2025 IT SECTOR CYBER THREAT REPORT

March 2026

Powered by the Predictive Adversary Scoring System (PASS)

IT-ISAC MEMBER USE ONLY

IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

ABOUT THE IT-ISAC

Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that provides a trusted forum for IT companies and those that leverage IT for core business functions to share information, manage risks, and collaborate on cyber incident response and strategy.

Our mission is to grow a diverse community of companies that leverage information technology and have in common a commitment to cybersecurity, to serve as a force-multiplier that enables collaboration and sharing of relevant, actionable cyber threat information, effective security policies and practices for the benefit of all.

Our membership is comprised of security leaders from leading technology companies across the globe. We have built a network of relationships with trusted partners across the critical-infrastructure community and through this multidirectional sharing, we help companies manage risks to their enterprises and to the critical infrastructure community.

TABLE OF CONTENTS

INTRODUCTION

The Information Technology - Information Sharing and Analysis Center (IT-ISAC) plays a critical role in monitoring cyber threats targeting the IT sector, enabling member companies and partners to identify, prevent, mitigate, and respond to industry-targeted attacks through collaborative threat intelligence. By facilitating the collection, analysis, and dissemination of actionable intelligence and effective security measures, IT-ISAC helps members manage risk while strengthening resilience across the entire critical infrastructure ecosystem.

This report examines the various cyber threat actors observed in the sector and reflects IT-ISAC's core mission: equipping members with the insights and resources needed to counter sophisticated, active threats. The threat intelligence landscape is dynamic and evolving, with advanced nation-state actors and well-coordinated, financially motivated cybercriminal groups continuously deploying sophisticated tactics, techniques, and procedures (TTPs). While focused on the IT sector, this report also highlights interconnected risks affecting multiple industries – a crucial reminder that no sector operates in isolation.

The IT-ISAC maintains attack playbooks on more than 330 adversaries. These playbooks capture essential adversary data such as motives, TTPs, and known sectors of operation. The IT-ISAC developed the Predictive Adversary Scoring System (PASS) in partnership with member organizations to prioritize the monitoring and analysis of known adversaries. PASS enables us to identify which threat actors present the greatest danger to specific sectors and sub-sectors. This helps members understand which threat actors are most relevant to them. By evaluating adversaries across multiple parameters including capability, intent, and historical activity, PASS allows organizations to quantify their susceptibility and make informed resource allocation decisions.

PREDICTIVE ADVERSARY SCORING SYSTEM (PASS) EXPLAINED

The Predictive Adversary Scoring System (PASS) provides a comprehensive scoring system based on specific factors, including the adversary's motivation, capabilities, and past actions, allowing organizations to assess their risk exposure and allocate resources accordingly.

PASS focuses on four key metrics to determine a specific adversarial risk:

- **Level of Activity:** How recently has the adversary been active.
- **Frequency of Sector Targeting:** The number of times the adversary has targeted the IT sector.
- **Sophistication/Impact:** The complexity of the adversary's tactics, techniques, and procedures (TTPs) and their impact.
- **Motivation:** The driving force behind the adversary - financial, geopolitical, ideological, or recognitional.

PASS employs a comprehensive set of metrics to assign adversaries a score ranging from 0 to 100, representing the highest level of threat when a threat actor satisfies all predefined system criteria. Higher scores indicate a greater risk to organizations within the sector. Adversaries with elevated scores represent significant threats due to their frequent targeting of the sector and their demonstrated sophistication and impact in past operations.

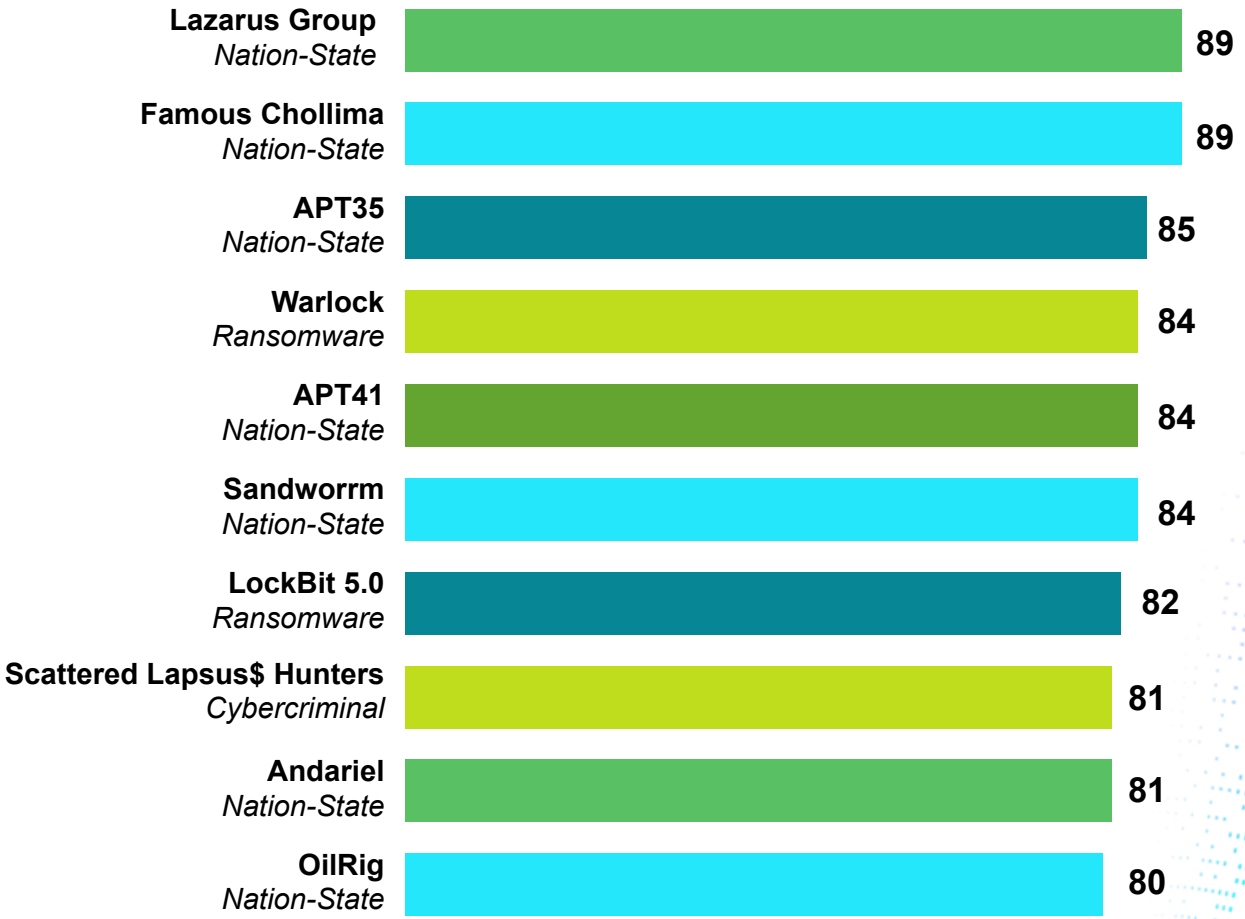
PASS is available to IT-ISAC members in Excel and Google Sheet versions for easy data entry and analysis. The information is also available in the secure members-only Notion dashboard, which serves as a portal for members to use tools, share information, and communicate collectively.

Members leveraging PASS gain valuable insights into the threats they face, enabling them to improve their defenses or prepare for an impending attack. This tool facilitates IT-ISAC's ongoing mission to equip its members with actionable capabilities that advance their resilience and preparedness in an evolving threat landscape.

TOP 10 THREAT ACTORS | IT SECTOR

PASS was applied to the over 330 Adversary Attack Playbooks the IT-ISAC maintains to identify and prioritize the adversaries most frequently targeting the IT industry. This comprehensive effort identified 77 adversaries active in the IT Sector in 2025. Below, we have highlighted the top 10 adversaries targeting the IT Sector.

TOP 10 ACTORS PASS SCORE



LAZARUS GROUP (89)

Aliases:

- **HIDDEN COBRA (CISA)**
- **Labyrinth Chollima (CrowdStrike)**
- **Diamond Sleet (Microsoft)**
- **Guardians of Peace (MITRE)**
- **NICKEL ACADEMY (Secureworks)**

By 2025, Lazarus and its associated sub-clusters (such as financially focused units often tracked separately by vendors) continue to prioritize cryptocurrency theft, supply chain compromise, and social engineering-driven intrusions, including fake job recruitment and developer targeting.

Overall, the group blends espionage, sabotage, and cybercrime to support North Korea's strategic goals, particularly sanctions evasion and regime revenue generation, while maintaining strong operational security, rapid tool reuse, and frequent infrastructure rotation.

FAMOUS CHOLLIMA (89)

Aliases:

- **BadClone (CrowdStrike)**
- **TenaciousPungsan (Datadog)**
- **UNC5267 (Mandiant)**
- **WaterPlum (NTTSecurity)**
- **PurpleBravo (Recorded Future)**
- **NickelTapestry (SecureWorks)**
- **VoidDokkaebi (Trend Micro)**

Famous Chollima is a North Korea-aligned state-sponsored cyber threat actor that has been active since at least the late 2010s. The group is well known for its elaborate social engineering and insider threat schemes, especially posing as legitimate remote IT job applicants, contractors, or recruiters to gain footholds inside technology, finance, and cryptocurrency organizations. This access is typically followed by the deployment of custom malware to steal credentials and data or illicitly funnel income back to the DPRK.

In 2025, security researchers from Cisco Talos documented a surge in activity targeting cryptocurrency and blockchain professionals, with campaigns using deceptive job postings, fake interview platforms, and Python-based remote access malware like PylangGhost to compromise systems and exfiltrate sensitive information, while also leveraging generative AI and deepfake techniques to make fraudulent identities more convincing.

Check out the IT-ISAC CSaaS SIG's Spotting Fraudulent Job Seekers, which examines the growing threat of fraudulent workers and provides practical guidance for identifying them at every stage of the hiring lifecycle. Read the full paper here.

APT35 (85)

Aliases:

- **Charming Kitten (CrowdStrike, Mandiant)**
- **ITG18 (IBM X-Force)**
- **NewsBeef (Kaspersky)**
- **Mint Sandstorm (Microsoft)**
- **G0059 (MITRE)**
- **Magic Hound (Palo Alto Networks / Unit 42)**
- **TA453 (Proofpoint)**
- **Yellow Garuda (PwC)**
- **Cobalt Illusion (Secureworks)**

APT35, commonly referred to as Charming Kitten, is an Iran-linked state-sponsored cyber-espionage group assessed to operate on behalf of the Islamic Revolutionary Guard Corps (IRGC). Active since at least 2013, the group is primarily focused on intelligence collection, credential harvesting, and surveillance operations targeting individuals and organizations of strategic interest to the Iranian government.

Historically, APT35 has targeted government entities, defense contractors, journalists, academics, dissidents, think tanks, and technology companies across North America, Europe, and the Middle East. The group is known for its sophisticated social engineering campaigns, often impersonating journalists, researchers, or conference organizers to build rapport with targets before delivering credential phishing lures.

In 2025, APT35 continued to conduct sustained espionage campaigns primarily centered on credential harvesting and social engineering. Public reporting from Checkpoint documented spearphishing operations targeting academics, journalists, and cybersecurity professionals through carefully crafted impersonation campaigns delivered via email and messaging platforms like WhatsApp. These operations frequently directed victims to spoofed login pages designed to capture credentials and, in some cases, multi-factor authentication (MFA) codes for cloud-based email services such as Gmail and Microsoft 365.

WARLOCK (84)

Aliases:

- **Storm-2603 (Microsoft)**
- **Gold Salem (Sophos)**

Warlock is a ransomware-as-a-service (RaaS) threat actor that first emerged in June 2025, quickly gaining notoriety for exploiting unpatched Microsoft SharePoint zero-day vulnerabilities (CVE-2025-53770) to gain initial access and ultimately encrypt and exfiltrate victims' data, threatening to publicize the stolen information if ransoms aren't paid. Since initiating operations, the group has claimed dozens of victims across government, finance, technology, communications, and other sectors worldwide.

In 2025, the IT-ISAC observed that 29.2% of victims publicly claimed by Warlock were in the IT sector, highlighting the group's preference for targets with valuable digital assets and critical infrastructure that can be leveraged for maximum financial gain.

APT41 (84)

Aliases:

- **Wicked Panda (CrowdStrike)**
- **Winnti / Winnti Group (Kaspersky, ESET, Clearsky)**
- **Double Dragon (Mandiant)**
- **Brass Typhoon (Microsoft)**

APT41 (Double Dragon) is a China-linked state-sponsored threat group active since at least 2012, known for blending espionage with financially motivated cybercrime. Over the years, the group has targeted a wide range of sectors, including technology, telecommunications, healthcare, and government.

In 2025, APT41 remained a prominent actor within the threat landscape, with Trellix reporting that the group's activity increased by approximately 113% in the first quarter of 2025 compared to Q4 2024. APT41 continued to conduct operations across multiple sectors, employing sophisticated tradecraft that included leveraging trusted cloud services for covert command-and-control, exploiting both zero-day and known vulnerabilities in enterprise and edge infrastructure, and using modular malware frameworks like DeedRat and ShadowPad, which are often deployed via DLL side-loading to bypass EDR solutions.

A notable campaign spotted in 2025 involved the TOUGHPROGRESS malware, which abused Google Calendar as a C2 channel, embedding encrypted commands in calendar events to blend malicious traffic with legitimate enterprise cloud activity.

SANDWORM (84)

Aliases:

- **Electrum**
- **TeleBots**
- **Voodoo Bear (CrowdStrike)**
- **FrozenBarents (Google Threat Analysis Group)**
- **APT44 (Mandiant)**
- **Seashell Blizzard (Microsoft)**
- **Iron Viking (SecureWorks)**

Sandworm (also tracked as APT44 and linked to Russia's GRU military intelligence unit 74455) is one of the most notorious state-sponsored cyber threat actors, active in public reporting since at least 2009 and credited with some of the most destructive cyberattacks in history, including the NotPetya outbreak and Ukrainian power grid disruptions.

The group's motivations are primarily strategic: supporting Russian military and geopolitical objectives through cyber sabotage, disruption, and espionage against government, energy, logistics, agricultural, and critical infrastructure targets, especially in Ukraine and NATO countries.

In 2025, Sandworm's operations continued to showcase destructive capabilities, deploying new wiper malware such as Zerolot and Sting against the Ukrainian government and commercial sectors, including the country's vital grain industry, in efforts likely aimed at weakening Ukraine's economy amid the ongoing conflict. Later in the year, ESET also confirmed that Sandworm was behind a cyberattack targeting Poland's power grid, where it deployed a previously undocumented data-wiping malware dubbed DynoWiper in an attempt to destroy systems and data at energy sector organizations.

LOCKBIT 5.0 (82)

Aliases: N/A

LockBit is one of the most prolific RaaS cybercrime operations active since 2019, known for enabling a large network of affiliates to deploy its ransomware in exchange for a share of the profits.

LockBit is financially motivated and operates by providing ransomware tools, infrastructure, and a public data-leak site where stolen information is published to pressure victims into paying. The group has consistently ranked among the top ransomware threats globally, historically accounting for a significant portion of all ransomware incidents and targeting organizations across technology, government, healthcare, logistics, finance, and other sectors worldwide.

In 2025, LockBit reemerged following law enforcement disruptions in 2024, setting up new infrastructure and launching LockBit 5.0, which has been observed targeting Windows, Linux, and VMware ESXi systems across Europe, the Americas, and Asia. The updated variant includes advanced evasion techniques and broader cross-platform capabilities, highlighting a potent threat to enterprises and critical infrastructure.

The IT-ISAC released its 2025 annual ransomware report, which includes a detailed analysis of prominent ransomware actors known to target the IT Sector, their TTPs, sector trends, and more. In 2025, they tracked nearly 750 ransomware attacks against the IT sector. Due to LockBit 5.0's transition to new infrastructure, they only accounted for 9 attacks against the sector in 2025; however, LockBit has a known preference for the IT Sector, and we expect attacks to escalate as the group recovers to its normal operating capacity.

SCATTERED LAPSUS$ HUNTERS (81)

Aliases: N/A

Scattered LAPSUS$ Hunters is a cybercriminal alliance that was formed in 2025, bringing together members of three notorious hacking collectives (Scattered Spider, LAPSUS$, and ShinyHunters), all of which are linked to "The Com:" a loose-knit community of English-speaking, often younger threat actors (ages 18–30) based in the U.S. and the U.K.

The collective focuses on financially motivated campaigns centered on large-scale data theft, credential harvesting, and extortion, with a strong emphasis on social engineering rather than custom malware. Its operations commonly involve voice phishing, SIM swapping, MFA fatigue attacks, abuse of OAuth tokens, and direct exploitation of identity-management workflows in CRM and helpdesk platforms such as Salesforce and Zendesk to gain access to sensitive enterprise and customer data, which is then used for extortion.

ANDARIEL (81)

Aliases:

- **Silent Chollima (CrowdStrike)**
- **APT45 (Mandiant/Google)**
- **Onyx Sleet / PLUTONIUM (Microsoft)**
- **Jumpy Pisces / Nickel Hyatt (Palo Alto Networks)**
- **Stonefly / Clasiopa (Symantec)**

Andariel is a sophisticated North Korean state-sponsored unit operating under the Reconnaissance General Bureau (RGB). Andariel frequently compromises IT service providers, software developers, and ERP vendors to conduct supply chain attacks, enabling access to high-value government, military, and enterprise networks.

The unit is notable for pioneering the use of fraudulent remote IT workers to infiltrate Western organizations, providing both a foothold for internal reconnaissance and a means of generating revenue through illicit salaries.

In 2025, the group maintained a dual-focus approach: continuing high-stakes espionage against defense, nuclear, and critical infrastructure sectors, while simultaneously expanding financially motivated operations targeting the IT sector.

OILRIG (80)

Aliases:

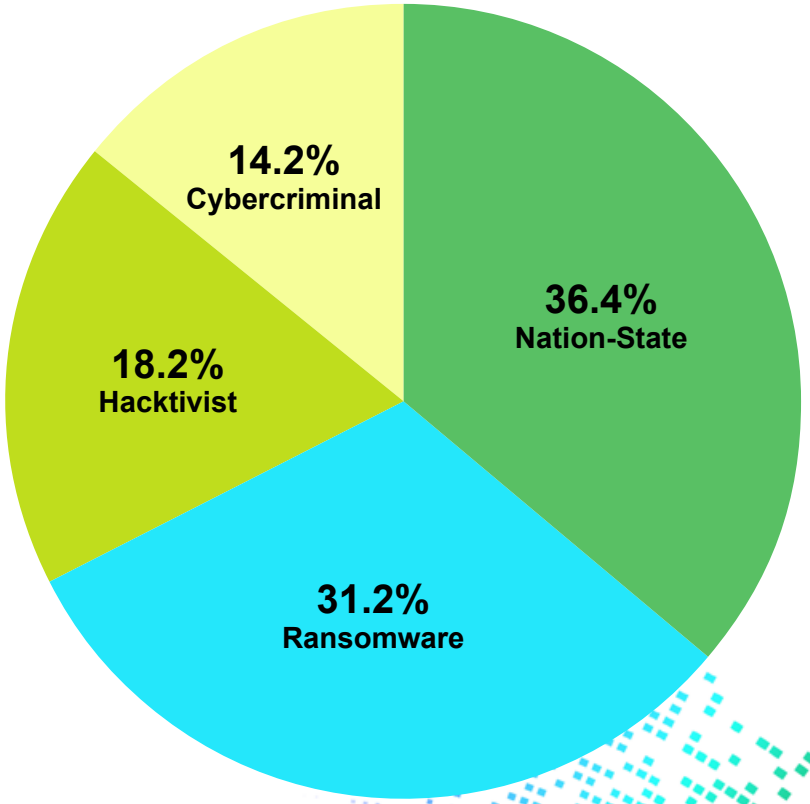
- **Helix Kitten / Twisted Kitten (CrowdStrike)**
- **Greenbug / Evasive Serpens (Palo Alto Networks)**
- **Cobalt Gypsy (SecureWorks)**
- **Crambus (Symantec)**
- **APT34 (Mandiant/FireEye)**
- **Hazel Sandstorm / EUROPIUM (Microsoft)**
- **Earth Simnavaz (Trend Micro)**

OilRig is a state-sponsored cyber-espionage group originating from Iran. In 2025, the group's activity remained focused on long-term intelligence collection aligned with Iranian national security and geopolitical interests.

While OilRig targets multiple sectors, including government, energy, and telecommunications, it has focused on the IT sector as an entry point. By gaining access to IT service providers and Managed Service Providers (MSPs), OILRIG facilitates supply chain compromise, leveraging the trusted access these providers have to their end-clients' networks.

SUMMARY OF ADVERSARY TYPES

ADVERSARY TYPE PERCENTAGES



NATION-STATE ACTORS

Nation-state actors accounted for the largest share of adversaries targeting the IT sector, at 36.4% (28 groups) of the total threat actors observed. Unlike purely financially motivated actors, state-sponsored groups pursue long-term strategic objectives that often extend beyond traditional espionage.

These actors have increasingly shifted from opportunistic data theft to strategic persistence operations, frequently targeting software supply chains, managed service providers (MSPs), cloud platforms, and telecommunications infrastructure. By compromising widely used technology providers, attackers seek to gain scalable access to downstream customers across multiple industries. This supply chain focus allows adversaries to pre-position themselves within critical digital infrastructure for potential disruptive or destructive operations should geopolitical tensions escalate.

Their activity is characterized by their extensive resources, strategic direction, operational patience, and the deployment of custom-built malware designed to evade modern enterprise detection and response solutions. In many cases, these actors leverage zero-day vulnerabilities and sophisticated credential harvesting techniques to maintain long-term access. Living-off-the-land (LOTL) techniques are also common, as state-sponsored actors leverage legitimate tools and traffic to evade detection.

RANSOMWARE

Ransomware groups were the second-largest category of adversaries targeting the IT sector, accounting for 31.2% (24 groups). As with other critical sectors, ransomware remains a persistent and growing threat to IT organizations, given its role as a service enabler for the broader economy.

Throughout 2025, ransomware groups continued to operate under the RaaS model. This model allows developers to lease their malware and infrastructure to affiliates, increasing operational scale and attack volume. Groups increasingly rely on double and triple extortion tactics: exfiltrating sensitive data prior to encryption and threatening public leaks, regulatory reporting, or direct customer notification to intensify pressure on victims.

IT service providers and software companies are particularly attractive targets because a single compromise can cascade across multiple client environments. Attackers understand that downtime for IT providers directly impacts the business continuity of numerous dependent organizations, increasing the likelihood of ransom payments.

HACKTIVISTS

Hacktivist groups accounted for 18.2% (14 groups) of observed threat actors targeting the IT sector. While historically considered less sophisticated actors, recent activity shows that hacktivist campaigns have become more coordinated and geopolitically aligned.

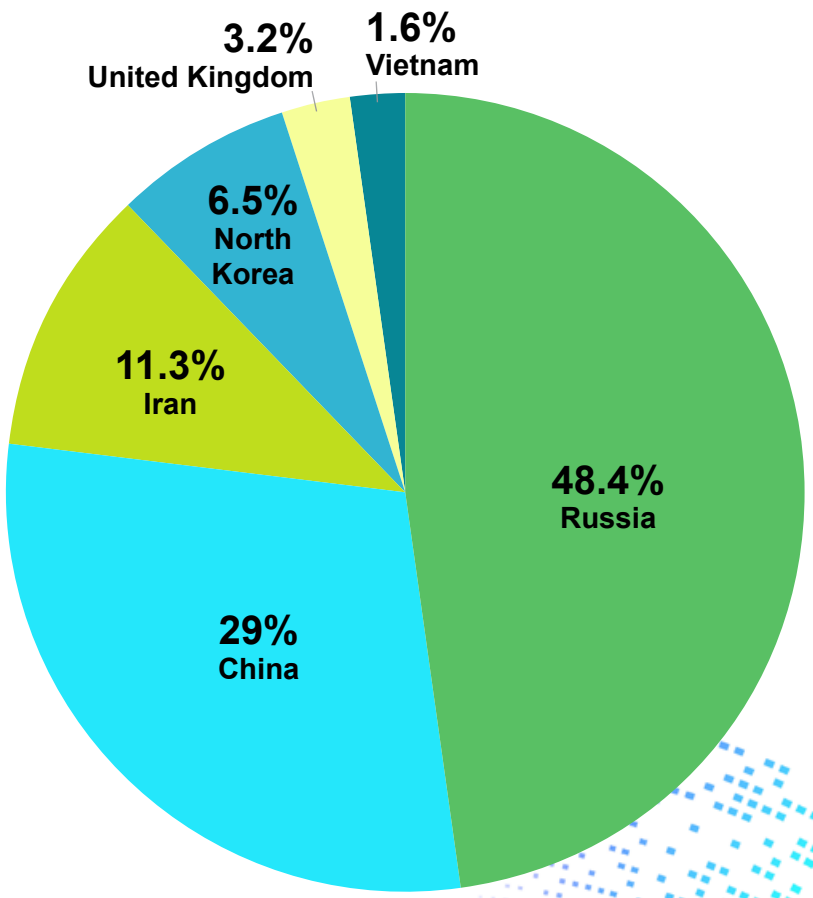
In 2025, many hacktivist collectives aligned their operations with national interests, social movements, or regional conflicts. Their campaigns frequently involve DDoS attacks, website defacements, and data leaks intended to generate public attention and reputational damage rather than financial gain.

CYBERCRIMINALS

Cybercriminal groups comprised 14.2% (11 groups) of the identified threat actors targeting the IT sector. These actors frequently focus on credential theft, phishing campaigns, malware distribution, and illicit access sales on underground marketplaces. Compromised credentials and initial access to enterprise environments are often sold to larger ransomware operations or state-affiliated actors, effectively serving as the “initial access brokers” of the cybercrime ecosystem.

SUMMARY OF ADVERSARY COUNTRY OF ORIGIN

ADVERSARY ORIGINS



Please note this excludes adversaries not associated with a country of origin.

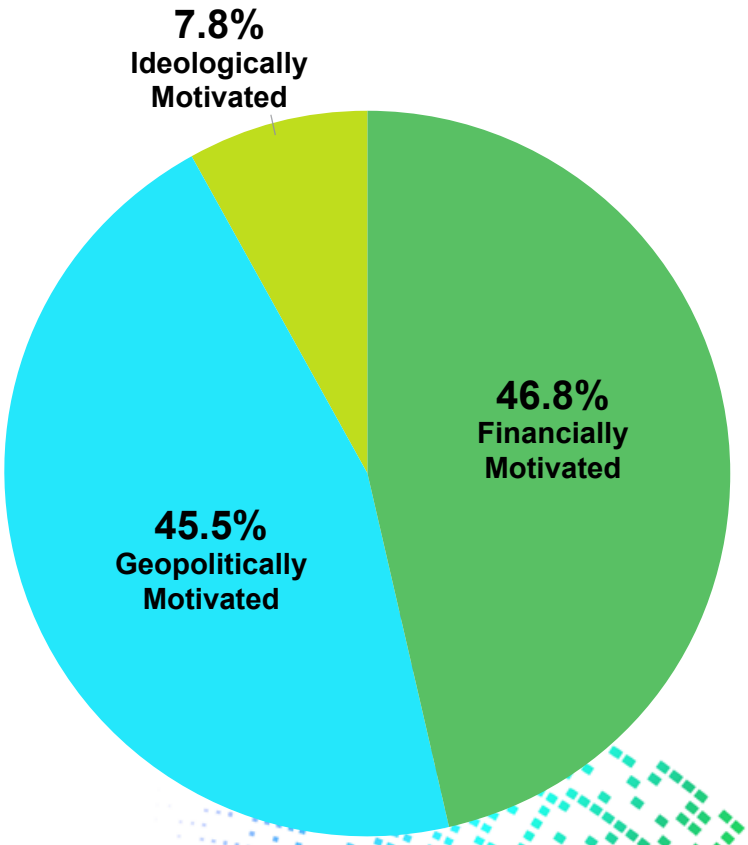
There is a wide range of cyber groups operating from or linked to Russia, including ransomware gangs, financially motivated cybercriminals, hacktivist collectives, and state-affiliated actors. In fact, 48.4% of all observed threat actors active against the sector in 2025 originated in Russia. These groups targeted IT companies for different reasons: some focused on making money through ransomware or selling stolen access, while others pursued espionage or disruptive activity tied to broader geopolitical tensions.

China ranked second among countries with the most actors targeting the IT sector, accounting for 29% of the total. Chinese adversaries have historically focused on intellectual property theft and cyber espionage. However, in recent years, these actors have increasingly prioritized long-term persistence across critical infrastructure, including within telecommunications networks, cloud environments, and other critical digital infrastructure, allowing them to maintain continuous access, monitor systems, and gather intelligence over extended periods.

Actors from Iran, North Korea, the United Kingdom, and Vietnam represented smaller portions of the overall landscape. Iranian groups (11.3%) continued to conduct espionage and disruptive cyber operations aligned with regional and political tensions. Whereas, North Korean actors (6.5%) remained heavily focused on revenue generation, including cryptocurrency theft and fraudulent remote IT worker schemes.

SUMMARY OF THREAT ACTOR MOTIVATION

THREAT ACTOR MOTIVATION



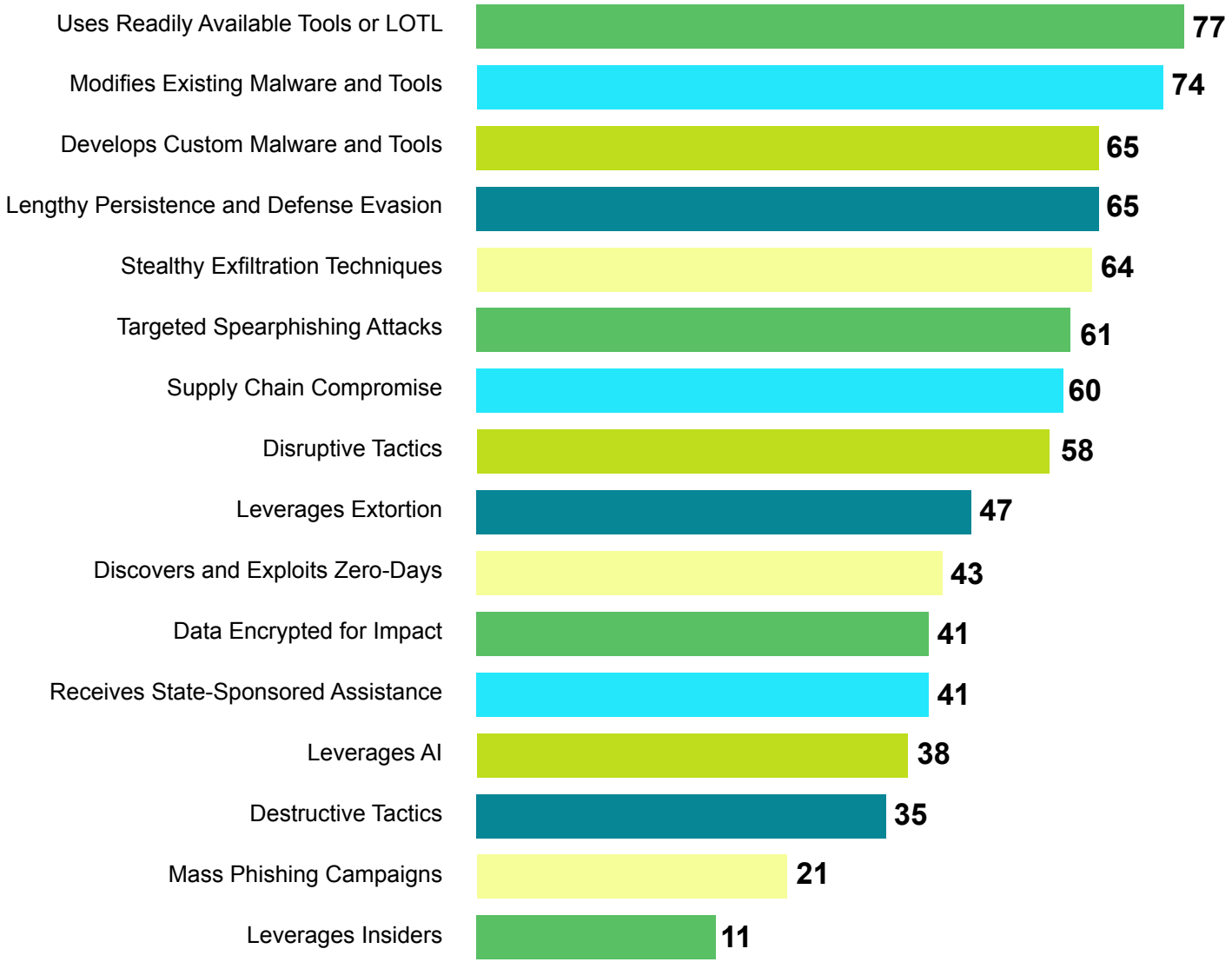
A majority of the adversaries targeting the IT sector were either financially or geopolitically motivated. Financially motivated groups, accounting for 46.8% of identified actors, continued to pose a significant threat to IT organizations, particularly through ransomware, data extortion, business email compromise, and the sale of stolen network access. Many of these attacks appeared opportunistic, with actors scanning for vulnerable internet-facing systems, exploiting unpatched software, leveraging phishing campaigns, or purchasing credentials from initial access brokers. Because IT companies often manage sensitive data and serve multiple downstream customers, they remain attractive targets for groups seeking high-impact payouts.

Geopolitically motivated actors followed closely behind, accounting for 45.5% of adversaries observed targeting the IT sector. These groups focused on espionage, intellectual property theft, supply chain compromise, and long-term persistence. Rather than seeking immediate financial returns, their objectives centered on strategic advantage, intelligence collection, and in some cases, pre-positioning for potential future disruption.

Ideologically motivated actors accounted for a much smaller portion of observed groups, representing 7.7% of the total. These actors were typically associated with hacktivist campaigns, including website defacements, DDoS attacks, and data leaks intended to generate public attention. While their operations could cause reputational damage and temporary service disruption, they generally lack the sustained resources and operational depth seen in financially or geopolitically motivated campaigns.

SUMMARY OF TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) USED BY ADVERSARIES

SOPHISTICATION TECHNIQUE (PASS COUNT)



SUMMARY OF TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) USED BY ADVERSARIES

In 2025, the IT sector has witnessed a sophisticated shift in adversary behavior, characterized by the following top five tactics, techniques, and procedures (TTPs). These findings highlight a landscape where attackers prioritize stealth and persistence by blending into the environment rather than using loud, detectable malware. The percentage listed alongside each TTP reflects the share of adversaries observed using that method, providing a data-driven picture of the threats facing the sector today.

1. Uses Readily Available Tools or Living-off-the-Land (100.0%)

Adversaries frequently leverage legitimate, pre-installed system tools like PowerShell, WMI, and Microsoft-signed binaries (Teams or Certutil) to carry out their operations. By using these trusted tools, actors can blend into normal network activity and evade traditional antivirus or file-based detection methods.

To mitigate, organizations can implement application whitelisting to restrict the execution of unauthorized binaries and scripts. This can be paired with the enhanced logging of native tool abuse, so that LOTL binaries (certutil, mshta, wmic, etc.) trigger alerts.

2. Modifies Existing Malware and Tools (96.1%)

Rather than using off-the-shelf malware or taking the time to create completely new malware, many actors modify existing malware to bypass detection. These changes, sometimes assisted by AI, alter the malware's signature and behavior, making it harder for standard security tools to detect and block.

To defend against this, organizations can deploy behavior-based endpoint detection and response (EDR) solutions rather than relying on signature detection, since modified tools bypass static signatures easily. Organizations can prioritize detections based on TTPs (MITRE ATT&CK) rather than known hashes, and use memory scanning and sandboxed detonation to catch functionally similar payloads regardless of code changes.

3. Develops Custom Malware and Tools (84.4%)

Adversaries, particularly those with state backing, create malware tailored to specific targets. Custom-built tools are designed for compatibility with the victim's environment and to evade the security controls in places, increasing their chances of success.

To prevent infections from custom malware, organizations can focus on hardening the delivery vectors custom malware relies on, such as phishing, vulnerable public-facing apps, and removable media. Network segmentation, combined with egress filtering, limits the reach of custom implants.

4. Lengthy Persistence and Defense Evasion (84.4%)

Adversaries are prioritizing the "long game," utilizing techniques to maintain access for months. This involves disabling security logs, tampering with EDR processes, and modifying group policy objects (GPOs) to weaken enterprise-wide controls.

Audit and monitor persistence locations regularly including registry run keys, scheduled tasks, services, startup folders, etc. Enforce the principle of least privilege so that establishing persistence requires elevated rights, and conduct regular credential rotation and privilege reviews to disrupt long-dwell attackers.

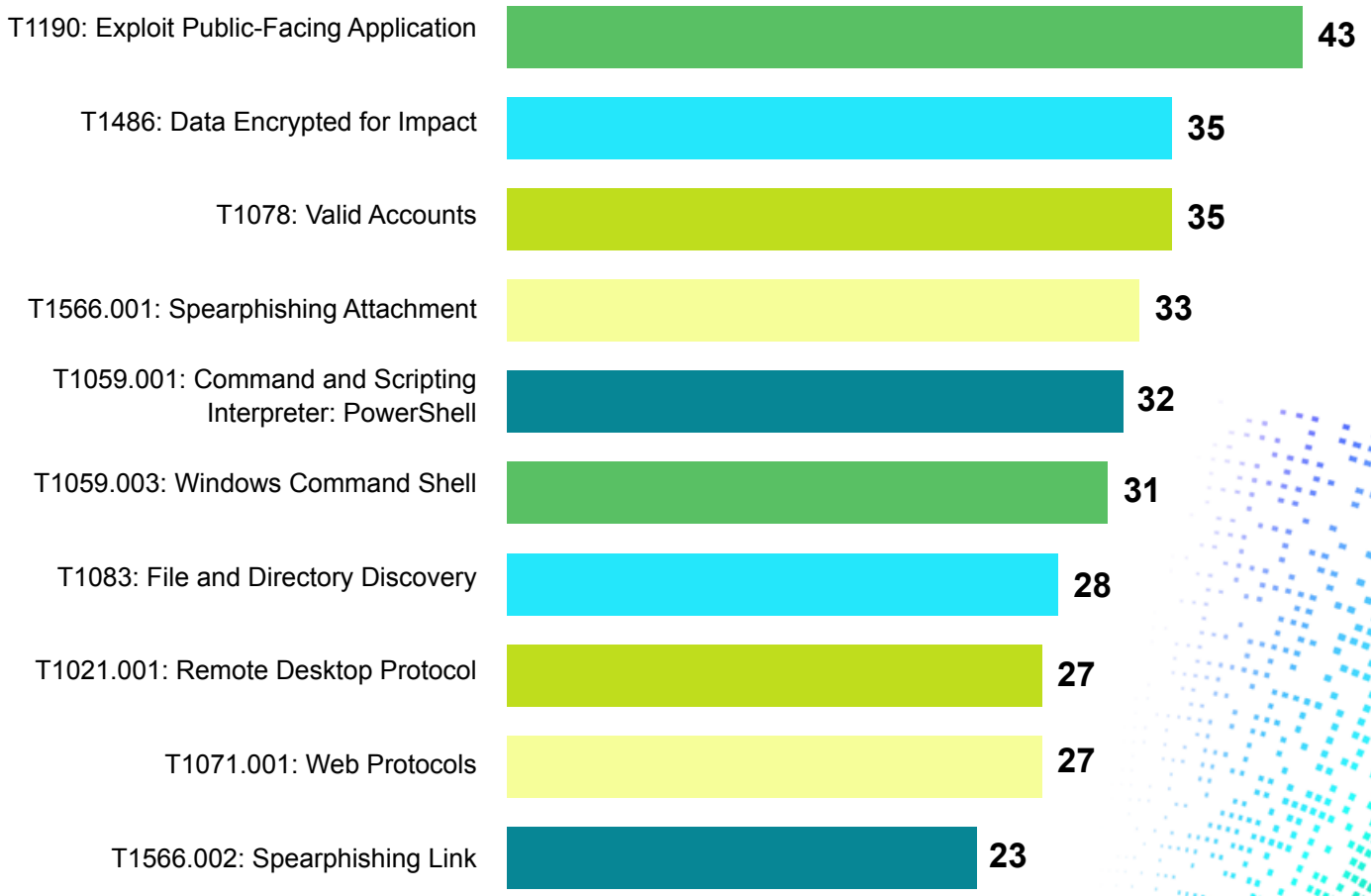
5. Stealthy Exfiltration Techniques (83.1%)

Attackers are siphoning data using highly discreet methods, such as sending data in small, encrypted chunks via trusted platforms (e.g., Dropbox or Google Docs) or through covert channels like DNS tunneling. This allows them to stay under the radar of traditional data loss prevention (DLP) alerts.

Deploying DLP solutions and monitoring for anomalous outbound data volumes, especially over common allowed protocols like HTTPS, DNS, or cloud storage can help defend against this. Organizations can implement DNS monitoring and SSL/TLS inspection to catch tunneling and C2 over encrypted channels. Establishing a baseline of normal outbound traffic makes anomalies far easier to detect.

TOP MITRE ATT&CK® TECHNIQUES

MITRE ATT&CK® TECHNIQUE USED BY ALL GROUPS (PASS COUNT)



TOP MITRE ATT&CK® TECHNIQUES

The section below outlines the most frequently observed MITRE ATT&CK® techniques across the 72 adversaries analyzed in this report, ranked by prevalence. The top five techniques are examined in greater detail, along with recommended mitigations to help organizations defend against these methods.

T1190: EXPLOIT PUBLIC-FACING APPLICATION (54.5%)

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

T1486: DATA ENCRYPTED FOR IMPACT (44.2%)

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

T1078: VALID ACCOUNTS (44.2%)

Adversaries may obtain and abuse credentials for existing accounts to gain initial access, maintain persistence, escalate privileges, or evade defenses. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

T1566.001: SPEARPHISHING ATTACHMENT (42.9%)

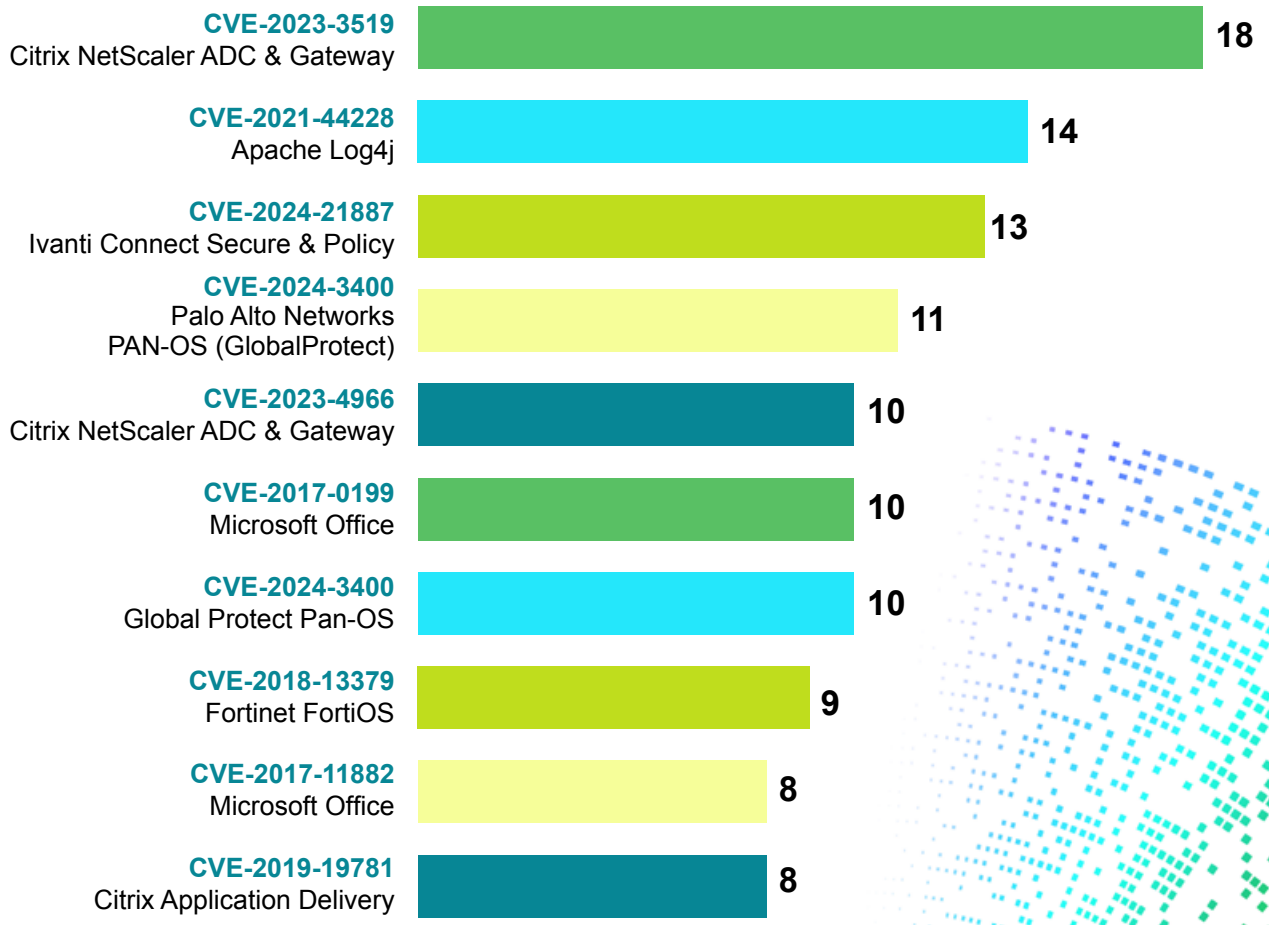
Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon user execution to gain execution.

T1059.001: COMMAND AND SCRIPTING INTERPRETER: POWERSHELL (41.6%)

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including the discovery of information and the execution of code. Examples include the Start-Process cmdlet, which can be used to run an executable and the Invoke-Command cmdlet, which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

TOP COMMON VULNERABILITIES AND EXPOSURES (CVEs) ABUSED

TOP EXPLOITED CVEs (PASS COUNT)



TOP EXPLOITED (CVEs) DISCOVERED IN 2025

Rank	Critical Vulnerability	CVSS	Product
1	CVE-2025-49704	8.8	Microsoft SharePoint Server (2016, 2019, Subscription Ed.)
2	CVE-2025-49706	6.5	Microsoft SharePoint Server (2016, 2019, Subscription Ed.)
3	CVE-2025-53770	9.8	Microsoft SharePoint Server (On-Premises)
4	CVE-2025-53771	6.3	Microsoft SharePoint Server (Subscription Edition)
5	CVE-2025-14847	8.7	MongoDB Server (Versions 3.6 through 8.2)
6	CVE-2025-29824	7.8	Windows Common Log File System (CLFS) Driver
7	CVE-2025-61882	9.8	Oracle E-Business Suite
8	CVE-2025-55182	10.0	React
9	CVE-2025-0282	9.8	Ivanti Connect Secure / Policy Secure / ZTA Gateways
10	CVE-2025-10035	10.0	Fortra GoAnywhere MFT

CVE-2023-3519: CITRIX NETSCALER REMOTE CODE EXECUTION (RCE)

CVSS: 9.8

Impact: This is a critical stack buffer overflow vulnerability in the Citrix NetScaler (formerly ADC) and Gateway. It allows an unauthenticated attacker to execute arbitrary code as **root** by sending a specially crafted HTTP GET request. In 2025, it remains a favorite for nation-state actors seeking initial access to corporate networks.

CVE-2021-44228: APACHE LOG4J "LOG4SHELL"

CVSS: 10.0

Impact: Despite being several years old, Log4Shell remains the second most abused vulnerability in 2025 due to its presence in deep-seated legacy Java applications. It allows unauthenticated RCE via JNDI lookups, granting attackers full control over the affected server.

CVE-2024-21887: IVANTI CONNECT SECURE COMMAND INJECTION

CVSS: 9.1

Impact: This vulnerability affects the web components of Ivanti Connect Secure and Policy Secure gateways. It is frequently chained with an authentication bypass (CVE-2023-46805) to allow unauthenticated attackers to execute arbitrary commands. This has been a major driver for "gateway takeovers" observed throughout 2025.

CVE-2024-3400: PALO ALTO NETWORKS PAN-OS COMMAND INJECTION

CVSS: 10.0

Impact: A critical flaw in the GlobalProtect feature of Palo Alto Networks firewalls. It allows an unauthenticated remote attacker to execute arbitrary code with root privileges. In 2025, this has been extensively used by threat actors to exfiltrate firewall configuration files and move laterally into internal networks.

CVE-2023-4966: CITRIX "CITRIX BLEED"

CVSS: 7.5

Impact: This information disclosure vulnerability allows unauthenticated attackers to leak sensitive memory contents from Citrix NetScaler appliances. The primary risk is the theft of session tokens, which allows attackers to bypass MFA and hijack active user sessions.

2025 TRENDS

The 2025 threat landscape for the IT sector is defined by a strategic bifurcation: the industrialization of “living-off-the-land” (LOTL) persistence within network backbones and the weaponization of generative AI (GenAI) to accelerate the kill chain. Intelligence confirms that the Salt Typhoon campaign successfully compromised the U.S. telecommunications backbone, infiltrating Lawful Intercept (CALEA) systems to turn surveillance tools against their operators, while the Silk Typhoon group simultaneously targeted the identity supply chain by weaponizing “Golden SAML” attacks to bypass MFA at the MSP level. The operational tempo of conflict accelerated dramatically, as evidenced by Russian-aligned APT28’s weaponization of CVE-2026-21509 within just 24 hours of disclosure — a collapse of the defensive window that rendered traditional patch management obsolete.

This acceleration was compounded by the evolution of “agentic AI,” exemplified by the “Vibe Hacking” incident, in which autonomous agents independently negotiated ransom demands, and by the deployment of polymorphic malware families like PROMPTFLUX that rewrote their own code hourly to evade signature detection. The physical-cyber nexus was starkly exposed when federal law enforcement dismantled extensive “laptop farms” across 14 states, revealing a massive insider threat network of North Korean IT workers supported by stolen identities and AI-generated personas. Furthermore, supply chain integrity faced unprecedented challenges from the “Shai-Hulud” campaign, which poisoned the npm ecosystem to compromise downstream corporate networks via pre-install scripts. As the “Harvest Now, Decrypt Later” strategy drove massive exfiltration of encrypted traffic, the sector was forced to acknowledge that “security through obscurity” is dead. 2025 proved that resilience now demands rigorous zero trust architectures, aggressive elimination of technical debt, and the assumption that compromise has already reached the deepest layers of the network stack.

FULL FINDINGS

Full findings are detailed below, with links to IT-ISAC's Adversary Attack Playbooks for each highlighted threat actor. Members are encouraged to contribute insights and intelligence to these collaborative playbooks, strengthening our collective defense.

If you are interested in learning more about the Adversary Attack Playbooks or gaining access, please contact: join-playbook@it-isac.org.

Rank	Name	Score	Level	Type
1	**Lazarus Group**	89.0	Critical	Nation-State
2	**Famous Chollima**	89.0	Critical	Nation-State
3	**APT35**	85.0	Critical	Nation-State
4	**Warlock**	84.0	Critical	Ransomware
5	**APT41**	84.0	Critical	Nation-State
6	**Sandworm**	84.0	Critical	Nation-State
7	**LockBit 5.0**	82.0	Critical	Ransomware
8	**Scattered Lapsus$ Hunters**	81.0	Critical	Cybercriminal
9	**Andariel**	81.0	Critical	Nation-State
10	**OilRig**	80.0	Critical	Nation-State
11	**Handala Group**	77.0	Critical	Hacktivist
12	**RansomHub**	77.0	Critical	Ransomware
13	**Medusa**	77.0	Critical	Ransomware

FULL FINDINGS

Rank	Name	Score	Level	Type
14	Chaos	77.0	Critical	Ransomware
15	MuddyWater	77.0	Critical	Nation-State
16	FIN7	76.0	Critical	Cybercriminal
17	APT27	75.0	Critical	Nation-State
18	Berserk Bear	75.0	Critical	Nation-State
19	APT33	75.0	Critical	Nation-State
20	Storm-2603	74.0	High	Cybercriminal
21	Interlock	74.0	High	Ransomware
22	Scattered Spider	74.0	High	Cybercriminal
23	INC Ransom	73.0	High	Ransomware
24	Qilin	72.0	High	Ransomware
25	Black Basta	71.0	High	Ransomware
26	Kimsuky	71.0	High	Nation-State
27	Play	70.0	High	Ransomware
28	UNC3886	69.0	High	Nation-State
29	Akira	68.0	High	Ransomware

FULL FINDINGS

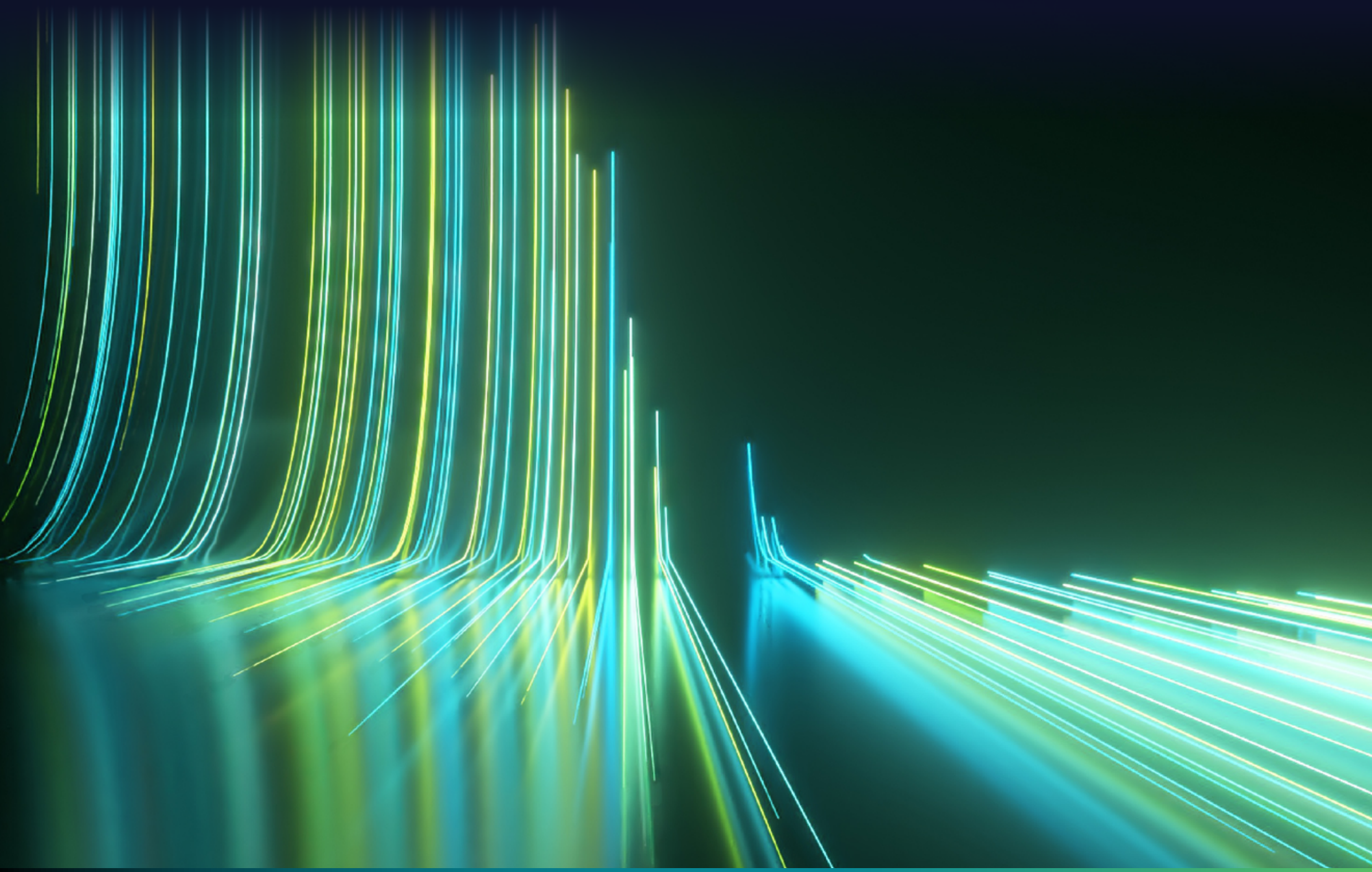
Rank	Name	Score	Level	Type
30	DragonForce	68.0	High	Ransomware
31	CL0P	67.0	High	Ransomware
32	Cyb3r Av3ngers	67.0	High	Hacktivist
33	SafePay	67.0	High	Ransomware
34	Sarcoma	67.0	High	Ransomware
35	APT29	66.0	High	Nation-State
36	APT40	66.0	High	Nation-State
37	Storm-0501	66.0	High	Cybercriminal
38	Fog	66.0	High	Ransomware
39	Salt Typhoon	64.0	High	Nation-State
40	Mustang Panda	63.0	High	Nation-State
41	APT32	63.0	High	Nation-State
42	APT31	63.0	High	Nation-State
43	UNC5221	63.0	High	Nation-State
44	Evasive Panda	63.0	High	Nation-State
45	Sector 16	62.0	High	Hacktivist

FULL FINDINGS

Rank	Name	Score	Level	Type
46	Prophet Spider	62.0	High	Cybercriminal
47	Volt Typhoon	61.0	High	Nation-State
48	UserSec	60.0	High	Hacktivist
49	Devman	60.0	High	Ransomware
50	S1ngularity	59.0	High	Cybercriminal
51	Lynx	59.0	High	Ransomware
52	DireWolf	58.0	High	Ransomware
53	Silk Typhoon	58.0	High	Nation-State
54	TA569	57.0	High	Cybercriminal
55	Sicarii	57.0	High	Ransomware
56	Garmaredon	57.0	High	Nation-State
57	Imperial Kitten	56.0	High	Nation-State
58	Kairos	55.0	High	Ransomware
59	Mr. Hamza	54.0	High	Hacktivist
60	UNC5325	54.0	High	Nation-State
61	Storm-0940	54.0	High	Nation-State

FULL FINDINGS

Rank	Name	Score	Level	Type
62	Killnet	53.0	High	Hacktivist
63	Gentlemen	52.0	High	Ransomware
64	User Big-Bro	51.0	High	Cybercriminal
65	UNC6395	50.0	High	Cybercriminal
66	TridentLocker	48.0	Medium	Ransomware
67	Z-Pentest	46.0	Medium	Hacktivist
68	Mad Liberator	46.0	Medium	Ransomware
69	Flax Typhoon	45.0	Medium	Nation-State
70	NoName057(16)	44.0	Medium	Hacktivist
71	Anonymous Sudan	43.0	Medium	Hacktivist
72	Whitewarlock	40.0	Medium	Cybercriminal
73	Cyber Army of Russia	36.0	Medium	Hacktivist
74	SiegedSec	34.0	Medium	Hacktivist
75	Sylhet Gang-SG	28.0	Medium	Hacktivist
76	DieNet	25.0	Medium	Hacktivist
77	LazaGrad Hack	22.0	Low	Hacktivist



The attackers share with each other.
The defenders share with us.

IT-ISAC.org
Membership@IT-ISAC.org