CRITICALSTART®

CYBER THREAT INTELLIGENCE REPORT

SECOND HALF 2025

The CRITICAL**START®** Mission

The Critical Start Second-Half 2025 Threat Report reflects our core belief that cybersecurity should reduce risk, not create noise.

Every day, our Security Operations Center investigates and resolves all threat alerts across industries, geographies, and technology environments. This report distills those real-world investigations to identify trends and actionable insights. It highlights where attackers are concentrating their efforts, how their tactics are evolving, and what consistently separates contained incidents from business disruption.

Our mission is simple: eliminate blind spots, remove alert fatigue, and ensure that every threat alert is investigated and acted on. The insights in this report are not theoretical. They are grounded in human-validated analysis across thousands of alerts, shaped by the same AI-accelerated workflows and disciplined response processes we use to protect our customers every day.

Threat actors continue to refine identity-based intrusion, user-assisted execution, and abuse of legitimate tools. As the landscape evolves, our approach remains focused on accountability, transparency, and measurable outcomes.

At Critical Start, we combine AI-accelerated analysis with expert human validation to eliminate noise, investigate every threat alert, and take decisive action backed by measurable SLAs. We believe response should be transparent, accountable, and outcome-driven, with our customers at the center of everything we do. Because we know that insight is valuable, but only action reduces risk.

Editorial Team

Gerard Chukwu
CTI AI Technologist

Hunter Whyle
Principal Product Manager Threat Content

Kristen Ouellette
VP Marketing

Crystal Chen
Digital Events Specialist

Harshita Pandey
Marketing Campaign Project Manager

Swapnil Khorate
Graphic Designer

Introduction

In the second half of 2025, the cybersecurity landscape has experienced notable changes, presenting new challenges for security professionals across industries. The latest H2 threat intelligence report reveals shifts in targeting preferences, attack methodologies, and operational patterns that security leaders across all sectors must consider. Overall, H2 2025 saw a 3.70% increase in high and critical severity alerts compared to H1 2025. For this report, Critical Start's Cyber Research Unit (CRU) analyzed 1,035 high and critical severity alerts investigated and mitigated by the Security Operations Center (SOC), providing insights into adversary behavior across industries and geographies.

One significant change is the shift in industry targeting patterns. The Manufacturing sector has overtaken Banking and Finance as the most targeted industry, moving up from second place in H1 2025. Healthcare has also moved into the top three most targeted industries, rising from tenth place in H2 2024. This shift may reflect a strategic change among threat actors, potentially driven by the importance of manufacturing operations and the sensitivity of healthcare environments. Business Services and Retail continue to be consistently targeted, suggesting ongoing focus on service providers and consumer markets.

These changes in industry targeting are accompanied by shifts in the threat actor ecosystem, which continues to evolve. In H1 2025, the CRU team identified the Qilin ransomware group as third, but by H2 2025, Qilin emerged as the top ransomware group. Incransom and Sinobi have also emerged in the top five, adding to the complexity of the threat landscape. Additionally, Akira's continued operational activity highlights ongoing innovation within the ransomware ecosystem. Despite the emergence of new threat actors, evolving attack surfaces, and innovative attacks, traditional methods such as credential dumping and lateral movement, often carried out using tools like Mimikatz and PsExec, remain effective

CRU also observed key strategic changes in threat actor behaviors, with attack timing and Tactics, Techniques, and Procedures (TTPs) being central to these shifts. The most active period for attacks has moved from the 1400 to 1700 UTC window to the 1500 to 1800 UTC window, with 1800 UTC emerging as the peak hour for activity. This change suggests a more calculated approach to attack timing, requiring increased vigilance during peak afternoon hours. Additionally, changes in TTPs highlight a shift in how adversaries are executing their strategies. Phishing has now surpassed Valid Account usage as the most commonly employed technique, indicating a greater reliance on exploiting user interaction and trusted infrastructure. Brute Force attacks have also risen within the Credential Access tactic, signaling a stronger focus on identity abuse. These trends align with comments from **Allie Bossow**, Manager of Customer Success at Critical Start, who notes that "across industries and company sizes, core threat themes remain consistent: phishing, malware, and ransomware. However, impact and exposure vary by sector. Notably, larger enterprises face more complex identity-based threats due to broader SaaS adoption and distributed workforces."

From the Cyber Incident Response Team (**CIRT**), **Chad Graham**, Manager, observed that credential-based intrusions and identity-driven TTPs continued to dominate customer environments through 2024 and H1 2025, carrying over into H2 2025. The most frequent incidents involved unauthorized access linked to credential abuse, such as MFA gaps, password reuse, and token theft indicators. Lateral movement investigations were triggered by anomalous authentication or privilege escalation behaviors. Post-compromise scoping often revealed gaps in visibility into authentication, VPN, firewall, or load balancer logs. Misconfiguration-driven breaches, particularly in identity and network controls, allowed attackers to bypass EDR/SIEM visibility.

The implications for security leaders are clear. Organizations must adapt their security strategies to address these evolving threats. According to **Allie Bossow**, many organizations are shifting toward a containment-first approach that focuses on blocking or isolating threats. This approach prioritizes asset containment during incidents and then follows with investigations. Organizations that enable rapid containment, even when it temporarily affects users, consistently reduce dwell time and limit business impact.

The cybersecurity landscape continues to present complex challenges due to technological advancements and shifting geopolitical dynamics. Threat actors are leveraging artificial intelligence to enhance the sophistication and scale of their attacks, including the development of AI-enabled malware like VoidLink and the automation of malicious activities such as highly personalized phishing and vulnerability exploitation. These advancements complicate detection and defense efforts, aligning with reports highlighting the growing prevalence of AI-assisted social engineering and ClickFix-style malware execution.

Within this increasingly complex environment, geopolitical tensions have escalated nation-state cyber activities, with state-sponsored groups launching sophisticated attacks on critical infrastructure and intellectual property to gain a strategic advantage. Additionally, software supply chain compromises are emerging as a significant risk, where adversaries exploit trust in developer ecosystems and update channels to access targets at scale. These developments underscore the need for defenses that account for artificial intelligence threats, advanced persistent threats (APTs), and the growing adoption of behavioral monitoring to mitigate escalating threats.

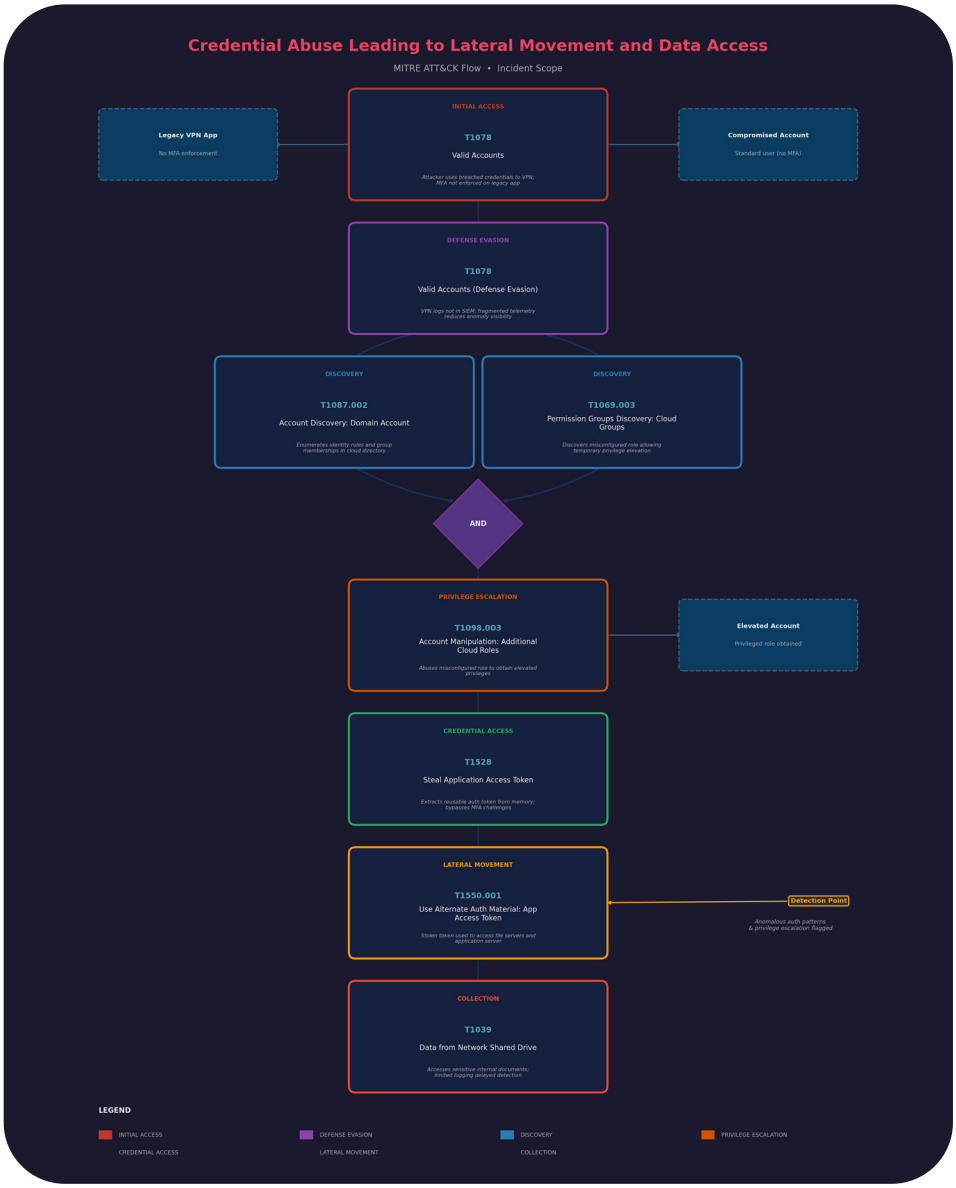


TABLE OF

CONTENTS

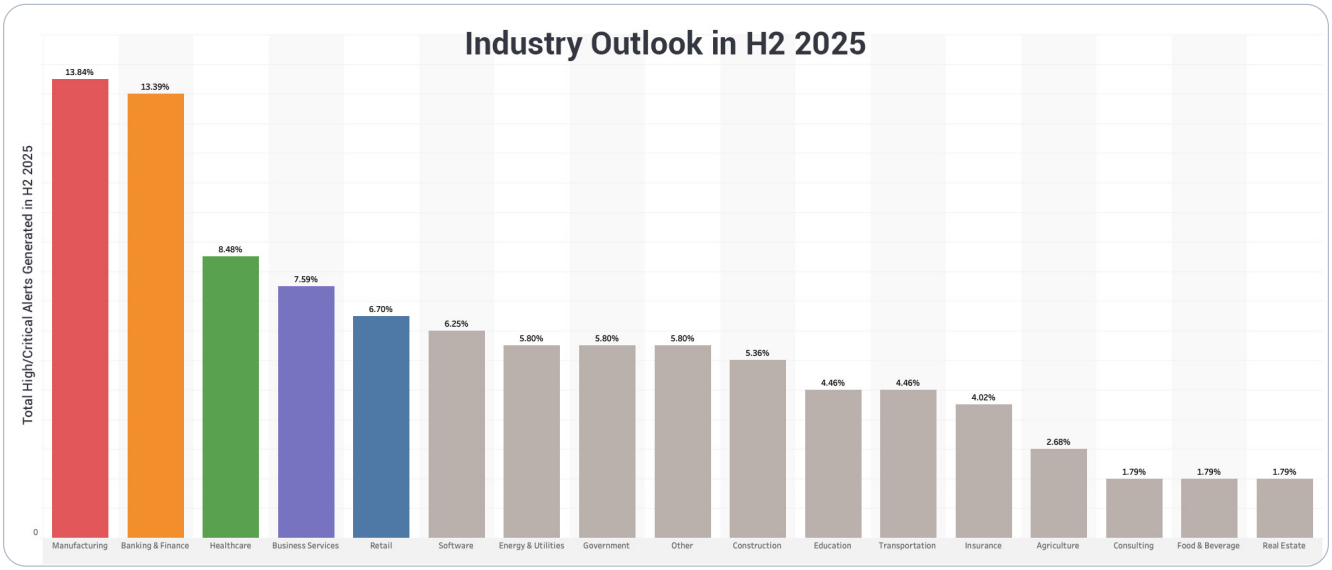
TABLE OF CONTENTS (continued)

Disclaimer

This report leverages real-world data gathered through internal monitoring and publicly available information. Citations have been provided when referencing open-source intelligence, and analysis based on research conducted by Critical Start's CRU team. To safeguard the privacy of our vendors and clients, we have kept certain data and statistics anonymous.

Industry Outlook

Critical Start's Cyber Research Unit assessed industry-level threat trends in the second half of 2025 based on first-party intelligence derived from the analysis of high- and critical-severity incidents resolved by the Security Operations Center. This analysis identified a concentrated pattern of adversary activity across five industries, with Manufacturing ranked first, followed by Banking and Finance in second position and Healthcare in third. Business Services and Retail completed the top five, respectively. This ordering reflects where adversary activity was most frequently observed during the reporting period.



When compared with the same period in 2024, the most significant change was the rise of Manufacturing and Healthcare. Manufacturing moved from third position in H2 2024 to first in H2 2025, representing the largest upward shift among all industries. Healthcare showed an even sharper relative increase, moving from tenth position in H2 2024 to third in H2 2025. Banking and Finance, Business Services, and Retail remained within the upper tier across both periods, indicating steady rather than volatile levels of adversary attention.

Looking across 2025, the same five industries appeared in both the first and second halves of the year, reinforcing their status as persistent targets rather than episodic outliers. Within that continuity, rank movement was still evident. Manufacturing advanced from second position in H1 2025 to first in H2 2025, while Healthcare rose from fifth to third over the same timeframe. Banking and Finance maintained a consistently high position across both halves of the year, suggesting sustained attacker interest without major fluctuation. These ranking patterns point to deliberate threat actor decision-making rather than random targeting. Manufacturing's rise reflects increasing focus on environments where operational disruption has immediate business impact. Healthcare's movement into the top three aligns with continued exploitation of critical service delivery and constrained tolerance for downtime. The continued presence of Banking and Finance, Business Services, and Retail within the top five reflects their enduring value as sources of financial access, sensitive data, and downstream access to broader business ecosystems.

For industries outside the top #5, the table below summarizes their movement from H1 2025 to H2 2025, as observed by Critical Start's CRU. Red indicates an increase, green indicates a decrease, orange indicates no movement.

	▲	▲	▼	▼	▼	—	—	—	▼	▲	—
PERIOD	**SW**	**E&U**	**GOV**	**CONST**	**EDU**	**TRA**	**INS**	**AGR**	**CONSUL**	**F&B**	**RE**
H1 2025	7th	8th	6th	5th	8th	9th	10th	11th	9th	13th	12th
H2 2025	6th	7th	7th	8th	9th	9th	10th	11th	12th	12th	12th

Observed attack strategies varied by industry, with distinct technique concentrations emerging across sectors. In Manufacturing and Retail environments, confirmed high- and critical-severity incidents most often saw users execute malicious files or payloads (T1204) after delivery via email or malicious websites, including drive-by downloads and spoofed login pages. These events frequently marked the transition from initial access into active compromise, highlighting continued risk from end-user execution paths in these sectors.

Banking and Finance incidents more commonly featured attempts to impair or modify security defenses (T1562) during intrusions. Confirmed cases showed attackers tampering with, disabling, or otherwise interfering with security controls to enable further progression. Healthcare organizations showed a higher concentration of phishing activity (T1566), with malicious email campaigns leading to credential exposure or enabling follow-on compromise. Business Services differed from other sectors, with a higher prevalence of brute force activity (T1110), indicating that credential attacks played a more prominent role in compromises affecting this industry.

These observations indicate that the Top 5 industries identified in H2 2025 remained consistently present across high- and critical-severity incidents, while the techniques observed within those incidents varied by sector. The following sections will detail specific tools and initial techniques being deployed against each sector, examining prevalent exploit tools, malware families, and recent attacks targeting these sectors, along with industry-specific vulnerabilities.

#1 Manufacturing

Attack Tools:

Mimikatz (Credential Dump Tool), PsExec (Remote CLI Tool), Advanced IP Scanner (Network Scanner Tool)

Prominent Malware:

SystemBC (RAT), RealBlindingEDR (EDR Killer), DragonForce (Ransomware)

Initial Access Techniques:

Exploit Public-Facing Application (T1190), Phishing (T1566), Drive-by Compromise (T1189)

Top Vulnerabilities:

CVE-2025-8088 (8.8)	A path traversal vulnerability in WinRAR, enabling remote code execution
CVE-2023-1389 (8.8)	A command injection vulnerability in TP-Lin Archer AX21, executed as root
CVE-2025-20281 (10)	A vulnerability in a specific Cisco ISE and Cisco ISE-PIC API that enables remote execution of arbitrary code by an unauthenticated attacker, with root privileges

Top Threat Actors:

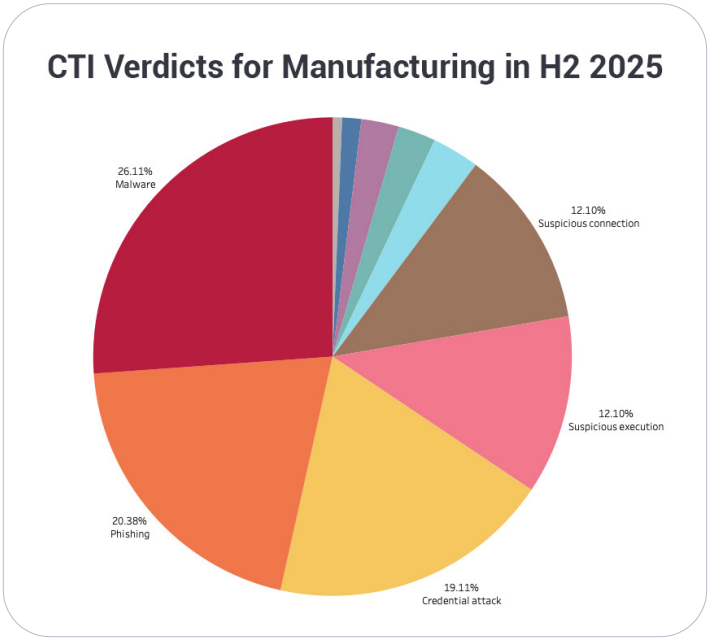
Qilin, Akira, Play

Top Country Targets:

USA (53.37%) **Germany (5.93%)** **United Kingdom (5.12%)**

In H2 2025, Manufacturing emerged as the #1 most targeted industry, up from #2 in H1 2025. Attacks rose 6.9% compared to the first half of the year. Successful operations by ransomware gangs and advanced persistent threats (APT) based according to OSINT sources reinforce this industry's position as a high-risk target for cyber threats. Manufacturing organizations remain prime targets for threat actors due to their critical role in global production and supply chain networks. Industrial manufacturers, automotive plants, electronics producers, among others make up this industry. Manufacturing environments rely on legacy operational technology (OT), within which industrial control systems (ICS) play a central role, and which increasingly interfaces with enterprise information technology (IT) networks. This convergence of legacy OT, ICS, and IT environments introduces multiple technical and human vulnerabilities for exploitation. As such, cyberattacks targeting manufacturing organizations can disrupt OT and ICS operations, resulting in significant production outages, financial losses, and cascading supply chain impacts.

Based on CRU's trend analysis of high- and critical-severity alerts mitigated by the SOC, malware activity was commonly observed within the manufacturing sector. In H1 2025, Malware attacks accounted for roughly 16.5% of attacks on Manufacturing but has gone up to 26.11% in H2 2025. This upward trend reinforces malware's continued effectiveness for threat actors targeting the manufacturing sector.

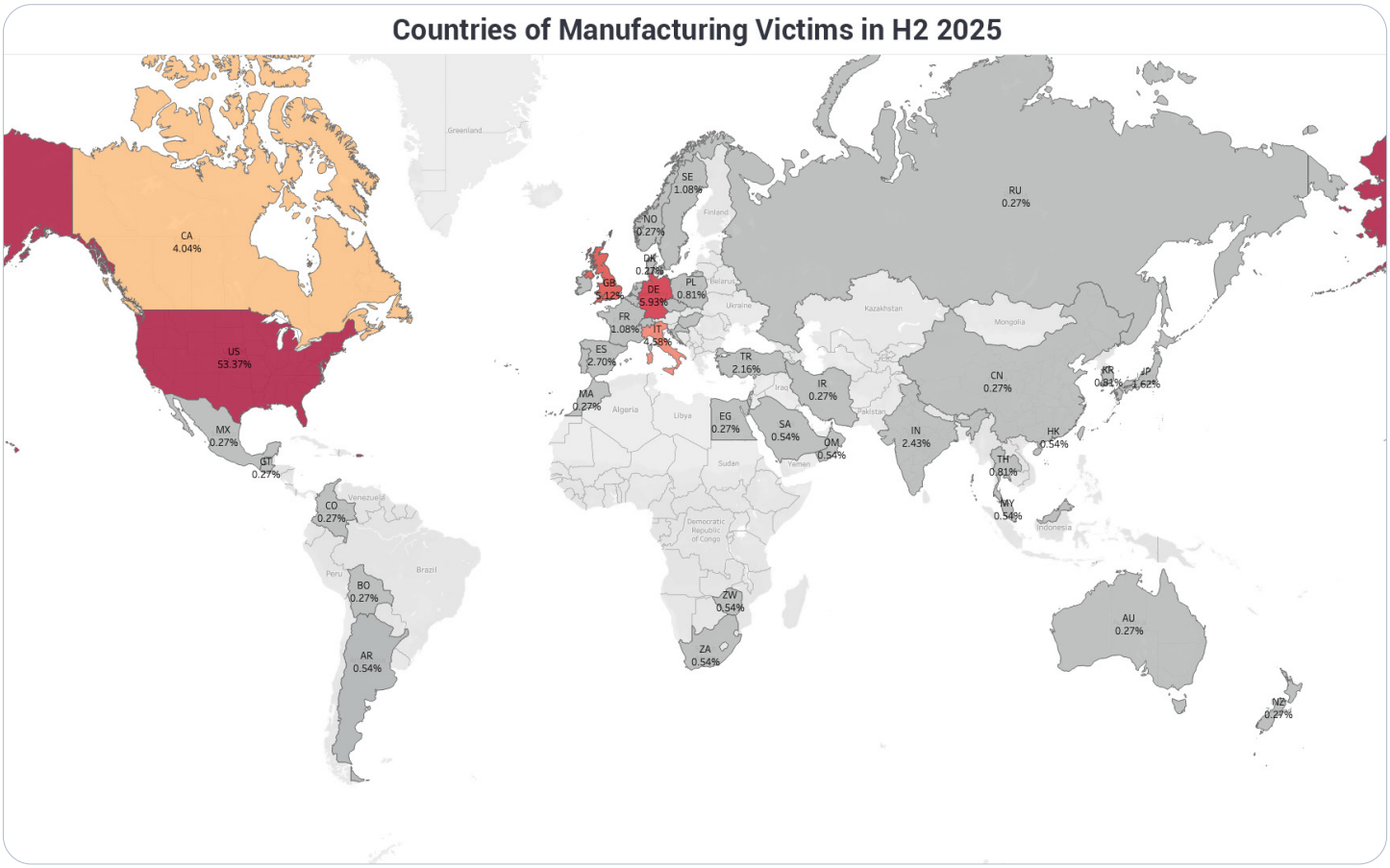


Threat actors frequently leveraged malicious files that appear legitimate to users, including .msi files (Windows installer packages used to install software), .exe files (standard Windows applications), .bat files (batch scripts that automatically run commands), .scr files (Windows screen saver files that can execute code), and .py files (Python scripts used for automation). The use of these file types allows attackers to blend malicious activity with normal business operations and increase the likelihood of successful execution.

This activity aligns with observations from **Jared Bronnenberg**, Principal Operations Engineer at Critical Start, who notes that "Attackers are increasingly shifting away from traditional malicious binaries and instead abusing legitimate Remote Monitoring and Management (RMM) and IT administration tools such as AnyDesk, ConnectWise ScreenConnect, NinjaOne, ManageEngine, and SolarWinds. Because these tools are digitally signed and trusted by endpoint security solutions, they can allow adversaries to bypass standard malware detection while quickly mapping environments and deploying additional payloads. As a result, SOC teams treat the unauthorized installation or use of RMM and IT management tools with the same urgency as conventional malware, prioritizing rapid investigation and containment based on prevalence and behavioral context."

To gain a broader view of observed threat activity in the manufacturing sector, CRU leveraged EDR telemetry that was pre-mapped to MITRE TTPs by the vendor and compared it with CRU's CTI verdicts. Using MITRE ATT&CK as the analytical framework, this correlation allows for a more complete understanding of attacker behavior across the attack chain. Analysis shows that User Execution (TA0002.T1204) accounted for roughly 22.22% of observed techniques, followed by Brute Force attacks (TA0006.T1110) at 15.03% and Phishing (TA0001.T1566) at 14.38%, highlighting attackers' continued reliance on user-driven actions, password-guessing attempts, and social engineering to gain access and move laterally.

Globally, OSINT revealed that the United States, Germany, and United Kingdom were the countries with the most victims in the manufacturing industry. This geographic concentration highlights regions with dense industrial activity and complex supply chains, making them particularly attractive targets for ransomware operators and advanced persistent threats. The trend underscores the need for organizations in these countries to adopt cross-border intelligence sharing, and targeted risk mitigation strategies aligned with observed attack patterns cut across initial access, execution, and credential access.



Recent Attacks:

Poland Power Sector, USA:

In late December 2025, Polish critical infrastructure operators experienced a cyberattack targeting several power and renewable energy facilities. During the incident, security researchers observed the use of a previously undocumented data-wiping malware called DynoWiper, which is designed to corrupt and overwrite files rather than extort. A Slovakian cybersecurity firm first identified the malware, and subsequent analysis by researchers noted overlaps in tactics, techniques, and procedures (TTPs) with prior campaigns, suggesting potential links to known threat groups such as Sandworm.

Luxshare, China:

In January 2026, Luxshare, a key electronics manufacturer and Apple supplier, reportedly suffered a cyberattack that exposed internal documents. The leaked data included production and operational information for devices like iPhones, AirPods, and Vision Pro. Researchers linked the incident to typical ransomware tactics involving data theft and extortion. Threat actors reportedly published the stolen data online to pressure the company.

https://thehackernews.com/2026/01/new-dynowiper-malware-used-in-attempted.html
https://cybersecuritynews.com/luxshare-data-exposed/

#2 Banking & Finance

Attack Tools:

Cobalt Strike (Penetration Test Tool), AnyDesk (Remote Access Tool), Mimikatz (Credential Dump Tool)

Prominent Malware:

Astaroth (Infostealer), SocGholish (framework), Netsupport (Remote Access Trojan)

Initial Access Techniques:

Phishing (T1566), Supply Chain Compromise (T1195), Trusted Relationship (T1199)

Top Vulnerabilities:

CVE-2025-29824 (7.8)	A privilege escalation vulnerability in Windows Common Log File System (CLFS) Driver
CVE-2024-40711 (9.8)	A deserialization of untrusted data vulnerability with a malicious payload that enables an unauthenticated remote code execution
CVE-2025-14847 (8.7)	An unauthenticated memory-read vulnerability in MongoBleed that enables attackers retrieve sensitive in-memory credentials

Top Threat Actors:

Qilin, Akira, Incransom, Everest

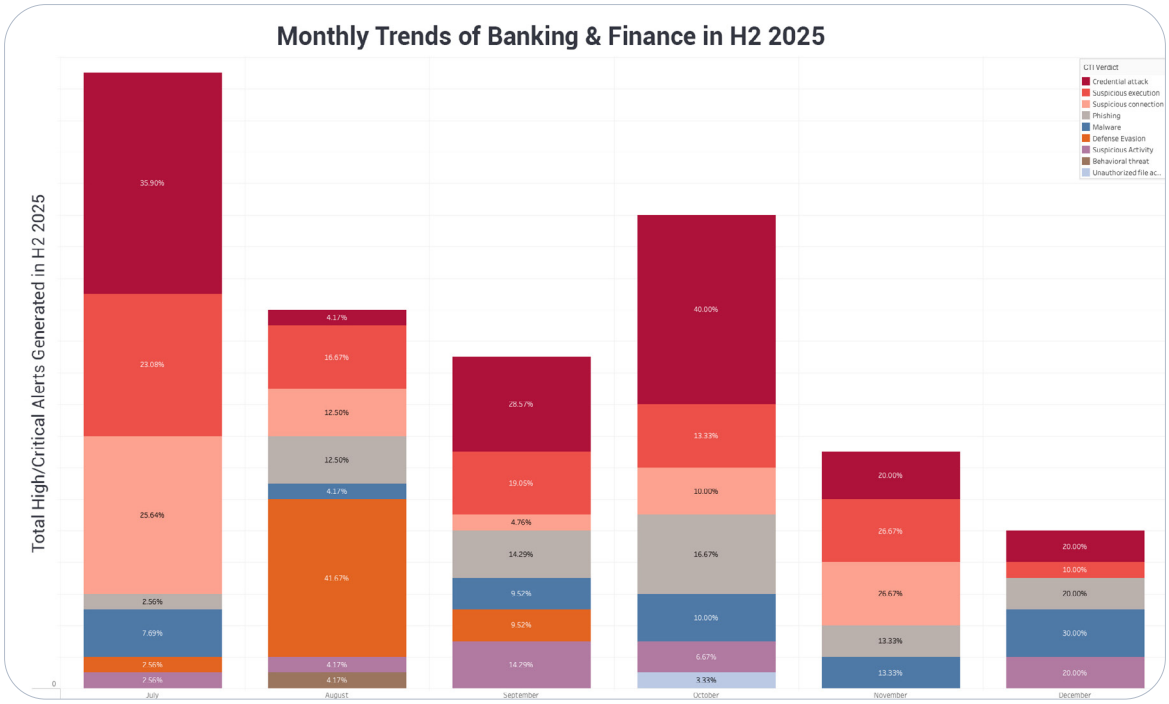
Top Country Targets:

USA (48.75%) **South Korea (5.00%)** **United Kingdom (5.00%)** **Canada (4.38%)**

In H2 2025, Banking and Finance ranked as the second most targeted industry, down from first place in H1 2025, with overall attacks declining by 11.76%. Despite this decrease, the sector remains a high-value target and continues to trade positions with Manufacturing as threat actors shift focus between industries with tightly connected financial and operational dependencies. This dynamic reflects attacker prioritization of high-risk, high-reward sectors.

The Banking and Finance industry spans a broad ecosystem that includes commercial banks, credit unions and community banks, securities and investment firms, payment card services, insurance providers, and cryptocurrency and digital asset platforms. The concentration of financial assets, sensitive identity data, and real-time transaction systems increases both the incentive for attack and the operational impact of successful compromise.

CRU analysis shows that activity in this sector is dominated by credential-focused and execution-driven techniques, reinforcing identity as the primary attack surface. Credential Attacks (27.34%), Suspicious Execution (18.71%), and Suspicious Connection activity (15.11%) were the most common CTI verdicts.



Password spraying was the predominant credential access method, frequently accompanied by credential dumping using tools beyond Mimikatz. A notable execution trend involved the malicious use of PowerShell, with attackers leveraging .ps1 script files and .psd1 PowerShell data files to perform discovery, privilege escalation, and post-compromise activity. The abuse of legitimate tools such as ScreenConnect and AutoIt3.exe further enabled attackers to blend into normal administrative workflows.

Mapping this activity to MITRE ATT&CK techniques reinforces these observations. Impair Defenses (TA0005.T1562) accounted for 12.07%, followed by Command and Scripting Interpreter (TA0002.T1059) at 11.21%, and Brute Force (TA0006.T1110) at 10.34%. In parallel, OSINT focused on the financial services sector highlights elevated use of Phishing (T1566) and Drive-by Compromise (T1189), indicating that user interaction and credential exposure continue to be the primary entry points. OSINT further indicates that victim activity was concentrated in the United States (48.75%), followed by South Korea (5.00%), the United Kingdom (5.00%), and Canada (4.38%), underscoring the global scope and systemic importance of this sector.

Taken together, these findings indicate that attacks against the Banking and Finance sector frequently progress from credential access into scripted execution and defensive evasion. This pattern reinforces the importance of identity controls, strong authentication enforcement, and continuous monitoring of administrative tooling and script execution. The persistence of credential-abuse activity underscores that systemic identity hygiene remains a necessary control across most financial environments.

While credential hygiene is foundational, it represents only one layer of defense. Compromised or misused credentials can provide attackers with access that allows execution of administrative tools, scripts, and other critical processes within the environment. As Principal SOC Engineer **Jared Bronnenberg** noted, "this makes comprehensive visibility across assets, tooling, and operational activity equally important. Unmanaged or undiscovered devices, combined with limited insight into administrative tool usage and process execution, create blind spots that adversaries can exploit without triggering alerts. Without clear visibility into systems, identities, and operational workflows, even a well-equipped SOC may struggle to detect and contain malicious activity".

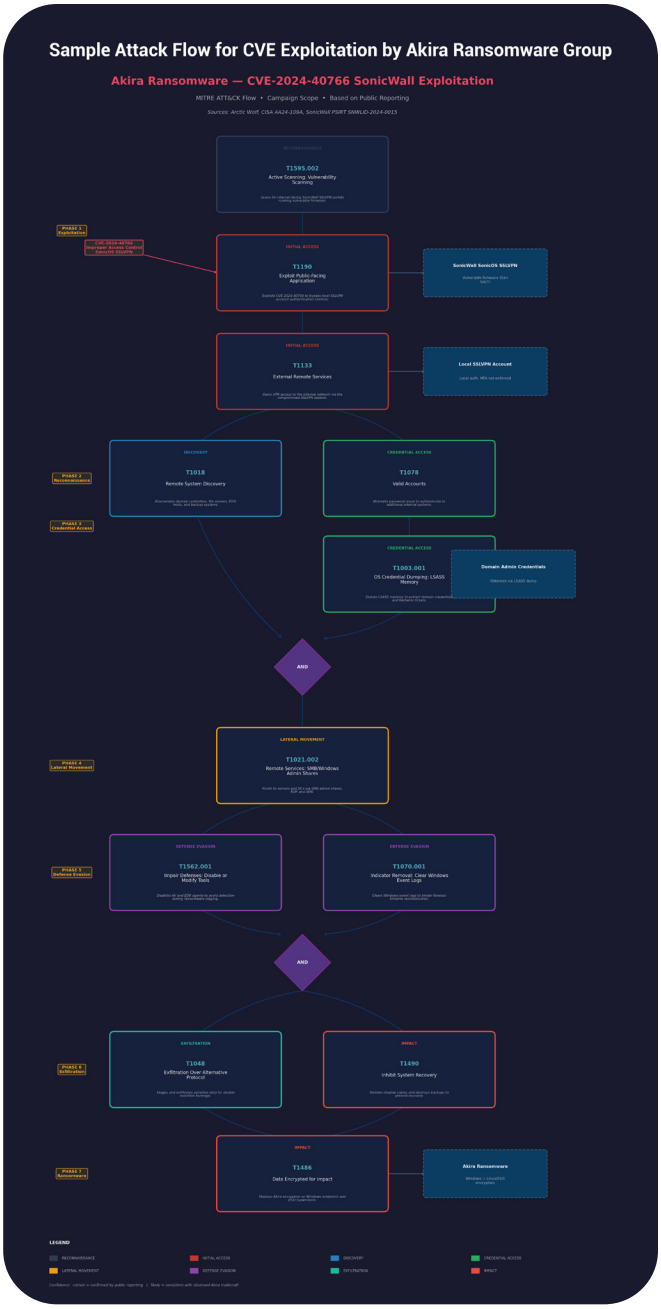
Recent Attacks:

Marquis Software Solutions, USA:

In August 2025, Marquis Software Solutions, a Texas-based financial software provider serving banks and credit unions, suffered a ransomware-related breach that exposed sensitive customer data for over 400,000 individuals across more than 74 U.S. banks and credit unions. The attackers gained unauthorized access via the company's SonicWall firewall, using information obtained from a prior security incident involving SonicWall's cloud backup service to circumvent network defenses. Stolen data included names, Social Security numbers, financial account details, and other personal information.

Sinqia S.A., Brazil:

In late August 2025, hackers breached the systems of Sinqia S.A., the Brazilian subsidiary of fintech processor Evertec, gaining unauthorized access to its connection with Brazil's real-time payment system, PIX. The attackers attempted to initiate fraudulent business-to-business transactions totaling about $130 million, but the activity was detected and stopped before customer funds were lost. Initial access was achieved using stolen credentials from an IT vendor account, allowing the threat actors to bypass controls and interact with the PIX environment.



https://www.bleepingcomputer.com/news/security/marquis-data-breach-impacts-over-74-us-banks-credit-unions/
https://www.bleepingcomputer.com/news/security/hackers-breach-fintech-firm-in-attempted-130m-bank-heist/

#3 Healthcare

Attack Tools:

NetScan (Network Monitoring Tool), RCLONE (File Manager Tool), Mimikatz (Credential Dump Tool)

Prominent Malware:

SystemBC (Remote Access Trojan), DragonForce (RaaS), Qilin (Ransomware)

Initial Access Techniques:

Phishing (T1566), Drive-by Compromise (T1189), Trusted Relationship (T1199)

Top Vulnerabilities:

CVE-2025-10035 (9.8)	A deserialization vulnerability in the License Servlet of Fortra's GoAnywhere MFT allows an actor with a validly forged license response signature to deserialize an arbitrary actor-controlled object, possibly leading to command injection
CVE-2020-1472 (10)	An unauthenticated Netlogon vulnerability that allows attackers to gain domain administrator privileges
CVE-2023-27532 (7.5)	A Veeam Backup & Replication vulnerability that allows attackers to retrieve encrypted credentials and potentially access backup infrastructure hosts

Top Threat Actors:

Qilin, Devman, Sinobi, Nova

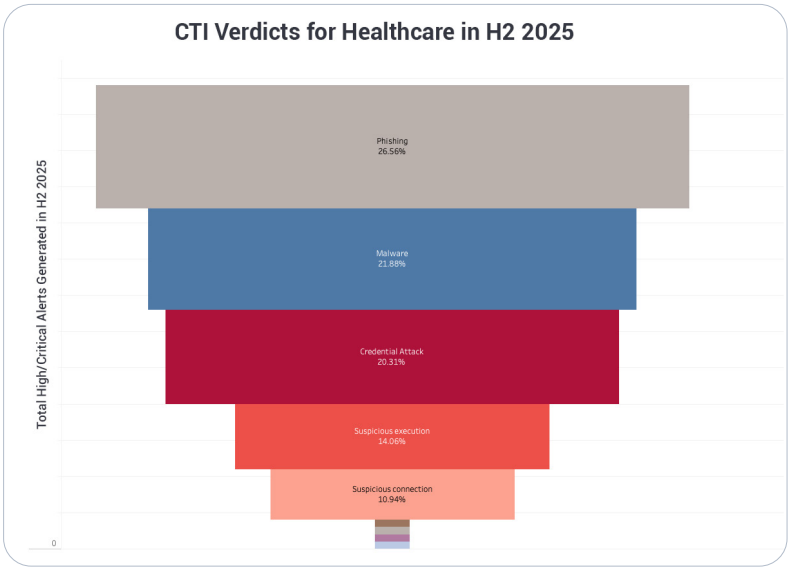
Top Country Targets:

USA (59.89%) **France (5.88 %)** **Brazil (4.81%)**

In H2 2025, Healthcare ranked as the third most targeted industry, rising two positions from H1 2025, where it ranked fifth. This increase coincided with peak medical coverage and enrollment activity leading into the January 1 coverage cycle, a period that historically increases user engagement and exposure to social engineering. The sector remains an attractive target due to its operational sensitivity, reliance system availability, and concentration of personal and clinical data.

The Healthcare industry encompasses a broad range of organizations, including hospitals and health systems, outpatient and specialty care providers, clinical laboratories, health insurers, medical device manufacturers, and pharmaceutical companies. The diversity of this ecosystem, combined with time-sensitive operations and regulatory pressure, amplifies the impact of disruption and increases susceptibility to phishing and credential-based attacks.

CRU observations show that phishing (26.56%), malware activity (21.88%), and credential attacks (20.31%) dominated threat activity in this sector. Malicious links were the most common engagement method and frequently led to adversary-in-the-middle (AiTM) attacks, where attackers intercept authentication flows to capture credentials and session tokens in real time. These techniques allow adversaries to bypass traditional MFA controls and establish initial foothold without deploying malware during initial compromise.



Mapping observed activity to MITRE ATT&CK techniques aligns with these findings. Phishing (TA0001.T1566) accounted for 19.67%, followed by Brute Force (TA0006.T1110) at 18.03%, and User Execution (TA0002.T1204) at 13.11%. Together, these techniques reflect a threat pattern centered on user interaction, credential compromise, and follow-on execution rather than immediate exploitation of infrastructure vulnerabilities.

Geographically, OSINT indicates that Healthcare victims were most concentrated in the United States (59.89%), followed by France (5.88%) and Brazil (4.81%), reflecting both healthcare system scale and regional digitization trends. These dynamics make healthcare environments uniquely sensitive to operational impact, emphasizing the need for targeted user awareness, strong identity controls, and rapid detection of anomalous access to safeguard both patient safety and operational resilience.

Recent Attacks:

AZ Monica, Belgium:

In January 2026, AZ Monica hospital in Antwerp and Deurne was forced to shut down all servers after a cyberattack disrupted its IT systems, leading to the cancellation of scheduled procedures and transfer of critical patients to other facilities. Emergency services continued at reduced capacity, and staff resorted to manual processes due to loss of digital records. At least 70 surgeries were postponed, and critical care teams were partially unable to operate as usual.

Heywood Healthcare, USA:

In October 2025, Heywood Healthcare, which operates Heywood Hospital and Athol Hospital in Massachusetts, experienced a significant cyberattack that caused a widespread network outage and forced systems offline to protect infrastructure and patient data. The incident triggered a Code Black and ambulance diversions as email, phone, radiology, and laboratory systems were disrupted. Investigation of the breach revealed unauthorized access to sensitive patient information, including names, Social Security numbers, medical records, and insurance details.

https://www.bleepingcomputer.com/news/security/belgian-hospital-az-monica-shuts-down-servers-after-cyberattack/
https://www.emeryreddy.com/blog/data-breach/heywood-healthcare-data-breach

#4 Business Services

Attack Tools:

MeshAgent (Remote Access Tool), AdFind (AD Reconn Tool), Mimikatz (Credential Dump Tool)

Prominent Malware:

BRICKSTORM (Backdoor), FormBook (Infostealer), ASyncRAT (Remote Access Trojan)

Initial Access Techniques:

Phishing (T1566), Drive-by Compromise (T1189), Exploit Public-facing Application (T1190)

Top Vulnerabilities:

CVE-2025-20281 (10)	A vulnerability in a specific Cisco ISE and Cisco ISE-PIC API that enables remote execution of arbitrary code by an unauthenticated attacker, with root privileges
CVE-2023-1389 (8.8)	A command injection vulnerability in TP-Lin Archer AX21, executed as root
CVE-2024-7120 (9.8)	An OS command injection vulnerability, from a remote attacker, found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90

Top Threat Actors:

Akira, Qilin, Incransom, DragonForce

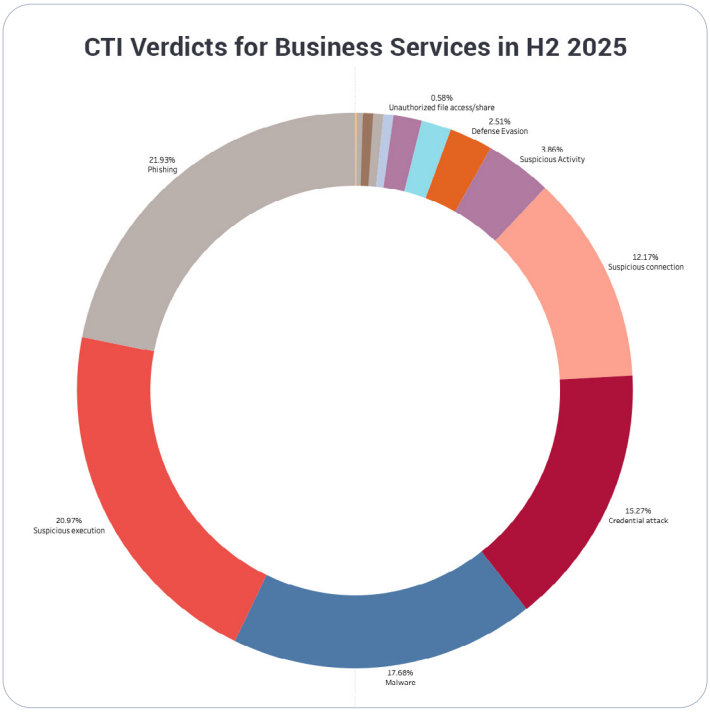
Top Country Targets:

USA (67.82%) Germany (4.10 %) Italy (3.79%) Canada (3.79%)

In H2 2025, Business Services ranked as the fourth most targeted industry, down from third position in H1 2025. Despite this slight decline, the sector remains a consistent target due to its role as a service provider to multiple downstream industries, often acting as an initial access point into broader business ecosystems.

The Business Services sector includes a wide range of organizations such as professional services firms, consulting and advisory companies, managed service providers, staffing and human resources firms, legal services, facilities management, and business process outsourcing providers. The dynamics of privileged access, sensitive client data, and connectivity to customer environments increases the value of compromise for threat actors seeking scale and lateral opportunities.

CRU's observations indicate that phishing (21.93%) was the most prevalent activity, followed closely by suspicious execution (20.97%) and malware (17.68%). Phishing activity frequently served as the initial access vector, while suspicious execution reflected the abuse of legitimate tools and scripts to establish persistence or perform follow-on actions. Malware activity in this sector often blended into routine business workflows, increasing dwell time and reducing early detection.



Mapping telemetry to MITRE ATT&CK techniques reinforces these trends. Brute Force (TA0006.T1110) accounted for 23.53%, followed by Phishing (TA0001. T1566) at 20%, and Steal Web Session Cookie (TA0006. T1539) at 14.12%, indicating a strong emphasis on credential access, session hijacking, and user-driven compromise. Together, these techniques reflect a threat pattern centered on identity abuse and session-level access rather than overt exploitation.

Geographically, OSINT shows that victims were predominantly located in the United States (67.82%), with additional activity observed in Germany (4.10%), Italy (3.79%), and Canada (3.79%), mirroring the global footprint of business service providers and their client bases.

These findings highlight that Business Services organizations face elevated risk due to their role as trusted intermediaries. Successful compromise can enable attackers to pivot into multiple customer environments, amplifying impact beyond a single victim. This reinforces the importance of strong identity controls, phishing resilience, and visibility into abnormal execution and session behavior within service-oriented environments.

Recent Attacks:

Willians & Connolly, USA:

In early October 2025, a major U.S. law firm confirmed that hackers breached a small number of attorney email accounts by exploiting a previously unknown software vulnerability. The firm said the intruders accessed internal emails, though it did not confirm whether sensitive client data was extracted. The incident was reported in the context of broader cyberattacks on law firms and professional services, with investigations underway by cybersecurity firms and U.S. authorities.

Ernest & Young (EY), USA:

In late October 2025, a 4 TB SQL Server backup file belonging to global professional services firm Ernst & Young (EY) was found publicly accessible on Microsoft Azure due to a cloud configuration error. The unprotected backup contained sensitive information such as database schemas, credentials, tokens, and other internal data, raising significant exposure risks. The discovery was made by security researchers during an internet scan, and EY remediated the issue after being notified.

https://therecord.media/us-law-firm-hackers-breached-email
https://cybersecuritynews.com/ey-data-leak/

#5 Retail

Attack Tools:

NetScan (Network Monitoring Tool), RCLONE (File Manager Tool), Mimikatz (Credential Dump Tool)

Prominent Malware:

CAPI (Backdoor), Qilin (Ransomware), Snipbot (Downloader)

Initial Access Techniques:

Exploit Public-facing Application (T1190), Phishing (T1566), Drive-by Compromise (T1189)

Top Vulnerabilities:

CVE-2025-53770 (9.8)	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2025-49706 (6.5)	Microsoft SharePoint Server Spoofing Vulnerability
CVE-2023-20269 (9.1)	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN Unauthorized Access Vulnerability

Top Threat Actors:

Qilin, Akira, Incransom

Top Country Targets:

USA (49.28%) **Canada (6.52 %)** **Italy (4.35%)** **France (4.35%)**

In H2 2025, Retail ranked as the fifth most targeted industry, dropping one position from H1 2025. Despite this shift in ranking, threat activity increased markedly on a year-over-year basis. A comparison between H2 2025 and H2 2024 shows a 50.00% increase in observed activity, indicating that relative position alone does not capture the true level of risk faced by the sector.

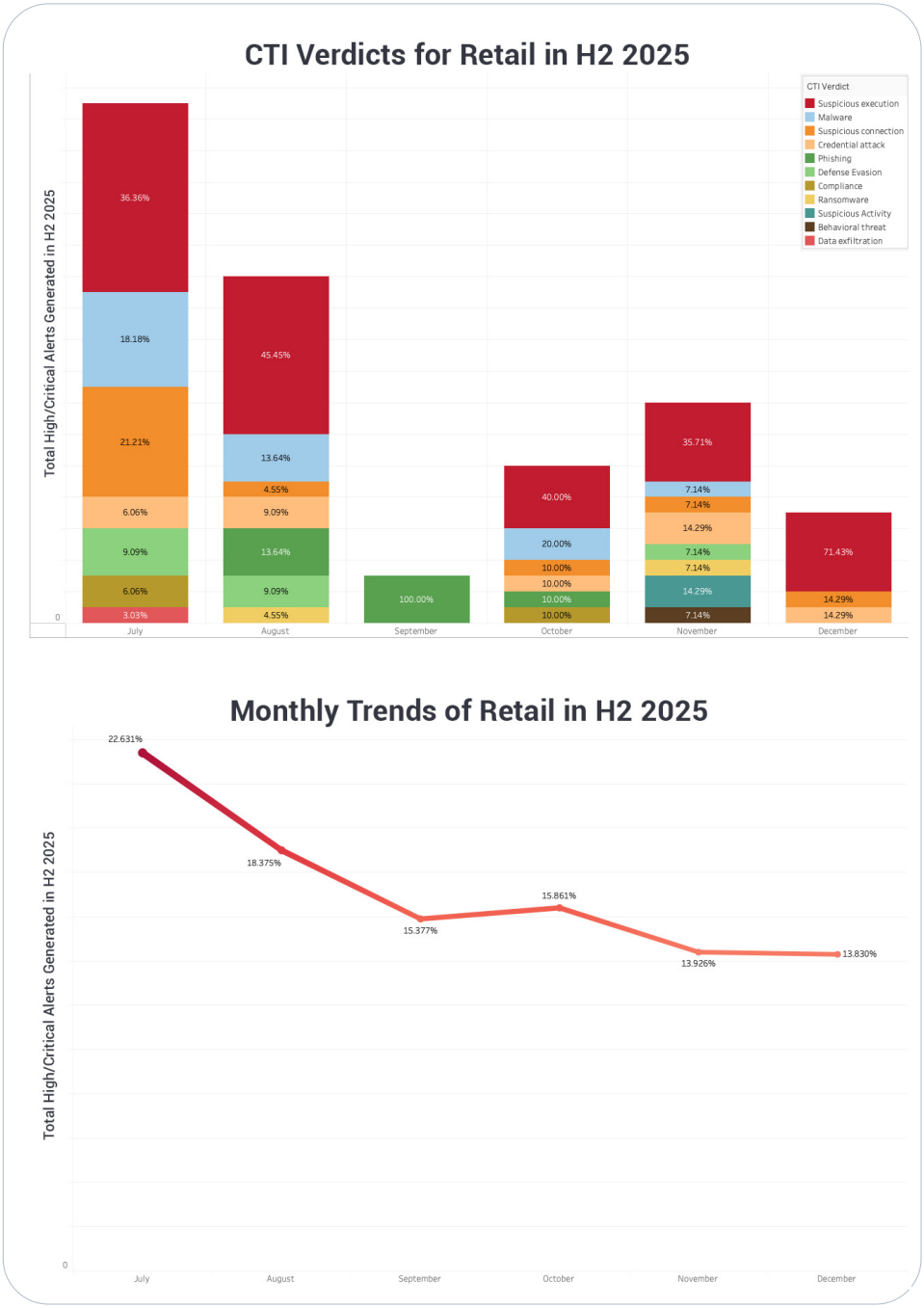
The Retail industry spans a broad and interconnected ecosystem, including brick-and-mortar retailers, e-commerce platforms, grocery and big-box chains, fashion and specialty retailers, payment processors, logistics and fulfillment partners, and point-of-sale and loyalty system operators. These environments are characterized by high transaction volumes, distributed infrastructure, frequent third-party integrations, and seasonal workforce fluctuations, all of which expand the attack surface.

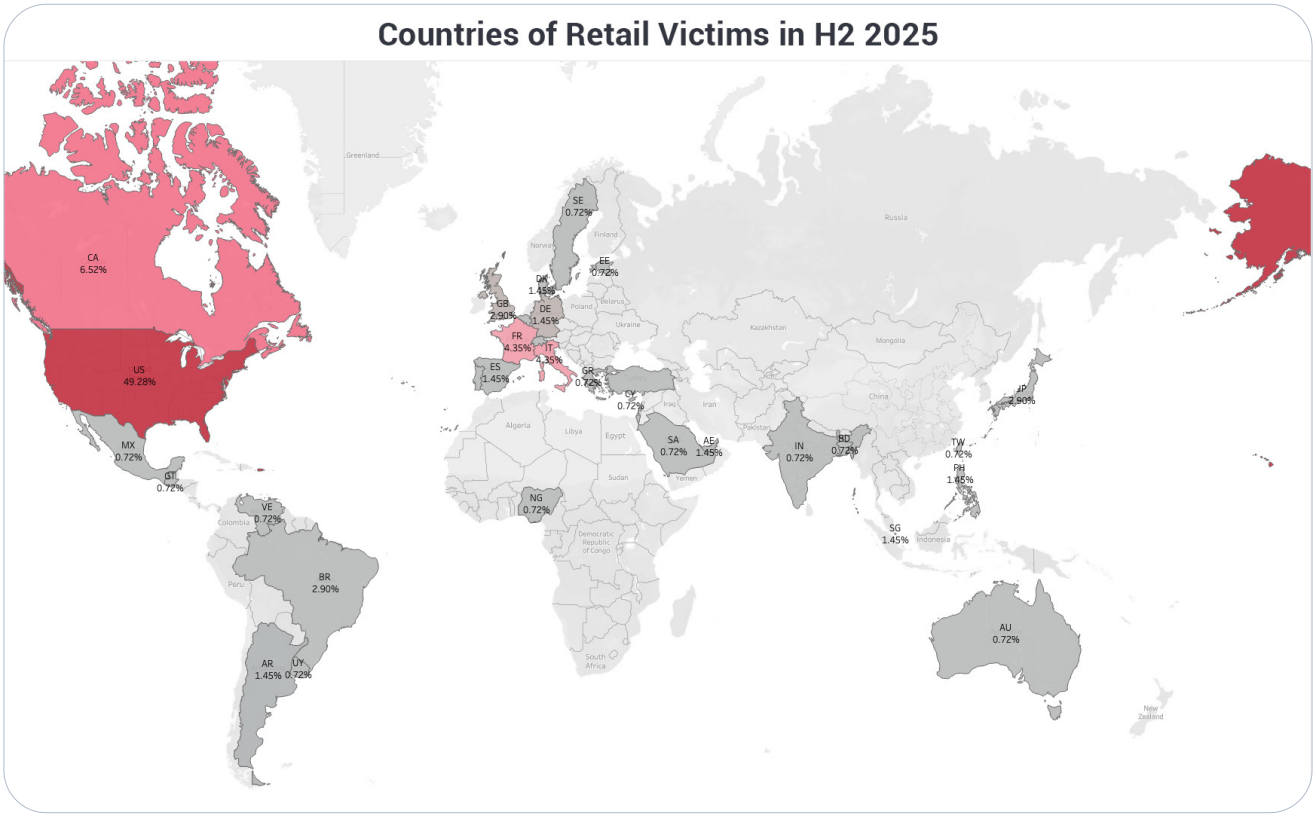
Seasonal analysis in H2 2025 revealed that retail threat activity does not peak during November and December as commonly assumed. Instead, July accounted for the highest volume of alerts at 22.63%, followed by August at 18.37%, while November and December consistently recorded the lowest activity at approximately 14%. This pattern indicates that summer months represent the most active threat period for retail, dispelling the notion that discount shopping and holiday sales alone drive targeting. Notably, July remained the most active month across both July 2024 and July 2025, while November, which had previously peaked alongside July in H2 2024, declined significantly in 2025.

The July spike was driven primarily by suspicious execution activity, with a concentration of registry-related events and anomalous process execution. Many alerts involved the abuse of legitimate system utilities, including PowerShell, utilman.exe, reg.exe, and AnyDesk, allowing attackers to modify configurations, establish persistence, or enable remote access while blending into normal administrative behavior.

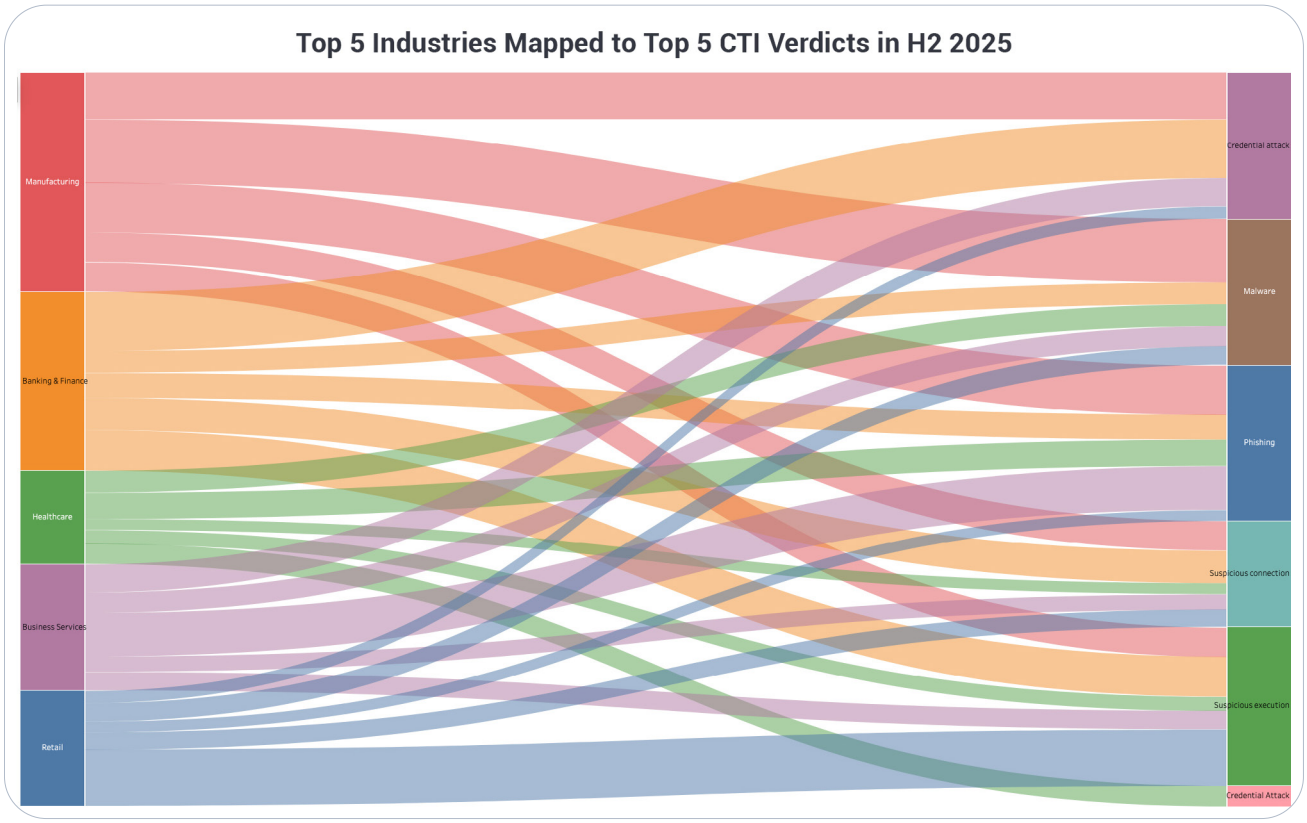
Mapping observed activity to MITRE ATT&CK techniques reinforces this execution-driven pattern. User Execution (TA0002.T1204) accounted for 16.67% of observed techniques, followed by Command and Scripting Interpreter activity (TA0002.T1059) at 8.97%. Defensive evasion techniques were also present, with Impair Defenses (TA0005.T1562) and Masquerading (TA0005.T1036) each representing 7.69% of activity. Together, these techniques reflect a reliance on user-initiated execution followed by scripting and evasion to persist within retail environments during peak operational periods.

Geographically, OSINT indicates that retail victims were primarily located in the United States (49.28%), followed by Canada (6.52%), Italy (4.35%), and France (4.35%), aligning with major consumer markets and retail footprints.





Put together, retail threat activity is shaped less by holiday-driven demand and more by operational timing and exposure during summer months, when system changes, staffing shifts, and execution activity increase. This reinforces the need for heightened visibility into execution behavior, registry modification, and remote access tooling during mid-year periods, when retail environments appear most susceptible to abuse.



H2 2025 data shows that threat activity across industries is driven by a consistent set of attacker behaviors rather than broad shifts in targeting. Credential Access (TA0006) appeared in the top three tactics across every industry and ranked first in several, confirming it as the primary enabler of follow-on activity. User Execution (TA0002) was most prominent in Retail and Manufacturing, where users were more frequently leveraged to initiate malicious files, scripts, or tools, while Phishing (TA0001) persisted across all sectors but rarely acted as the sole driver outside of Manufacturing.

At the technique level, repeated use of TA0006.T1110, TA0001.T1566, and TA0002.T1204 reflects a shared attacker playbook applied across industries. Banking and Finance diverges from this pattern by placing greater emphasis on defense impairment (TA0005.T1562), indicating a stronger focus on disabling security controls and reducing visibility after access is established.

Overall, attackers continue to concentrate on a small set of high-value industries while adapting their methods to sector-specific workflows. The data shows that compromise is most often achieved through identity abuse, user-initiated execution, and the misuse of legitimate administrative tools and system processes rather than novel or highly specialized techniques.

Recent Attacks:

Leroy Merlin, France:

In December 2025, French home improvement and gardening retailer Leroy Merlin disclosed a cyberattack that exposed personal information of customers in France, including names, phone numbers, email addresses, postal addresses, dates of birth, and loyalty program details. The company said it detected the incident, blocked unauthorized access, and began notifying affected individuals. There is no indication that banking data or account passwords were compromised.

Askul Corp., Japan:

In October 2025, Japanese retailer Askul suffered a ransomware-related cyberattack that forced it to halt online orders and product shipments across its e-commerce platforms, disrupting its logistics network. The incident caused major operational outages for Askul's own services as well as for partner retailers like Muji and Loft that rely on its distribution systems. Following the attack, Askul confirmed that customer and supplier data was exposed and publicly claimed by the extortion group RansomHouse.

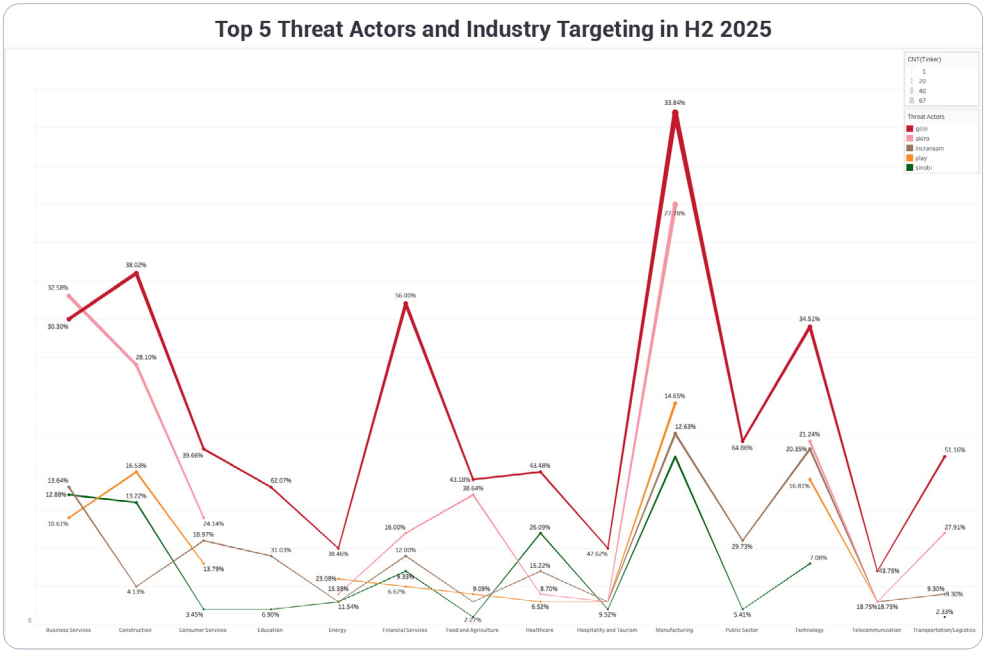
https://www.bleepingcomputer.com/news/security/french-diy-retail-giant-leroy-merlin-discloses-a-data-breach/
https://therecord.media/askul-japan-retailer-cyberattack-disruption

Threat Actors & Malware Families

Analysis of H2 2025 ransomware and data-leak trends, based on OSINT and dark web reporting, highlights a notable shift in threat actor prominence. Qilin rose to the top, moving from outside the top five in H2 2024 to third in H1 2025, and now first in H2 2025. Akira maintained a steady second position, reflecting sustained operational tempo, while Play remained in the top five, displaced to fifth by emerging actors. Incransom and Sinobi advanced to third and fourth positions, signaling a diversification of operators capable of campaigns at scale.

The concentration of threat actor targeting observed in OSINT and dark web sources is pronounced. Qilin, Akira, Incransom, Play, and Sinobi collectively account for over 43% of documented victims, with Qilin alone representing 18.10% of all incidents, followed by Akira at 10.12%. This indicates that a limited number of groups are driving the majority of observed ransomware and data-leak campaigns. Targeting patterns show strong alignment across industries. Manufacturing is the primary focus for all five actors, with Construction, Business Services, Banking & Finance, and Technology frequently appearing in their campaigns. This reflects deliberate prioritization of sectors where operational disruption creates leverage, rather than opportunistic attacks.

The following section provides a focused snapshot of malware and tooling, observed tactics and techniques, and the industries and geographies most impacted, equipping defenders with concrete reference points derived from OSINT and dark web intelligence for monitoring, detection, and risk mitigation.



FYI: A small subset of alerts lacked sufficient attribution and were excluded from this analysis. These represent approximately 0.1% of the total dataset and do not materially affect the overall findings.

1 Qilin

SNAPSHOT

GEOGRAPHICAL LOCATION OF TARGETS

United States | Japan | Australia | United Kingdom

PRIMARY INDUSTRIES

Manufacturing | Construction | Agriculture | Banking & Finance | Healthcare

PRIMARY TOOLS

AnyDesk (Remote Access Tool)
Cobalt Strike (Pen Test Tool)
Mimikatz (Cred Dump Tool)

COMMON VULNERABILITIES

CVE-2023-27532 | CVE-2025-6264 | CVE-2025-53770

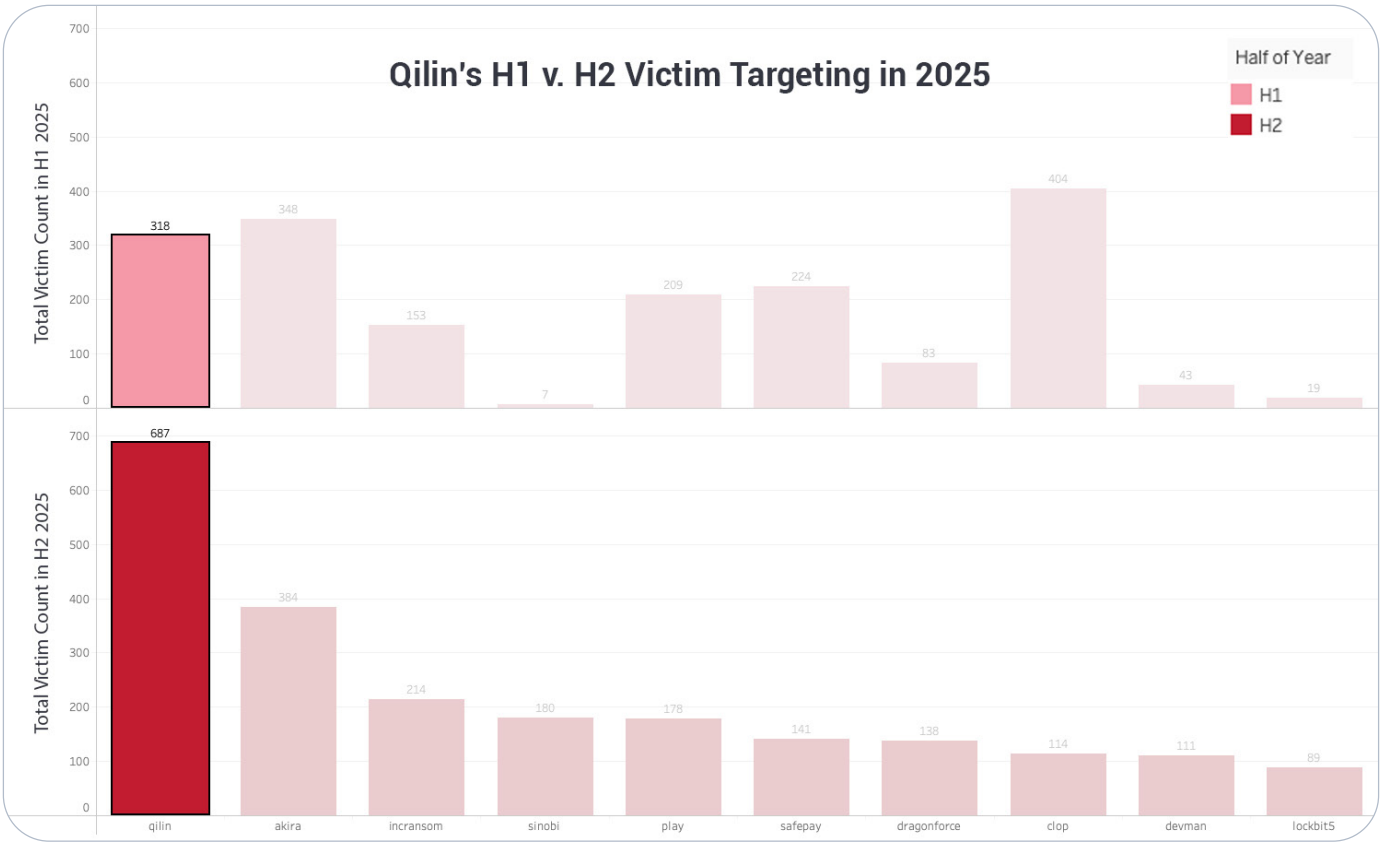
INITIAL ACCESS VECTORS

- Phishing campaigns with malicious attachments
- Compromised VPN and RDP credentials
- Exploitation of public-facing applications
- Supply chain compromise via managed service providers

PRIVILEGE ESCALATION AND PERSISTENCE

- Embedded Mimikatz module for token manipulation
- Targets lsass.exe, winlogon.exe, wininit.exe for token theft
- Symbolic link manipulation via fsutil for remote/local resolution
- Abuse of RMM platforms for persistent control

https://www.tripwire.com/state-of-security/qilin-ransomware-what-you-need-know
https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/
https://www.darktrace.com/blog/a-busy-agenda-darktraces-detection-of-qilin-ransomware-as-a-service-operator



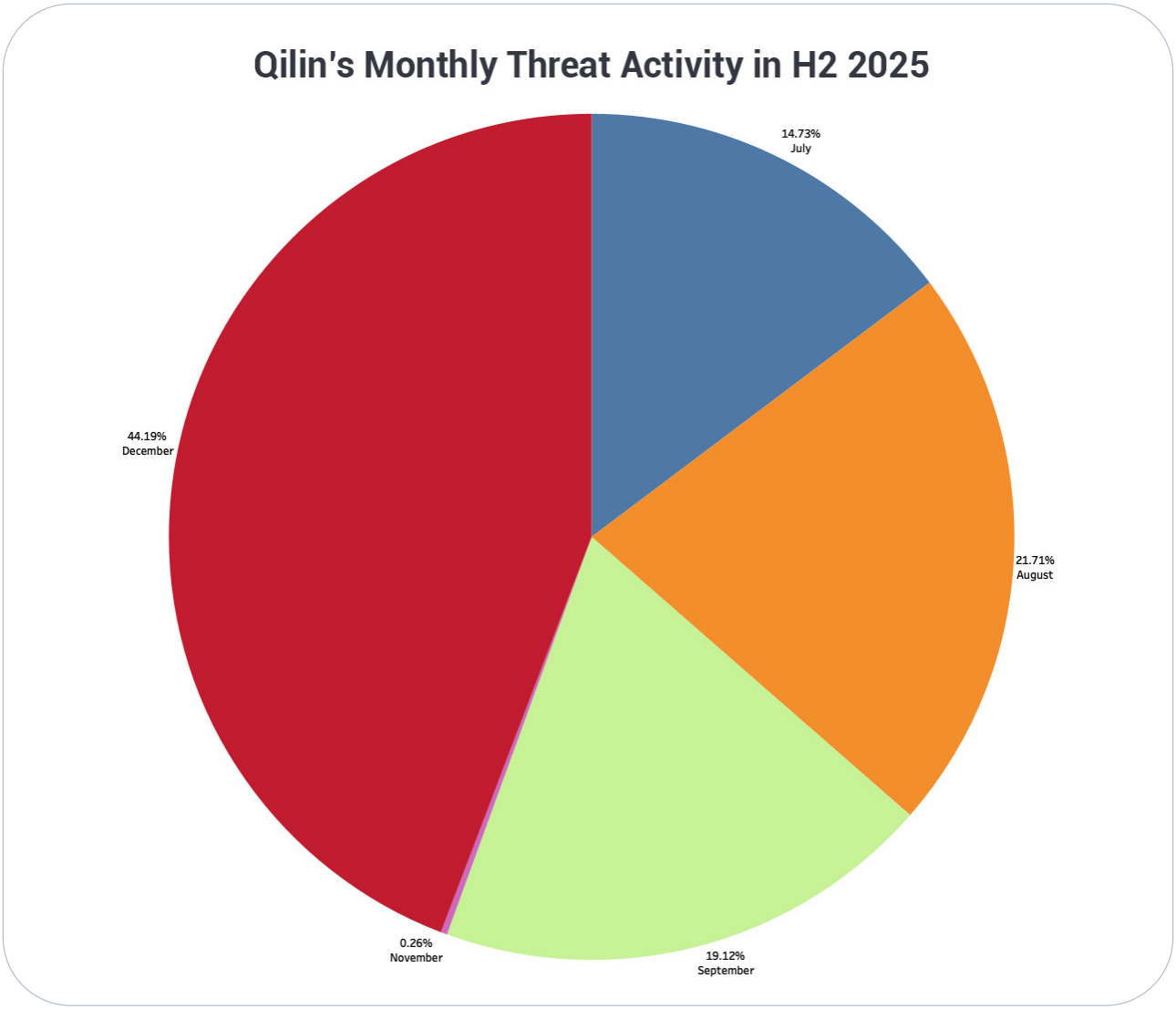
Qilin operates as a ransomware-as-a-service (RaaS) group offering cross-platform binaries compiled in Rust (primary) and Golang. Since 2022, the group recruits third-party affiliates to deploy customized Qilin payloads in exchange for a significant share of ransom proceeds, with administrators maintaining the infrastructure, negotiation interfaces, and a public data leak site hosted on Tor for double-extortion leverage. Qilin associates compromise victims primarily through phishing, exploiting vulnerabilities in public-facing applications, stolen VPN or RDP credentials, and legitimate remote management tools. Once inside, operators escalate privileges, disable defenses, perform network enumeration and lateral movement using common tools, and exfiltrate sensitive data before triggering encryption. Exfiltrated data is then used in extortion pressure via public posting on the group's leak site if victims refuse to pay.

Qilin systematically destroys recovery options by starting, reconfiguring, and then permanently disabling the Volume Shadow Copy Service through a scripted sequence of net and wmic commands. Affiliates with access to backup consoles manually delete tape archives, disable scheduled jobs, and remove backup configurations. The cipher utility is invoked to overwrite free disk space and eliminate file remnants. Systems are rebooted following encryption to ensure registry changes take effect and to disrupt incident response. The ransomware is effective across Windows, Linux, and virtualized environments, enabling broad impact across enterprise infrastructure.

The group exhibits characteristics consistent with Russian-speaking cybercriminal networks, including the use of Russian in affiliate recruitment and the presence of code that prevents execution on systems configured with Russian or CIS region languages. Operational tempo and victim notification timing suggest Eastern European working hours. While no direct state sponsorship has been established, the operational environment suggests a permissive or tolerated status within the region of origin.

In H2 2025, Critical Start's observations of Qilin's activity showed that attacks were predominantly directed at U.S. organizations, which accounted for approximately 48.58% of all recorded incidents. France and Italy followed far behind, representing 4.65% and 3.62% of attacks, respectively. This disproportionate targeting highlights a clear focus on the U.S., with European countries appearing as secondary or opportunistic targets. Compared to H1 2025 and H2 2024, this pattern has been consistent, with the U.S. repeatedly emerging as a top target for major ransomware groups, underscoring its continued vulnerability.

Industry-wise, Manufacturing was the most impacted sector, accounting for 17.31% of attacks. This high level of targeting likely reflects the critical nature of manufacturing operations, which are highly dependent on continuous production and can be significantly disrupted by ransomware incidents. Construction was the next most affected sector, with 11.89% of attacks, highlighting the growing ransomware risk to organizations managing large projects, supply chains, and infrastructure. Banking & Finance followed closely at 10.85%, indicating that financial institutions remain attractive targets due to their sensitive data, critical services, and potential for financial gain. Other sectors experienced lower but notable attack rates, emphasizing that ransomware groups continue to diversify their targets beyond traditional high-value industries.



https://socradar.io/blog/dark-web-profile-qilin-agenda-ransomware/
https://www.picussecurity.com/resource/blog/qilin-ransomware
https://blog.barracuda.com/2025/07/18/qilin-ransomware-growing
https://www.darktrace.com/blog/a-busy-agenda-darktraces-detection-of-qilin-ransomware-as-a-service-operator

2 Akira

SNAPSHOT

GEOGRAPHICAL LOCATION OF TARGETS

United States | Canada | United Kingdom | Germany

PRIMARY INDUSTRIES

Manufacturing | Business | Construction | Education | Banking & Finance

PRIMARY TOOLS

RCLONE (File Manager Tool)
Mimikatz (Cred Dump Tool)
FileZilla (File Exfil Tool)

COMMON VULNERABILITIES

CVE-2023-20269 | CVE-2024-40766 | CVE-2023-27532

INITIAL ACCESS VECTORS

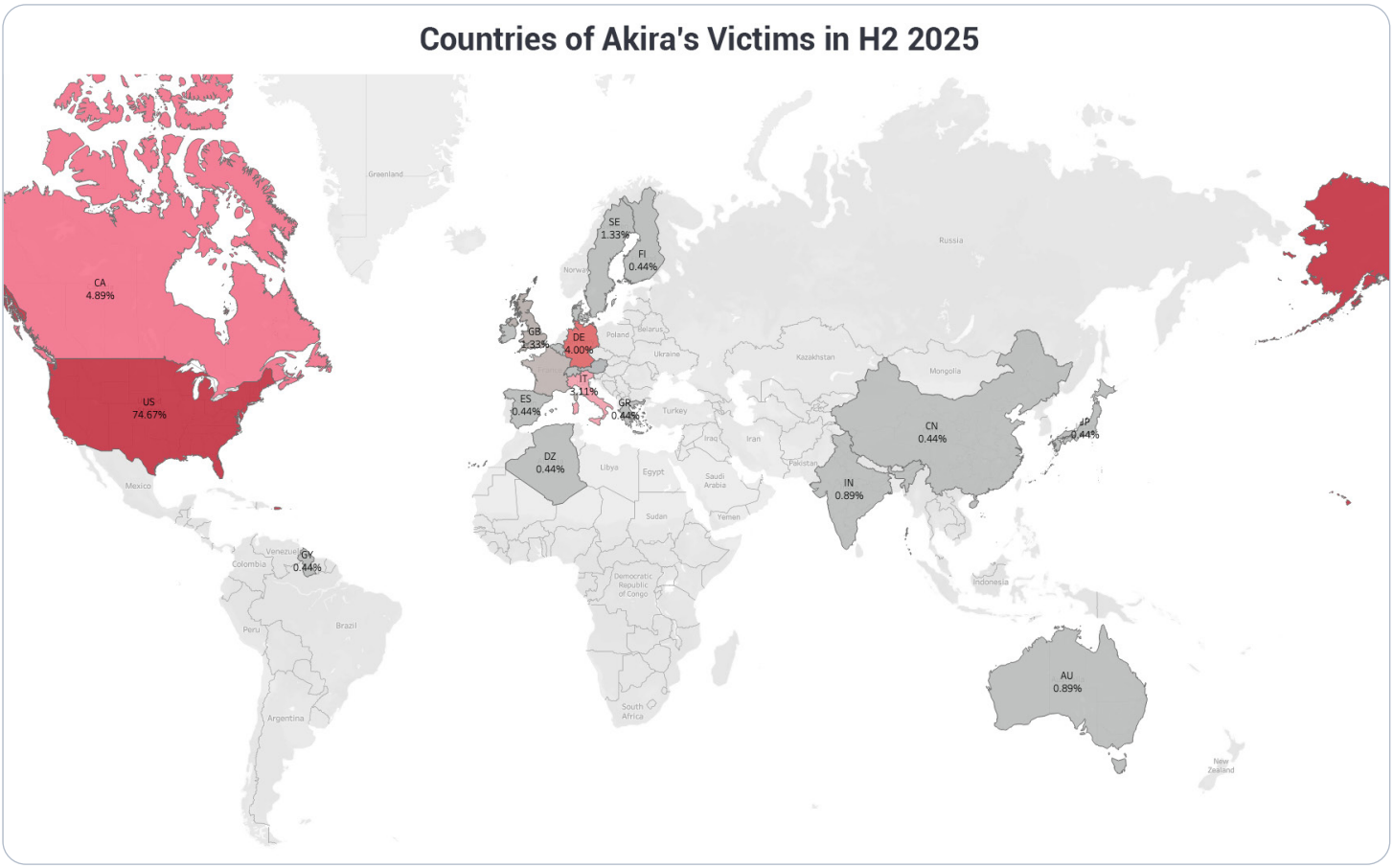
- VPN/RDP services without phishing-resistant MFA
- CVE exploitation
- Compromised credentials from initial access brokers
- Spearphishing campaigns and brute force attacks

PRIVILEGE ESCALATION AND PERSISTENCE

- Mimikatz and LaZagne for credential extraction
- LSASS memory dumping via comsvcs.dll
- NTDS.dit and SAM database extraction
- Creation of administrative accounts (e.g., itadm)

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
https://www.ibm.com/think/x-force/spotlight-akira-ransomware-x-force
https://www.darkreading.com/endpoint-security/akira-ransomware-lightning-fast-data-exfiltration-2-hours

Akira operates as a RaaS platform with cross-platform capabilities targeting Windows systems and VMware ESXi virtual machines, with recent expansion to Nutanix AHV hypervisors. The ransomware evolved from early C++ implementations to include Rust-based variants (Akira_v2) and briefly deployed a Megazord encryptor. Ransom notes (akira_readme.txt or fn.txt) contain unique victim codes for accessing Tor-based negotiation portals. Akira exhibits code overlap and operational connections to the defunct Conti ransomware group. Akira affiliates primarily exploit vulnerabilities in internet-facing services. The group extensively targets VPN products lacking MFA through credential theft, brute forcing, and password spraying using tools like SharpDomainSpray. Initial access is also achieved via SSH through compromised router IP addresses and exploitation of ESXi hypervisor vulnerabilities (CVE-2023-28252, CVE-2024-37085). Akira has demonstrated capability to compromise multiple hypervisor platforms beyond VMware ESXi. Akira employs multi-layered evasion including disabling Windows Defender, adding AV exclusions, and terminating security processes through BYOVD techniques exploiting vulnerable drivers. The group modifies registry keys including DisableRestrictedAdmin to enable credential-less login and UserList to hide accounts from login screens. Akira establishes C2 channels through tunneling utilities like Ngrok to create encrypted sessions that bypass perimeter monitoring. The group deploys SystemBC malware functioning as both a remote access trojan and proxy bot, alongside commercial penetration testing frameworks like Cobalt Strike for lateral movement and privilege escalation. Data collection and exfiltration occur rapidly, with documented cases showing data theft within two hours of initial access. Akira uses archiving tools (WinRAR, 7-Zip) to compress stolen data and transfer utilities (WinSCP, FileZilla, RClone, PuTTY/PSCP) to exfiltrate via FTP, SFTP, and cloud storage services including MEGA. Exfiltrated data is weaponized on the group's Tor leak site if ransom demands are not met. The group's rapid evolution from C++ to Rust implementations and expansion across multiple hypervisor platforms demonstrates sophisticated development capabilities and operational maturity consistent with experienced ransomware operators.



In H2 2025, Akira's activity was overwhelmingly concentrated in the United States, which accounted for nearly three-quarters (74.67%) of all observed incidents. Canada followed at 4.89%, representing the closest geographic neighbor affected, while Germany accounted for 4.00%, highlighting limited activity in Europe. This stark concentration suggests that Akira prioritizes high-value U.S. targets while also opportunistically targeting organizations in other regions.

Industry-wise, Akira primarily targeted Manufacturing, representing 24.44% of all observed activity. This sector's reliance on continuous production and complex supply chains makes it particularly vulnerable to disruption. Business Services followed at 19.11%, reflecting the attractiveness of organizations that manage large volumes of sensitive client data and critical IT systems. Construction accounted for 15.11% of attacks, highlighting the risks to firms managing large-scale projects, supply chains, and infrastructure development. Other sectors experienced lower levels of targeting, indicating that while Akira concentrates on high-impact industries, it maintains a broader attack footprint.

3 Incransom

SNAPSHOT

GEOGRAPHICAL LOCATION OF TARGETS

United States | Canada | United Kingdom | Germany

PRIMARY INDUSTRIES

Manufacturing | Education | Software & IT | Government | Business Services

PRIMARY TOOLS

Mimikatz (Cred Dump Tool)
PsExec (Remote Access Tool)
AnyDesk (Remote Access Tool)

COMMON VULNERABILITIES

CVE-2023-3519 | CVE-2023-48788 | CVE-2024-57726-28

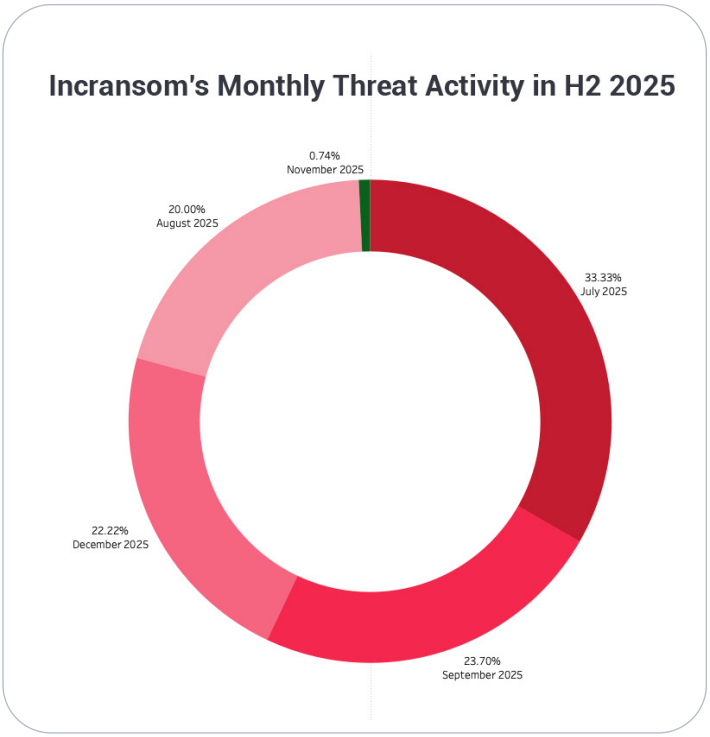
INITIAL ACCESS VECTORS

- Phishing and spear-phishing with credential theft and payload delivery
- Valid credentials from password reuse, prior breaches, or IABs
- Exploitation of public-facing apps
- RDP access using stolen or brute-forced accounts

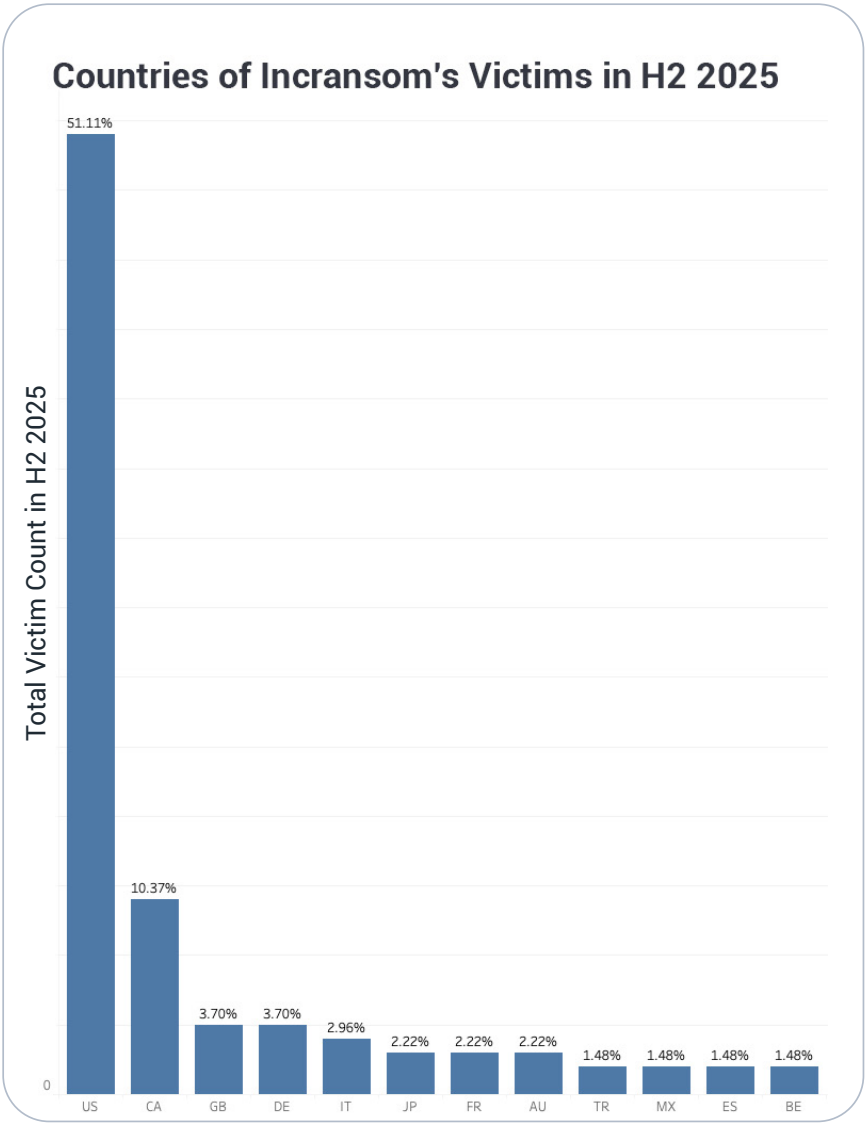
PRIVILEGE ESCALATION AND PERSISTENCE

- Valid domain accounts leveraged for long-term access
- Credential theft with Mimikatz and lsass-style tooling
- RDP persistence with compromised admin credentials
- Renamed/"living off the land" services (e.g., PsExec as winupd)

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-inc
https://www.halcyon.ai/threat-group/inc-ransom
https://cyble.com/threat-actor-profiles/inc-ransom/



INC Ransom (also tracked as GOLD IONIC) runs a mature RaaS/data-extortion operation focused on corporate networks. Affiliates deploy Windows and ESXi encryptors that rename files with a .inc extension and drop INC-README.txt/.html notes, often changing desktop wallpaper and, in some cases, printing ransom notes via networked printers. Operations revolve around a Tor leak portal with surface-web mirroring (e.g., incapt[.]blog) used to publish victim announcements and proof-of-leak data. The group systematically abuses common admin and remote-access tooling, favoring operational stealth over bespoke malware development. Affiliates typically gain footholds via phishing to harvest credentials or drop loaders, then pivot using VPN/RDP access with those credentials. A parallel path is direct exploitation of edge infrastructure, particularly Citrix NetScaler ADC/Gateway RCE (CVE-2023-3519), Fortinet EMS SQLi RCE (CVE-2023-48788), and SimpleHelp RMM flaws (CVE-2024-57726/57727/57728). Valid accounts sourced from initial-access brokers or earlier compromises are a recurring theme, with RDP and remote admin channels abused as the primary ingress for interactive operations. Once inside, operators escalate by harvesting credentials from memory and local stores using tools such as Mimikatz or lsass-style scripts, seeking domain admin and service accounts that unlock broad lateral movement. Persistence is less about implants and more about durable credentialed access: RDP sessions, VPN accounts, and domain-level credentials are maintained over time. The group often deploys PsExec under the misleading name winupd and installs remote-access tools (e.g., AnyDesk) as if they were routine IT components, blending into normal administrative workflows. After establishing access, affiliates conduct systematic reconnaissance using AdFind to map Active Directory, NETSCAN.EXE and Advanced IP Scanner for service and host discovery, and standard Windows tools and browsers (including Internet Explorer) to enumerate shares and browse remote file systems. Before encryption, data is collected and staged on key servers using 7-Zip or WinRAR. Operators manually inspect documents and images with native apps (Wordpad, Notepad, MSPaint) to triage the most sensitive content. For exfiltration, they install and configure MEGASync or use Rclone to push archives to attacker-controlled cloud storage accounts. Once data theft is complete, the Windows and ESXi variants of the encryptor are deployed, often stopping VMs on hypervisors before encrypting storage. Encrypted files receive the .inc extension, and ransom notes are dropped widely to direct victims to the Tor portal where payment and leak negotiations occur. Public reporting to date characterizes INC as a financially driven, non-state group with sophisticated tradecraft and an expanding affiliate ecosystem rather than an ideologically or state-directed actor.



In H2 2025, CRU observed Incransom activity predominantly targeting organizations in the United States, which accounted for 51.11% of all listed victims. Canada followed at 10.37%, while the United Kingdom and Germany shared third place, each representing 3.70% of observed victims. This distribution indicates a strong focus on North America, with more limited targeting across Europe. During the same reporting period, Manufacturing was the most impacted industry, accounting for 18.52% of Incransom's victims. Software & IT followed closely at 17.04%, reflecting the high value of organizations that provide core technology services and interface with multiple industries due to widespread reliance on digital infrastructure. Business Services ranked third at 13.33%, highlighting the appeal of firms that manage sensitive client data and provide outsourced or professional services.

4 Sinobi

SNAPSHOT

GEOGRAPHICAL LOCATION OF TARGETS

United States | Canada | Australia | India | United Kingdom

PRIMARY INDUSTRIES

Manufacturing | Construction | Business Services | Healthcare | Education

PRIMARY TOOLS

RCLONE (File Manager Tool)
WinSCP (Data Exfil Tool)
AnyDesk (Remote Access Tool)

COMMON VULNERABILITIES

CVE-2024-53704 | CVE-2024-40762

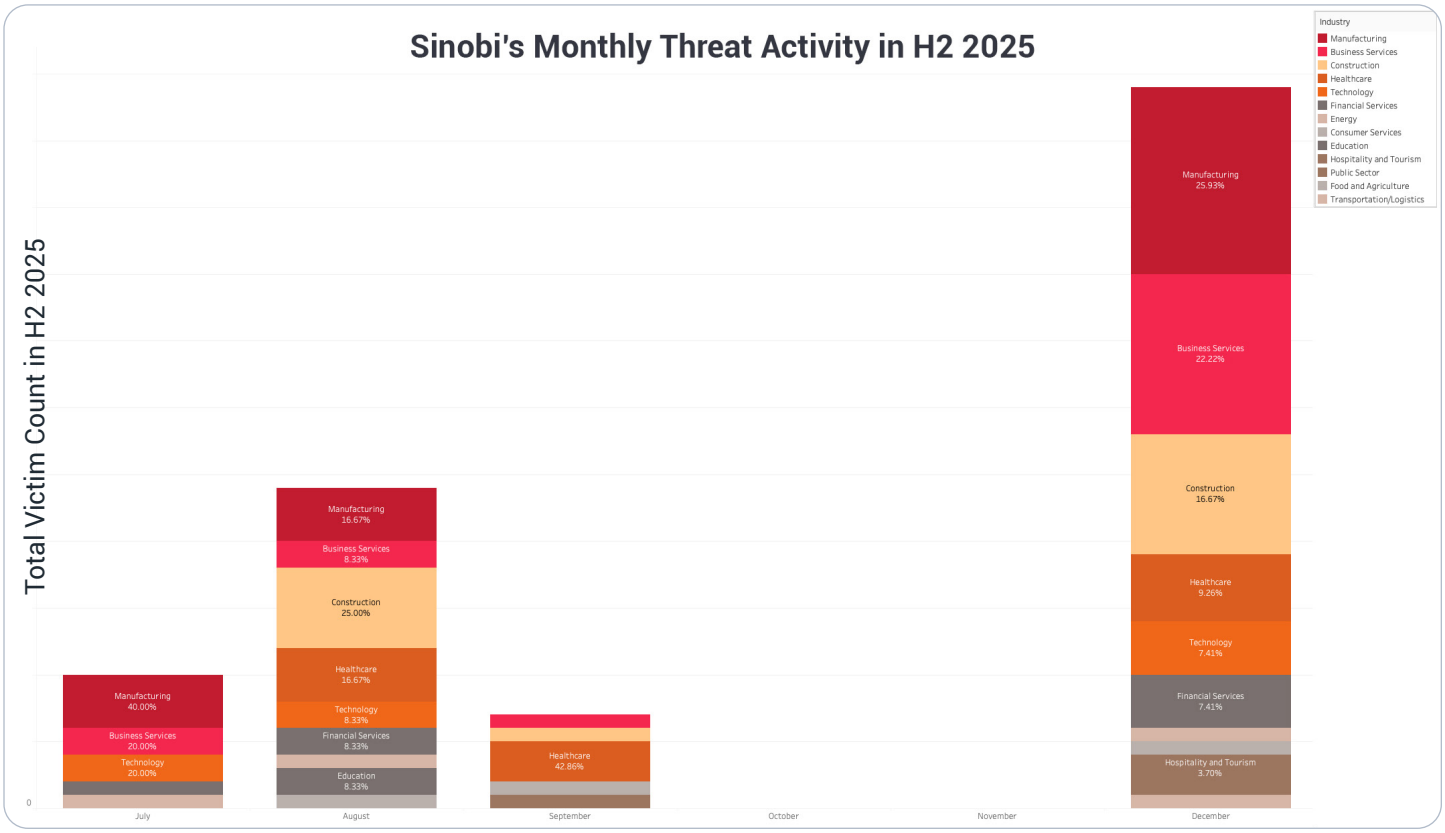
INITIAL ACCESS VECTORS

- Compromised SonicWall SSL VPN and other VPN/firewall credentials
- Initial Access Broker (IAB) purchases and darknet credential markets
- Exploits against remote access and edge systems (Citrix/Fortinet, etc.)
- Phishing via commodity phishing kits and third-party MSP compromise

PRIVILEGE ESCALATION AND PERSISTENCE

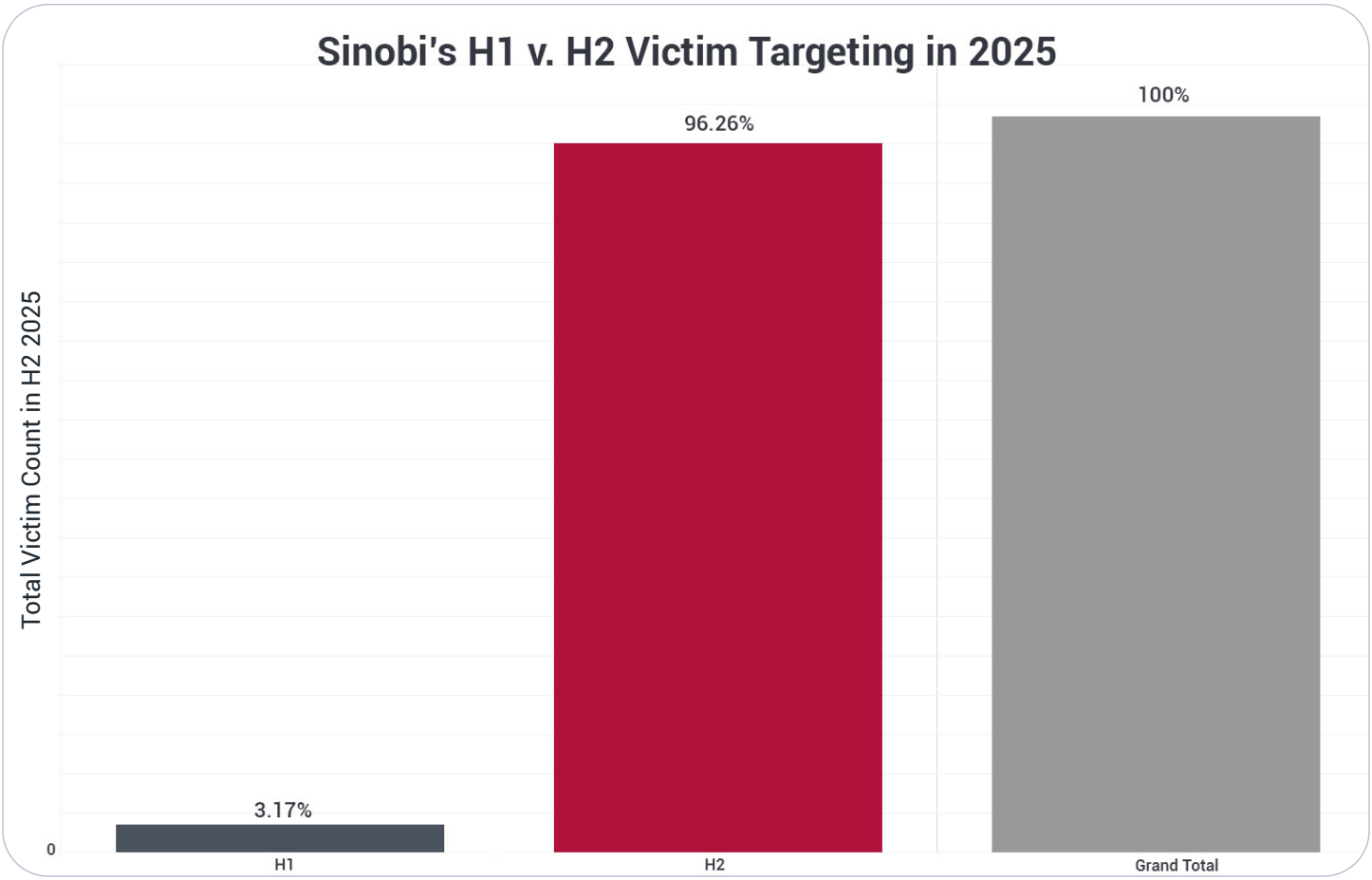
- Use of over-privileged domain accounts from VPNs/MSPs
- Creation of new local/domain admin accounts for redundancy
- Disabling and uninstalling EDR via service and config abuse
- Persistence through configured remote-access tools and standing credentials

https://blog.barracuda.com/2025/11/17/sinobi--the-bougie-exclusive-ransomware-group-that-wants-to-be-a
https://www.surefirecyber.com/threat-actor-profile-sinobi/
https://www.halcyon.ai/threat-group/sinobi



Sinobi emerged in mid-2025 as a "bougie-exclusive" brand emphasizing stealthy, high-value operations rather than volume attacks. Core operators maintain the ransomware code, Tor infrastructure, negotiations, and laundering, while a small, screened affiliate network handles intrusion and deployment. Intrusions are characterized by modular tooling, heavy living-off-the-land (LotL/LOLBins) usage, and quiet hands-on-keyboard activity. Code overlap, leak-site similarities, and tradecraft strongly suggest Sinobi is a rebrand or offshoot of Lynx. Sinobi's affiliates leverage native Windows commands, service control (sc), and legitimate uninstallers like Revo Uninstaller to tamper with defenses. Custom binaries are kept sparse, often named generically (bin.exe) and staged in typical enterprise paths. By operating a closed, invite-only affiliate program and avoiding noisy underground recruitment, Sinobi reduces its visibility to law enforcement and researchers, complementing its technical stealth with organizational OPSEC. After gaining admin-level access, Sinobi affiliates pivot across servers and workstations using RDP and configured remote-access utilities. They deploy small reconnaissance scripts that enumerate Active Directory (domain info, privileged accounts), locate file shares, and inventory endpoint security products that must be neutralized. Data exfiltration begins once reconnaissance is complete and high-value repositories have been identified.

Operators stage data into archives and then transfer it using Rclone or WinSCP to attacker-controlled cloud storage or hosting infrastructure. Exfiltrated datasets include financial records, IP, customer/employee PII, and regulated data that magnify legal and reputational exposure. The same material is later featured on Sinobi's Tor leak site and its clear-web mirrors, providing "proof" during negotiations and escalating pressure if victims delay or refuse payment. The group allegedly avoids high-profile government and critical-utility targets, favoring "commercial-but-critical" organizations that are more likely to pay large ransoms while drawing less geopolitical attention.



Being relatively new compared to the other groups observed, Sinobi demonstrated a limited geographic spread in H2 2025, with listed victims originating from just nine countries. The United States accounted for 84.21% of victims, followed by Italy at 4.21% and India at 3.16%. Industry targeting in H2 2025 showed Manufacturing as the most affected sector at 23.16%, followed by Business Services at 17.89% and Construction at 16.84%.

5 Play

SNAPSHOT

GEOGRAPHICAL LOCATION OF TARGETS

United States | Canada | Australia | Japan | Vietnam

PRIMARY INDUSTRIES

Healthcare | Transportation & Logistics | Software & IT | Manufacturing | Real Estate

PRIMARY TOOLS

ProcDump (Process Monitoring Tool)
Mimikatz (Cred Dump Tool)
Grixba (Infostealer)

COMMON VULNERABILITIES

CVE-2022-41082 | CVE-2020-12812 | CVE-2023-4966

INITIAL ACCESS VECTORS

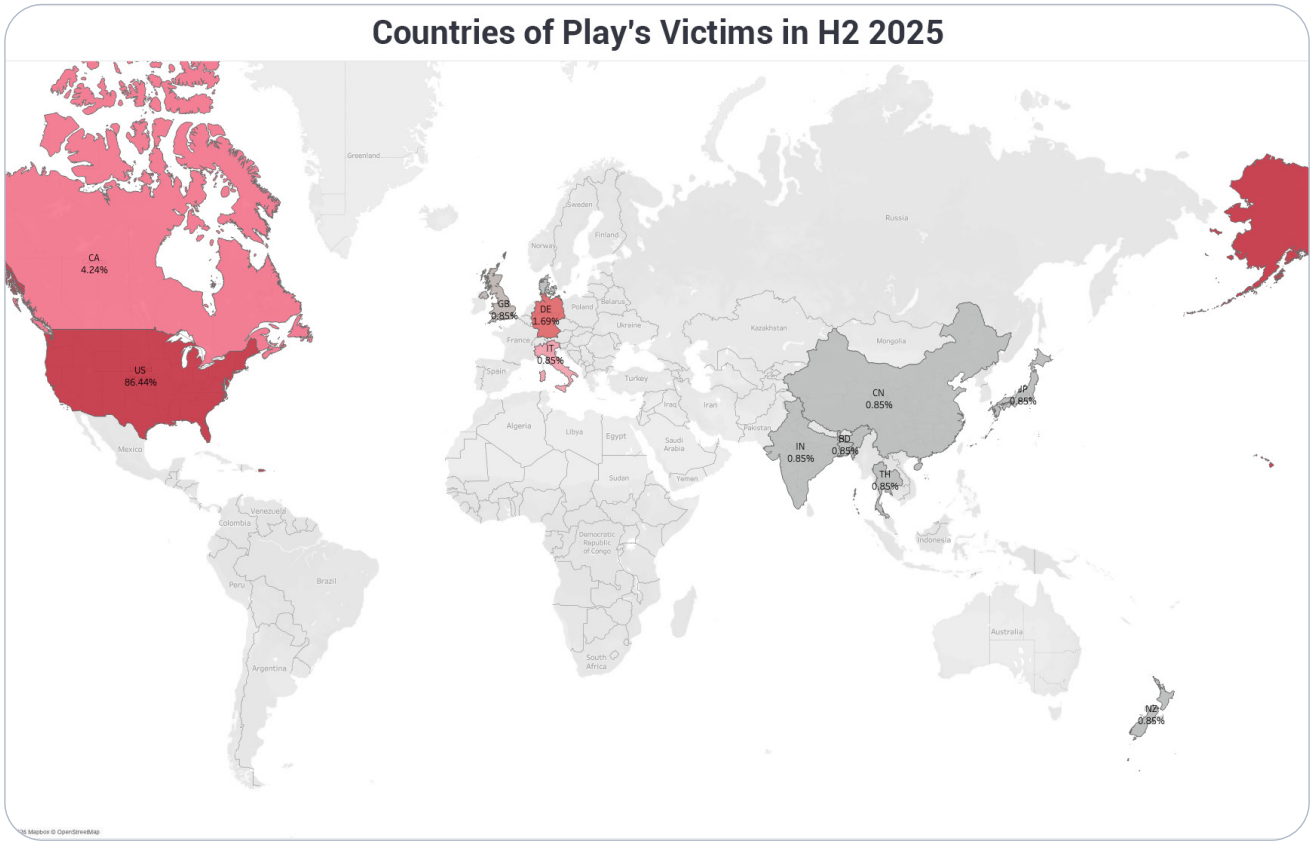
- Exploitation of known vulnerabilities in Fortinet FortiOS and Microsoft Exchange
- Abuse of valid accounts, often purchased from Initial Access Brokers (IABs)
- Exploitation of RMM tools (e.g., SimpleHelp CVE-2024-57727)
- Use of external-facing services like RDP and VPNs

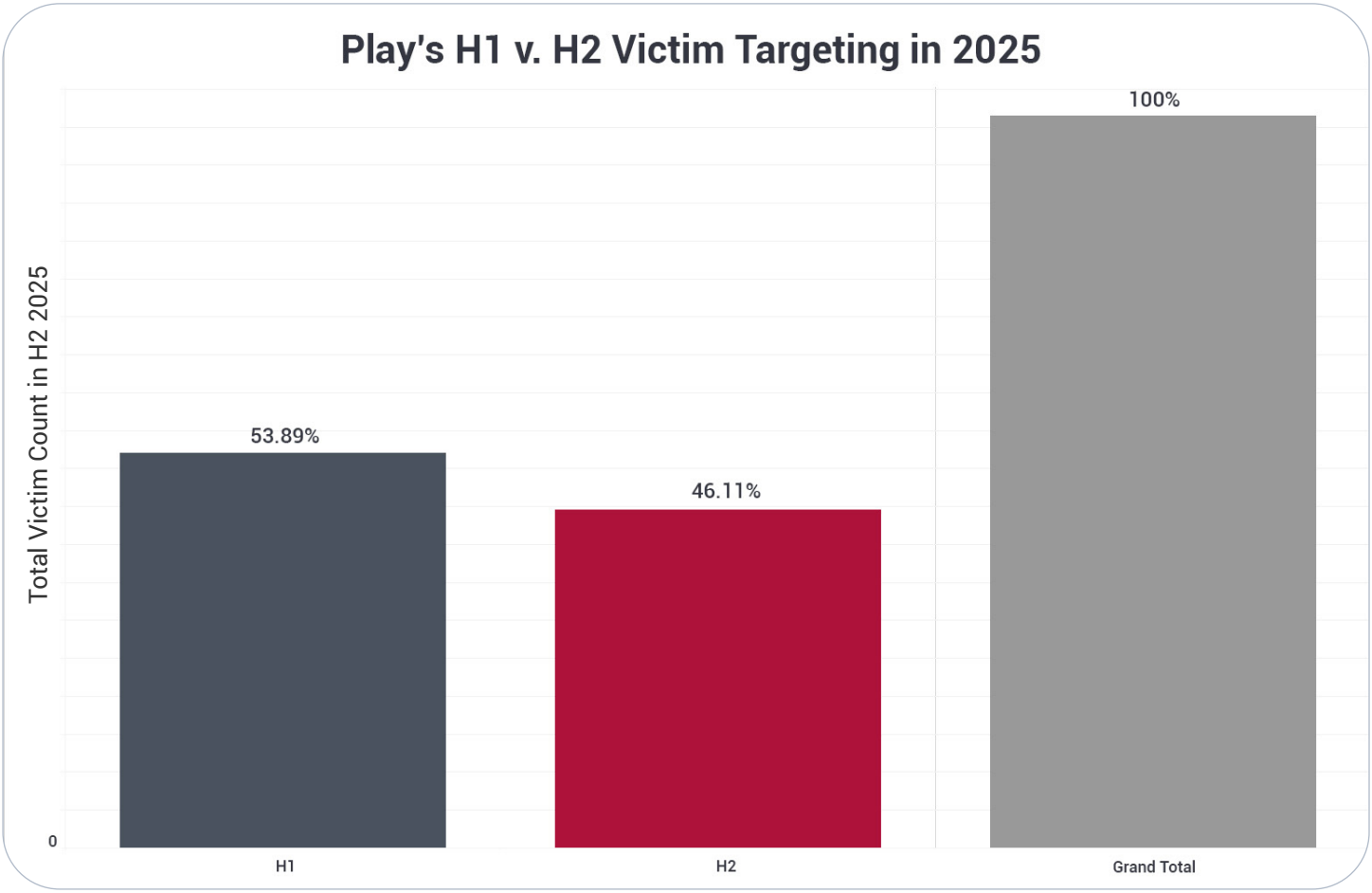
PRIVILEGE ESCALATION AND PERSISTENCE

- Use of Mimikatz and ProcDump for credential harvesting
- Deployment of WinPEAS and BloodHound to map attack paths
- Creation of scheduled tasks (schtasks) for automated execution
- Use of custom backdoors like SVCHost.dll to maintain access

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
https://www.sentinelone.com/anthology/play/
https://cyble.com/threat-actor-profiles/play-ransomware-group/

Play (also known as PlayCrypt) emerged in June 2022 and quickly became one of the most prolific ransomware threats, with approximately 900 affected entities reported by the FBI as of May 2025. Unlike the common Ransomware-as-a-Service (RaaS) model, Play operates as a closed group to maintain tighter control over negotiations and operational security. They employ a double extortion strategy, exfiltrating massive datasets before deploying encryption. If victims refuse to pay, the group threatens to leak data on their Tor site and often makes direct, threatening phone calls to various departments within the victim organization to increase pressure. Play actors gain initial footholds primarily by targeting unpatched edge devices and public-facing applications. Additionally, they leverage stolen or purchased credentials to log into VPNs and RDP sessions. Recent campaigns have also seen the group or its associates exploiting vulnerabilities in Remote Monitoring and Management (RMM) to achieve remote code execution. Once initial access is achieved, Play operators focus on escalating privileges to Domain Admin status. They use Mimikatz and ProcDump to extract credentials from LSASS memory and run WinPEAS or BloodHound to identify misconfigurations and escalation paths. The group's reconnaissance is powered by Grixba, a custom-built tool that scans networks for active hosts, IP ranges, and security software. They move laterally across the environment using commercial C2 frameworks like Cobalt Strike and SystemBC. For hands-on movement, they rely on PsExec (and a custom version called PSexesvc.exe) alongside native RDP. Tools like AdFind and nltest are used to query Active Directory, allowing the actors to identify domain controllers and high-value file servers for data staging. Before triggering encryption, Play actors identify and aggregate sensitive data. They use WinRAR to split and compress large datasets into .RAR format to facilitate faster transfer. These archives are then moved out of the network using WinSCP over SFTP/SSH to actor-controlled servers. The group also exfiltrates the output of their Grixba tool, which includes detailed network maps and browser histories, providing them with additional context to use during the extortion phase. To ensure the victim cannot easily recover, Play deletes Volume Shadow Copies and other backup artifacts. The ESXi variant is particularly destructive, as it invokes shell commands to power off all running Virtual Machines before encrypting their virtual disks (.vmdk, .vmx, etc.). The ransomware also uses the Restart Manager API to kill processes that might be holding files open (such as databases or office apps), ensuring that the maximum amount of data is successfully encrypted and rendered inaccessible. Play does not discriminate by industry but shows a clear preference for large enterprises and critical infrastructure providers.





In H2 2025, Play's listed victims were predominantly concentrated in the United States, which accounted for 86.44% of observed victims. Canada followed at 4.24%, while Germany represented 1.69% of activity, underscoring Play's narrow geographic focus during the reporting period. From an industry perspective, Manufacturing was the most impacted sector in H2 2025, accounting for 24.58% of Play's victims. Construction followed at 16.95%, indicating sustained targeting of organizations within the construction sector. Software & IT ranked closely behind at 16.10%.

Across H2 2025, the top five observed ransomware threat actors, Qilin, Akira, Incransom, Sinobi, and Play, demonstrated a consistent geographic emphasis on the United States, which remained the primary target across all groups. Akira and Play showed the strongest concentration, with U.S.-based victims accounting for more than three-quarters of their observed activity. Qilin and Incransom also maintained a clear U.S. focus with secondary targeting in Canada and select European countries. Sinobi, while more limited in scale due to its relative maturity, similarly concentrated the majority of its activity within the United States, with minimal distribution across Europe and Asia.

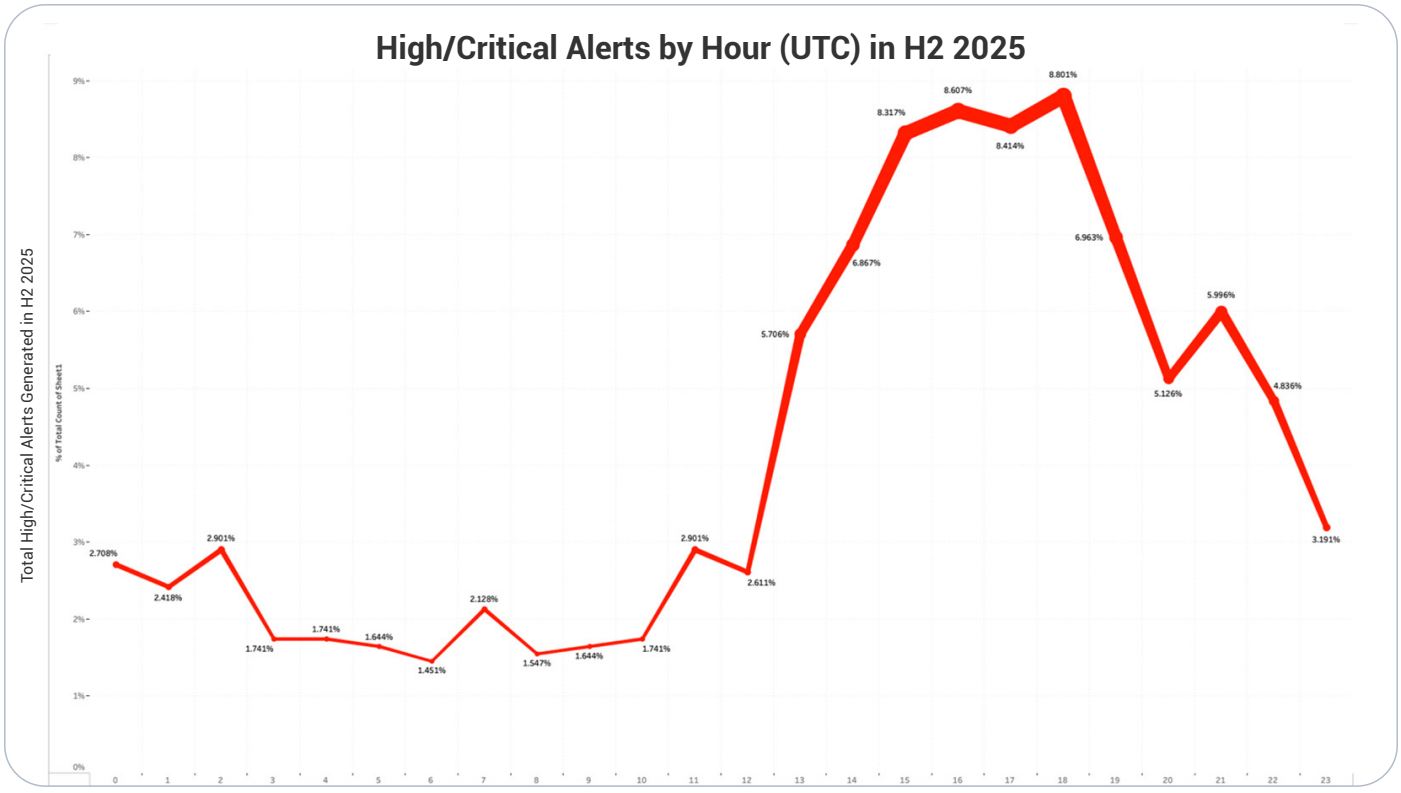
From an industry perspective, Manufacturing emerged as the most consistently targeted sector across all five actors. Construction and Business Services also appeared frequently among the top targeted industries, while Technology and Software and IT featured more prominently for actors such as Play and Incransom. Overall, the combined activity of these threat actors indicates a sustained focus on U.S.-based organizations operating in manufacturing, service-oriented, and technology-dependent sectors throughout H2 2025. These patterns indicate that ransomware groups are not only targeting specific countries and industries but also share common tradecrafts. Despite differences in their targets, these actors often rely on similar tactics, techniques, and procedures (TTPs). This overlap in tradecrafts means that organizations face a compounded risk from multiple attacks using similar methods. Multi-layered defenses, continuous monitoring, and coordinated incident response plans are critical to defending against these evolving and overlapping threats.

Timeline & TTP Trends

CriticalStart's MDR capabilities provide CRU with deep visibility into security alerts through direct APIs and integrations with over 100 log sources across an organization's entire security ecosystem. This includes coverage of email systems, identity platforms, cloud infrastructure, network environments, and endpoints. Leveraging this data in 2025, CRU analyzed high and critical alerts to identify temporal attack trends, feeding insights into the CORR platform and providing a detailed, enterprise-wide view of when attackers are most active.

Timing of attacks offers actionable intelligence for defenders, highlighting hours of greatest risk and helping organizations optimize monitoring, detection, and response. Recognizing these temporal patterns allows security teams to anticipate attacker behavior, allocate resources efficiently, and strengthen defenses during periods of peak operational impact.

In H2 2025, high and critical alert activity began increasing around 1300 UTC, intensifying through the afternoon. The most active hours were 1500 UTC (8.32%), 1600 UTC (8.61%), 1700 UTC (8.41%), and 1800 UTC (8.80%), with 1800 UTC emerging as the single highest hour. Taken together, the four-hour window from 1500 to 1800 UTC accounted for approximately 34.14% of all high and critical alerts in H2 2025, representing both a broader and later execution window compared to H1 2025, where the 1400 to 1700 UTC period accounted for 32.60% of alerts. For context, in H2 2024, activity was also clustered between 1400 and 1700 UTC, but the pattern was more uneven and less sustained, suggesting shorter or campaign-based execution rather than prolonged operations.



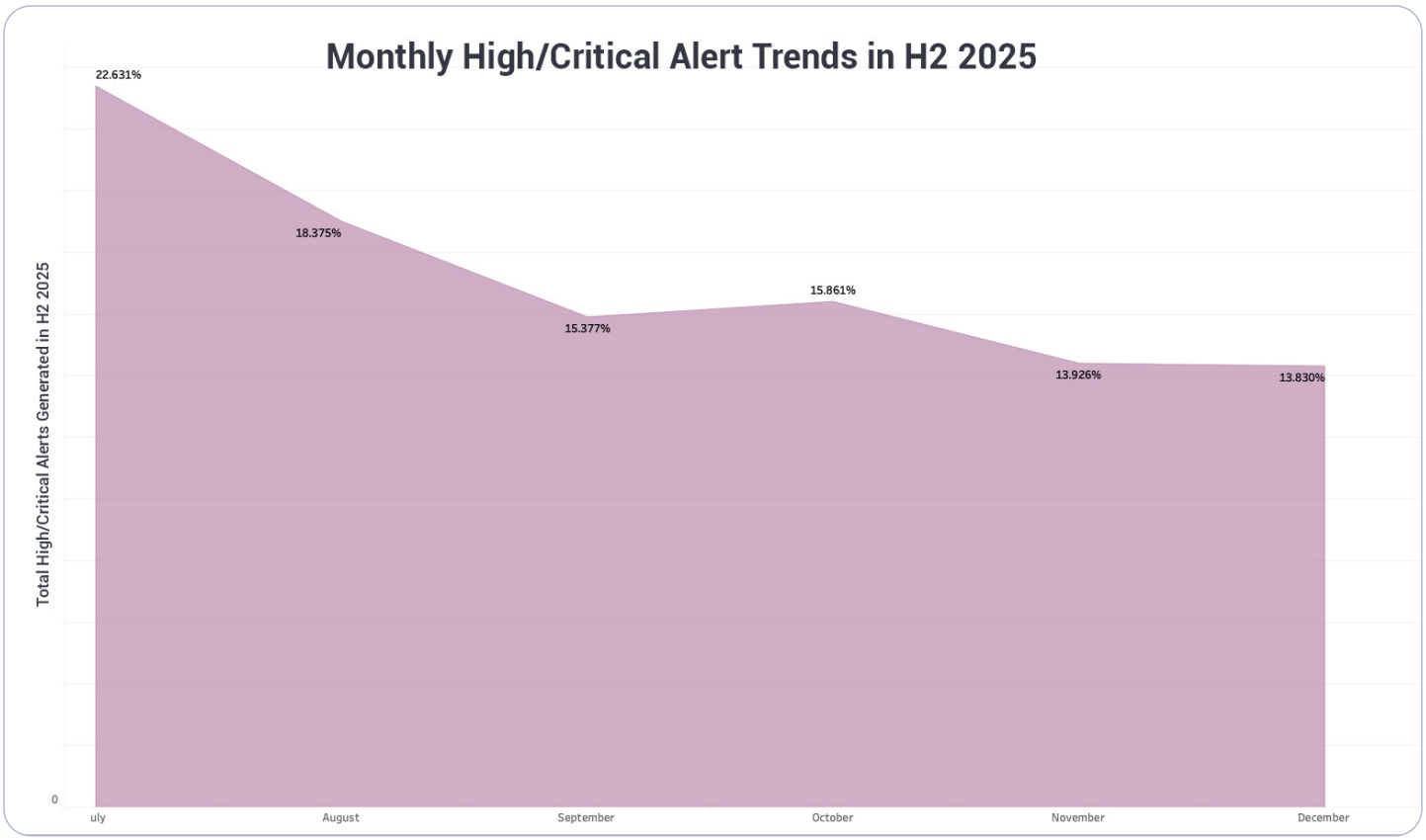
From an attacker standpoint, the shift toward later and sustained activity indicates attackers are timing execution to coincide with periods of high workstation and application usage across EMEA and overlapping with U.S. business hours. This allows malware execution, credential use, and lateral movement to blend more effectively into legitimate activity, maximizing operational impact.

Given these findings, organizations should ensure monitoring, detection, and response capabilities are fully prepared during periods of peak activity. Planning for these high-activity windows allows teams to reduce risk and respond more effectively to threats when they are most likely to occur.

Seasonal Trends

In H2 2025, monthly high- and critical-level alerts show a distinct pattern compared to prior periods. July emerged as the most active month, accounting for 22.63% of alerts, followed by August at 18.38% and October at 15.86%. September saw a slight dip to 15.38%, indicating that attacker activity is not strictly following the traditional holiday or discount-shopping cycle.

This pattern deviates from H2 2024, when October, November, and December collectively accounted for roughly 61% of high- and critical incidents. The 2024 spike was closely tied to the holiday shopping season and associated increases in e-commerce activity, which created both opportunity and distraction for organizations. In contrast, the 2025 data suggest that attackers are adapting their strategies, exploiting periods outside the traditional shopping season, such as midsummer, when organizational attention may shift toward vacations, reduced staffing, or seasonal operational changes.



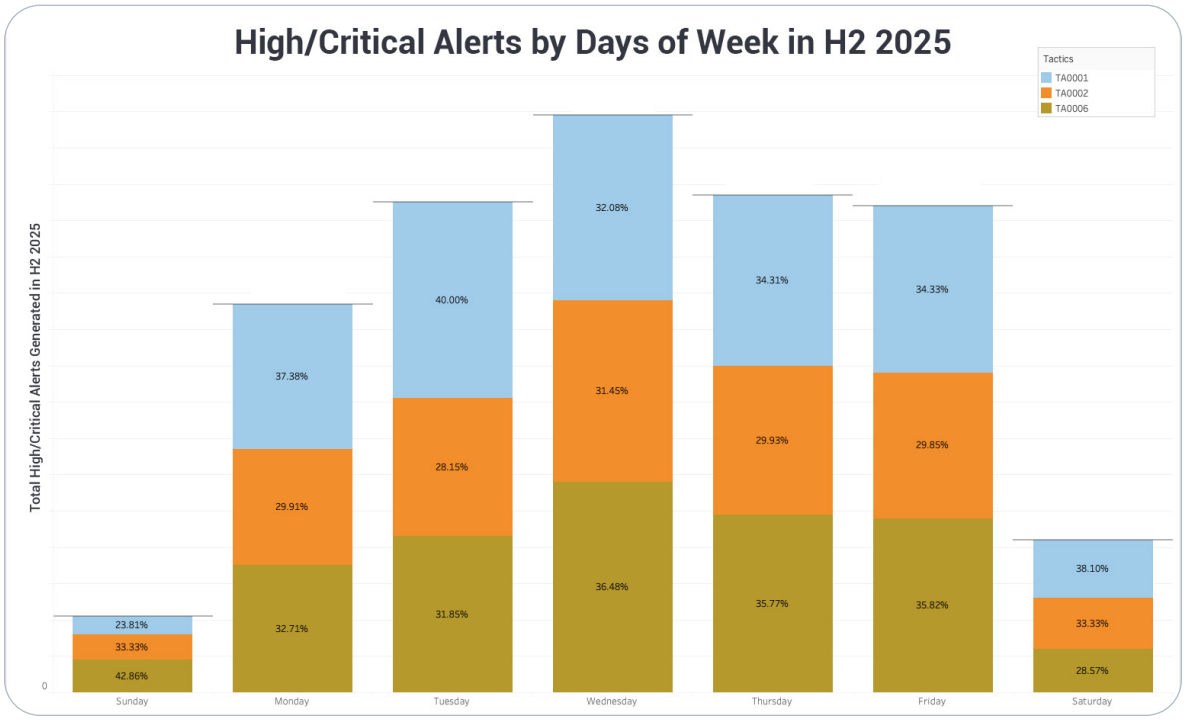
The July peak is particularly notable, as it occurs during the summer in the Northern Hemisphere, a period traditionally considered lower risk for enterprise-focused cyber campaigns. This indicates that attackers may be leveraging periods of reduced vigilance or inconsistent staffing, rather than relying solely on high transaction volumes, to maximize the likelihood of successful exploitation.

The slight decline in September followed by sustained activity in October also suggests that attackers are spreading their operations more evenly across months, rather than concentrating exclusively around known high-value periods. This evolution points to more sophisticated operational planning, where threat actors balance impact, detection avoidance, and opportunity, rather than adhering to predictable seasonal spikes.

For organizations, the 2025 monthly trends highlight that risk is no longer strictly seasonal. Security monitoring, awareness campaigns, and incident response planning should consider year-round coverage, including traditionally "low-traffic" months such as July, to maintain resilience against attackers who are actively shifting their operational timing to exploit periods of reduced vigilance.

Days of the Week

In H2 2025, Wednesday accounted for the highest share of activity at 21.63%, followed by Thursday at 18.64%. Tuesday at 18.37% and Friday at 18.23% followed closely, reinforcing a consistent mid-week concentration. This represents a shift from H2 2024, when Tuesday and Friday were the most active days. The transition began in H1 2025, where Thursday and Wednesday emerged as the top two days, and persisted throughout 2025. Overall, weekday activity dominated the reporting period.



The concentration of activity during weekdays suggests that attackers are increasingly optimizing for operational impact rather than simply reduced visibility. Weekdays offer sustained workstation usage, broader access to internal applications, and higher likelihood of user interaction with enterprise systems. Compared to weekends, when activity may shift toward mobile devices or limited access workflows, weekday execution provides greater opportunities for attackers to achieve tangible outcomes such as credential abuse, lateral movement, or business disruption.

CRU's CTI verdicts further reinforce this distinction by technique. Malware Execution activity was predominantly reported mid-week, indicating a preference for execution during periods of active endpoint usage. While executing malware over weekends could benefit from reduced staff monitoring, it often results in lower overall impact due to decreased workstation use and faster automated containment through EDR controls. As organizations have matured their weekend monitoring and response capabilities in response to historical attacker behavior, the advantage of weekend execution has diminished, making weekday execution a more reliable path to value for attackers.

Conversely, phishing campaigns involving malicious links were more frequently reported on weekends, aligning with their role as an initial access mechanism rather than an immediate impact vector. Weekend phishing allows attackers to establish a foothold quietly, when users may be more relaxed, less vigilant, or checking email casually. Depending on the lure, this timing can increase click-through rates while delaying detection until normal operations resume, at which point follow-on activity can be staged during high-value weekday periods.

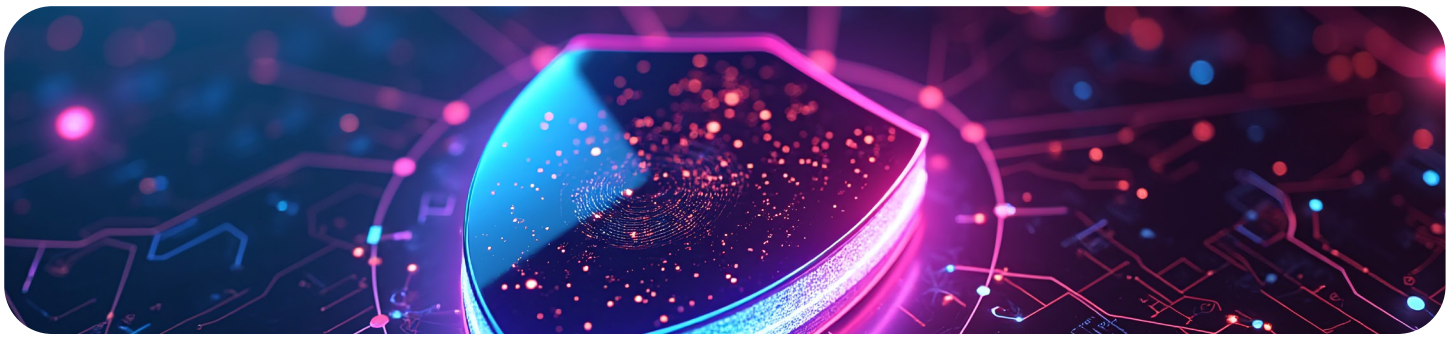
Taken together, these trends suggest that attackers are segmenting activity by objective. Initial access is increasingly attempted during lower-friction periods such as weekends, while execution and post-compromise actions are deferred to weekdays when system usage and user interaction maximize impact. Organizations should align defenses accordingly by maintaining strong weekend phishing visibility and rapid triage, while prioritizing mid-week readiness to prevent escalation from previously established access.

Timing

High and critical alert activity has shown clear evolution over recent periods, revealing patterns that can inform operational monitoring and response. In H1 2024, alerts were heavily concentrated between 1600 and 2100 UTC, suggesting that attackers often targeted the tail end of the business day when organizations were winding down operations or transitioning to after-hours. By H2 2024, the peak window shifted earlier to 1400–1700 UTC, with 1700 UTC emerging as the most active hour and 1400 UTC closely following. This shift toward daytime hours may reflect adversaries' intent to blend activity with periods of active system use, taking advantage of higher user engagement and transitional workflows.

In H2 2025, the pattern shifted slightly later to 1500–1800 UTC, with 1800 UTC now representing the single highest hour. While the four-hour window remains consistent in duration with H2 2024, activity during this period appears more sustained, indicating that attackers are maintaining operations continuously rather than in uneven bursts. Compared to H1 2024's concentrated end-of-day activity and H2 2024's uneven mid-afternoon peaks, H2 2025 shows a trend toward prolonged engagement during key operational hours, emphasizing the persistence of attacker focus across the business day.

These timing trends have clear operational implications. Security teams should ensure that monitoring, detection, and response capabilities are fully prepared throughout the afternoon and early evening, rather than concentrating solely on traditional peak hours. Planning for these sustained windows allows organizations to detect and respond more effectively, reducing the chance that attacker activity will go unnoticed during periods of high operational activity.



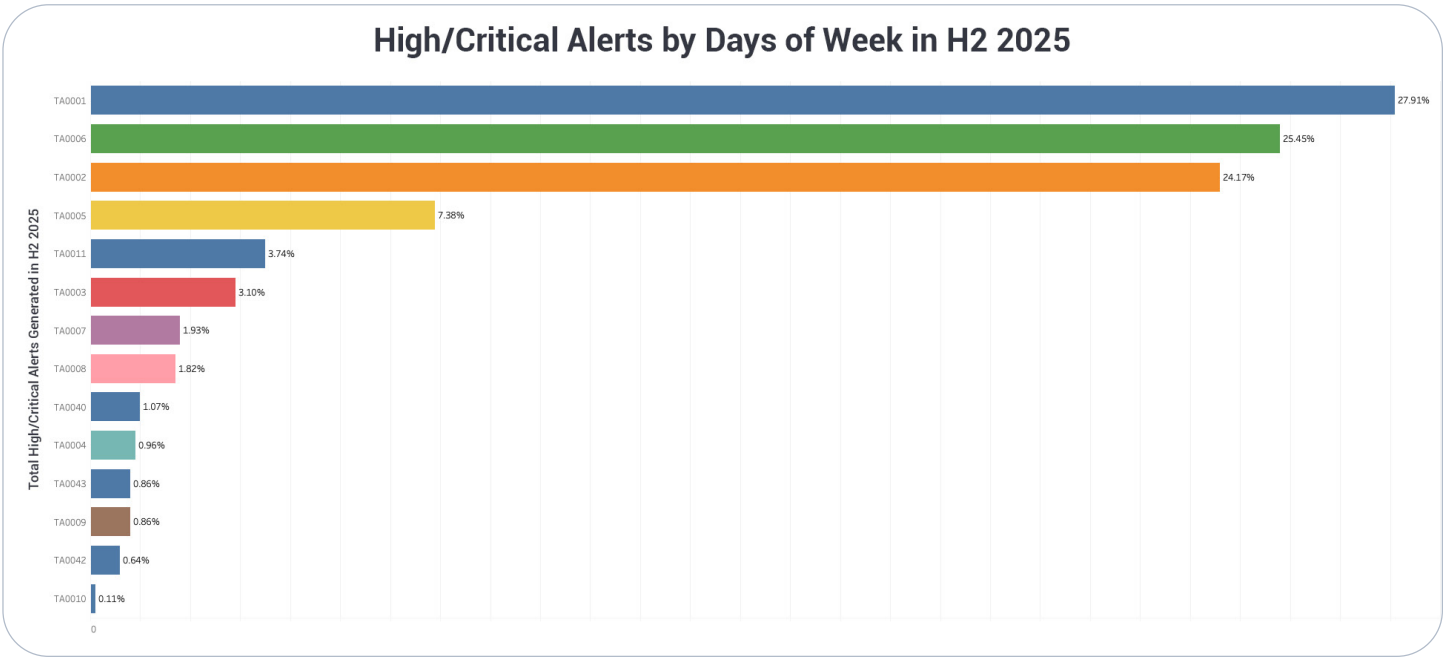
MITRE Tactics and Techniques

MITRE ATT&CK tactics and techniques provide a structured framework for understanding adversary behavior across the attack lifecycle. Analysis of high and critical incidents using this framework enables CRU to identify which stages adversaries prioritize and how those priorities evolve over time.

During H2 2025 (July–December 2025), Initial Access (TA0001) was the most frequently observed tactic across all industries, accounting for 27.91% of high and critical alerts. Credential Access (TA0006) followed closely at 25.45%, with Execution (TA0002) at 24.17%. Together, these three tactics accounted for 77.53% of all high and critical alerts, highlighting that the majority of adversary activity remains concentrated on the early and foundational stages of the attack lifecycle.

Initial Access represents the methods used by attackers to gain a foothold within target environments, whether through phishing, exploitation of vulnerabilities, or credential abuse. Credential Access covers techniques designed to steal account information or elevate privileges, enabling adversaries to move laterally and maintain persistence. Execution captures the methods used to run malicious code on systems, which often serve as the bridge between initial compromise and subsequent impact.

The clustering of these three tactics demonstrates a clear adversary focus on entering networks, establishing control, and acquiring the access necessary to support follow-on actions. The continued prominence of Initial Access reinforces that defending against the initial foothold remains a top priority for organizations, as successful entry consistently enables downstream activity that drives the most severe incidents.

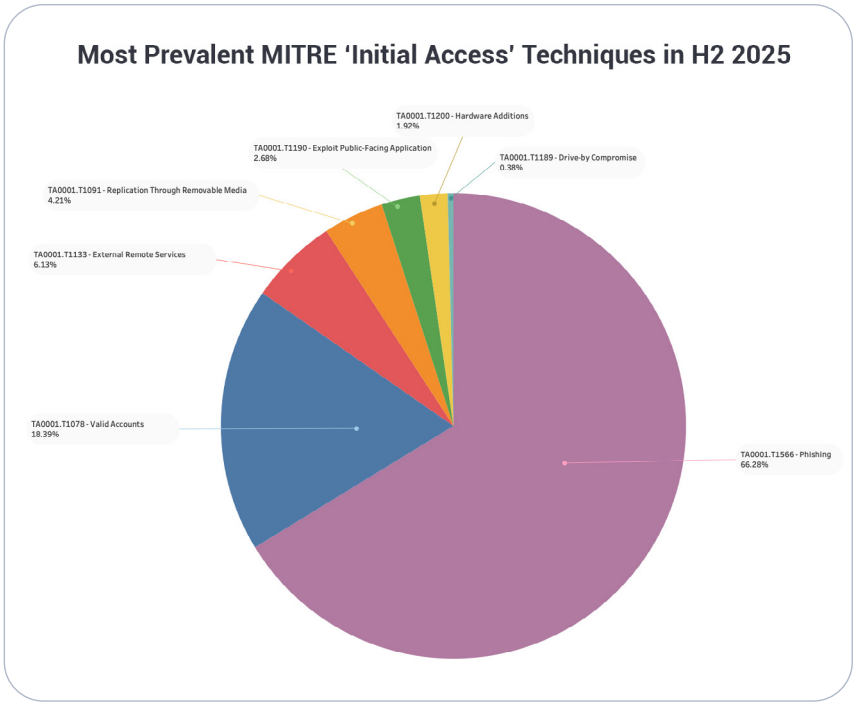


MITRE Techniques

Techniques under Initial Access (TA0001)

Techniques under Initial Access provide insight into how adversaries are achieving entry and which vectors are currently prioritized, offering organizations actionable context for targeting defensive measures.

Within Initial Access, Phishing (TA0001.T1566) was the number one observed technique during H2 2025, accounting for 66.28% of all initial access–related high and critical alerts. Valid Accounts (TA0001.T1078) ranked second at 18.39%. External Remote Services (TA0001.T1133) ranked third at 6.13%. This marks a clear shift from H2 2024 through H1 2025, when Valid Accounts consistently dominated initial access activity. Year over year, phishing increased by approximately 26%, while valid account usage declined by roughly 34%. Aside from Hardware Additions (TA0001.T1200), all other initial access techniques increased year over year.



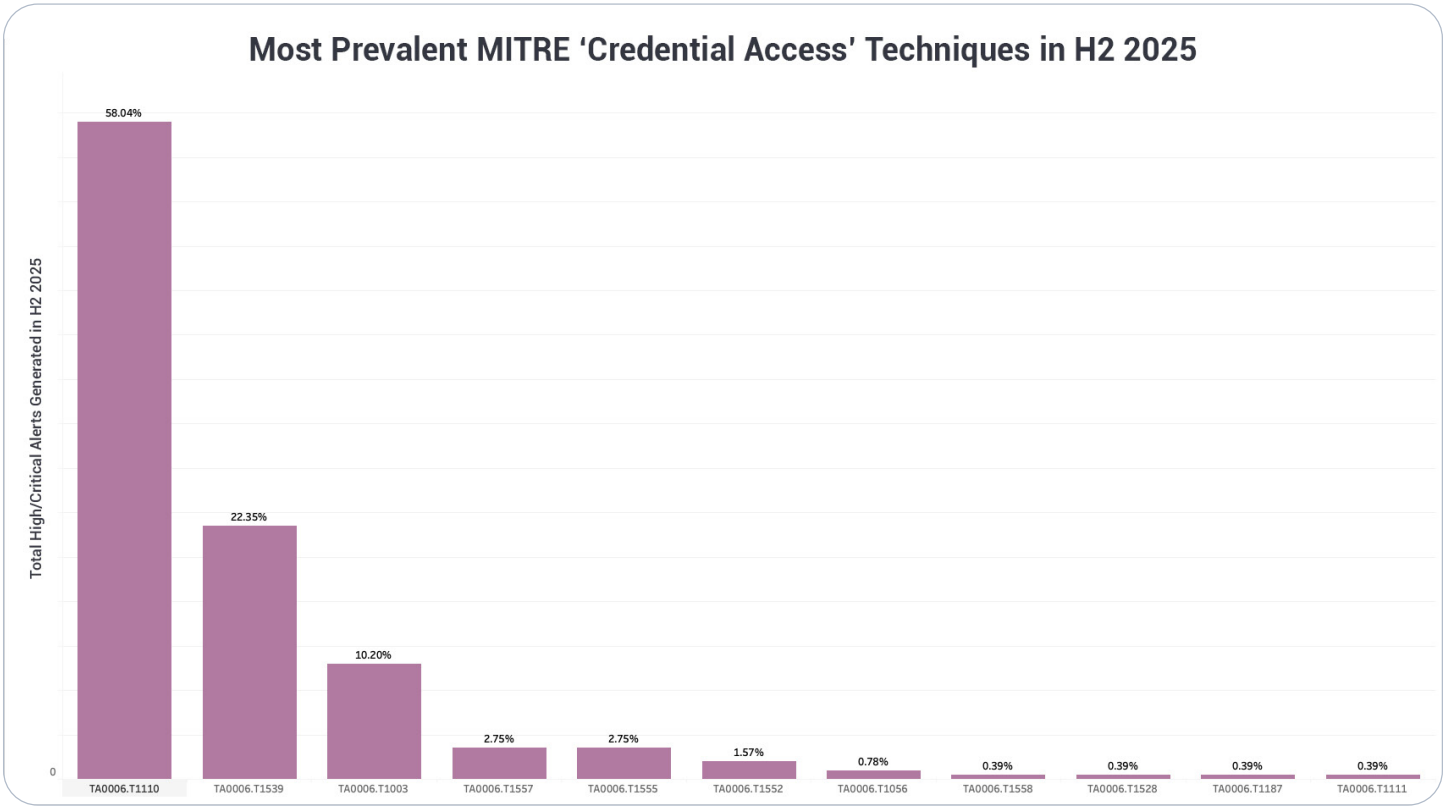
The shift toward phishing highlights a growing reliance on user interaction and trusted infrastructure to bypass technical controls, reinforcing the need for controls that address both human and system-level vulnerabilities. SOC observations help explain this shift. According to **Jared Bronnenberg**, Principal SOC Engineer, attackers are moving away from DGA-based and disposable domains toward compromised legitimate websites and trusted file-sharing services, allowing phishing infrastructure to inherit positive reputation and evade early blocking. **Bronnenberg** also noted the widespread use of "Cloudflare Turnstile tokens and VM-detection scripts" to evade automated analysis, where scanners are redirected to "benign content such as https://www.google.com/search?q=Google.com," while real users are served malicious payloads. Once active, these phishing frameworks often deploy "client-side JavaScript to harvest cookies and session tokens," enabling follow-on credential access without direct password capture. **Bronnenberg** further observed increasing automation in infrastructure compromise and rotation, with AI-driven customization of phishing lures assessed as an imminent next step.

External Remote Services (TA0001.T1133) at #3, while significantly less prevalent than phishing or valid account abuse, this technique reflects a continued adversary interest in leveraging legitimate remote access methods, including VPN, SSH, and commercial remote administration tools such as AnyDesk and ScreenConnect, to establish entry. CRU observed increased use of these methods, often deployed after initial credential compromise or social engineering. In the context of MITRE, External Remote Services highlights how adversaries can blend into normal administrative activity by abusing tools and protocols that are commonly allowed within enterprise environments. Although its overall volume remains lower, the presence of this technique underscores the importance of monitoring remote access activity for anomalous usage, particularly when access occurs outside standard operational workflows or without prior authorization.

Techniques under Credential Access (TA0006)

Credential Access (TA0006) ranked as the second most frequently observed tactic during H2 2025, reflecting its central role across multiple stages of the attack lifecycle. While often associated with post-compromise activity, several credential access techniques are routinely used before initial access to enable entry into target environments. This dual use underscores why identity remains a primary attack surface and why credential abuse consistently features in high and critical incidents.

Critical Start's CIRT Manager, **Chad Graham**, reinforces this observation, stating that "Identity remains the most fertile attack surface." In line with this, across escalations from SOC to CIRT, the most frequent incidents involved unauthorized access linked to credential abuse, including MFA gaps, password reuse, and token theft indicators. **Graham** notes that organizations enforcing multi-factor authentication, maintaining consistent identity governance, and eliminating common one-click compromise paths such as exposed RDP, legacy firewall rules, and orphaned accounts experience significantly lower incident severity and shorter response timelines.



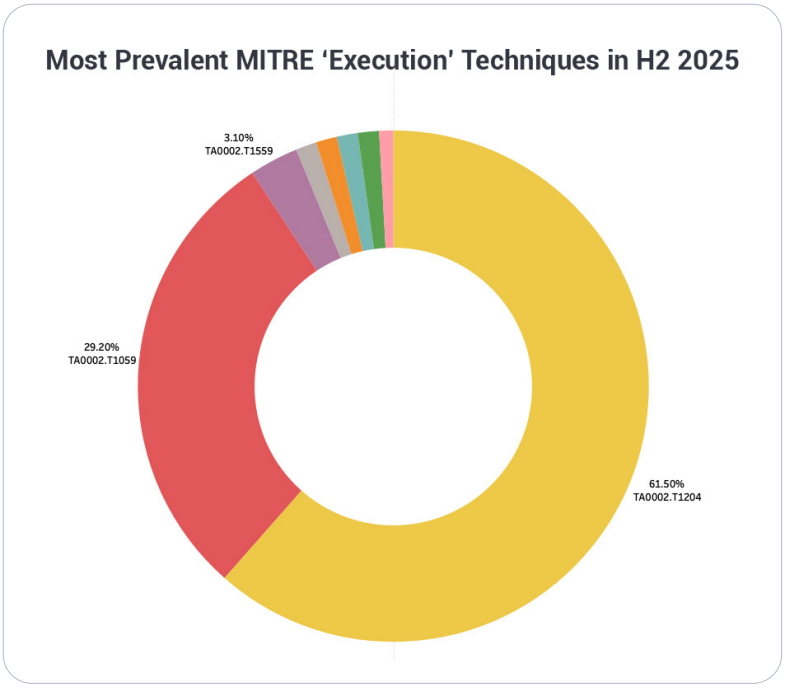
Within Credential Access, the most frequently observed techniques during H2 2025 were Brute Force (TA0006.T1110) at 58.04%, Steal Web Session Cookies (TA0006.T1539) at 22.35%, and OS Credential Dumping (TA0006.T1003) at 10.20%. Brute Force often enables initial access through external authentication interfaces, while session cookie theft allows adversaries to bypass traditional login controls and assume authenticated user sessions. OS Credential Dumping typically reflects deeper host-level compromise, supporting lateral movement and privilege escalation after access has been established.

Taken together, these techniques illustrate how adversaries target credentials throughout the attack lifecycle, from enabling initial entry to sustaining and expanding access. The prominence of Credential Access reinforces the need for identity-focused defenses. Organizations should prioritize consistent MFA enforcement, strong identity governance, and the removal of exposed or unnecessary access paths such as publicly accessible remote services and dormant accounts. Monitoring for anomalous authentication behavior and session misuse remains critical to disrupting credential abuse at every stage of an intrusion.

Techniques under Execution (TA0002)

Execution (TA0002) ranked as the third most frequently observed tactic during H2 2025, reflecting its role in enabling adversaries to activate payloads and advance activity after gaining access. Execution techniques are commonly observed immediately following initial access and later in the intrusion lifecycle. Increasingly, execution is also used as the mechanism through which initial access itself is achieved. In all cases, these techniques allow attackers to run malicious code, scripts, or binaries within a target environment.

During H2 2025, the most frequently observed Execution technique was User Execution (TA0002.T1204), accounting for 61.50% of execution-related high and critical alerts. This highlights continued adversary reliance on user interaction to initiate malicious activity, commonly through phishing content, deceptive links, or socially engineered prompts that cause users to launch files or run commands.



CRU's trend analysis aligns with patterns observed in day-to-day SOC investigations. According to **Jared Bronnenberg**, attackers are increasingly shifting away from attacker-initiated execution paths such as direct malware execution or exploitation of vulnerable applications and services, and toward user-assisted execution. SOC investigations have observed ClickFix and fake CAPTCHA campaigns where users are guided through steps that result in execution of malicious one-liner commands, frequently using PowerShell. These campaigns are heavily social engineering–assisted and effectively merge Initial Access and Execution, as the execution activity occurs outside the traditional perimeter and directly enables internal access. This blurs the boundary between tactics, with execution functioning as the access mechanism rather than a post-compromise action. Critical Start's recent Security Advisory [CS-SA-26-0101] Strategic Phishing Campaigns Leverage CAPTCHA and Email Routing Misconfiguration details the exploit of CAPTCHA pages, as part of ClickFix. We see users being prompted to perform tasks not limited to copying and pasting commands from dialog boxes, etc.

Further, according to **Jared Bronnenberg**, SOC investigations have also identified malicious browser extensions, including fake generative AI tools, that appear legitimate but execute injected code within the browser to harvest tokens, cookies, and other sensitive data. These techniques further demonstrate how execution can be achieved without exploiting a vulnerability or delivering a traditional malware payload.

Command and Scripting Interpreter (TA0002.T1059) was the second most observed execution technique at 29.20%, reflecting continued abuse of native scripting environments to run commands, automate attacker activity, and blend malicious behavior with legitimate administrative operations. Event Triggered Execution (TA0002.T1559) accounted for 3.10% of execution-related alerts, indicating more selective use of execution paths that rely on system events or application behavior to trigger malicious code.

Overall, the distribution of execution techniques reflects a clear adversary preference for user-assisted execution over attacker-initiated malware execution or vulnerability-based exploitation. This shift reduces attacker dependency on exploit development and increases reliance on social engineering to bypass technical controls. It also illustrates that execution is no longer just a post-compromise activity but can serve as an initial access vector. Defenders should prioritize restricting untrusted execution, improving visibility into script and browser-based execution, and detecting execution patterns that indicate socially engineered entry into the environment.

Critical Start's CRU analysis of H2 2025 adversary activity using the MITRE ATT&CK framework shows that attackers are focusing on a small set of high-impact tactics. The primary tactics observed are Initial Access, Credential Access, and Execution. Initial Access remains critical because it determines whether an attacker can establish a foothold, with techniques increasingly shaped by user interaction and reliance on externally accessible services and infrastructure. Execution has evolved beyond a purely post-compromise function and is now frequently used as an entry mechanism itself, allowing attackers to trigger code execution through socially engineered actions that occur before traditional access controls are engaged. Credential Access then enables attackers to sustain operations by expanding access, escalating privileges, and maintaining persistence.

Viewed together, these tactics reflect an attacker preference for approaches that minimize technical complexity while maximizing control over the environment. Rather than relying on exploit development or bespoke malware, adversaries are structuring intrusions around human-driven execution paths and identity-based access that are difficult to prevent once initiated. The implication for defenders is clear: effective detection and prevention must extend beyond blocking access attempts to include visibility into execution behavior and credential usage across the environment. Organizations that understand and monitor how these tactics reinforce one another are better positioned to interrupt intrusions early and limit overall impact.

Organizational Close-Ups

SOC Closeup

The Cyber Response Unit (**CRU**) is spotlighting a multi-stage malware attack from July, which was successfully detected and mitigated by the SOC. This case provides key insights into evolving threat actor tactics, techniques, and procedures (TTPs), including sophisticated phishing, Living off the Land execution, and DLL side-loading. The collaboration between CRU and SOC highlights the value of coordinated detection and response, which is particularly pertinent for an MDR provider, demonstrating how timely intelligence, endpoint monitoring, and rapid containment work together to prevent compromise and protect client environments.

SOC Highlight: Sophisticated "Copyright Infringement" Malware Campaign

Alert ID: 123456789

Detection Source: Microsoft Defender for Endpoint

Month/Year: July 2025

Industry: Manufacturing

Overview

The Security Operations Center (SOC) identified a sophisticated malware campaign leveraging a "Copyright Infringement" lure. The campaign demonstrated advanced techniques, including Living off the Land (LotL) execution and abuse of legitimate, code-signed applications to side-load malicious DLLs. The malware ultimately deployed a Python-based information stealer, triggered when the user opened a file presumed to be a standard PDF document. The attacker employed phishing as the initial delivery vector, relying on user interaction with a seemingly benign attachment. This method allowed the campaign to bypass conventional antivirus sandboxes.

Initial Detection

An alert from Microsoft Defender for Endpoint flagged anomalous activity involving:

- pythonw.exe executing via a Registry Run Key
- svchost.exe executing from an unusual directory

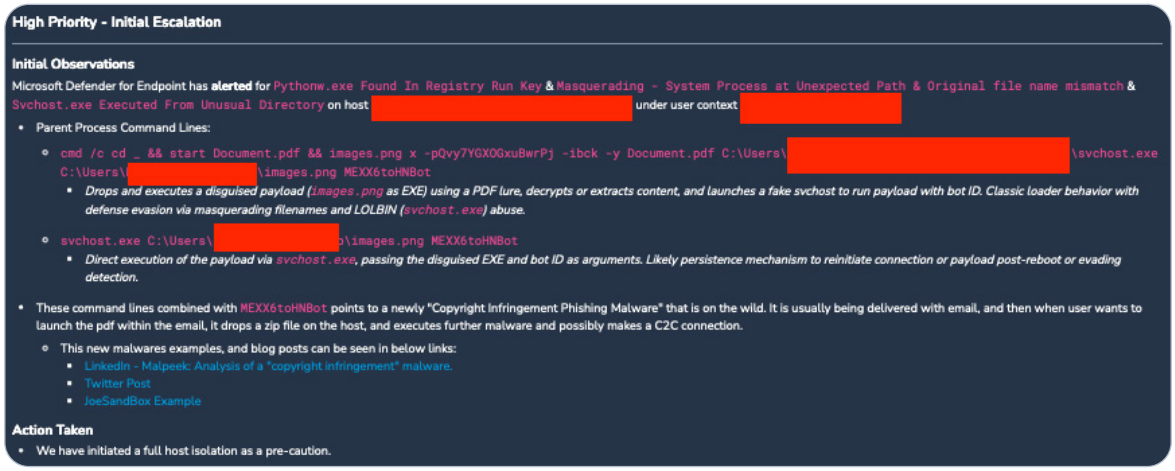
The SOC's immediate objectives were to determine whether this represented a false positive or a targeted intrusion, contain the affected host, and identify the entry vector to prevent potential data exfiltration.

Investigation Phases

The SOC conducted a rapid, three-phase investigation:

1 Endpoint Forensics & De-obfuscation

- Analyzed parent process command lines and identified a highly suspicious execution chain.
- The attacker launched a file named Document.pdf, which was a legitimate PDF reader, with an argument pointing to images.png. Further analysis of the argument containing the string MEXX6toHNBot revealed it was not an image file but an obfuscated malicious payload.
- Observed classic loader behavior, including filename masquerading and LOLBIN abuse (svchost.exe) to evade endpoint defenses.



High Priority - Initial Escalation

Initial Observations

Microsoft Defender for Endpoint has **alerted** for `Pythonw.exe Found In Registry Run Key` & `Masquerading - System Process at Unexpected Path & Original file name mismatch` & `Svchost.exe Executed From Unusual Directory` on host [redacted] under user context [redacted]

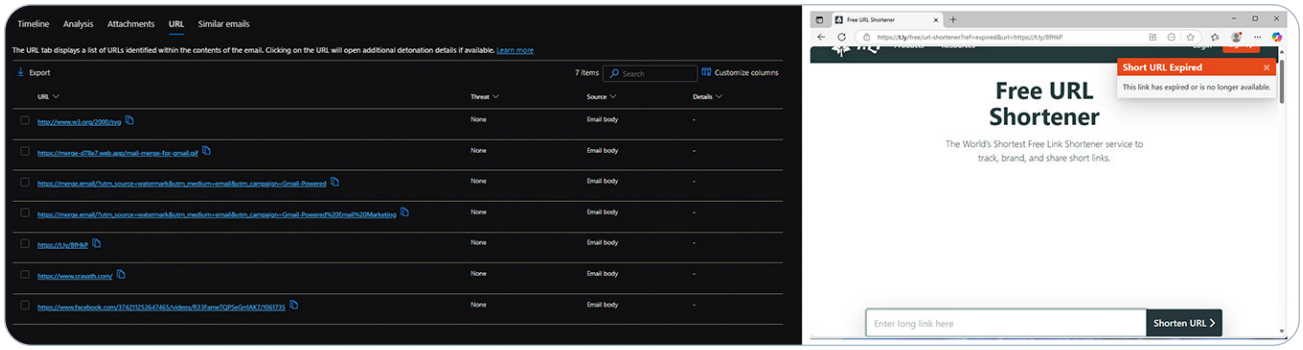
- Parent Process Command Lines:
  - `cmd /c cd _ && start Document.pdf && images.png x -pQvy7YGXOGxuBwrPj -ibck -y Document.pdf C:\Users\[redacted]\svchost.exe C:\Users\[redacted]\images.png MEXX6toHNBot`
    - *Drops and executes a disguised payload (`images.png` as EXE) using a PDF lure, decrypts or extracts content, and launches a fake svchost to run payload with bot ID. Classic loader behavior with defense evasion via masquerading filenames and LOLBIN (`svchost.exe`) abuse.*
  - `svchost.exe C:\Users\[redacted]p\images.png MEXX6toHNBot`
    - *Direct execution of the payload via `svchost.exe`, passing the disguised EXE and bot ID as arguments. Likely persistence mechanism to reinitiate connection or payload post-reboot or evading detection.*
- These command lines combined with `MEXX6toHNBot` points to a newly "Copyright Infringement Phishing Malware" that is on the wild. It is usually being delivered with email, and then when user wants to launch the pdf within the email, it drops a zip file on the host, and executes further malware and possibly makes a C2C connection.
  - This new malwares examples, and blog posts can be seen in below links:
    - LinkedIn - Malpeek: Analysis of a "copyright infringement" malware.
    - Twitter Post
    - JoeSandBox Example

Action Taken

- We have initiated a full host isolation as a pre-caution.

2 OSINT & Threat Correlation

- Leveraged the unique string MEXX6toHNBot to cross-reference recent open-source threat intelligence, including security blog posts, Joe's Sandbox reports, and researchers on X.
- Identified a specific threat report linking the string to an info-stealer campaign using "Copyright Infringement" lures.
- Confirmed the campaign methodology and associated Indicators of Compromise (**IOCs**) aligned with observed behavior on the endpoint.



3 Root Cause & Origin Analysis

- Conducted email log queries filtering for subjects containing "Copyright."
- Identified the entry email: "Final Legal Notice Prior to Litigation – International Copyright Violation".
- The email included a URL shortener that had expired, indicating likely evasion tactics.
- Analysis revealed discrepancies between the sender display name and the sender email address (generic Gmail account), confirming it as the primary initial attack vector.

Containment & Mitigation

Host isolation was implemented within 10 minutes of alert detection.

Full attack chain documentation was submitted in an initial escalation report approximately 20 minutes post-detection.

Audit logs confirmed no lateral movement or data exfiltration occurred.

The campaign was effectively neutralized before persistence could escalate, and the client verified no damage or data loss.

This incident highlights a highly evasive threat actor utilizing LotL techniques, DLL side-loading, and phishing with convincing social engineering lures. Rapid detection, endpoint analysis, and proactive containment prevented compromise of sensitive data, demonstrating the effectiveness of coordinated SOC operations.

CIRT Closeup

Operational Bottlenecks and How Customers Can Improve Cyber Incident Response

Chad Graham, Cyber Incident Response Team (CIRT) Manager, shares valuable insights from his experience managing cyber incidents. His team's H2 work identified several operational gaps that delayed or complicated containment. These issues were not related to tool failures but rather to gaps in processes, such as incomplete asset visibility, unclear escalation protocols, and unpreparedness for rapid response. Addressing these gaps can help organizations improve their preparedness, reduce delays, and achieve better outcomes when engaging CIRT.

Limited Environment Visibility

A common delay during early scoping came from incomplete asset coverage, including partial EDR deployment, unknown hosts, or insufficient logging outside the security stack. In multiple engagements, CIRT had to first establish a basic inventory and logging baseline before containment could begin. To avoid such delays, organizations must ensure complete endpoint coverage, regularly validate agent health, centralize firewall and VPN logs, and either retire or bring legacy assets under management.

Unclear Escalation Paths Between SOC and CIRT

Several customers were uncertain about when to escalate incidents beyond the SOC, which led to slow handoffs. This often arose from internal ambiguity about what CIRT provides compared to MDR triage. To resolve this, organizations should clearly document escalation criteria in Incident Response plans and ensure that all internal teams, including SOC, IT, network, and executives, understand when CIRT assumes the lead role.

Missing Prerequisites for Rapid Containment

CIRT frequently encountered situations where multi-factor authentication (MFA) was not enforced on critical accounts, or key system logs were unavailable or difficult to access. In regulated environments, such as those governed by the Criminal Justice Information Services (CJIS), some customers had not pre-established the necessary legal or compliance pathways, which delayed engagement. Organizations should enforce MFA universally, regularly validate log retention and access, and pre-establish legal frameworks, such as counsel-directed Statements of Work or clearance requirements, before an incident occurs.

Decision-Maker Availability During High-Severity Events

Even when technical steps were clear, containment efforts were delayed when key stakeholders were unavailable to approve urgent actions, such as system isolation, password resets, or configuration changes. Appointing an internal incident commander with the authority to approve urgent actions and ensuring alignment with the recommended communication cadence based on severity can reduce delays and improve the response during these critical moments.

Trending Cybersecurity Concerns

The current threat landscape reflects a continued shift away from single-vector exploitation toward techniques that scale through trust, automation, and human behavior. Adversaries are increasingly targeting the systems, workflows, and decision points that organizations rely on to operate efficiently, including developer ecosystems, AI-enabled platforms, and routine user interactions. These trends emphasize stealth, abuse of legitimacy, and indirect access paths that challenge traditional perimeter and signature-based defenses. The following concerns highlight how attackers are adapting their tradecraft to exploit foundational technologies and behaviors, and why defenders must evolve detection, validation, and user-focused controls to keep pace.

1

Software Supply Chain & Developer Ecosystem Compromise

Adversaries are increasingly abusing trusted development tooling and update channels, including malicious VS Code and Open VSX extensions, npm and PyPI packages, trojanized installers, and compromised vendor update servers, to gain initial access at scale. These techniques allow attackers to inherit developer trust, bypass perimeter defenses, and propagate through automated build and update workflows.

2

AI/LLM Attack Surface Expansion & AI-Enabled Malware

Threat actors are actively targeting AI and LLM integrations and using AI to accelerate malware development, expanding the attack surface beyond traditional infrastructure. This convergence lowers barriers to entry, increases attacker speed and adaptability, and introduces new risks tied to semantic manipulation, model abuse, and AI-assisted offensive capabilities.

3

ClickFix-style Malware Execution by User

ClickFix techniques have evolved into a reliable initial-access method that exploits user trust and routine workflows to trigger manual execution of malicious commands. By shifting execution responsibility to the user, attackers bypass many technical controls and rely on social engineering rather than software exploitation.

1 Software Supply Chain and Developer Ecosystem Compromise

In 2025–2026, adversaries have increasingly weaponized trust and automation within the software supply chain and developer tooling ecosystems, turning build systems, IDE marketplaces, package registries, and update channels into high-impact initial-access vectors. Rather than relying on overt brute-force or phishing campaigns, attackers are exploiting the mechanisms developers and organizations depend on to build, distribute, and update software.

One stark example is the eScan antivirus supply chain compromise, where attackers gained unauthorized access to a regional update server and distributed a malicious update through the vendor's official channel. The trojanized update executed a multi-stage payload that disrupted legitimate update flows, modified system configurations, and established persistence with remote command-and-control capabilities before defenders had visibility. This highlights a key takeaway: when trusted update infrastructure is compromised, endpoint defenses that rely on vendor trust are effectively bypassed. Detection must focus on behavioral analysis and anomaly monitoring rather than signature verification alone.

Open-source package registries remain high-yield targets. In the npm ecosystem, malicious packages such as bitcoin-main-lib, bitcoin-lib-js, and bip40 were uploaded under names mimicking legitimate libraries. These packages leveraged automated installation hooks to deliver NodeCordRAT, which stole browser credentials, API tokens, and crypto wallet data, using Discord for command and control. From a defender's perspective, this underscores a systemic weakness: automated dependency resolution and unverified install scripts amplify risk downstream. Teams should adopt pre-install validation, lockfile auditing, and runtime dependency monitoring to catch malicious behavior before execution.

The Open VSX and VS Code extension ecosystem further illustrates this threat. In a recent campaign, attackers compromised an established publisher's credentials to push malicious updates to four widely used extensions. The payload, linked to the GlassWorm loader, remained dormant until the extensions reached a certain number of downloads, then executed selectively on profiled hosts to exfiltrate developer credentials and crypto wallets. By exploiting legitimate publisher identities and download histories, attackers bypassed superficial trust signals. The defender takeaway is clear: reputation alone is fragile. Continuous verification of code integrity, build provenance tracking, and monitoring for unexpected publisher behavior are essential to detect stealthy attacks.

Collectively, these incidents reveal a broader trend: attackers are shifting from targeting individual systems to compromising the trusted infrastructure serving millions of developers. Once a build pipeline, update server, or package registry is compromised, attackers inherit the implicit trust of downstream users. Since these platforms are deeply embedded in development workflows with automatic install and update behaviors, the scale and stealth of impact can be enormous.

Defenders must adopt a strategic approach:

Prioritize supply chain hygiene

Enforce strict access controls on CI/CD systems and repository credentials, rotate and protect tokens, and use short-lived, least-privilege credentials for publishing pipelines.

Adopt runtime behavior monitoring

Deploy EDR and workload telemetry capable of detecting unusual network connections, persistence mechanisms, or process injection patterns.

Enhance verification and provenance

Implement deterministic builds, reproducible artifacts, signed packages, and tools that validate dependency trees against known good baselines.

Educate and empower developers

Integrate security training into the development lifecycle, emphasizing typosquatting detection, install script review, and vetting of third-party tools and extensions.

In an era where build systems and developer ecosystems are frontline attack surfaces, defenders who augment trust with verification, visibility, and risk-aware automation will be best positioned to mitigate both immediate and downstream impacts of supply chain compromise.

- *https://securelist.com/escan-supply-chain-attack/118688*
- *https://cybersecuritynews.com/hackers-weaponized-open-vsx-extension/*
- *https://securityboulevard.com/2026/01/malicious-npm-packages-deliver-nodecordrat/*
- *https://cybersecuritynews.com/attackers-hijacking-official-github-desktop-repository/*

2 AI/LLM Attack Surface Expansion & AI-Enabled Malware

In H2 2025, adversaries significantly expanded the attack surface by operationalizing artificial intelligence and large language models (LLMs) across offensive campaigns. AI continues to play a central role in social engineering and phishing operations. As **Brian Roye**, Senior Security Consultant at Critical Start, observed, "the threat landscape has been defined by a shift toward the weaponization of generative AI. Notably, AI-enhanced phishing and deepfake social engineering have eliminated traditional 'red flags,' allowing attackers to hijack legitimate email threads and bypass standard filters."

Beyond these initial use cases, AI's role in offensive operations has evolved well beyond generic, template-based lures. Attackers now leverage generative AI to hijack legitimate email threads, generate highly contextualized and adaptive messaging, and eliminate traditional indicators of fraud. In parallel, threat actors are increasingly targeting AI systems themselves. They are actively probing enterprise LLM endpoints at scale, exploiting semantic and logic-level vulnerabilities in AI workflows, and leveraging AI systems to generate, modify, and adapt malware. Reconnaissance campaigns against enterprise LLM implementations illustrate the scale and intent of this activity.

Researchers observed more than 91,000 attack sessions targeting misconfigured or exposed LLM APIs across major model families, including OpenAI, Google, Anthropic, and others. These scans are not random noise. They deliberately probe for vulnerabilities like SSRF and misconfigurations that could expose sensitive AI APIs or lead to unauthorized access. Understanding this early phase matters because attackers are mapping these surfaces to identify the weakest entry points before launching more sophisticated follow-on attacks.

Beyond surface mapping, practical abuses of AI assistants have emerged. In one example, researchers crafted malicious calendar event invites that embed natural language payloads which Google's Gemini AI unwittingly executes when users query their schedule. The AI processed these innocuous-looking prompts, exposing private calendar details to attackers without any direct user interaction. This form of semantic prompt injection demonstrates that the threat surface for AI systems includes language and context itself, not just code or protocols. Traditional pattern-based defenses become ineffective against such attacks because the payloads are linguistically benign yet semantically harmful when interpreted by the model.

The evolution of AI-assisted malware represents a more structural transformation of the threat landscape. A notable case is VoidLink, an advanced cloud-native Linux malware framework that researchers found was largely developed using generative AI. Check Point Research's analysis indicates that an individual operator used AI to accelerate design, planning, and coding tasks, enabling the malware to grow into a modular, feature-rich framework in under a week. While VoidLink itself has not been widely deployed in the wild yet, its sophistication signals a turning point: AI can now materially amplify the speed and complexity of malware development. This undermines traditional assumptions about attacker resourcing and timeline constraints, meaning defenders must assume high-quality threats could originate from much smaller teams.

These trends show that AI and LLM integration is not merely a theoretical risk but a present and practical attack surface.

Organizations must adjust their security strategies accordingly:

Redesign threat modeling for AI systems

Consider language and semantic context as potential vectors, not just code, ports, or API endpoints.

Strengthen defenses around AI artifacts

Track model behavior for anomalies, enforce output sanitization, and apply contextual validation for actions triggered via AI workflows.

Monitor and harden LLM integrations

Audit configurations, restrict exposed model endpoints, and monitor for unusual LLM API usage that could signal reconnaissance or abuse.

Prepare for AI-assisted malware

Traditional static signatures are insufficient against malware that evolves its code, obfuscates dynamically, or is generated with AI support. Runtime monitoring, behavioral analytics, and threat hunting are essential.

In this era of AI-expanded attack surfaces and emerging AI-enabled malware, defenders must blend classic security rigor with new practices that account for the interplay of language, automation, and model behavior. Staying ahead requires visibility into how AI is used internally and externally, and a willingness to treat AI components not as black boxes but as critical parts of the trusted computing base that demand deliberate protection. AI-expanded attack surfaces and emerging AI-enabled malware, defenders must blend classic security rigor with new practices that account for the interplay of language, automation, and model behavior. Staying ahead requires visibility into how AI is used internally and externally, and a willingness to treat AI components not as black boxes but as critical parts of the trusted computing base that demand deliberate protection.

- *https://securityboulevard.com/2026/01/exploiting-google-gemini-to-abuse-calendar-invites-illustrates-ai-threats/*
- *https://www.greynoise.io/blog/threat-actors-actively-targeting-llms*
- *https://securityboulevard.com/2026/01/voidlink-represents-the-future-of-ai-developed-malware-check-point/*
- *https://www.bleepingcomputer.com/news/security/viral-moltbot-ai-assistant-raises-concerns-over-data-security/*
- *https://www.darktrace.com/blog/thread-hijacking-how-attackers-exploit-trusted-conversations-to-infiltrate-networks*

3 ClickFix-style Malware Execution by User

The ClickFix family of attacks has evolved from simple execution triggers into a potent social engineering vector that threat actors now leverage as an initial-access mechanism by convincing users to manually infect their own systems. Originally observed as "human verification" lures where victims were asked to execute commands in their browser or terminal, ClickFix has matured into visually convincing decoy pages, corrupted extensions, and cleverly disguised payloads that exploit trust and urgency.

At its core, a ClickFix attack manipulates user behavior. Victims are redirected to a fake "fix" page — often through phishing, SEO poisoning, or malvertising — that simulates a legitimate error message or system prompt and then instructs users to run a command on their machines. The command, typically placed in the clipboard via JavaScript, initiates a multi-stage infection that can download and execute malware like infostealers or remote access trojans. Because the execution origin is the user's own action, many defenses that rely on blocking unsolicited binaries or exploit traffic are bypassed.

Recent ClickFix campaigns have become more convincing and harder to detect. One prevalent variant now presents a full-screen fake Windows Update interface that mirrors the real update process, complete with familiar progress bars and messaging. Users are told to open the Windows Run dialog and paste a command, which triggers a pipeline involving built-in Windows tools (mshta.exe, PowerShell) to pull down obfuscated code. Advanced variants even hide payloads using steganography inside PNG images, reconstructing shellcode from pixel data in memory — techniques that evade traditional file-scanning defenses.

Attackers have also adapted ClickFix to browser extension abuse. A malicious Chrome extension masquerading as a legitimate ad blocker was used in a campaign dubbed "CrashFix" where the extension intentionally crashes the browser and then displays a fake remediation prompt. Following the prompt, users are again tricked into executing malicious commands that ultimately install a previously undocumented remote access trojan, ModeloRAT. The attacker chain relies on user frustration and trust in familiar extension functionality, illustrating how ClickFix can be weaponized through platform abuse, not just deceptive pages.

ClickFix-style tactics are not limited to Windows. On macOS, the MacSync infostealer leverages similar social engineering to persuade victims to paste Terminal commands into their shell to complete a supposed installation or fix. Once executed, these commands circumvent native defenses like Gatekeeper and install data-stealing malware, illustrating that ClickFix adapts across operating systems and environments.

Phishing remains a primary distribution method. Campaigns targeting hotel staff have used booking-related lures and fake CAPTCHAs to lead victims to ClickFix pages where PureRAT or similar malware is deployed, showing how social trappings like urgency and legitimacy are exploited to lower a user's guard.

The evolution of ClickFix highlights a key shift in adversary strategy: social engineering is now an active exploitation surface for initial access, not just a prelude to follow-on actions. Security teams must recognize that ClickFix leverages human trust and interface mimicry rather than software vulnerabilities alone.

Defenders should focus on:

User education and behavior change

Emphasize never running or pasting commands from unverified sites or prompts, no matter how convincing.

Detection of anomalous sequences

Monitor for unusual process chains like Run dialog executions triggered from browsers or abnormal invocation of native utilities.

Browser extension controls

Enforce strict policies on extension installations, vetting, and runtime behavior monitoring.

Visibility into social engineering paths

Integrate telemetry from email gateways, web filters, and endpoint detection points to map and block the initial lure vectors.

Implement software inventory tracking

Maintain an up-to-date inventory of all software used in the environment, ideally with internal owners or points of contact. This enables quick reference when breach notifications are issued, ensuring that impacted systems can be easily identified and addressed.

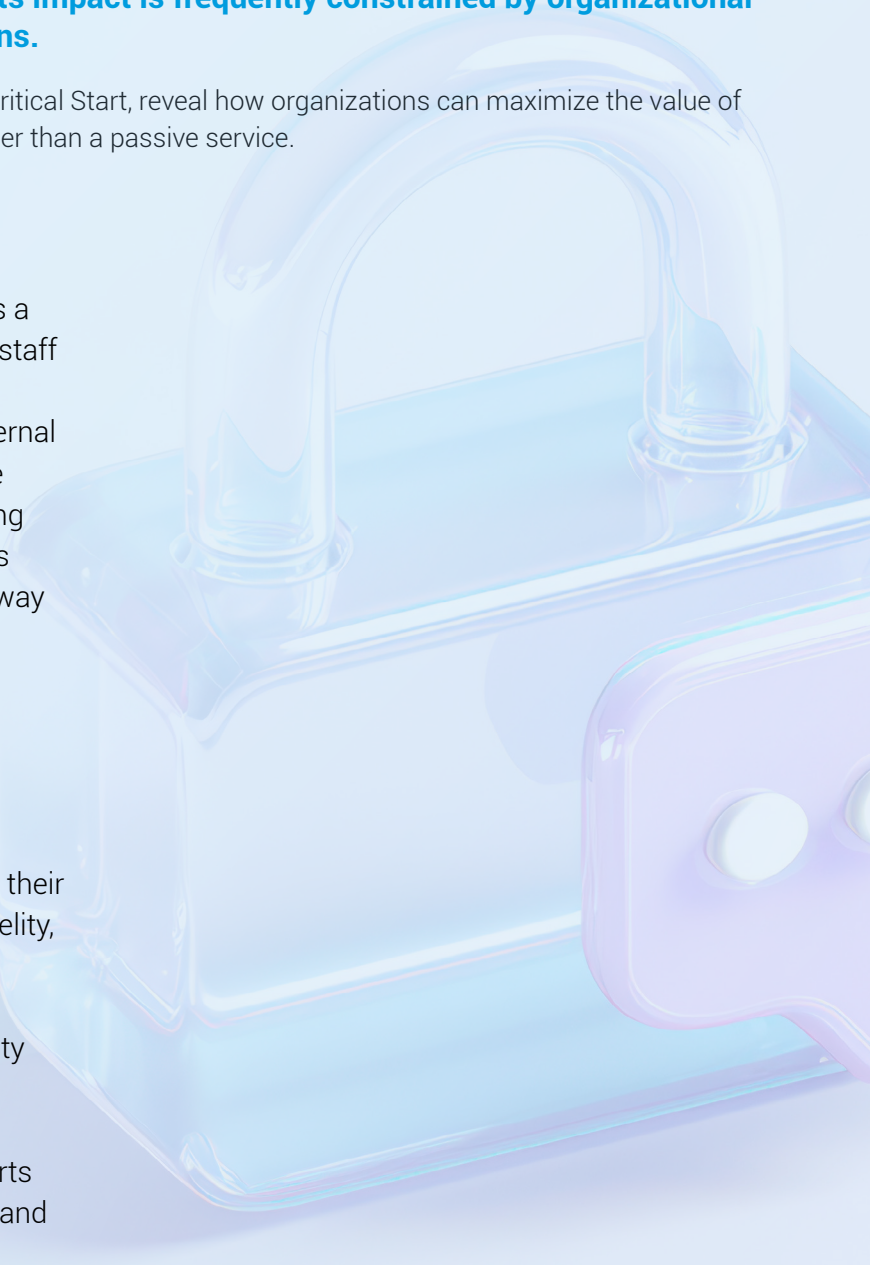
ClickFix-style attacks succeed because they exploit trust and familiarity with system UI and workflows. Reducing the effectiveness of this vector requires strengthening both technical controls and user awareness to interrupt the chain before a user executes malicious actions.

- *https://thehackernews.com/2026/01/fake-booking-emails-redirect-hotel.html*
- *https://cybersecuritynews.com/crashfix-hackers-using-malicious-extensions/*
- *https://cybersecuritynews.com/macsync-macos-infostealer-leverage-clickfix-style-attack/*
- *https://www.malwarebytes.com/blog/news/2025/11/new-clickfix-wave-infects-users-with-hidden-malware-in-images-and-fake-windows-updates*
- *https://www.bleepingcomputer.com/news/security/fake-ad-blocker-extension-crashes-the-browser-for-clickfix-attacks/*

Organizational Mitigation Strategies

This report details a myriad of threats shaping the cybersecurity landscape. Often, the effectiveness of mitigation strategies is determined less by the technologies deployed and more by how organizations operationalize them. Managed Detection and Response (MDR) is a foundational component of modern security programs, yet its impact is frequently constrained by organizational misconceptions rather than technical limitations.

Insights from **Brian Roye**, Senior Security Consultant at Critical Start, reveal how organizations can maximize the value of MDR when it is treated as an operational partnership rather than a passive service.



> Many organizations mistakenly view MDR as a "set it and forget it" replacement for internal staff or as a simple software upgrade. In practice, MDR is most effective when it augments internal teams, with clearly defined ownership, active engagement, and shared context. Establishing this alignment early reduces response delays and ensures the service functions as a two-way relationship, where organizational feedback directly improves detection accuracy and long-term resilience. Similarly, moving away from the assumption that all MDR providers are interchangeable or that higher alert volume equates to stronger security enables organizations to select partners aligned with their specific risk tolerance. Emphasizing high-fidelity, investigated signals over raw alert volume reduces fatigue and builds the trust required for teams to act decisively during true security incidents. Addressing these misconceptions early transforms MDR from a transactional service into a strategic capability that supports faster containment, clearer communication, and improved security outcomes."
>
> **– Brian Roye**
>
> Senior Security Consultant, Critical Start

The following section outlines specific mitigation strategies mapped to the threats identified throughout this report.

Surge in Identity-Based Intrusions

To mitigate identity-based intrusions, organizations should implement multi-layered authentication controls. First, enforce the use of robust Multi-Factor Authentication (MFA) across all systems, prioritizing critical services and applications. Implement adaptive authentication, where the system evaluates login behaviors and adjusts security requirements dynamically based on risk factors such as time of access, IP address, and geolocation. Next, deploy anomaly detection systems to monitor for suspicious login patterns, such as repeated failed login attempts and login bursts from unexpected regions. Ensure all accounts, especially those with administrative privileges, have unique, complex passwords and are regularly reviewed for unnecessary access permissions. Finally, use a combination of behavioral analytics and machine learning to detect abnormal account usage, session token theft, and bypass attempts in real-time. Regular penetration testing should also be conducted to identify weaknesses in MFA implementations and credential management practices.

Escalation of User-Assisted Execution (ClickFix-Style Activity)

A critical response to the rise in user-assisted execution attacks is comprehensive user training and awareness. Create simulated phishing and social engineering attack scenarios to teach users how to recognize and report suspicious requests, particularly those involving system repairs or unsolicited software updates. In parallel, organizations should implement endpoint detection and response (EDR) tools that monitor for and block potentially dangerous PowerShell or Command Prompt commands. These tools should flag any script execution that deviates from known legitimate usage patterns. Tighten permissions so that users cannot execute unauthorized or high-risk scripts without administrative approval, and set up application whitelisting to ensure only pre-approved applications run. Additionally, an anti-phishing filter that scans for known malicious websites, coupled with URL reputation checks, should be employed to minimize the risk of browser-based lures.

Living-off-the-Land (LoTL) Abuse of Legitimate Administrative Tools

To mitigate the risks of LoTL attacks, organizations must monitor and restrict the use of administrative tools like PsExec, WMIC, and RDP. Enforce strict controls on who has access to these utilities and implement least-privilege access policies to minimize the ability for lateral movement. Network segmentation is critical—by isolating critical systems and limiting internal communication to only necessary personnel and tools, attackers are more likely to be caught if they attempt to escalate their privileges or spread laterally. Implementing endpoint monitoring for suspicious administrative tool usage is also essential, with alerts triggered by unusual activities or access patterns. Additionally, using Application Control or whitelisting tools to block unauthorized Remote Monitoring and Management (RMM) tools like AnyDesk and TeamViewer will help prevent attackers from using these low-noise utilities to establish persistence and evade detection.

Industry-Specific Targeting Shifts

As industries such as manufacturing and healthcare face increased targeting, organizations in these sectors need to adopt industry-specific threat intelligence feeds to stay ahead of emerging threats. Develop and regularly update incident response plans tailored to the specific threats facing your industry, ensuring they cover not only technical countermeasures but also business continuity and legal/regulatory obligations. For example, healthcare providers should focus on securing patient data through end-to-end encryption and ensuring that their medical devices are not vulnerable to remote exploitation. Manufacturing firms should strengthen their supply chain security by implementing software integrity checks and regularly auditing third-party vendors. Beyond technical measures, creating strong partnerships with government and industry organizations for threat intelligence sharing will provide early warnings of evolving attack patterns, helping mitigate risks before they escalate.

Increased Operational Tempo and Shift in Attack Timing

To counter the increasing operational tempo and more predictable attack timings, organizations should continuously monitor network traffic and logs for abnormal activity during peak times, especially around the 1500-1800 UTC window. This includes using Security Information and Event Management (SIEM) tools to correlate logs from multiple sources and identify threats in real time. Consider implementing a Security Operations Center (SOC) team with a rotating shift structure to ensure coverage during high-risk windows. Additionally, increase the frequency of vulnerability scanning and patch management activities leading up to high-traffic periods. Review incident response workflows to ensure swift escalation and remediation, enabling faster containment of threats during these critical hours. Additionally, integrate machine learning capabilities into intrusion detection systems to detect and respond to attacks that fall outside of typical patterns or times.

"Customers play an active role in maximizing the effectiveness of their MDR partnership. Maintaining accurate and up-to-date asset inventories ensures the SOC has complete visibility into the environment it is tasked with protecting, including new users and devices as they are added.

Establishing clear escalation contacts and defining response availability is equally critical. Knowing who to engage, how to reach them, and when they are available, particularly during after-hours incidents, directly impacts how quickly threats can be contained."

-Jared Bronnenberg
Principal SOC Engineer

Ransomware Ecosystem Evolution

To address the evolution of the ransomware ecosystem, particularly with the rise of groups like Qilin and Incransom, organizations must prioritize the hardening of their networks against credential theft and exploitation. Enforce strong password hygiene and implement strict access controls, ensuring that only necessary personnel have access to sensitive data and critical systems. Network segmentation, along with the deployment of advanced endpoint protection tools, will help contain any successful ransomware deployment and prevent lateral movement. Consider implementing robust backup strategies that include frequent, offline backups and test recovery procedures to ensure systems can be quickly restored in the event of a ransomware attack. Additionally, invest in threat intelligence services that track the activity of known ransomware groups, providing early warnings and actionable intelligence to prevent attacks. For organizations with global reach, ensuring compliance with local data protection laws and practicing sound operational security is critical to reducing the risk of data extortion or theft.

Persistence of Legacy Attack Tools

To address the continued use of legacy attack tools like Mimikatz and PsExec, organizations need to prioritize patch management and endpoint hardening. Regularly update all systems to ensure vulnerabilities in legacy tools and unpatched software are closed. Disable or restrict the use of legacy tools where possible, and monitor for unauthorized usage of administrative utilities. Use network monitoring solutions to track unusual traffic patterns and detect common indicators of attack that may be linked to these older tools. To reduce the attack surface, implement a least-privilege access model and continuously audit user permissions, ensuring that users and administrators have access only to the tools and systems necessary for their roles. Also, ensure security teams stay informed about the latest tactics and techniques used in the abuse of legacy tools, enhancing threat detection strategies.

AI-Enabled and AI-Assisted Attacks

To combat AI-powered threats, organizations must adopt advanced AI-based defense mechanisms themselves. Implement machine learning models to analyze large volumes of traffic and behavior data, helping to detect anomalies indicative of AI-assisted phishing or malware delivery. Enhance traditional anti-phishing systems with natural language processing (NLP) capabilities that can detect personalized and AI-generated phishing emails, assessing tone, content, and patterns indicative of impersonation. Train security teams to recognize new AI-assisted tactics, ensuring that response protocols include handling AI-assisted social engineering attacks. Additionally, incorporate AI in vulnerability management, using automated tools to proactively scan and identify security gaps in systems that might be leveraged by attackers using AI-powered techniques. Lastly, monitor the use of AI in adversarial social engineering campaigns and deploy countermeasures, including voice verification and biometric authentication for high-risk transactions.

Expansion of Software Supply Chain and Developer Ecosystem Attacks

To mitigate risks from software supply chain and developer ecosystem attacks, organizations should implement rigorous code integrity checks and monitor third-party dependencies closely. Establish security controls within the Continuous Integration/Continuous Deployment (CI/CD) pipeline to ensure that only verified and signed code is deployed to production environments. Additionally, conduct regular security assessments and audits of the software libraries and packages used by development teams, ensuring that no compromised code is introduced into your infrastructure. Supply chain risk management should include vetting and continuously monitoring third-party vendors for vulnerabilities and potential exposure to attacks. Work with industry peers to share threat intelligence and develop standardized security practices for the development and deployment of secure software. This approach will reduce the likelihood of attackers exploiting weaknesses in the development lifecycle to infiltrate systems.

Geopolitical and Nation-State Pressure

In response to ongoing nation-state campaigns, particularly against critical infrastructure, organizations should implement strong perimeter defenses, including advanced firewalls, intrusion detection systems, and network traffic monitoring to detect and block malicious state-sponsored activity. In high-risk sectors such as healthcare and manufacturing, establish a dedicated team for monitoring geopolitical threats, using threat intelligence feeds to stay informed about nation-state tactics, techniques, and procedures (TTPs). Use advanced threat-hunting techniques to proactively detect suspicious activities that could be linked to geopolitical tensions. Regularly assess and update disaster recovery and business continuity plans, ensuring that operations can continue even in the event of significant disruption. Additionally, collaborate with government agencies and industry organizations to share threat intelligence and receive guidance on protecting against nation-state threats.

As we move through H1 2026, the threat landscape continues to evolve at a rapid pace, demanding constant vigilance and swift adaptation from organizations. Attackers are refining their methods, leveraging everything from AI-powered phishing to more complex supply chain intrusions. To stay ahead, organizations must consistently assess and update their security strategies to match these shifting tactics. Threat intelligence remains a cornerstone of effective defense, providing the insights needed to spot new threats and trends early. By implementing the specific mitigation strategies outlined, businesses can reduce their exposure to the most advanced cyber threats, including ransomware, credential-based attacks, and targeted exploits. Maintaining a proactive, intelligence-driven approach is essential for securing systems against the increasingly sophisticated tactics used by today's cyber adversaries.

For more information, visit us at:

https://www.criticalstart.com/contact/