stuffing attacks and gain unauthorized access to corporate systems.

Well-known groups selling this type of information on the darknet provide the data and streamline these resources to make it easy for a threat actor of any skill level to carry out an attack successfully. This lowers the barrier to entry for cybercriminals and significantly amplifies the risk of account takeovers, financial fraud, and corporate espionage.

Among the most active cybercriminal groups in this market are:

- **BestCombo (20%):** This high-volume supplier of stolen credentials frequently sells fresh breaches bundled into massive, ready-to-use lists.
- **BloddyMery (12%):** Known for aggregating and enhancing leaked data, this group makes stolen credentials more valuable for resale and enhances targeted attacks.
- **ValidMail (12%):** This group specializes in credential validation services, ensuring buyers receive only functional login details, which increases attack success rates.

Credential Theft-as-a-Service: the industrialized rise of infostealers

Credentials available on the darknet are not just from past data breaches. In 2024, FortiGuard Labs observed a 500% increase in logs from systems compromised by infostealer malware, with 1.7 billion stolen credential records shared in underground forums. The top identified infostealers include:

- **Redline (60%):** The most widely used infostealer, Redline is favored for its affordability, ease of use, and ability to target multiple data sources. Sold on underground forums for as little as $150, it steals credentials from web browsers, email clients, cryptocurrency wallets, and messaging apps like Telegram and Discord. Its high adoption rate has made it a popular choice for IABs, who sell stolen logins to ransomware operators and other cybercriminal groups.
- **Vidar (27%):** Known for its advanced capabilities, Vidar specializes in harvesting credentials and session tokens and multi-factor authentication (MFA) bypass data. This allows attackers to maintain persistent access to accounts even after passwords are reset. Vidar's modular structure enables easy customization, letting cybercriminals tailor its functions to steal VPN credentials, banking logins, and cloud authentication tokens.
- **Racoon (12%):** Unlike other infostealers, Racoon focuses on mass data exfiltration, collecting financial records, stored passwords, credit card information, and cryptocurrency wallets. Distributed via phishing campaigns and cracked software downloads, Racoon has gained popularity for its stealthy nature, making it difficult to detect until stolen credentials appear on darknet marketplaces.

Exploit brokers: how attackers obtain and develop their capabilities

Underground forums don't just trade access and credentials—they also serve as a marketplace for sophisticated exploit kits targeting a wealth of vulnerabilities. In 2024, more than 40,000 vulnerabilities were added to the National Vulnerability Database, representing a 39% increase over 2023.

In 2024, 331 zero-day vulnerabilities were identified in darknet forums with a high percentage of available exploits.

- 182 (55%) had publicly available proof-of-concept (POC) exploit code
- 106 (32%) featured fully functional exploit code ready for attacks
- 98 (30%) were actively being exploited in ransomware and APT campaigns

In addition to prioritizing patch management practices for high-severity CVEs, regular darknet monitoring offers defenders a glimpse into which vulnerabilities are likely to be exploited by threat actors. This intelligence allows security teams to take proactive steps to guard against potential attacks.

AI-enabled cybercrime: the role of AI in the automation of cybercrime

The growing cybercrime market is thriving on cheap and accessible wins. And as AI evolves, it's already lowering the barrier to entry for aspiring cybercriminals, increasing access to the tactics and intelligence needed to execute attacks regardless of an adversary's technical knowledge. Beyond enhancing accessibility, AI enables malicious actors to create more believable phishing threats.

The FortiGuard Labs team has identified numerous AI-driven tools that are helping adversaries gain new efficiencies, including:

- **DeepFaceLab and Faceswap:** Widely used by fraudsters, these deepfake tools create realistic AI-generated videos to bypass identity verification procedures on banking and cryptocurrency platforms. Attackers use them to impersonate executives, gain access to accounts, and launder illicit funds.
- **FraudGPT and WormGPT:** These AI-powered text generators help cybercriminals craft compelling phishing emails, fake business communications, and fraudulent legal documents. Unlike ChatGPT, these tools have no ethical restrictions, allowing attackers to refine scams, generate malicious code, and conduct social engineering at scale.
- **BlackmailerV3:** An AI-driven extortion toolkit that automates customized blackmail emails, BlackmailerV3 uses scraped personal and corporate data to add credibility to its communications. The tool is often used in sextortion scams, fake legal threats, and CEO fraud attempts.
- **AI-generated phishing pages (EvilProxy, Robin Banks):** These platforms use AI to auto-generate phishing websites that mimic legitimate login portals for banking, cloud services, and enterprise platforms. Some, like EvilProxy, also offer Adversary-in-the-Middle (AiTM) capabilities, allowing attackers to steal MFA-protected credentials.
- **ElevenLabs and Voicemy.ai:** Attackers leverage these AI voice synthesis tools to clone voices for vishing (voice phishing), deepfake scam calls, and bypassing voice authentication systems used in financial institutions and corporate access controls.
- **AI-powered social engineering bots (Goose, Telegram fraud bots):** These chatbots impersonate customer support representatives and use AI-generated conversations to trick victims into sharing sensitive information, such as credit card details, MFA codes, and passwords.

3. From Exposure to Initial Access and Exploitation: How (and Where) Attackers Get the Keys to the Kingdom

The cybersecurity battlefield has shifted dramatically. Attackers no longer have to identify vulnerabilities manually. Instead, they can leverage automated scanning, machine learning (ML), and neatly packaged exploit kits to weaponize newly disclosed security flaws within hours of discovery.

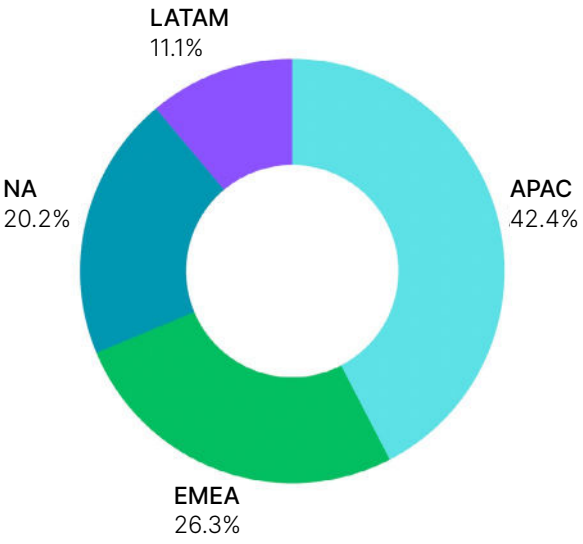
FortiGate

FortiOS

In our latest analysis, Fortinet IPS sensors detected over 97 billion exploitation attempts, showcasing how cybercriminals are continuously probing for exposed systems. The question is no longer if an organization will be targeted—it's a matter of when and how quickly.

Attackers are methodical and persistent and operate without borders. While all regions face significant risk, Asia-Pacific (APAC) accounts for the largest share (42%) of recorded exploitation attempts, followed by Europe, the Middle East, and Africa (EMEA) (26%), North America (20%), and Latin America (11%).

Global Distribution of Exploitation Attempts



Attackers' favorite entry points

Not all vulnerabilities are equal. Some have proven to be critical exposure points and are relentlessly exploited by cybercriminals seeking access to enterprise networks. FortiGuard Labs IPS telemetry highlights key vulnerabilities that remain highly attractive to adversaries. Here are some of the most popular entry points for attackers looking to compromise organizations:

Windows SMB Information Disclosure Vulnerability (CVE-2017-0147)

Representing 26.7% of exploitation attempts in 2024, this vulnerability remains one of the most sought-after by attackers aiming to infiltrate enterprise networks via the Server Message Block (SMB) protocol. The prevalence of SMB in detections is likely a result of automated scanning, but it is a good reminder for organizations to ensure that the bare minimum of services are exposed to attackers. This can be especially important for organizations operating OT products running obsolete software.

Apache Log4j Remote Code Execution (CVE-2021-44228)

With 11.6% of activity, this vulnerability continues to be a threat, proving that many organizations have yet to implement the necessary security fixes and that attackers are still testing for aging vulnerabilities.

Netcore Netis Devices Hardcoded Password (CVE-2019-18935)

This IoT vulnerability accounts for 8% of all exploitation attempts, further illustrating attackers' focus on poorly secured and misconfigured systems.

These attack vectors demonstrate a key challenge for security teams: While attackers often exploit weaknesses faster than defenders can respond, tried and true attack vectors still work because too many organizations fail to maintain proper cyber hygiene. Patch management delays, misconfigurations, and poor network segmentation create ideal conditions for automation-driven exploits to succeed.

IoT Device	% of Exploitation Attempts	Associated CVE	CVSS Score	Potential Impact
Netcore Netis Routers	18.4%	CVE-2019-18935	9.8	Remote control, botnet recruitment
WiFi P2P GoAhead Cameras	10.5%	CVE-2017-18377	8.3	Unauthorized access, espionage, data exfiltration
Zyxel Firewalls and Routers	3.2%	CVE-2022-30525	9.8	Remote access, configuration tampering
TP-Link Archer AX21 Routers	2.1%	CVE-2023-1389	9.0	Traffic hijacking, credential theft, persistence
GPON Routers (Multiple Brands)	0.9%	CVE-2018-10561	9.4	Persistent access, botnet inclusion, DDoS attacks

IoT devices are consistently easy targets in automated exploitation

The surge in exploitation against IoT devices highlights a fundamental security gap: Many organizations fail to treat IoT security with the same rigor as traditional IT assets. Attackers capitalize on default credentials, outdated firmware, and exposed management interfaces to gain persistence, and they use these devices as pivot points to execute larger-scale attacks. These devices also often serve as a safe haven for botnets.

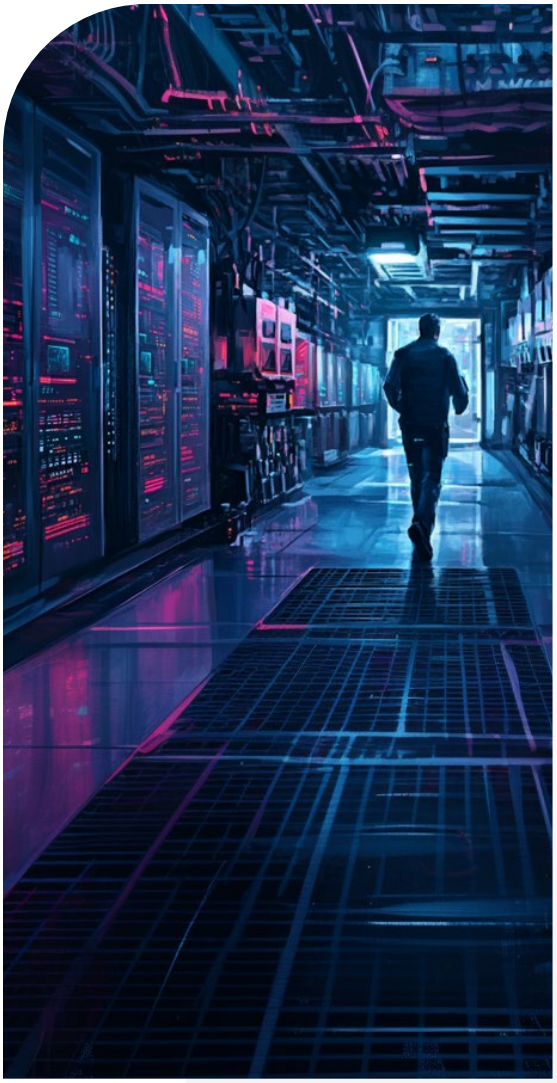
In the latest analysis period, over 20% of all recorded exploitation attempts targeted IoT devices, underscoring the growing threat. The table above shows the most targeted IoT devices and their associated CVEs, CVSS scores, MITRE ATT&CK techniques, and potential impacts.

Exploitation surges consistently coincide with new vulnerability disclosures, demonstrating that attackers rapidly integrate IoT vulnerabilities into their exploitation frameworks. The most targeted IoT devices are routers, cameras, and network hardware.

Routers account for the highest percentage of attacks, particularly those manufactured by Netcore, TP-Link, and D-Link, which have been actively exploited in multiple CVE-listed vulnerabilities.

Surveillance cameras, such as those from Zavio and GoAhead-based devices, remain attractive targets for attackers seeking persistent access for espionage, lateral movement, or botnet recruitment.

4. Beyond Initial Access: Post-Exploitation, Lateral Movements, and C2



Once an attacker breaches a system, what happens next? The fact is, initial access is just the beginning of a much more sophisticated attack chain. In the post-exploitation phase, cybercriminals consolidate their presence, move stealthily across networks, and establish persistent control over compromised environments. But how can organizations detect these activities before they escalate into full-blown breaches?

FortiGate

FortiOS

Anti-Botnet

FortiNDR

In this section, we analyze some of the most critical post-exploitation techniques observed in 2024, focusing on NDR detections related to privilege escalation (TA0004), lateral movement (TA0008), and C2 communications (TA0011), answering key questions that security teams must address and sharing critical insights to help organizations stay ahead of adversaries.

What type of malware was used for post-exploitation in 2024?

Cybercriminals rely on sophisticated malware to establish long-term persistence within compromised environments. The FortiGuard Labs team identified several notorious malware strains as being particularly active in 2024, including the following Remote Access Trojans (RATs):

- **Xeno RAT:** This feature-rich, open-source malware can capture screens, exfiltrate data, use persistence mechanisms, and leverage Socks5 reverse proxy.
- **SparkRAT:** This highly sophisticated RAT supports command execution, system manipulation (shutdown, restart, hibernation), and file/process control.
- **Async RAT and Trickbot:** These well-known malware families are commonly associated with cyber espionage, credential theft, and persistent network intrusion.

These RATs allow attackers to steal credentials, exfiltrate data, and execute commands remotely, making them an essential part of cyber adversaries' modern post-exploitation toolkits.

How do attackers move laterally across networks without detection?

Once inside a network, cybercriminals rarely stay in one place. They aim to expand their access, seeking sensitive data, higher privileges, and additional targets. By understanding the tactics attackers use to execute these activities, security teams can detect and halt lateral movement before it leads to widespread compromise.

The FortiGuard Labs team detected various lateral movement tactics in 2024, including:

- Malicious executable downloads within SMB traffic, a method frequently used to propagate malware across Windows, macOS, and Linux systems
- Anomalies in SMB protocol implementation, particularly incorrect Process Identifier (PID) field usage in the IMpacket package, a known IOC
- WMI ExecMethod lateral movement detections, where FortiNDR Cloud behavioral models flagged adversarial sequences attempting to execute commands remotely
- RDP-based lateral movement, which played a role in 88% of incidents investigated in 2024

Attackers frequently abuse RDP for credential-based movement across networks, making it a significant gap in many detection strategies.

How are attackers using Windows systems against organizations?

Attackers frequently abuse built-in system utilities to evade security controls and execute malicious code. In 2024, the FortiGuard Labs team observed cybercriminals using multiple execution techniques, including:

- Malicious portable executables (PE) downloaded across networks are a key indicator of ongoing exploitation.
- Trojan downloaders used by APT groups highlight a continued reliance on stealthy malware delivery mechanisms.
- Windows Management Instrumentation (WMI)-based execution of encoded PowerShell commands is often used for fileless attacks and stealthy lateral movement.

Attackers also increasingly use living-off-the-land techniques to blend in with legitimate Windows operations, making traditional signature-based detection ineffective. Behavioral analytics is key to spotting deviations from normal system activity.

How do attackers map and manipulate Active Directory?

Cybercriminals must understand their target environment before launching a full-scale attack. But how can organizations detect unauthorized reconnaissance activities?

FortiGuard Labs successfully identified multiple adversarial discovery techniques used in 2024, including:

- DCShadow attacks, where attackers introduce a rogue domain controller to manipulate AD
- DCSync attacks, allowing unauthorized replication of domain controller data
- Active Directory Enumeration, involving suspicious queries for users, groups, and domain trusts
- Network scanning flagged devices attempting to enumerate network sessions and shared resources

How do attackers maintain control over compromised systems?

Once inside a network, attackers establish a C2 channel to communicate with infected machines. But how do defenders detect these covert interactions?

FortiNDR Cloud successfully identified a variety of C2 techniques, including:

- SSL C2 beacons, commonly used to evade detection within encrypted traffic
- Cobalt Strike DNS requests, a favored tool among red teams and threat actors alike
- DNS tunneling and long DNS queries, which are often exploited to bypass traditional security controls

By leveraging deep neural network-based ML models, the FortiGuard Labs team flagged multiple Domain Generation Algorithm (DGA) domains used by malware to create constantly changing C2 endpoints. Additionally, its integration with the Fortinet Security Fabric enabled the detection of botnet IPs, helping organizations block malicious communications at the firewall level.

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning	“Exploit Public-Facing Application”	“Command and Scripting Interpreter: PowerShell”	“External Remote Services”	Valid Accounts	“Obfuscated Files or Information: Stripped Payloads”
	Hardware Additions	“Command and Scripting Interpreter”	“Server Software Component: Web Shell"	“Scheduled Task/Job: Scheduled Task”	“Indicator Removal: Clear Windows Event Logs”
	“Phishing: Spearphishing Link”	Windows Management Instrumentation		“Valid Accounts: Domain Accounts”	“Rogue Domain Controller”
		User Execution		“Create or Modify System Process: Windows Service”	“Deobfuscate/ Decode Files or Information”
		“Exploitation for Client Execution”		Subvert Trust Controls	“System Binary Proxy Execution: Regsvr32”
		“System Services: Service Execution”		“Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay”	
				Scheduled Task/ Job: At	
				“Exploitation for Privilege Escalation”	
				“Create or Modify System Process”	
				“Boot or Logon Autostart Execution”	

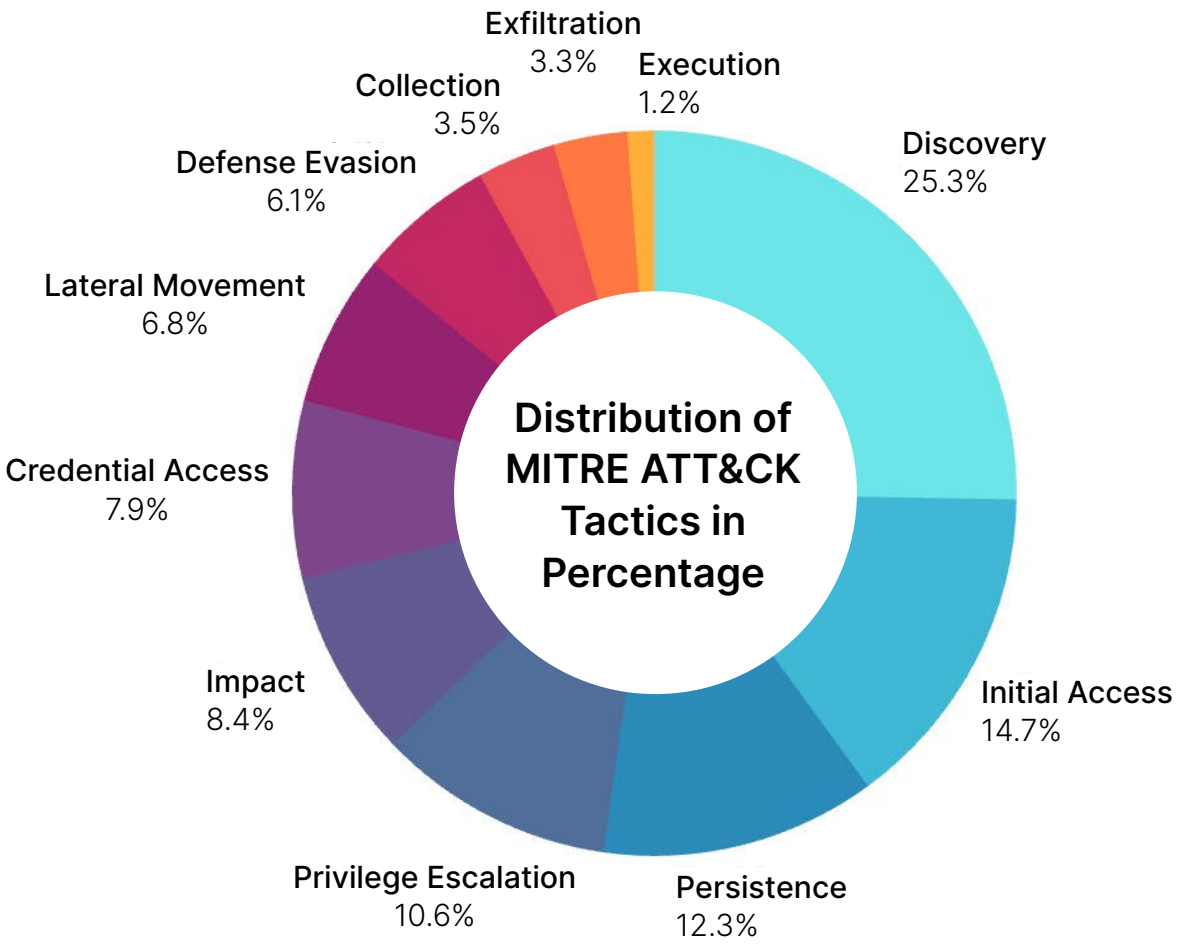
FortiNDR ATT&CK Matrix

Credential Access	Discovery	Lateral Movement	Command and Control	Exfiltration	Impact
Brute Force	“Network Service Discovery”	Remote Services	“Application Layer Protocol”	“Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol”	Network Denial of Service
Forced Authentication	“Account Discovery: Domain Account”	“Remote Services: SMB/Windows Admin Shares”	“Proxy: External Proxy”	Exfiltration Over Alternative Protocol	Resource Hijacking
“OS Credential Dumping: DCSync”	“File and Directory Discovery”	“Remote Services: Windows Remote Management”	“Remote Access Software”	Exfiltration Over C2 Channel	
“Steal or Forge Kerberos Tickets: AS-REP Roasting”	“Permission Groups Discovery: Local Groups”	Lateral Tool Transfer	“Ingress Tool Transfer”	“Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol”	
“Steal or Forge Kerberos Tickets: Kerberoasting”	Network Share Discovery	“Remote Services: VNC”	Proxy	Exfiltration Over Web Service	
OS Credential Dumping	“Permission Groups Discovery: Domain Groups”	“Exploitation of Remote Services”	“Application Layer Protocol: DNS"		
	“System Network Connections Discovery”		“Application Layer Protocol: Web Protocols”		
	“System Information Discovery”		Non-Standard Port		
	“System Owner/ User Discovery”		“Non-Application Layer Protocol”		
	“System Network Configuration Discovery”		“Proxy: Multi-hop Proxy”		
	Remote System Discovery		Web Service		

5. The Cloud Battlefield: Navigating the New Cybersecurity Landscape

FortiCNAPP

The shift to cloud computing has redefined enterprise security, providing essential agility and scalability but exposing organizations to evolving attack vectors. Cloud environments are now a battleground where adversaries exploit misconfigurations, compromised identities, and insecure APIs. Using Lacework FortiCNAPP, the FortiGuard Labs team analyzed 2024 threat telemetry and uncovered a concerning trend: Cloud-focused attacks are becoming more sophisticated by leveraging automation and multi-stage persistence techniques. This section offers insights into the evolving threat landscape related to the cloud, along with strategic recommendations to bolster cloud defenses.

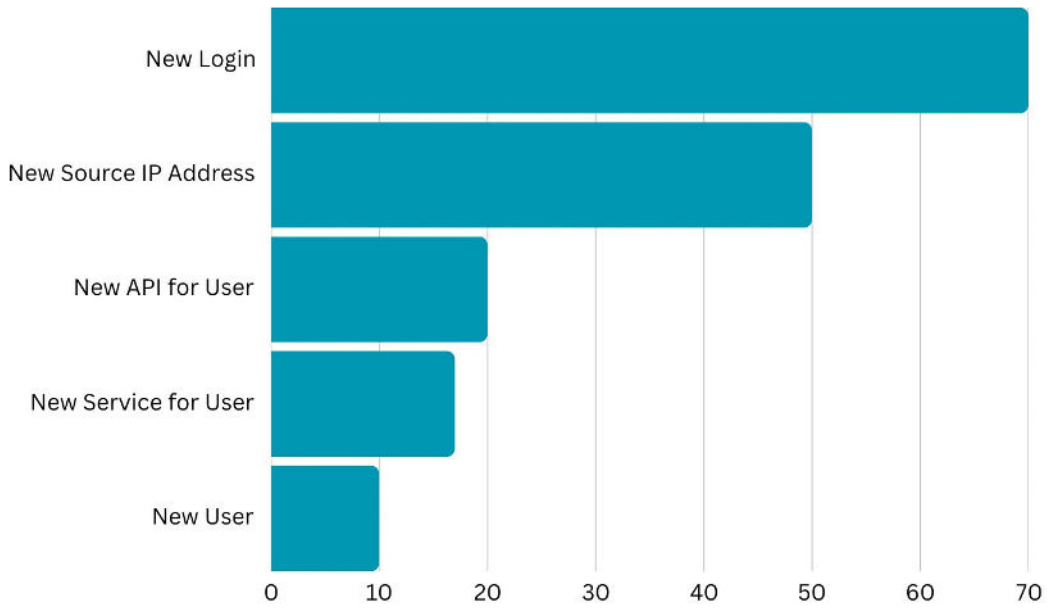


The silent breach: identity compromise in the cloud

Imagine this: A DevOps engineer logs in to a cloud console from a coffee shop. Within hours, an unknown source accesses the same account from another country. At first glance, it seems like an anomaly, perhaps an overlooked VPN connection. But as composite Lacework FortiCNAPP alerts reveal, this is the first stage of an identity compromise that leads to lateral movement, privilege escalation, and data exfiltration.

The following are some of the most prevalent tactics attackers used in 2024 to compromise cloud environments:

- **Discovery (TA0007):** This is the most prevalent tactic, with 25.3% of all incidents mapped, indicating that attackers extensively probe cloud environments before launching full-scale attacks.
- **Initial Access (TA0001):** Our analysis reveals that adversaries most often enter cloud environments through exposed credentials, phishing exploits, and misconfigured cloud authentication settings.
- **Persistence (TA0003) and Privilege Escalation (TA0004):** Attackers are increasingly creating new identities or modifying existing permissions to gain a foothold in enterprise cloud environments.



Security Events Distribution

Indicators of cloud identity compromise include:

- **New logins from unusual locations:** Seventy percent of cases involved new logins from unexpected geographies.
- **New API activity for existing users:** Attackers often test the waters by invoking new APIs on behalf of a compromised account (this occurred in 20% of cases).
- **Credential leaks in code repositories:** Publicly accessible API keys and credentials found on GitHub and GitGuardian are frequently exploited to access cloud environments.

Cloud workloads under siege: the rise of compromised hosts

Cloud servers, containers, and Kubernetes clusters are increasingly the targets of persistent threat actors. While organizations expect adversaries to focus on external breaches, our Lacework FortiCNAPP analysis shows that attackers often operate within the environment, leveraging legitimate services to camouflage their activities.

Common tactics and techniques used in compromised cloud hosts include:

- **Execution via Command and Scripting Interpreters (T1059):** Forty-seven detected incidents reveal attackers executing payloads through Bash, PowerShell, and Python scripts.
- **Command and Control via Web Services (T1102):** Twenty-three cases indicate adversaries abusing legitimate cloud-hosted applications to maintain persistent access.
- **Resource Hijacking (T1496):** Twenty-four incidents showcase the rampant abuse of cloud resources for cryptojacking, affecting both cost and performance.

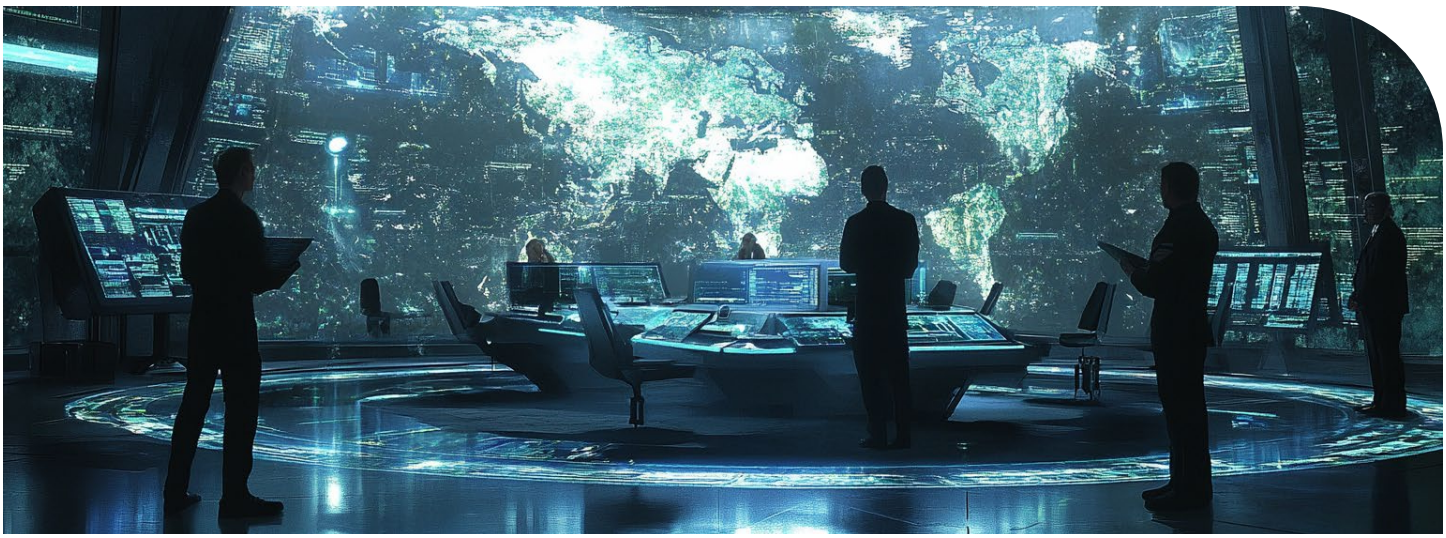
The evolution of cloud threats: what CISOs must know

The rapid expansion of cloud services demands a shift in how security leaders approach cloud risk management. Here are the top challenges CISOs and their teams should keep in mind as they secure their cloud environments:

- **Cloud misconfigurations remain the Achilles' heel.** Open storage buckets and over-permissioned identities continue to be leading vectors of attack. The tactic Exploit Public-Facing Applications (T1190) remains prevalent across breaches.
- **API security is now a top priority.** Attackers increasingly abuse cloud APIs to move laterally, escalate privileges, and extract sensitive data. APIs exploited for identity compromise are mapped to Cloud Instance Metadata API Exploitation (T1556.004).
- **Multi-stage cloud attacks are the new norm.** Instead of single-vector attacks, adversaries now combine credential theft, reconnaissance, and API abuse to maximize impact. The tactic Valid Accounts (T1078) continues to enable attackers to bypass traditional security controls.

Our analysis using Lacework FortiCNAPP underscores the urgency for proactive threat intelligence, automated detection, and resilient identity and API security strategies. Cyber adversaries are not slowing down, and neither should we.

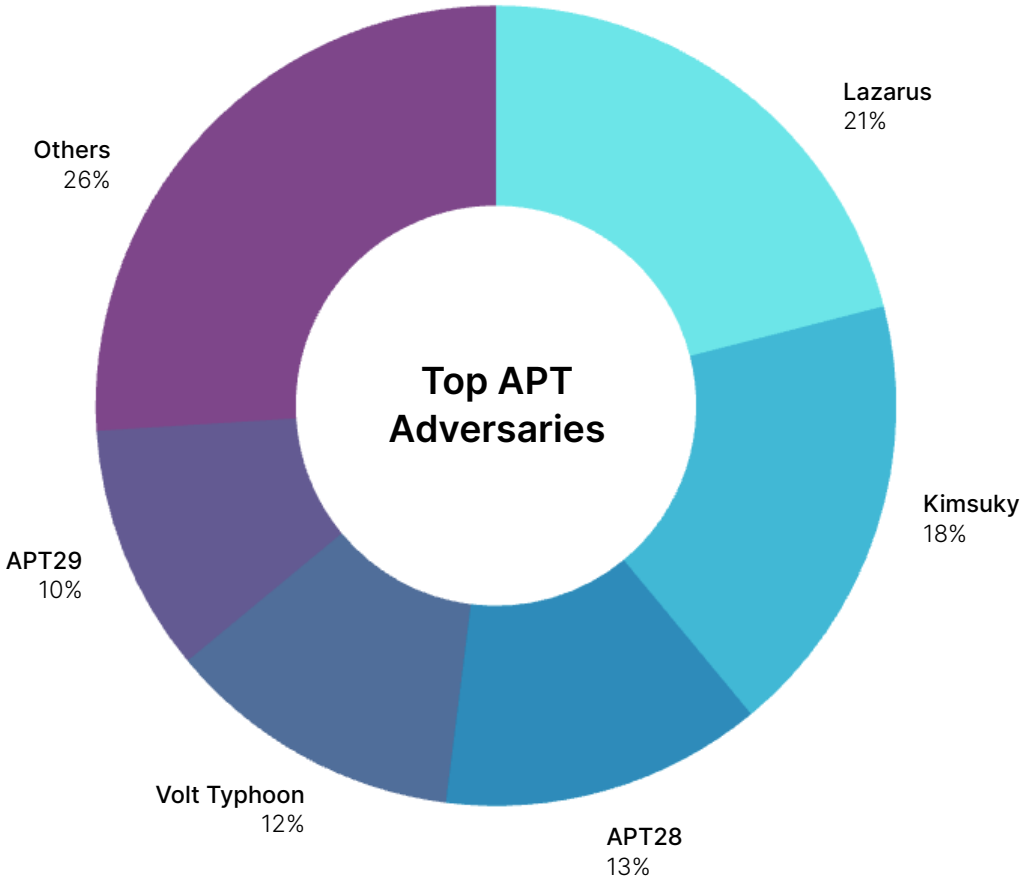
By implementing a zero-trust mindset, improving identity security, and prioritizing cloud workload protection, CISOs can ensure their organizations remain resilient in an era when cloud threats are more persistent and sophisticated than ever.



6. Adversary Landscape Analysis

FortiRecon

The threat landscape of 2024 was marked by the rapid evolution of cybercriminal groups, the rise of new ransomware actors, the increasing sophistication of hacktivist attacks, and the ongoing operations of state-sponsored espionage groups. The FortiGuard Labs team identified and analyzed these trends to provide a comprehensive view of the tactics, techniques, and procedures (TTPs) employed by adversaries.



Ransomware landscape: the evolution of digital organized crime

The RaaS ecosystem continues to expand, with new groups emerging and establishing double and triple extortion models. In 2024, RansomHub (13%), LockBit 3.0 (12%), Play (8%), and Medusa (4%) were the most active ransomware groups, accounting for 37% of the 1,638 identified victims used in our analysis.

Affected sectors and geographic distribution

- The most targeted sectors were manufacturing (17%), business services (11%), construction (9%), and retail (9%).
- The top three countries impacted were the United States (61%), the United Kingdom (6%), and Canada (5%).

The ransomware landscape saw the rise of 13 new groups operating leak sites in 2024, including RansomHub, HellCat, Argonauts Ransomware, InterLock, Bashe (APT73, Eraleig), Termite, Sarcoma, Nitrogen, Lynx, Ransomcortex, and Valencia. This indicates a fragmentation of the cybercriminal ecosystem and diversification in attack methodologies.

RaaS on the darknet

At least six major RaaS services were advertised in underground forums, including PlayBoy, Rape, Medusa, Wing, BEAST, and Cicada 3301. This trend toward hand-holding services lowers the technical entry barrier for cybercriminals, allowing less-skilled adversaries to execute sophisticated attacks.

Hacktivism and ransomware: a dangerous convergence

Hacktivist groups such as CyberVolk, Handala, and KillSec started leveraging ransomware, marking a strategic shift toward more disruptive attacks. This development blurs the line between ideological activism and financially motivated cybercrime.

The Ikaruz Red Team (IRT), previously known for web defacements and nuisance attacks, transitioned into small-scale ransomware operations using leaked LockBit 3.0 builders to target organizations in the Philippines.

Hacktivism: geopolitical targeting and cyber wars

Hacktivists adopted more aggressive tactics in 2024, using Telegram as their primary coordination platform. RipperSec (20%), Z-BL4CX-H4T (14%), and DATABASE LEAKS CYBER TEAM INDONESIA (11%) were the most active groups.

Over 60% of hacktivist campaigns focused on geopolitical causes, with hashtags such as #SavePalestine, #OpIsrael, #OpIndia, and #OpUSA dominating the narrative.

Around 300 vulnerabilities were discussed in hacktivist Telegram channels.

- 182 (61%) have publicly available PoC exploit code.
- 95 (32%) have fully functional exploits available.
- 89 (30%) were exploited by ransomware and APT groups in public campaigns.

Espionage: the quiet cyber war

State-sponsored actors continued to operate with high levels of sophistication. China and Russia led cyber activity, with groups like Lazarus (21%), KIMSUKY (18%), APT28 (13%), Volt Typhoon (12%), and APT29 (10%) conducting advanced campaigns. Not surprisingly, government institutions remain the primary focus, followed by organizations in the technology and education sectors.

Conclusion: Helping CISOs Defeat Adversaries

A static security posture is a failed security posture. And the evidence clearly demonstrates that attackers are accelerating their reconnaissance efforts and rapidly exploiting vulnerabilities, moving and adapting rapidly to create an environment where the time between vulnerability detection and exploitation is rapidly shrinking.

CISOs must act swiftly and decisively to minimize risks and strengthen their defenses. To do this, they need immediate, strategic action that can close exposure gaps before attackers can strike. CTEM can transform security from reactive defense into dynamic risk reduction, enabling CISOs to simulate real-world adversary actions and eliminate security blind spots. Implementing an adaptive security strategy anchored in CTEM is essential for confronting the next wave of global threats.

The CISO playbook for adversary defense

1. **Simulate real-world attacks with adversary emulation**
   - Conduct red and purple teaming exercises mimicking threats like LockBit ransomware and APT29 espionage methods.
   - Utilize MITRE ATT&CK for accurate, behavior-based attack simulations.
2. **Reduce attack surface exposure**
   - Deploy attack surface management (ASM) tools to detect exposed assets, leaked credentials, and exploitable vulnerabilities.
   - Continuously scan darknet forums for emerging ransomware domains and phishing infrastructure.

3. **Prioritize high-risk vulnerabilities**
    - Direct remediation efforts toward those vulnerabilities being actively discussed by hacktivists and cybercrime groups.
    - Use risk-based prioritization frameworks like Exploit Prediction Scoring System (EPSS) and CVSS for effective patch management.
4. **Automate security testing with Breach and Attack Simulation (BAS)**
    - Regularly test endpoint, network, and cloud defenses against real ransomware payloads.
    - Validate a zero-trust architecture by simulating malicious lateral movement.
5. **Leverage dark web intelligence and threat attribution**
    - Monitor darknet marketplaces for emerging ransomware services (such as PlayBoy, Rape, and Medusa).
    - Track hacktivist recruitment and coordination efforts to preemptively address threats like DDoS and web defacement attacks.

Additionally, organizations must adopt advanced threat intelligence and real-time defense tools such as FortiRecon for comprehensive attack surface monitoring and employ advanced IPS solutions for immediate exploitation blocking.

Cyberthreats no longer wait for vulnerabilities to be patched—they strike rapidly before most organizations can respond. To successfully navigate this escalating threat landscape, CISOs must anticipate threats at machine speed, automate defenses, and continuously manage exposure to stay one step ahead of adversaries.

For questions related to this report, please contact us.

If you're reading a physical copy of this report, you can download the digital copy at **Fortiguard.com/ThreatLandscapeReport**

FORTINET

www.fortinet.com

May 1, 2025 4:16 PM / MKTG-1414-A-0-EN