CYBER THREAT INTELLIGENCE REPORT

FIRST HALF 2024

CRITICALSTART®

The CRITICAL**START**® Mission

At Critical Start, our mission is to prevent business disruptions by stopping breaches before they occur. We achieve this by providing the most effective and comprehensive cybersecurity services designed to minimize risk and enhance organizational security.

Critical Start is at the forefront of delivering advanced cybersecurity solutions that not only detect and respond to threats but also proactively reduce the risk of a breach. Critical Start Managed Detection and Response (**MDR**) serves as the foundational pillar of Managed Cyber Risk Reduction (**MCRR**). Unlike traditional security solutions that focus solely on threat detection and response, Critical Start's integrated approach provides the following to minimize business disruption and maximize operational efficiency:

- Security operations signal assurance provided by asset inventory & log source monitoring
- Support for all IT and OT threat types & log sources
- Human-driven, monitoring, investigation and response
- All threats regardless of priority are responded to within contractual SLAS
- Business impact contextualization powered by asset criticality

Rob Davis, Critical Start CEO states, "Managed Detection and Response (MDR) is a reactive solution that is akin to the fire department or a fire extinguisher that responds to threats when they occur. MDR aims to contain incidents promptly, preventing them from escalating into major breaches that could cause significant damage to an organization's operations and reputation. However, cybersecurity strategies cannot rely solely on reactive controls. In our experience, a main source of initial compromises is unmonitored infrastructure. By integrating comprehensive asset inventory and criticality into our MDR solutions along with identification of endpoint security gaps, we empower organizations with unparalleled visibility and control over their IT environments. This proactive approach is akin to installing sprinkler systems and conducting safety inspections in buildings to reduce fire risks."

By partnering with Critical Start, organizations can confidently navigate the complex cybersecurity landscape, achieving optimal risk reduction and operational efficiency. Our integrated approach, with its focus on asset inventory, criticality ratings, comprehensive support, expert-driven response, and timely threat management, provides unparalleled protection and risk reduction. With Critical Start, you can achieve the highest level of security maturity while minimizing business disruption and maximizing operational efficiency.

Introduction

The ever-evolving threat landscape presents cybersecurity defenders with a continuous stream of challenges, both familiar and novel. These challenges, manifested as security events or incidents, define the dynamic environment in which we operate and necessitate ongoing adaptation. New threat groups emerge, dissolve, or merge on a near-monthly basis. This constant flux, coupled with the increasing sophistication of attacks targeting specific industries, suggests a refinement of Advanced Persistent Threat (**APT**) techniques, complicating detection using AI, machine learning, and advanced social engineering in spear-phishing campaigns. Additionally, the sophistication of Malware-as-a-Service (**MaaS**) is on the rise introducing new and adaptive attack vectors, including advanced phishing schemes and polymorphic malware designed to evade detection continually.

This report presents a comprehensive analysis of open-source threat intelligence, combined with internal event aggregations from over 20 supported Endpoint Detection and Response (**EDR**) products. The CRITICAL**START**®, Cyber Research Unit (**CRU**) meticulously reviewed 3,438 high and critical alerts generated by these EDR solutions alongside 4,602 reports detailing ransomware and database leak activities across 24 industries in 126 countries.

The Critical Start H1 2024 Report leverages insights from our leadership and experts in our CRU, as well as valuable contributions from our Executive Leadership Team (**ELT**). We extend our sincere gratitude to the ELT for their critical role in shaping our understanding of the cyber threat landscape. Their strategic vision and expertise have significantly enriched our analysis. This comprehensive report caters to security leaders, managers, analysts, and enthusiasts seeking strategic, operational, and tactical intelligence to proactively enhance their organization's security posture. The combined insights from our CRU experts and ELT provide a robust foundation for organizations to build more resilient cybersecurity strategies.

Sincerely,
The Critical Start CRU

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 team. To safeguard the privacy of our vendors and clients, we have kept certain data and statistics anonymous. Additionally, this report features AI-generated artwork using Adobe Firefly with prompts from Critical Start's CRU.

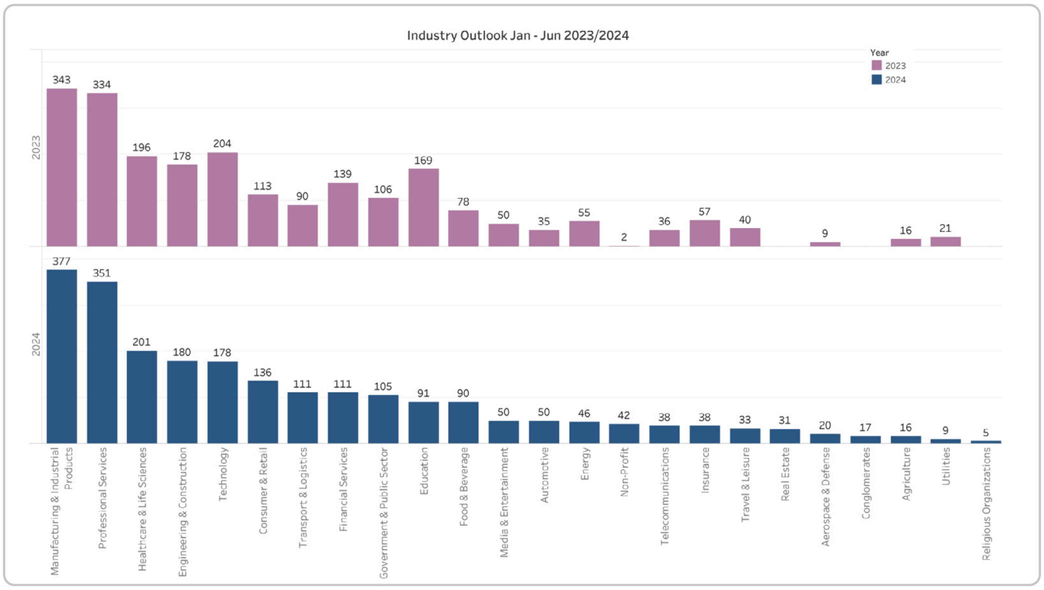
Industry Outlook

Industries are the engine of global economies, driving innovation, employment, and prosperity. However, this very engine is increasingly vulnerable to cyberattacks, jeopardizing not only economic well-being but also national security. These attacks disrupt production, supply chains, and livelihoods, leading to economic instability and job losses. They also target essential services, posing a significant risk to national defense capabilities. Critical Start's CTO, Randy Watkins, highlights the recent rise in cyberattacks reflects diverse attacker motives, making robust cybersecurity measures critical.

> **From a National Security perspective, the cyberattacks on industries such as Manufacturing and Industrial Products, Healthcare & Life Sciences, among others observed in H1 2024 reflects diverse attackers' motives. Attacks on our critical infrastructure not only undermine economic stability but also challenge the nation's defense capabilities. The collaboration between state-sponsored groups and criminal entities complicates attribution and underscores the need for robust cybersecurity measures.**
>
> **- Randy Watkins, CTO.**

The first half of 2024 saw a worrying trend in cyberattacks targeting specific industries. The CRU identified Manufacturing & Industrial Products, Professional Services, Engineering & Construction, Technology, and Healthcare & Life Sciences as the most impacted sectors. These attacks often utilize supply chain vulnerabilities, exploiting interconnected systems for unauthorized access.

This upcoming section delves deeper into the cybersecurity landscape of H1 2024. The CRU analyzed the most prevalent exploit tools, prominent malware families, and common attacker tactics used against these five industries. Additionally, we'll explore sector-specific vulnerabilities and showcase recent real-world attacks.



Industry Outlook (continued)

1. Manufacturing & Industrial Products

Critical Start's CRU reports that Manufacturing and Industrial Products remains the top targeted industry by cyber threat actors in H1 2024. This industry is leading with 377 confirmed reports of ransomware and database leak hits in the first half of the year.[1]

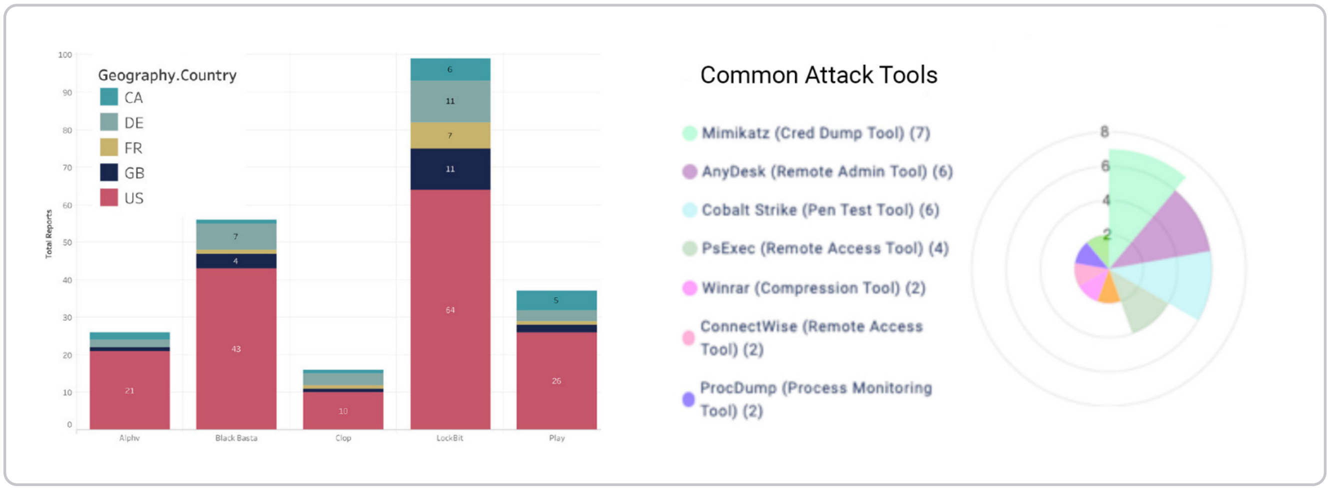
Attack Tools: Mimikatz (Cred. Dump), AnyDesk (Remote Admin), Cobalt Strike (Pen Test)

Prominent Malware: Cactus, Medusa, PlugX

Common TTPs (Initial Access): Spearphishing Attachments, Exploitation of Remote Services and Public-Facing Application

Top Vulnerabilities:

1. **CVE-2023-3519 (9.8):** Unauthenticated Remote Code Execution
2. **CVE-2021-44228 (10):** Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1)



Recent Attacks:

- **Crown Equipment Corporation, USA:** In June 2024, Crown Equipment Corporation, a leading global manufacturer of material handling equipment headquartered in New Bremen, Ohio, disclosed that it had been targeted by a cyberattack perpetrated by an international cybercriminal organization. The incident reportedly disrupted the company's manufacturing operations, necessitating a temporary suspension of production and impacting their publicly accessible website.
- **Targus International LLC, USA:** On April 8, 2024, B. Riley Financial, Inc. filed a disclosure with the United States Securities and Exchange Commission (**SEC**) announcing that Targus International LLC, a subsidiary specializing in mobile computing accessories, had been impacted by a cyberattack three days prior. The attack disrupted Targus's business operations, and initial investigations indicated unauthorized access to company file servers. The Red Ransomware group has claimed responsibility for the incident.

[1]Manufacturing & Industrial Products data includes entities involved in the transformation of raw material into finished products for commercial supplies.

Industry Outlook (continued)

2. Professional Services

The first half of 2024 witnessed a worrying surge in reported database leaks and ransomware attacks. Compared to 2023, these incidents jumped by 15%, with 351 cases reported in 2024 compared to 334 in the previous year. Legal services organizations, including courthouses, and supply chains have become prime targets due to the wealth of intellectual property and sensitive data they possess. This rise in cybercrime also coincides with an increase in Business Email Compromise (BEC) scams within this industry.[2]

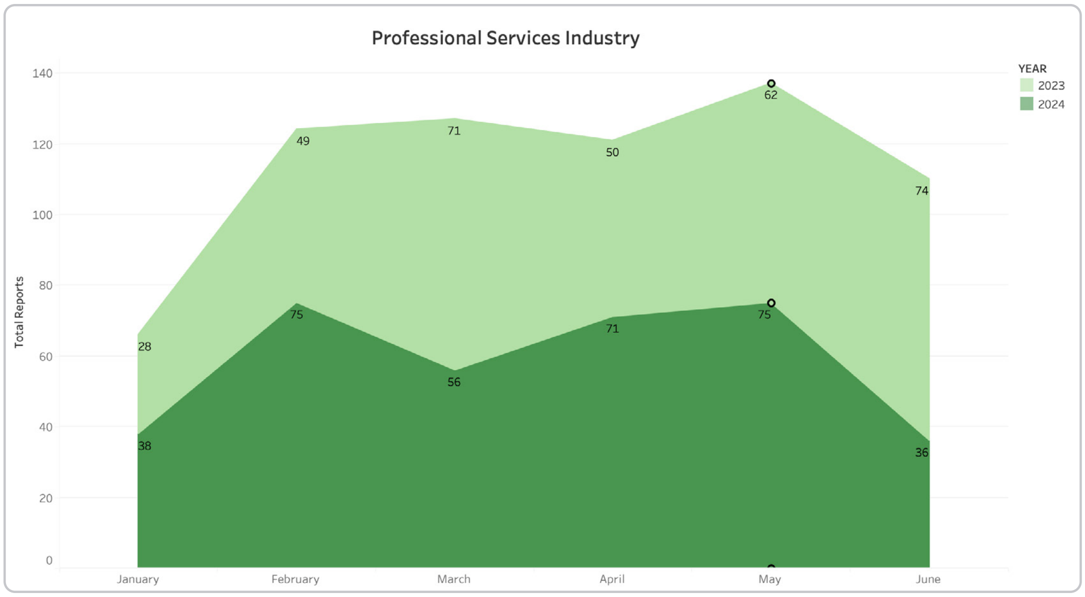
Attack Tools: PsExec (Remote Access), AnyDesk (Remote Admin), Atera agent (Remote Access)

Prominent Malware: BianLian, Mispadu, BlackSuit.

Common TTPs (Initial Access): Spearphishing Attachments, External Remote Services

Top Vulnerabilities:

1. **CVE-2021-40438 (9):** Apache HTTP Server-Side Request Forgery (**SSRF**)
2. **CVE-2023-4966 (7.5):** Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability



Recent Attacks:

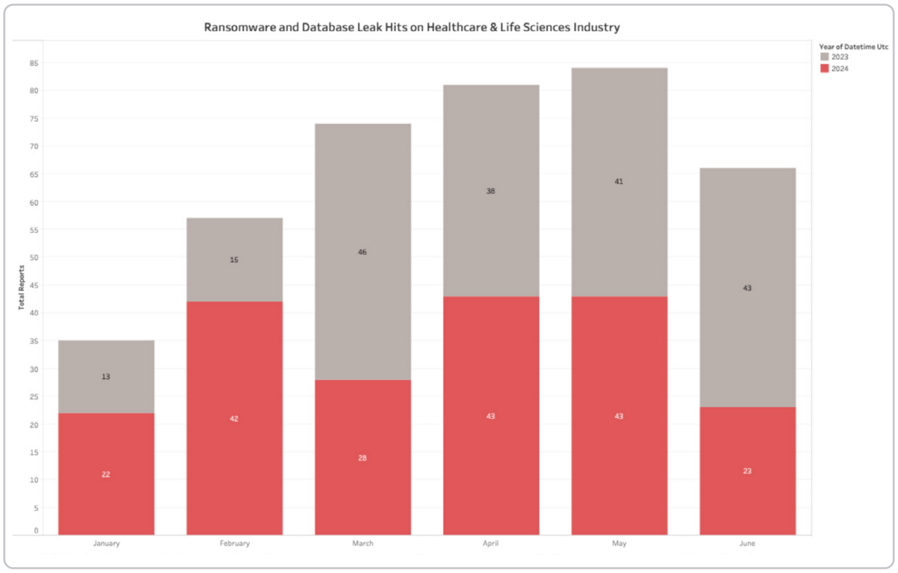
- **Keating Consulting Group, USA:** On January 11, 2024, Keating Consulting Group, a provider of accounting services, became the target of CEO fraud attack. A malicious actor initiated the attack by sending a phishing email to an external accountant employed by the firm. The email content deceived the recipient, leading them to disclose sensitive Accounts Receivable information, including email addresses, full names, and outstanding balances.
- **TRC Staffing Services Inc., USA:** TRC Staffing Services Inc. identified and addressed unauthorized access to its systems on March 25, 2024. The incident involved an external system intrusion, and potentially exposed sensitive information of 158,593 individuals, including names and Social Security Numbers. According to public reports, the attack is attributed to the BlackSuit cybercrime group.

[2] Professional Services data includes Consulting, Legal and Accounting Services, Advertising & Marketing, and 2Business Services.

Industry Outlook (continued)

3. Healthcare & Life Sciences

In the first half of 2024, CRU observed that the ransomware and database leak incidents targeting Healthcare & Life Sciences entities went up by 180% in February 2024 compared to the same period in 2023. This coincides with the attack on Change Healthcare and other healthcare providers. Notably, the months of February, April, and May had the most attacks, collectively accounting for 63.68% of all incidents in H1 2024. Geographically, the United States entities were impacted by 68.66% of incidents while the United Kingdom was the second most hit with 5.47%.[3]



Attack Tools: Mimikatz (Cred. Dump), PsExec (Remote Access), Cobalt Strike (Pen Test)

Prominent Malware: BlackCat/ALPHV, Black Basta, Medusa

Common TTPs (Initial Access): Supply Chain compromise, Valid Accounts

Top Vulnerabilities:

1. **CVE-2020-1472 (10):** Microsoft Netlogon Privilege Escalation Vulnerability
2. **CVE-2022-21587 (9.8):** Oracle E-Business Suite Unspecified Vulnerability

Additionally, the United States Department of Health and Human Services Office for Civil Rights (HHS OCR) identified a surge in healthcare data breaches, with ~367 incidents affecting 44 million individuals in the first half of 2024. Business associates were involved in nearly 16% of these breaches. 77% of these reported breaches were primarily attributed to hacking /IT incidents with network servers being the most impacted location of breached information (~65%), amongst email, laptop, paper/films, and others.

[3] *Healthcare & Life Sciences data includes healthcare providers, insurance plans, clearing houses, and research labs.*

Industry Outlook (continued)

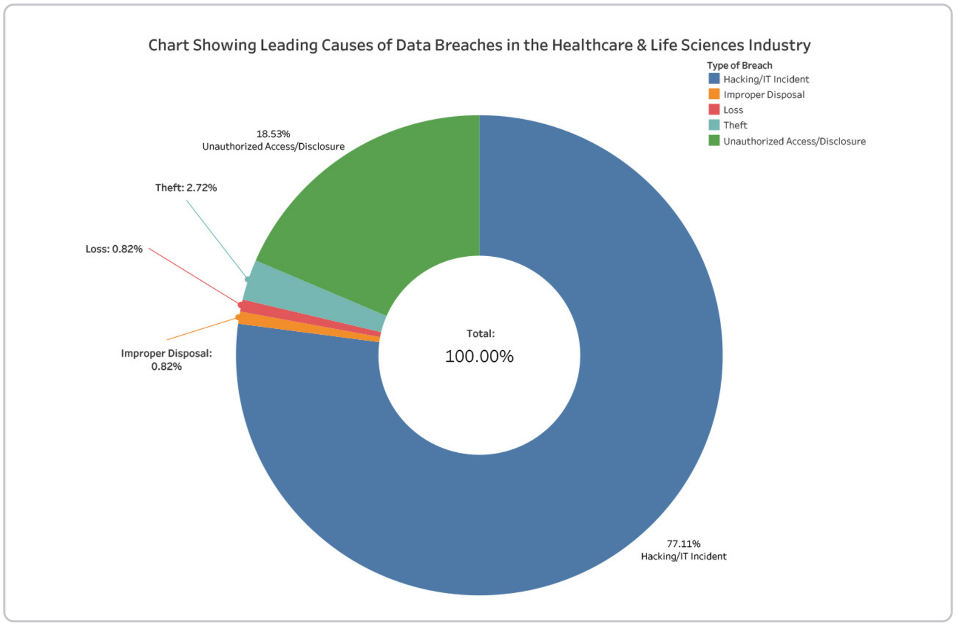


Chart Showing Leading Causes of Data Breaches in the Healthcare & Life Sciences Industry

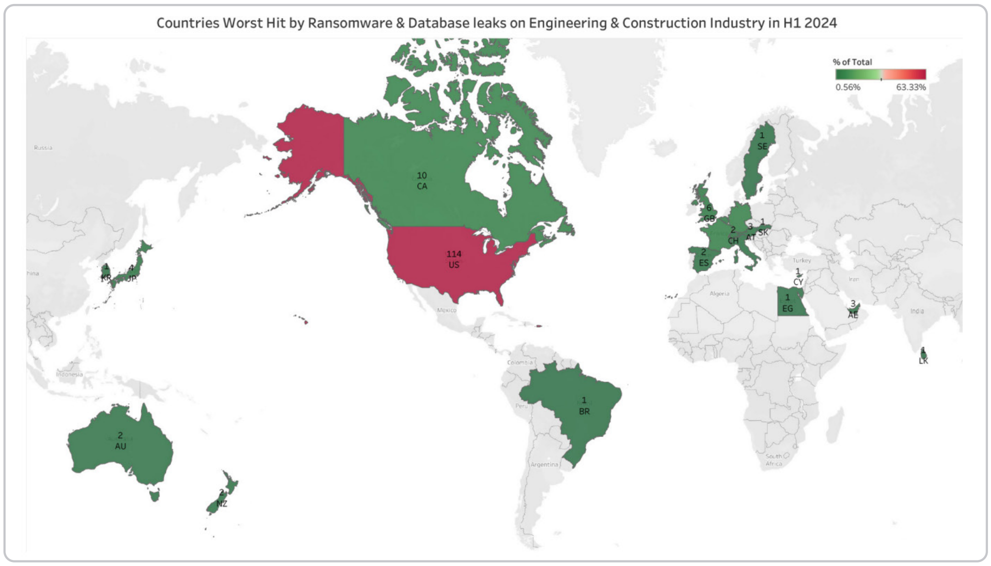
Recent Attacks:

- **Change Healthcare, USA:** A significant ransomware cyberattack targeted Change Healthcare, a subsidiary of UnitedHealth Group and a leading healthcare provider, on February 21, 2024. The ALPHV/BlackCat ransomware group is believed to be responsible for the attack, which resulted in the unauthorized disclosure of patient records despite reported ransom payments of approximately $22 million. This incident represents the most impactful ransomware attack on the Healthcare & Life Sciences sector in the first quarter of 2024. Beyond the financial costs associated with ransom payment, recovery efforts, and potential litigation, Change Healthcare endured weeks of system downtime, disrupting operations for pharmacies and causing a backlog of unpaid claims.
- **Ascension Hospitals, USA:** On May 8, 2024, Ascension, a leading Catholic healthcare system in the United States with 140 hospitals across 19 states, experienced a ransomware attack. The attack's initial access vector was traced back to a malicious file downloaded by an employee. The incident disrupted Ascension's supply chain and the organization advised all business associates to temporarily disconnect from their systems to mitigate further risk. The Black Basta ransomware group is believed to be responsible for this attack.
- **Los Angeles County Department of Public Health, USA:** The Los Angeles County Department of Public Health (**LACDPH**) disclosed a data breach impacting approximately 200,000 individuals. According to reports, the incident involved unauthorized access to protected health information (**PHI**) and financial records. The initial access vector stemmed from a phishing campaign conducted between February 19 and 20, 2024, where threat actors compromised the login credentials of 53 LACDPH employees. The impact of this phishing attack extended to other Los Angeles County Health agencies in subsequent months.

Industry Outlook (continued)

4. Engineering and Construction

The Engineering and Construction industry remained a consistent target for cyberattacks in the first half of both 2023 and 2024. [4]The United States bore the brunt of cyberattacks in the first half of 2024, experiencing a staggering 46.15% increase compared to 2023. Conversely, attacks on the United Kingdom plummeted by 64.71%, while Germany saw a 12% decrease. Belgium, however, witnessed a dramatic 400% surge (from 1 to 5 incidents). Even more concerning, four organizations within the United States were hit with repeat attacks, sometimes by different cybercriminals. The fastest turnaround time between attacks was a swift 24 hours.


Countries Worst Hit by Ransomware & Database leaks on Engineering & Construction Industry in H1 2024

Attack Tools: Mimikatz (Cred. Dump), ProcDump (Process Monitoring), Cobalt Strike (Pen Test)

Prominent Malware: Medusa, CatDDos, DarkGate, StrelaStealer

Common TTPs (Initial Access): Exploit Public-Facing Application, and Execution of PowerShell

Top Vulnerabilities:

1. **CVE-2020-1472 (10):** Microsoft Netlogon Privilege Escalation Vulnerability
2. **CVE-2023-4966 (7.5):** Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability

Recent Attacks:

- **Arup Group, UK:** Arup Group, a global engineering and construction consultancy headquartered in London, disclosed that it was targeted in a social engineering scam involving deepfakes. The incident resulted in unauthorized financial transfers totaling HK$200 million (approximately USD $25.6 million).
- **Skender Construction, USA:** A prominent United States medical office construction firm disclosed a cyberattack that compromised the personal information of 1,067 individuals. The exposed data reportedly included driver's licenses and other identifying documents. The company confirmed the incident had occurred on February 15, 2024.

[4]Engineering & Construction data includes Construction and Real Estate companies.

Industry Outlook (continued)

5. Technology

Critical Start data indicated a 12.75% decrease (from H1 2023) in database leaks and ransomware attacks targeting technology companies. While technology companies appear to be experiencing fewer attacks, cybercriminals are strategically targeting critical technologies that underpin major economic industries. For instance, reports show that auto dealerships experienced significant sales disruptions following the CDK Global cyberattack in June.[5]

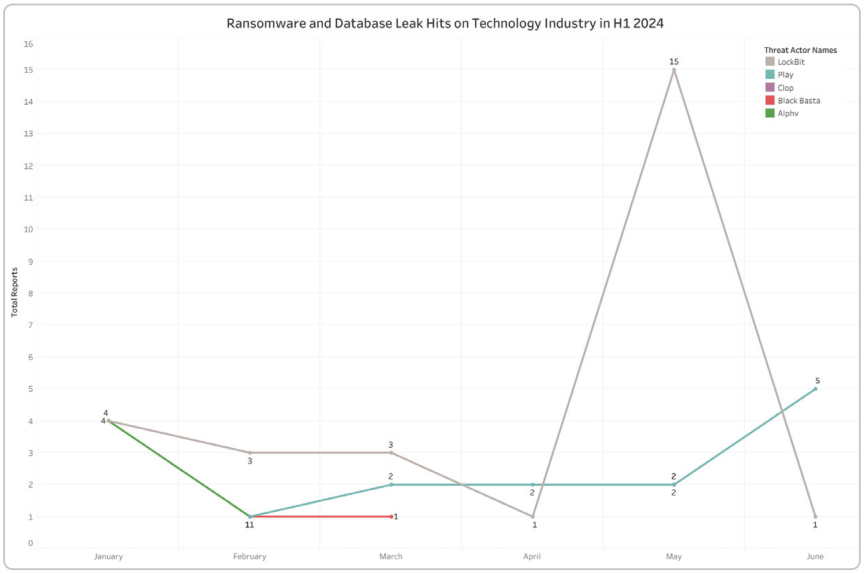
Attack Tools: Mimikatz (Cred. Dump), Sliver (C2 framework), Cobalt Strike (Pen Test)

Prominent Malware: XMRig, PlugX/Korplug, SparkRAT

Common TTPs (Initial Access): Valid Accounts, Supply Chain compromise

Top Vulnerabilities:

1. **CVE-2024-21887 (9.1):** Ivanti Connect Secure and Policy Secure Command Injection Vulnerability
2. **CVE-2023-42793 (9.8):** JetBrains TeamCity Authentication Bypass Vulnerability

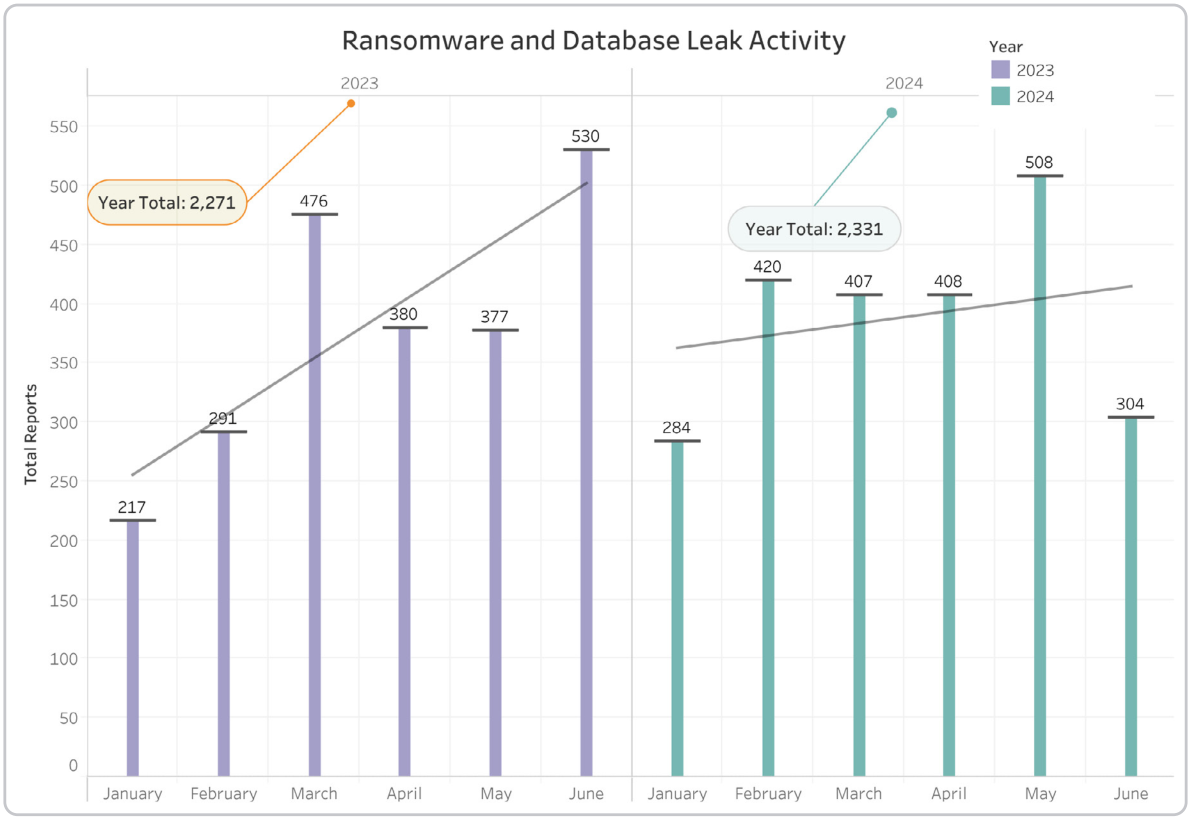


Recent Attacks:

- **CDK Global, USA:** On June 18 and 19, 2024, CDK Global, a cloud-based auto dealership software provider, experienced a ransomware attack that led to a nationwide shutdown of their systems, affecting approximately 15,000 retail locations. This incident caused significant disruptions in supply chain operations, as auto dealers depend on CDK Global's software for vehicle acquisition, financing, repairs, and maintenance tracking. Reports indicate that the BlackSuit ransomware gang is responsible for the attack. This underscores serious concerns about data breaches and the potential for cyber threat actors to exploit stolen data for social engineering attacks, thereby expanding their potential victim base.
- **Snowflake Inc., USA:** Cyber threat actors on May 31, 2024, infiltrated Snowflake's systems and gained access to multiple Snowflake customer databases using stolen valid credentials obtained from infostealers. Snowflake is an American cloud computing-based data-as-a-service company that offers cloud-based data storage and analytics services to its customers. Reports estimate that a minimum of 165 companies have been impacted with millions of individual records accessed by the cyber threat actor. Researchers have identified UNC5537 as the culprits and observed malicious activities on Snowflake customer instances linked to them.

[5] *Technology data includes telecommunications, Software & IT, and managed service providers.*

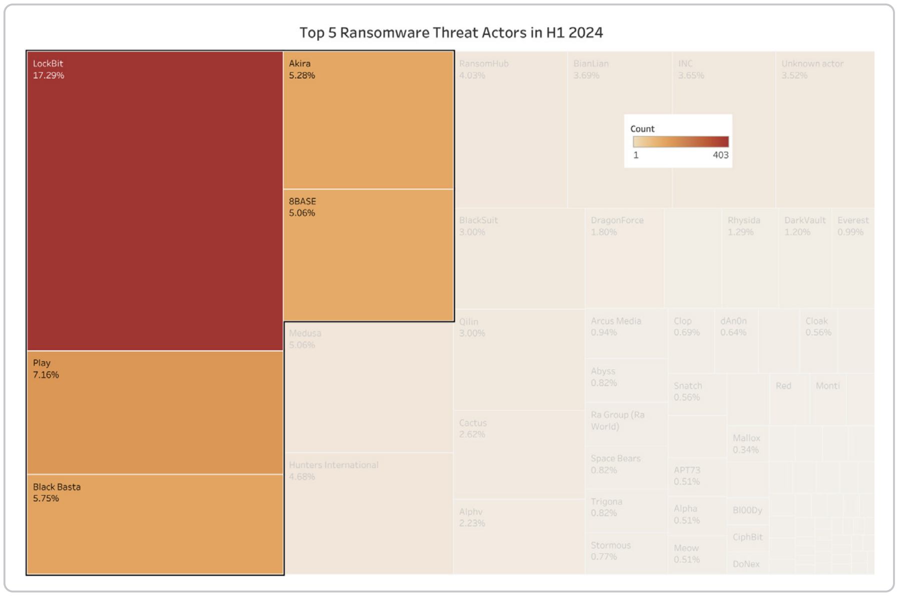
Industry Outlook (continued)



Ransomware and Database Leak Activity

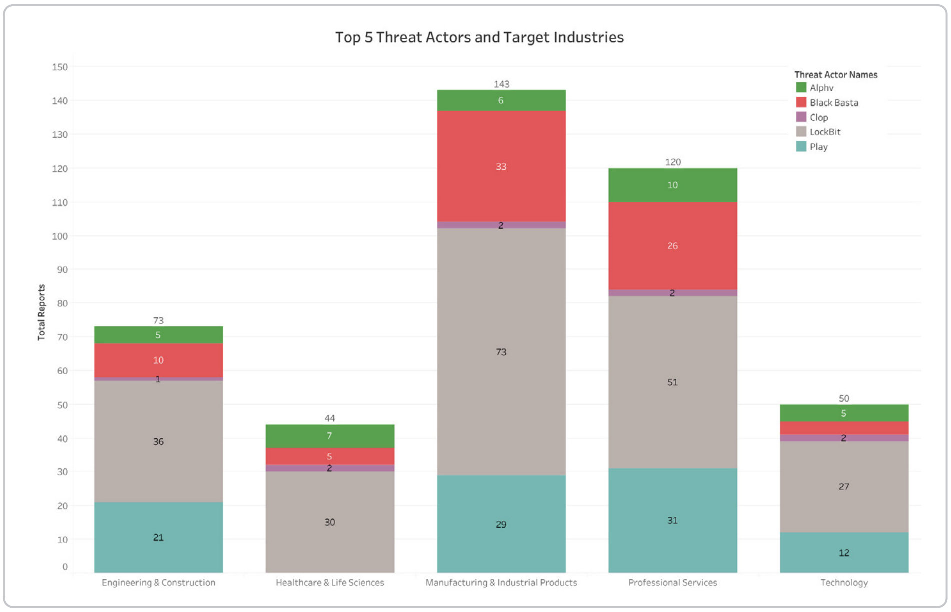
- In the first half of 2024, Critical Start observed 2,331 security incidents or a 2.64% increase in ransomware and database leak activities going from 2,271 in 2023.
- Ransomware and database leak incidents targeting Healthcare & Life Sciences entities went up by 180% in February 2024 compared to the same period in 2023.
- The construction industry experienced ransomware attacks exclusively, with no reported incidents of data breaches.
- Professional Services saw a 5.09% increase in database leaks and ransomware incidents compared to H1 2023.

Threat Actors & Malware Families



The first half of 2024 painted a concerning picture of the ransomware threat landscape. A relatively small group of actors, namely LockBit, Play, Black Basta, Akira, and 8BASE, were responsible for a staggering 40.54% of all reported ransomware incidents and database leak events, totaling a troubling 2,331 attacks within just six months. These threat actors primarily focused on five industries: Manufacturing & Industrial products, Professional Services, Engineering & Construction, Technology, and Healthcare & Life Sciences. This concentration of attacks by a handful of actors highlights their potential for significant disruption.[6]

The charts above and below highlight the Top 5 threat actors we discuss in this section.

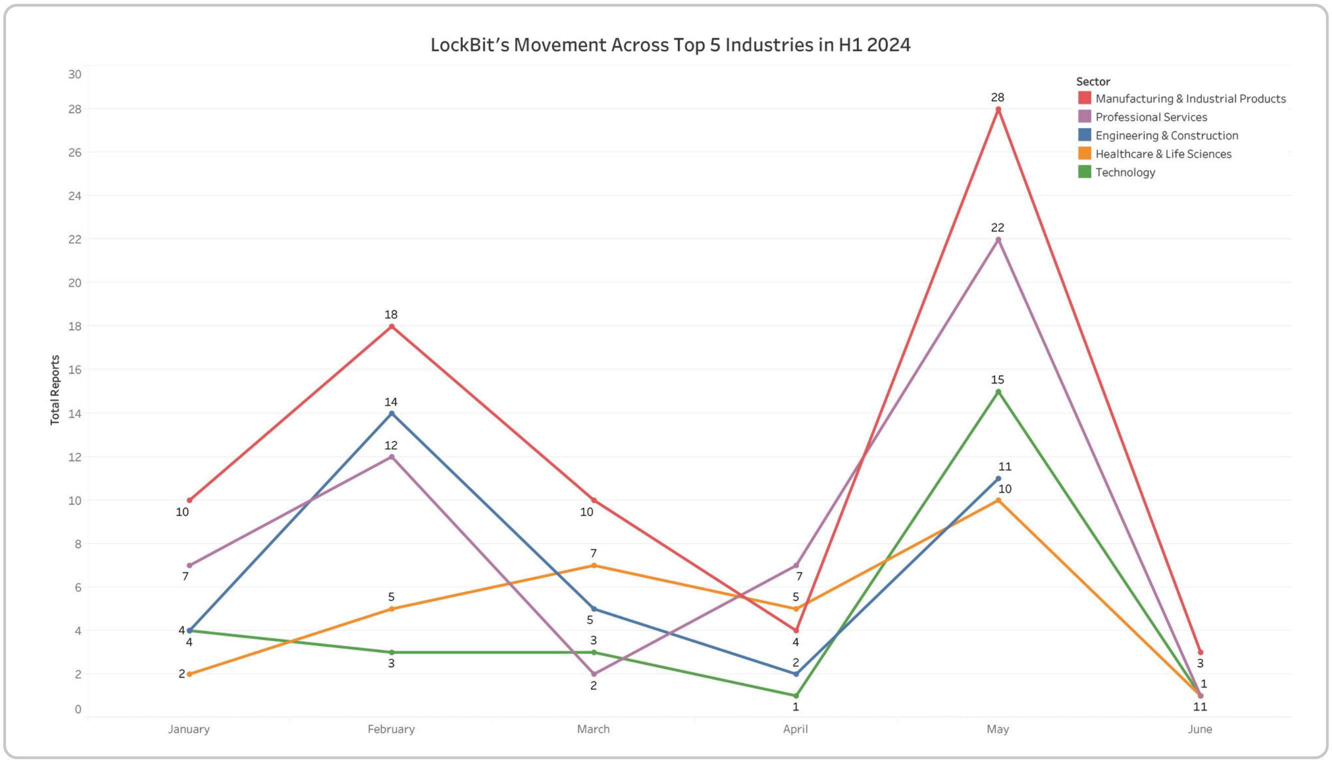


[6] https://www.halcyon.ai/raas-mq/q1-2024

Threat Actors & Malware Families (continued)

1. LockBit

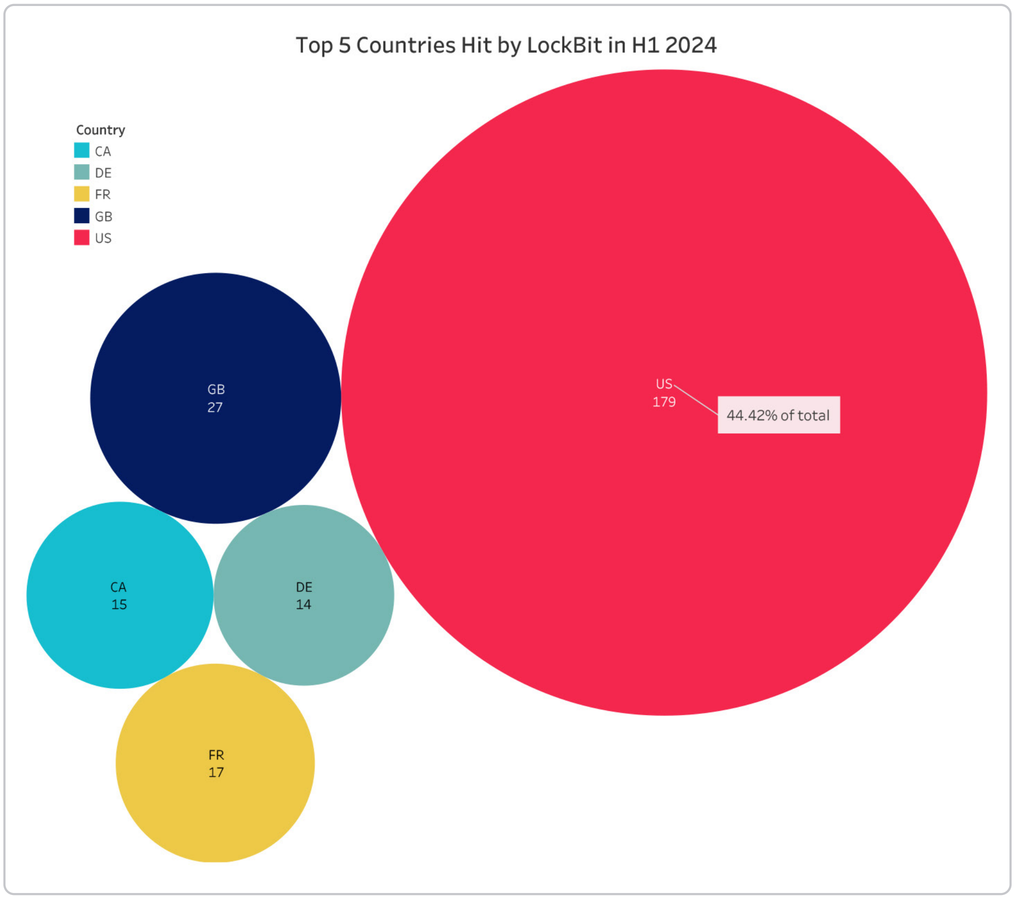
LockBit, a Russia-based group that operates on a Ransomware-as-a-Service (**RaaS**) model and is known for targeting critical infrastructure, has been a persistent threat. In the first half of H1 2024, they licensed their ransomware variants to other criminals, with 403 attacks accounting for 18% of total targets being in the Manufacturing & Industrial Products sector.



Geographically, LockBit focused on the United States (44.42%), United Kingdom (6.70%), France (4.22%), Canada (3.72%), and Germany (3.47%). However, a turning point came in February 2024. A coordinated international effort led by the U.K.'s National Crime Agency (**NCA**) and the FBI, codenamed "Operation Cronos," disrupted LockBit's operations. This involved seizing their public websites, taking control of servers, and retrieving decryption keys. Though initially successful, LockBit retaliated with renewed vigor, focusing attacks on five specific industries, as detailed in the following charts. This highlights the ongoing threat posed by RaaS models and the importance of continued vigilance despite law enforcement efforts.

Threat Actors & Malware Families (continued)

LockBit, a Russia-based group that operates on a Ransomware-as-a-Service (**RaaS**) model and is known for targeting critical infrastructure, has been a persistent threat. In the first half of H1 2024, they licensed their ransomware variants to other criminals, with 403 attacks accounting for 18% of total targets being in the Manufacturing & Industrial Products sector.



LockBit, a ransomware threat first observed in 2019, has evolved to its current iteration, LockBit 3.0, identified in June 2022. LockBit affiliates typically gain initial access through public-facing application vulnerabilities and Spearphishing emails. Once inside a network, LockBit 3.0 leverages PsExec for malicious code execution and potentially Chocolatey for additional malware deployment on Windows systems. Valid accounts are exploited for persistence and privilege escalation, often coupled with modifying group policies or abusing elevation controls. The end goal of a threat actor using LockBit is data encryption and/or exfiltration for ransom.

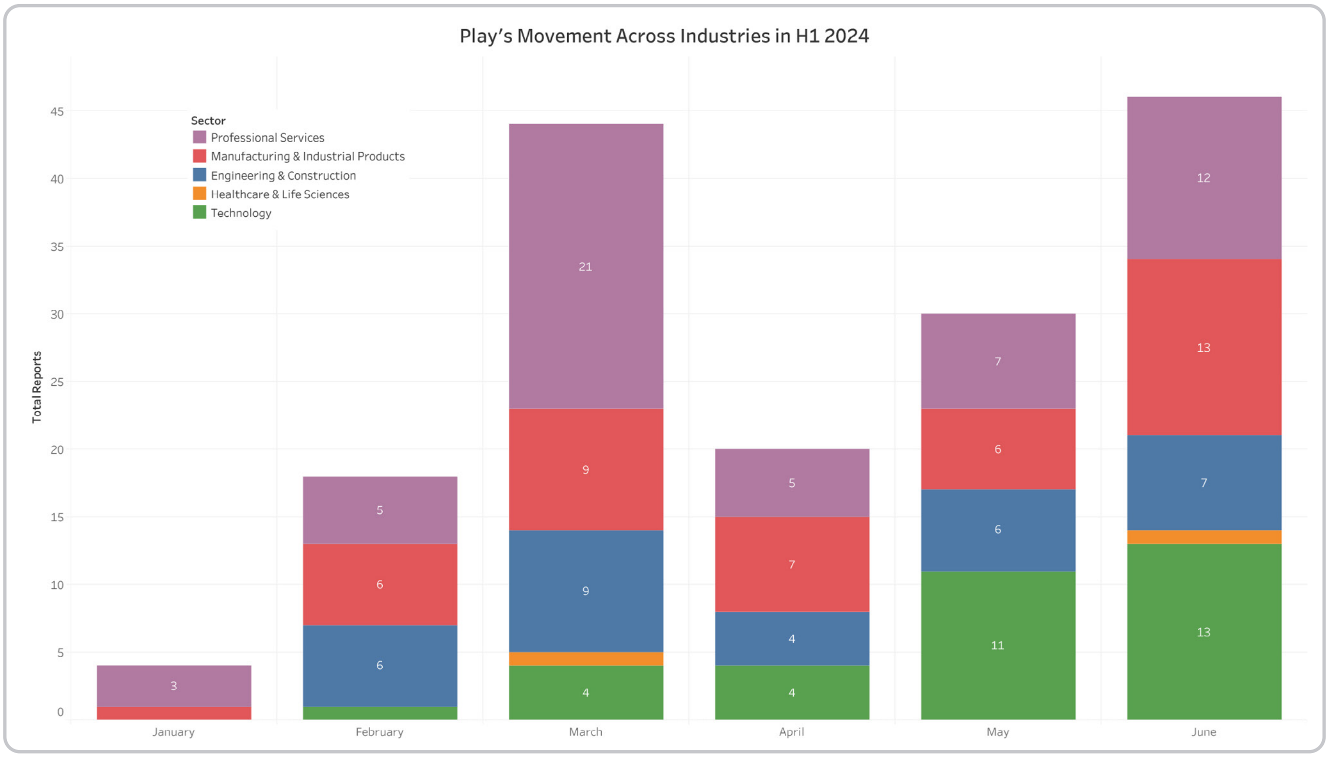
A critical trend emerged in late 2023 with the FBI's warning regarding the rise of repeat ransomware attacks and increased data destruction tactics. This trend continued into the first half of 2024, per Critical Start's observations. Our trend analysis revealed a concerning pattern of repeat attacks targeting multiple websites of the same organization, particularly within the healthcare sector. These repeated attacks, spaced out over an average of 28 days, suggest a deliberate strategy by cybercriminals to maximize the impact within compromised healthcare environments. Notably, LockBit was identified as the culprit in approximately 3% of these repeat attacks, underlining the need for heightened vigilance from healthcare organizations.

Threat Actors & Malware Families
(continued)

2. Play

Play, also known as Playcrypt, is notorious for using double-extortion tactics against their victims and prefers direct email communication for negotiations. They are known to modify the filename extensions of their victims with their ".play" alias. In the first half of 2024, we ranked them the second most dangerous group after assessing a total of 167 (7.43%) ransomware and database leak incidents they perpetrated. In H1 2024, Play focused its targeting on the Professional Services industry and increased their overall attacks on different industries and critical infrastructure by 51.81%.

Per our observations of Play's geographical targets, the United States accounted for 79.04% of all Play's victims between Jan-Jun 2024. We also assessed reports of attacks on entities in Canada (8.38%), Germany (2.99%), and United Kingdom (2.40%). Other countries including Sweden, Poland, and the Netherlands were above (1.20%). The following charts illustrate the impact of Play on our top 5 targeted industries and compares their H1 2023 activities with H1 2024.


Play's Movement Across Industries in H1 2024

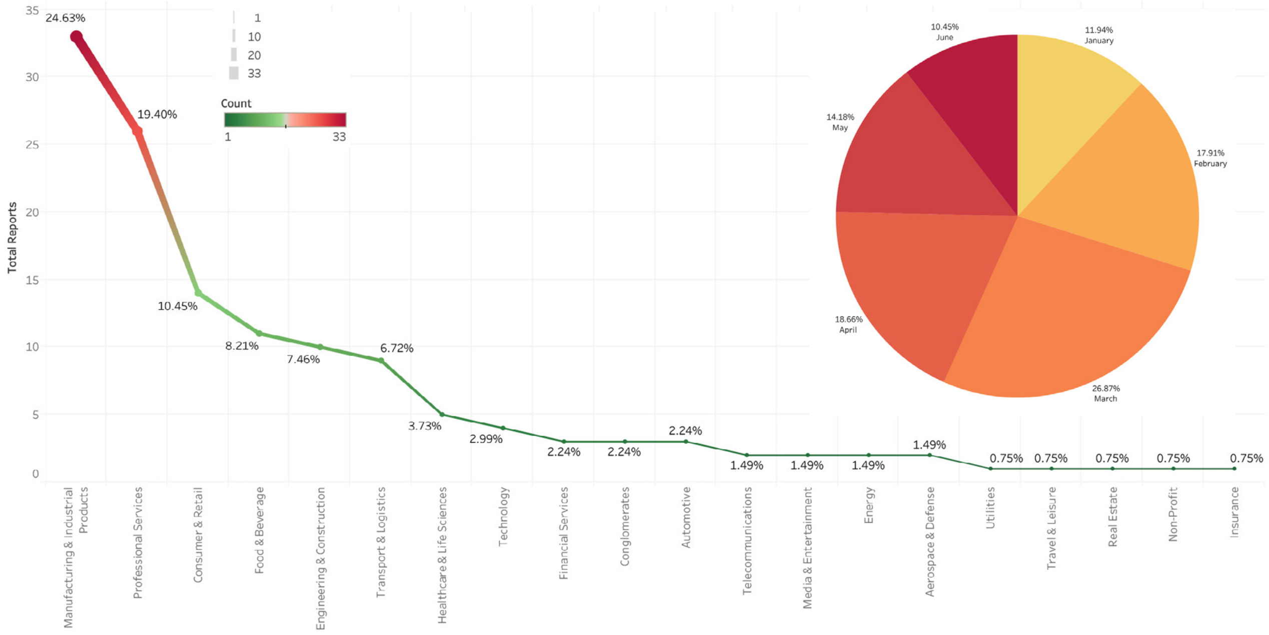
The Play ransomware group is a highly effective cybercriminal organization. They employ a multi-pronged approach to infiltrate target networks. They exploit weaknesses in popular applications like FortiOS and Microsoft Exchange (CVE-2018-13379, CVE-2020-12812, ProxyNotShell CVE-2022-41040, CVE-2022-41082). Additionally, attackers also exploit stolen credentials and abuse legitimate remote access protocols such as RDP and VPNs. Upon network infiltration, they meticulously map the environment using tools including Grixba and bypass security software with utilities such as IOBit and GMER. To expand their reach within the network, they employ a powerful command and control framework, notably Cobalt Strike, and steal administrator credentials using tools such as Mimikatz. Play's objective goes beyond data encryption. They strategically exfiltrate sensitive information and exploit it as a bargaining chip. Their ruthless tactics include publishing stolen data on their leak site or public forums, even after receiving ransom payments, highlighting their reputation as an unpredictable and persistent threat.

Threat Actors & Malware Families (continued)

3. Black Basta

Black Basta emerged on the cyber threat landscape in April 2022 and has rapidly established itself as a significant global ransomware group. Similar to LockBit, our observations in the first half of 2024 (H1 2024) indicate a concentration of Black Basta attacks targeting entities within the Manufacturing & Industrial Products industry.

Black Basta's Industries Hits and Monthly Incident Count in H1 2024



Black Basta utilizes a C++ based malware suite designed to exploit vulnerabilities in both Windows and Linux systems. This includes targeting application-specific weaknesses, as evidenced by their exploitation of CVE-2024-1709 in ConnectWise. Spearphishing campaigns serve as their primary attack vector, with documented instances of employing Qakbot malware for initial access. Once inside a compromised system, Black Basta leverages legitimate administrative tools like BITSAdmin and PsExec for lateral movement within the victim's network. Additionally, they establish persistent remote access through Cobalt Strike beacons. Their escalation of privileges frequently involves exploiting known Windows vulnerabilities, such as CVE-2021-34527 and CVE-2021-42287. Finally, Black Basta deploys the ChaCha20 encryption algorithm with an RSA-4096 public key to encrypt victim files. This process concludes with the addition of random file extensions, often including ".basta".[7]

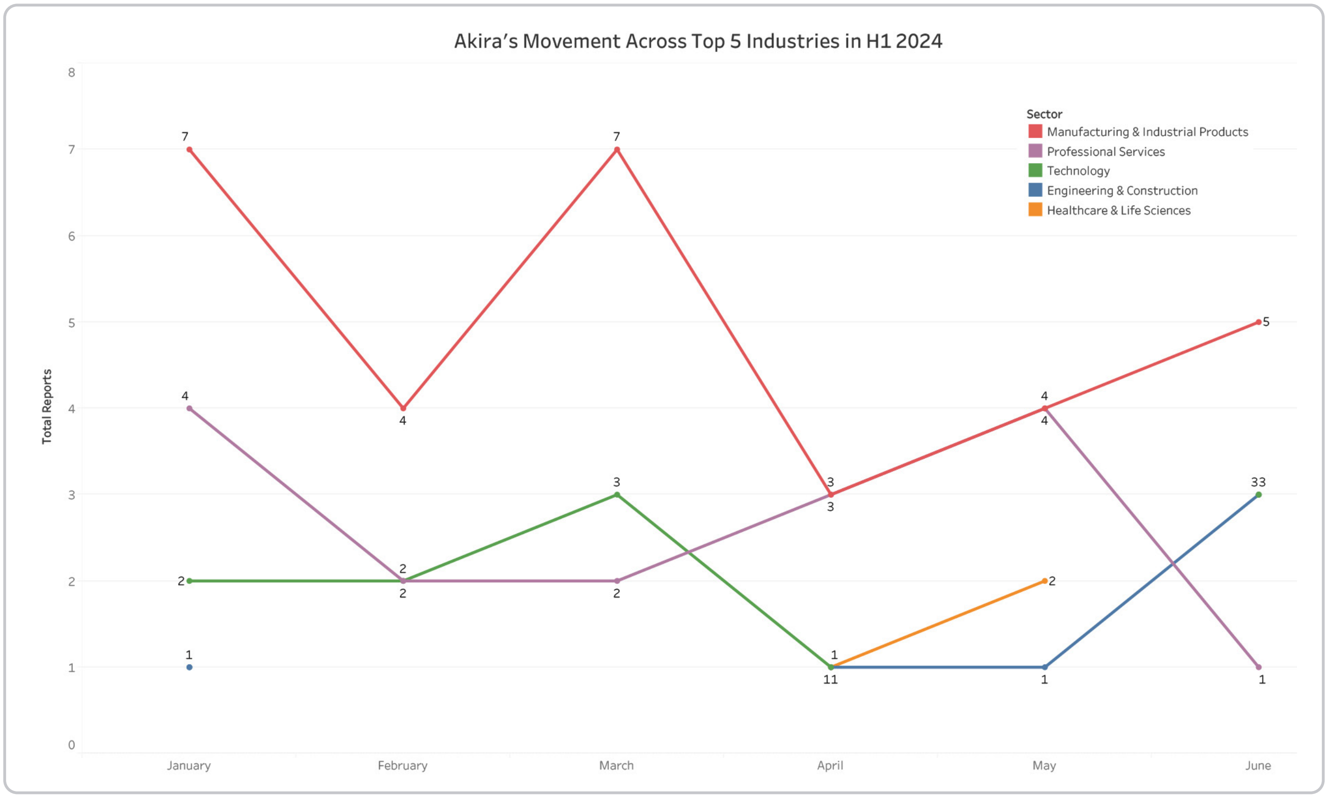
[7] https://h-isac.org/black-basta-threat-actor-emerges-as-a-major-threat-to-the-healthcare-industry/

Threat Actors & Malware Families
(continued)

4. Akira

The Akira ransomware group emerged as a significant threat in March 2023. The Akira ransomware group demonstrates a capacity for rapid evolution. They utilize a range of variants, including the original Akira strain and more recent iterations like Akira_v2 and Megazord. This tactic is a hallmark of ransomware groups seeking to evade detection. Notably, Megazord, a Rust-compiled variant identified in August 2023 employs a distinct file encryption strategy. Unlike Akira, which appends the ".akira" extension to encrypted files, Megazord utilizes the ".Powerrangers" extension. By introducing new variants, these groups aim to both enhance their capabilities and complicate efforts to identify and mitigate their attacks.

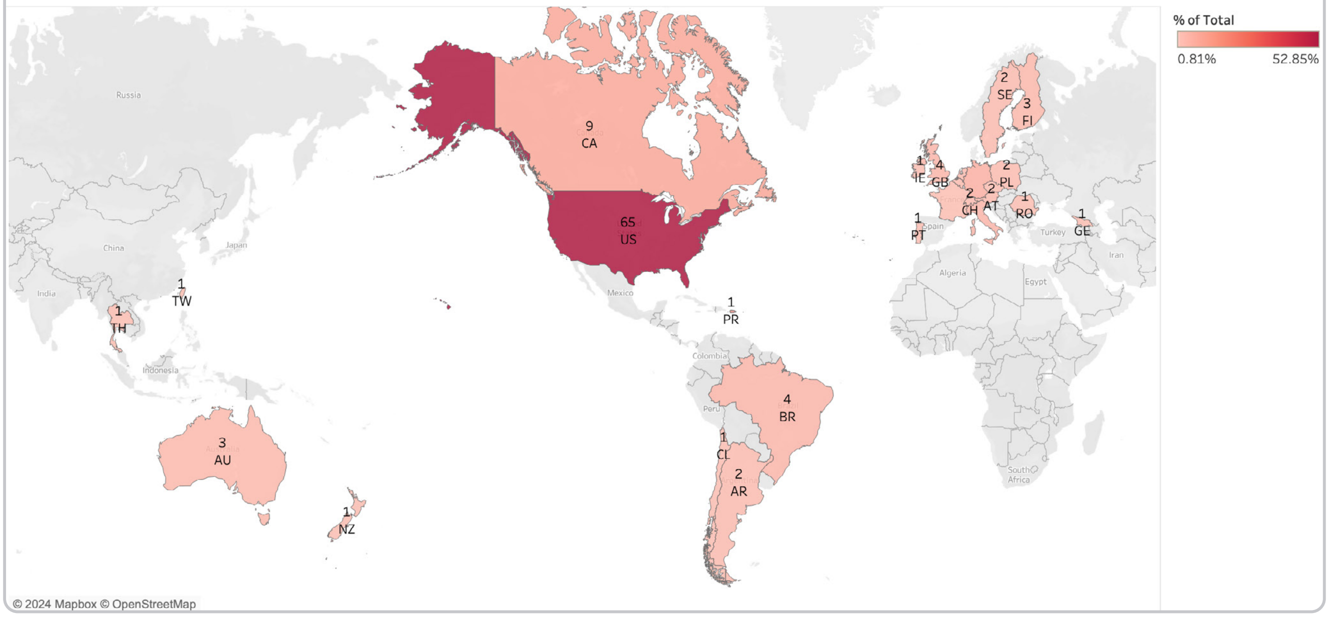
Our data for the first half of 2024 indicates that the Manufacturing & Industrial Products industry was a significant target for the Akira ransomware group. Nearly a quarter (24.39%) of all Akira attacks during this period were directed at entities within this sector



Examining the geographical distribution of these attacks within the Manufacturing & Industrial Products industry, we observed a focus on North America and Europe. Over half (52.85%) of the targeted entities were located in the United States, followed by Canada (7.32%) and Germany (4.88%). A smaller percentage (3.25%) of attacks targeted entities in other countries, including Brazil, Italy, and the United Kingdom.

Threat Actors & Malware Families
(continued)

Geographical Locations of Akira's Victims in H1 2024



© 2024 Mapbox © OpenStreetMap

The Akira ransomware group employs a calculated approach to infiltrate victim networks. They often exploit weaknesses in network defenses by leveraging stolen credentials or targeting vulnerabilities in VPN software that lacks multi-factor authentication (**MFA**). Known Cisco vulnerabilities such as CVE-2023-20269 (Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability) and CVE-2020-3259 (Cisco ASA and FTD Information Disclosure Vulnerability) have been used as entry points.

Once inside, the attackers utilize various techniques to escalate privileges and move laterally within the network. They may employ kerberoasting to obtain service account credentials by requesting and cracking Kerberos tickets.[8] Additionally, they might attempt to dump user credentials from the Local Security Authority Subsystem Service (**LSASS**) memory space, a technique known as credential dumping. Following the initial compromise, Akira ransomware operators often attempt to disable security software like Microsoft Defender and backup services such as ShadowProtect. This disarms potential defenses and allows them to proceed with encrypting the victim's data. Finally, the stolen information is exfiltrated using tools like WinSCP, RClone, and FileZilla through Secure File Transfer Protocol (**SFTP**) and File Transfer Protocol (**FTP**).

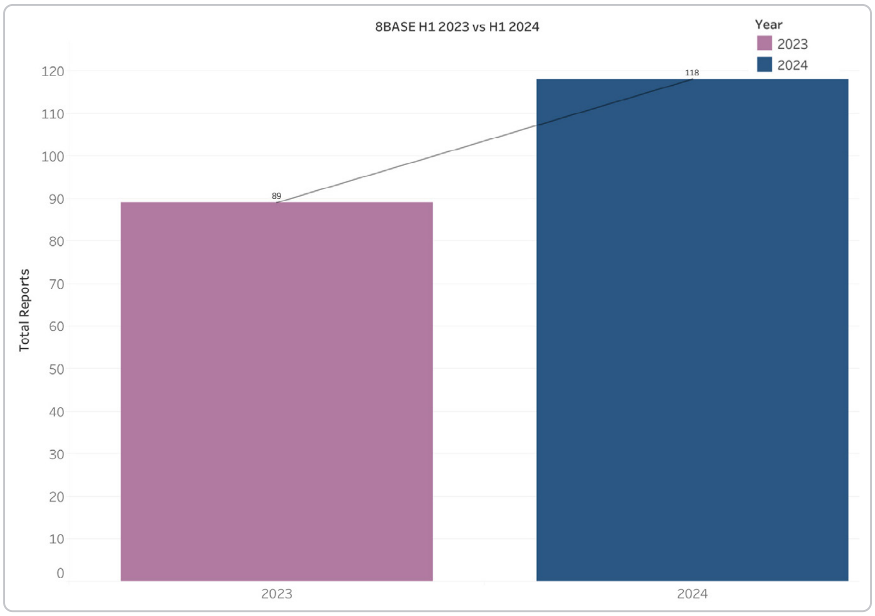
This multi-step process demonstrates the methodical approach the Akira group takes to compromise and steal sensitive data from their targets. Their tactics highlight the importance of implementing robust security measures, including regular patching, multi-factor authentication, and comprehensive monitoring of network activities.[9,10]

[8] *https://www.criticalstart.com/resources/critical-start-learning-objective-kerberoasting/*
[9] *https://www.cynet.com/blog/megazord-ransomware-technical-analysis-and-preventions/*
[10] *https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a*

Threat Actors & Malware Families
(continued)

5. 8BASE

8Base ransomware group emerged as a significant threat in late 2022 or early 2023. Some speculate a possible connection to the earlier RansomHouse group due to similar tactics and communication style. 8Base gained notoriety for their surge in activity around mid-2023, contributing to a notable rise in ransomware attacks globally. They primarily leverage a "double extortion" strategy, encrypting victim data and threatening public exposure if a ransom isn't paid alongside decryption costs. Their targets span a broad range of industries, including businesses of various sizes in real estate, legal services, hospitality, manufacturing, and finance. They exploit known vulnerabilities in software and operating systems, along with stolen credentials, to gain access. Tools like SmokeLoader and Phobos malware are also part of their arsenal. Operating as a RaaS (Ransomware-as-a-Service) group, they potentially allow other cybercriminals access to their methods.



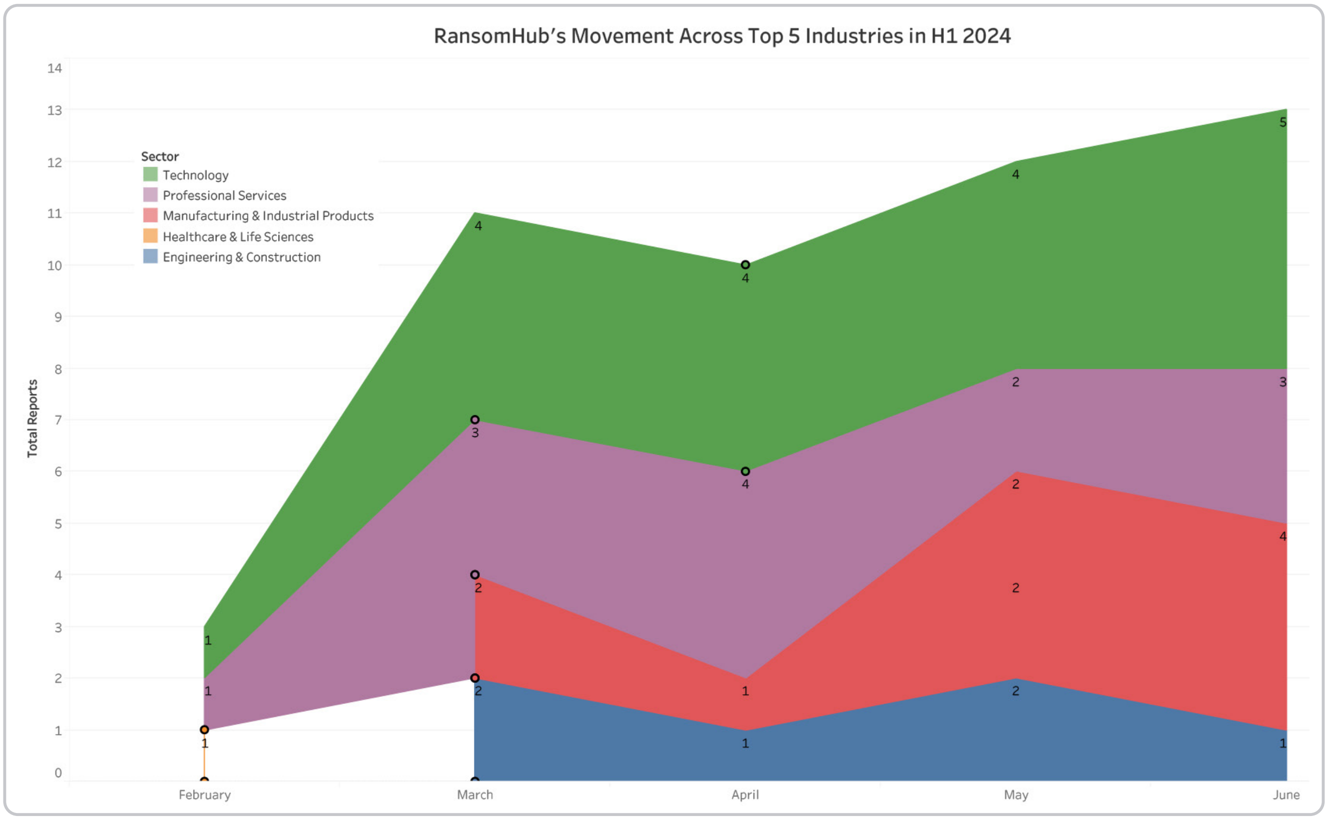
The 8Base ransomware group exhibited a significant surge in activity during the first half of 2024 (H1 2024), with a year-on-year increase of 32.58% compared to H1 2023. Notably, the Professional Services industry emerged as the second most impacted sector in H1 2024, following the Manufacturing & Industrial Products industry which maintained its position as the primary target. This places 8Base as the fourth threat actor on our Top 5 list predominantly targeting the Manufacturing & Industrial Products industry. While the United States remained the most affected country with 26.27% of attacks concentrated there between January and June 2024, 8Base also demonstrated a geographically diverse targeting strategy, impacting entities in Switzerland (3.39%), Austria (4.24%), Sweden (5.93%), Japan (6.78%), and other locations. This expansion highlights their evolving approach and the widening scope of their operations.

The 8Base ransomware group employs a calculated strategy to infiltrate victim networks and maximize the impact of their attacks. Spearphishing emails are their weapon of choice for initial access, allowing them a foothold within a system. Once inside, they wield an arsenal of credential access tools like Mimikatz, ProcDump, and LaZange to escalate their privileges and establish a persistent presence. Researchers have observed techniques like UAC bypass and automatic command prompt execution at login to grant them broader control over compromised systems. To ensure their encryption process runs smoothly and avoids disruptions, 8Base often disables critical system processes related to databases and backups, such as msftesql.exe or sqlagent.exe. This multi-stage approach demonstrates the methodical nature of 8Base's attacks, highlighting the importance of robust cybersecurity measures to defend against them.

Threat Actors & Malware Families (continued)

Emerging Group: RansomHub

The first half of 2024 saw a surge in ransomware activity, with new groups like Arcus Media, Blackout, Cicada3301, and the particularly prolific RansomHub emerging. While some speculate RansomHub is a rebranded Knight Ransomware, Knight itself remains active, targeting government, public sector, and transport & logistics (some overlap with RansomHub's targets) in countries like Colombia, Argentina, Brazil, Spain, and the United States. However, RansomHub stands out for its sheer volume, infiltrating a staggering 94 victims. True to their name, they operate as a Ransomware-as-a-Service (RaaS) group, providing a platform for global attackers united by a single motive: financial gain.[11]

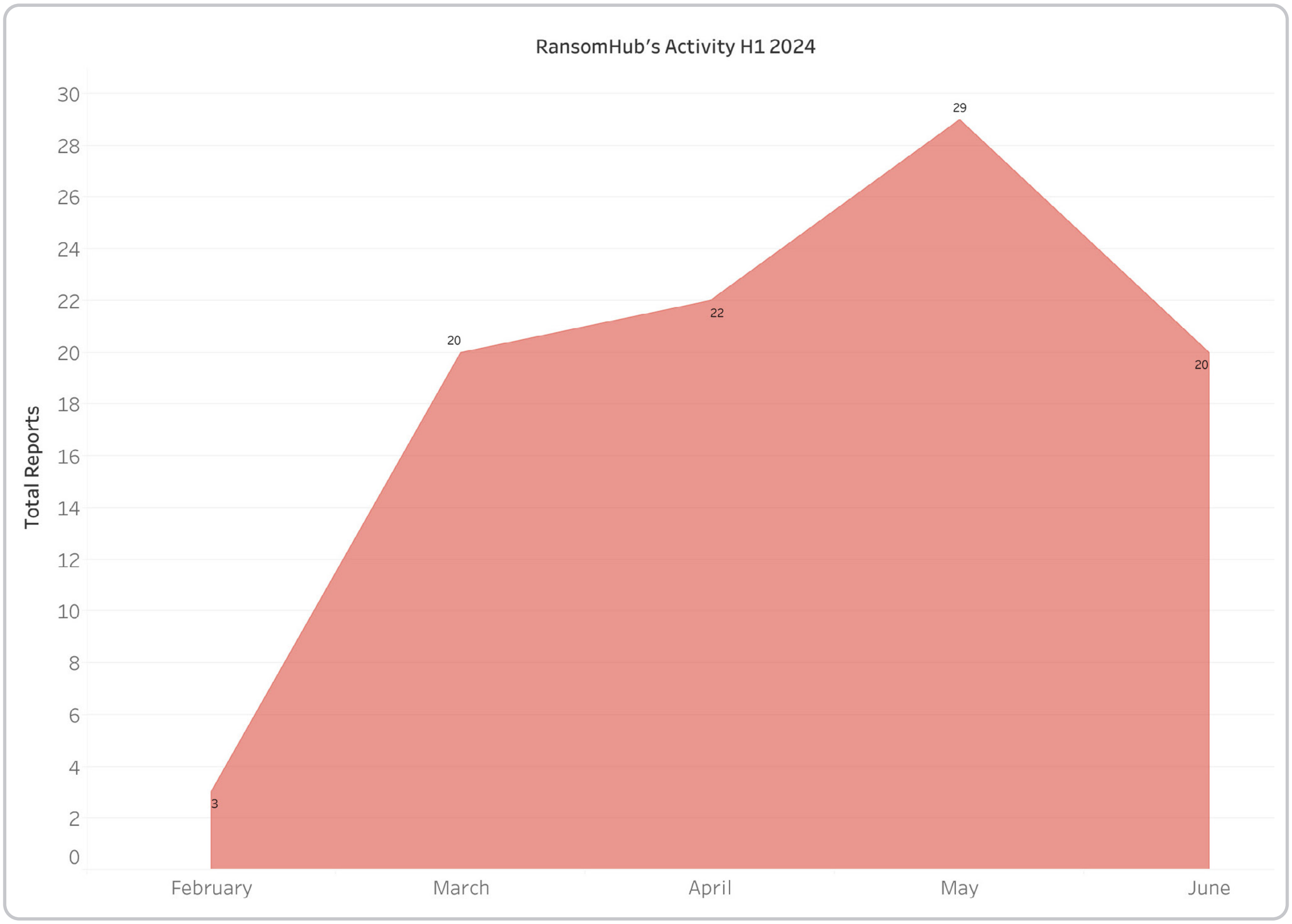


[11] *https://socradar.io/dark-web-profile-ransomhub/*

Threat Actors & Malware Families (continued)

RansomHub exploits various vulnerabilities, notably CVE-2020-1472, a critical Microsoft Netlogon Privilege Escalation Vulnerability. Security researchers have identified several tools used by the group for reconnaissance and remote access during their attack phase, including NetScan, Splashtop, and Atera. After infiltrating a victim's network, RansomHub executes a series of malicious actions. These include stopping the Internet Information Service (IIS) using command-line interface (CLI) commands such as cmd.exe /c iisreset.exe /stop, manipulating virtual machines (VMs), and deleting shadow copies. Such activities result in service disruptions, data loss, and prevent the restoration of deleted VMs from previous backups. This comprehensive attack strategy demonstrates RansomHub's capability to cause significant damage to targeted systems and hinder recovery efforts.[12]

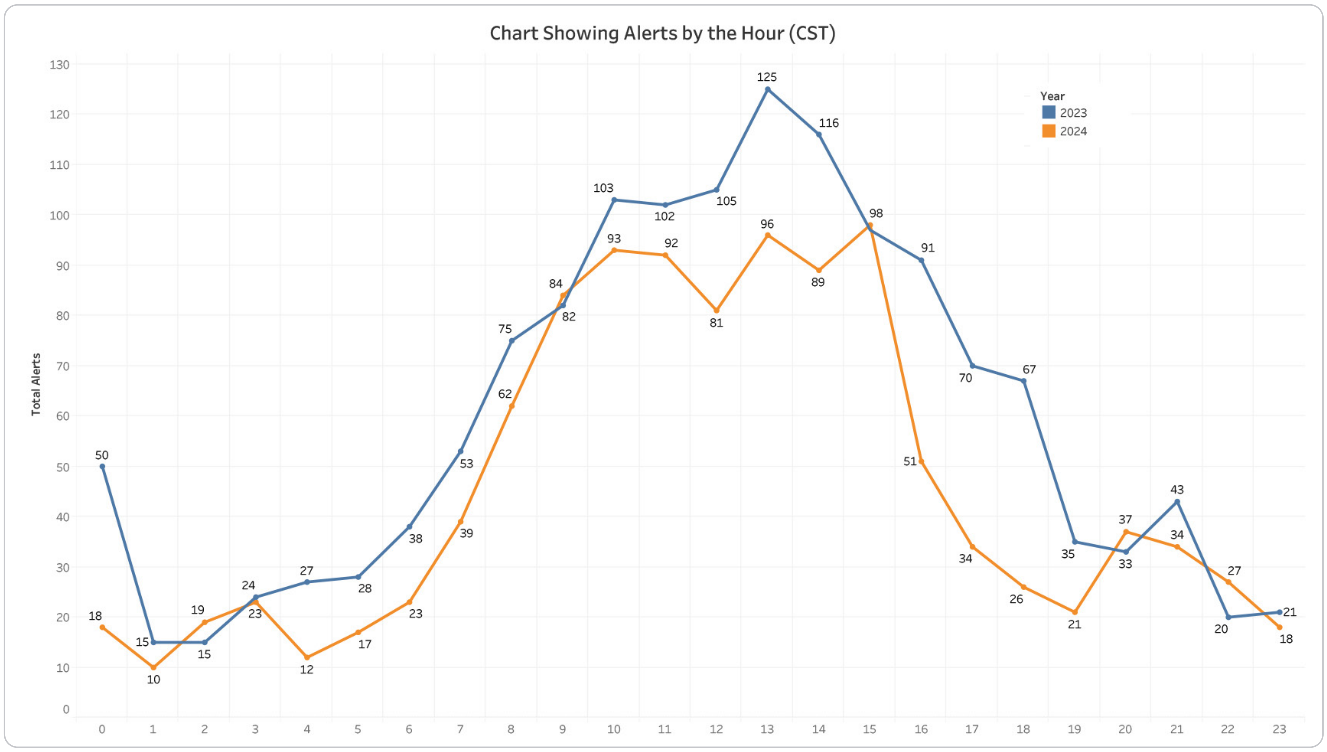
Critical Start's H1 2024 data reveals RansomHub's (established in February 2024) primary targets: Technology (19.15%), Professional Services (13.83%), and Financial Services (8.51%). Notably, the United States (25.53%) and Brazil (11.07%) were their top hit countries.



[12] https://www.recordedfuture.com/research/ransomhub-draws-in-affiliates-with-multi-os-capability-and-high-commission-rates

Timeline & TTP Trends

Critical Start’s CRU discovered several trends in cyber incidents between January and June of 2024. The data utilized for these insights were pulled from the Cyber Operations Risk & Response™ (**CORR**) platform.



- Most incidents (60.32%) occurred mid-week, with Tuesdays seeing the highest volume (21.02% of all alerts).
- A typical pattern emerged: fewer alerts towards the month’s end, followed by a rise at the beginning of the next. April being an outlier.
- Compared to the same period in 2023, there was a decrease in attacks in all months except in February 2024, which saw a slight increase of 2.84%.
- In 2024, we observed the highest concentration of attacks between 10am and 3pm CST. This represents a slight shift from 2023, when attack activity was most intense from 10am to 4pm CST.
- Overall, the total number of high/critical alerts in H1 2024 (1,104) represents a significant decrease of 23.07% compared to the same period in 2023 (1,435).
- Initial Access was the most prevalent tactic, with Phishing being the primary corresponding technique accounting for 58.98% of all assessed incidents.
- Cyber Threat actors are resorting to sending multiple malicious links to potentially enhance success rates, evaluate susceptibility of an individual, or sustain pressure.

Timeline & TTP Trends (continued)

Timeline Analysis

Critical Start's platform identified a significant increase in security incidents on three distinct days within H1 2024. Further investigation revealed that two of these spikes likely coincided with the Change Healthcare attack on February 21, 2024. The third incident highlights the potential persistence of threat actors, employing multiple attempts with targeted malicious links to gain initial access.

1. **On February 13, 2024**, 23% of the high/critical security incidents targeted a healthcare manufacturing company. The attack itself presents an unusual sequence. The initial detection occurred at 11:22 PM CST, with Taterf malware. The Risk & Security Operations Center (**RSOC**) quickly detected malicious activity and noted the use of multiple malicious links by the threat actors.

   However, it's important to acknowledge that the observed sequence, with user execution followed by a Spearphishing attempt, deviates from the typical attacker strategy. While this incident involves multiple links, it's valuable to consider the more common motivations behind threat actors deploying multiple phishing emails. These motivations can include increasing their chances of success by sending a series of emails with varied approaches to exploit different vulnerabilities or cater to various user interests. They might also use initial emails to test a target's awareness of phishing tactics and adapt their methods for subsequent attempts. Additionally, multiple emails can signify a sustained campaign designed to keep the target engaged and eventually compromise their system, a tactic frequently used in Spearphishing.

   On Feb 21, 2024, a total of 25 high/critical incidents were identified, with over half (52%) targeting a single healthcare manufacturing company. Additionally, a known healthcare entity and organizations within transportation, energy, financial services, and manufacturing were also targeted. The attackers employed a diverse set of tactics. The healthcare manufacturer was initially compromised through a phishing attempt with a malicious attachment (TA001.T1566). The report also suggests the possibility of compromised valid accounts in the cloud (TA001.T1078.004) as another potential attack vector for this company. Stolen web session cookies (TA006.T1539) were observed in a separate attack, potentially targeting another manufacturing company outside of healthcare, indicating credential theft might be a broader tactic. An anomalous single factor sign-in attempt at the healthcare entity suggests a potential unauthorized access effort. Additionally, active scanning (TA0043.T1595) was detected, indicating potential reconnaissance or discovery activity by the attackers to identify vulnerabilities within targeted environments.

   The observed widespread targeting across various industries, with a particular focus on healthcare manufacturing, suggests a potentially well-coordinated campaign. **It is important to note that the Change Healthcare attack occurred on February 21, 2024, which coincides with the timeframe of the two reported incidents above.**

Timeline & TTP Trends (continued)

2. **On June 06, 2024**, a sophisticated cyberattack targeted a construction company. Nearly half of all critical incidents (47.62%) were aimed at this single entity. The attack unfolded rapidly. It began with a user attempting to execute a malicious file in the early morning hours (3:27 AM CST). Later that day, attackers successfully compromised the system through a drive-by download from a phishing site (Adversary-in-the-middle (Aitm)). This initial breach was followed by a flurry of attempts within minutes, indicating a fast-paced and aggressive assault.

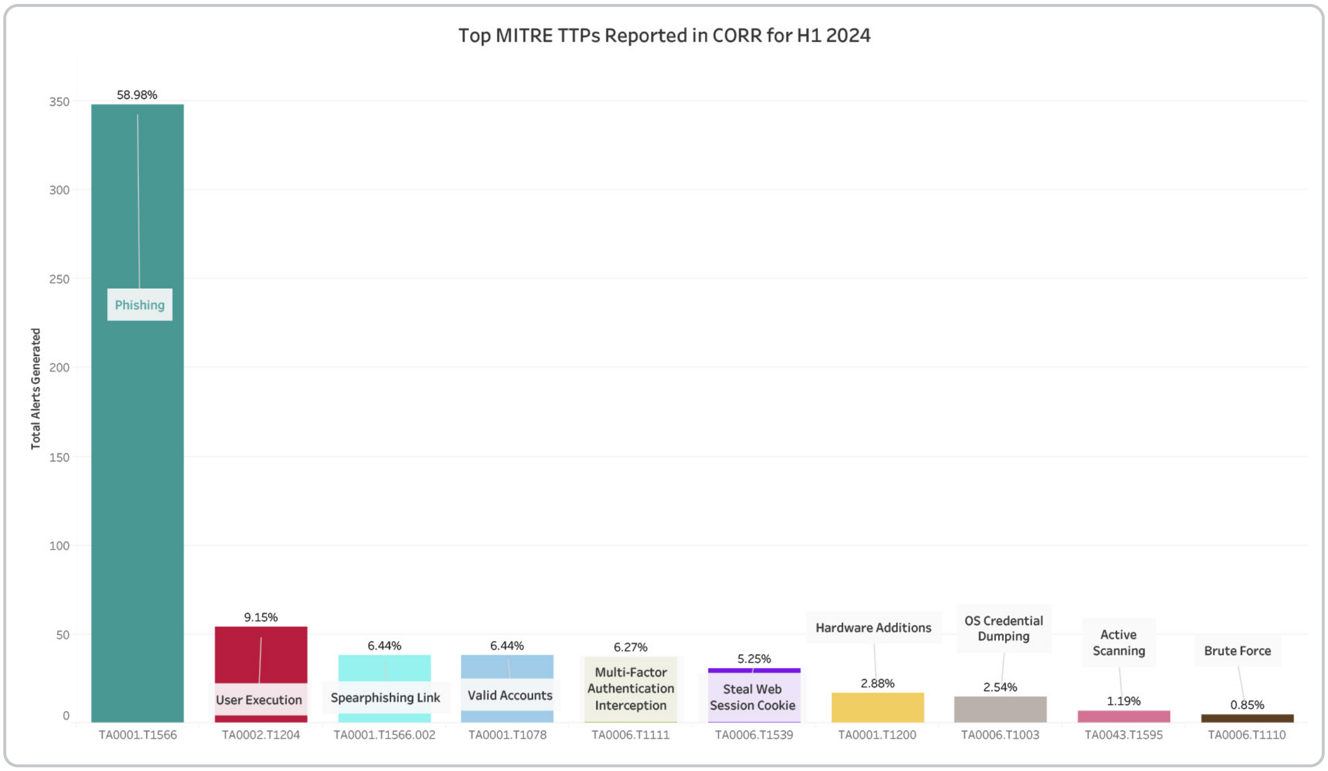
   The attackers used various methods to gain access and maintain control. These included phishing emails with malicious attachments, drive-by downloads, and potentially even tricking users into running malicious files. The report also suggests stolen credentials or brute force attacks were used to gain access to valid user accounts. Once inside, the attackers aimed to establish persistence by exploiting these compromised accounts. They even tried techniques like stealing web session cookies and potentially setting up Aitm attacks to capture additional login credentials. The attackers also scanned for peripheral devices, possibly searching for more systems to exploit.

   The potential impact of this attack is severe. Data breaches could expose sensitive construction project information. Critical operations could be disrupted, and the company could face financial losses from stolen data or extortion attempts. These attacks pose significant risks across various industries. Phishing attacks, compromised accounts, and stolen credentials could lead to data breaches, potentially exposing sensitive healthcare data. Further, malware installation attempts could disrupt critical operations, leading to financial losses.

Timeline & TTPs Trends (continued)

MITRE Tactics

Our analysis of high/critical security alerts in H1 2024 revealed Initial Access was primarily established through Phishing attacks, accounting for 58.98% of all assessed incidents. The second highest rated tactic observed was Execution via User Execution at 9.15%. Notably, 24.93% of the high/critical incidents lacked a corresponding MITRE ATT&CK TTP tag. This absence may indicate uncertainty in their classification due to the evolving threat landscape, emerging novel Tactics, Techniques, and Procedures (**TTP**s) not yet documented in the MITRE ATT&CK® Framework, or potential platform tagging deficiencies that need to be addressed.



Trending Concerns

- **Business Email Compromise (BEC) Attacks:** Previously focused on large corporations, BEC scammers are now targeting smaller, less cybersecurity-conscious businesses.
- **Deepfakes and Social Engineering:** Reports show a surge in deepfake attacks, with a staggering 3,000% increase in deepfake fraud attempts in 2023 alone and a predicted cost of $1 trillion globally in 2024.
- **Abuse of Open-Source Repositories:** In 2024, attackers are increasingly using these repositories to launch two main types of attacks: repo confusion attacks and supply chain attacks.

Trending Concerns (continued)

Business Email Compromise (BEC) Attacks

Business Email Compromise (BEC) attacks remain a top cybersecurity concern for businesses in 2024. These attacks are particularly dangerous because they don't rely on exploiting software vulnerabilities. Instead, cyber threat actors leverage social engineering tactics to manipulate employees into handing over sensitive information or authorizing fraudulent transactions. The goal of a BEC attack is to disrupt business operations. This can take various forms, from tricking employees into authorizing fraudulent transfers – leading to a staggering $2.9 billion in losses in 2023 alone – to compromising sensitive data or deploying malware that can cripple a company's systems.

Europe witnessed a staggering 123.8% year-over-year increase in BEC attacks, compared to a still significant 72.2% rise in the Americas (United States, precisely). This highlights the global reach of these scams and the urgent need for businesses to bolster their defenses. Cybercriminals are becoming increasingly sophisticated in their tactics. Capitalizing on current events like international conflicts, they craft believable scams that exploit people's emotions and a false sense of urgency. For example, they might pose as a charity collecting donations for a crisis-stricken region or impersonate a disgruntled business partner aligned with the opposing side in a political conflict.

Further, the attack surface is expanding. Vendor Email Compromise (**VEC**) attacks are on the rise, targeting a company's vendor network. These scams attempt to trick vendors into sending payments to fraudulent accounts. This trend underscores the importance of implementing robust security measures across a company's entire supply chain. Additionally, the use of generative AI in BEC attacks makes it difficult for employees to identify the email as malicious. This technology allows attackers to create highly realistic emails that mimic writing styles and logos and content. These AI-generated emails can easily deceive victims who aren't trained to identify subtle inconsistencies.

Defending against Business Email Compromise (BEC) attacks in 2024 requires a comprehensive, multi-layered approach. Organizations can implement technical safeguards such as adding organization-wide rules to flag external communications, enabling spoof intelligence to identify mismatched sender addresses, and deploying advanced security solutions to intercept malicious emails before they reach inboxes. Equally important are non-technical measures. These include staying informed about the latest cybercriminal tactics, implementing robust social engineering awareness training for employees, and fostering a security-conscious culture within the vendor network to mitigate Vendor Email Compromise (VEC) risks. By integrating these technical and human-focused strategies, businesses can create a more resilient defense against the evolving threat of BEC scams. This holistic approach combines technological tools with employee education and organizational culture shifts to form a robust shield against sophisticated email-based attacks.

Recent Attack: On June 5th, 2024, the Manager of the Town of Arlington, Massachusetts officially disclosed that the town fell victim to a business email compromise perpetrated through social engineering and led to a wire fraud totaling $445,945.73. They traced the threat actor activities back to September 12, 2023. The wire fraud was made possible through a seemingly legitimate email requesting a change in payment method.

References:

1. https://www.thesslstore.com/blog/business-email-compromise-statistics/
2. https://arcticwolf.com/resources/blog/defending-against-business-email-compromise/
3. https://abnormalsecurity.com/blog/bec-attacks-europe
4. https://blog.knowbe4.com/bec-attacks-accounted-for-more-than-one-in-ten-social-engineering-attacks-in-2023
5. https://statescoop.com/massachusetts-town-loses-445000-email-scam/

Trending Concerns (continued)

Deepfakes in Social Engineering Attacks

Deepfakes, cleverly manipulated audio and video content designed to appear real, are a growing weapon for cybercriminals. These forgeries are used to launch phishing and social engineering scams, causing financial losses, data theft, and reputational damage across various industries. Reports show a surge in deepfake attacks, with a 3,000% increase in deepfake fraud attempts in 2023 alone. This growth can likely be attributed to two key factors:

- The affordability and user-friendly nature of deep learning models have made deepfake creation accessible to a wider range of attackers, even those without technical expertise.
- Phishing is already a successful method for cybercriminals, and deepfakes add another layer of deception, making these scams even more lucrative.

Deepfakes can come in various forms, posing a threat to different areas:

Deepfake audio (voice cloning): This allows fraudsters to impersonate real people's voices to gain access to accounts or manipulate financial workers. Banks are especially vulnerable as deepfakes can bypass voice verification systems.

Deepfake video: Used to impersonate executives, create fake advertising, or bypass biometric verification systems.

Deepfake text: Mimics writing styles for large-scale social engineering and phishing attacks.

The impact of deepfakes is widespread. Financial institutions are prime targets for deepfake audio scams. Fake customer testimonials or product images can damage any brand's reputation. Deepfakes can also manipulate stock markets by spreading false information and erode trust in media and elections. The predicted cost of deepfake fraud is a staggering $1 trillion globally in 2024. Social media further amplifies the dangers as deepfakes can spread easily on these platforms, potentially causing significant losses for social media companies and fostering societal unrest.

Trending Concerns (continued)

Randy Watkins, CTO provided the following commentary “One of the most concerning developments is the rise of deepfake technology. The ability to convincingly replicate voices and images with just minutes of source material poses significant risks. Imagine the potential implications of world leaders being impersonated in videos or audio recordings, potentially sparking international conflicts or influencing elections. Detecting these deepfakes will be crucial, but it’s a race against time in a landscape where social media spreads information rapidly.”

To effectively combat this growing threat, a multi-layered approach is necessary. Advancements in AI-powered detection are crucial for identifying various forms of deepfakes. Different detection solutions cater to specific needs:

- Real-time voice deepfake detection is essential for organizations with call centers or customer service teams.
- Text and image detectors can benefit financial institutions by strengthening Know Your Customer (**KYC**) and Anti-Money Laundering (**AML**) procedures.
- Image, video, and text detection models can help news organizations verify the authenticity of their sources.
- Content moderation solutions are necessary for social media platforms to prevent the spread of fake content.
- Audio deepfake detection is important for government institutions to identify manipulated communications used for political manipulation or identity theft.

In addition to detection technology, user education is essential. Training employees and individuals to recognize phishing attempts and be more discerning about online information is a critical line of defense. Implementing security solutions that leverage AI for anti-phishing and secure browsing can further bolster defenses. Finally, staying updated by regularly patching vulnerabilities in systems is crucial for maintaining a strong defense against deepfakes. By combining these strategies, organizations can be better prepared to address the evolving threat of deepfakes.

References:

1. https://www.forbes.com/sites/forbestechcouncil/2024/06/18/navigating-the-perils-of-deepfakes/#:~:text=The%20Rise%20Of%20Cybercrime,second%20half%20of%202023%20alone.
2. https://bufferzonesecurity.com/the-rise-of-deepfake-phishing-attacks/
3. https://securityintelligence.com/posts/new-wave-deepfake-cybercrime/

Trending Concerns (continued)

Abuse of Open-Source Repositories

Open-source code repositories, a cornerstone of collaboration in the developer world, are unfortunately becoming targets for malicious activity. In 2024, attackers are increasingly using these repositories to launch two main types of attacks: repo confusion attacks and supply chain attacks.

Repo confusion attacks involve creating fake copies of popular repositories on platforms like GitHub. These copies are booby-trapped with malware, designed to trick developers into downloading them instead of the legitimate ones. Once downloaded, this malware can steal data, infect systems, or introduce vulnerabilities into other software projects. Attackers make these fakes appear convincing by automating the process of cloning popular repositories, adding malware, and re-uploading them with similar names. They might even create thousands of copies to spread across the web and make them easier to find. The challenge for developers is spotting these fakes, especially since they often have similar names and appearances to the real ones. Additionally, automated detection systems may miss some malicious repositories.

Supply chain attacks target the open-source software supply chain itself. In this scenario, attackers compromise a legitimate open-source project and inject malicious code directly into it. This way, the malicious code gets downloaded and used unknowingly by other developers, potentially infecting their systems or applications. An example of this from 2024 was malicious code being injected into popular Python packages.

To protect against this vulnerability organizations should prioritize a layered defense. Firstly, educate developers to spot red flags in repositories like low engagement or unclear descriptions. Secondly, implement a vetting process to check code licenses, scan for vulnerabilities, and analyze dependencies. Automated scanning tools throughout the development pipeline can continuously identify threats. Regularly updating software with the latest security patches is also crucial. Staying informed about vulnerabilities in popular open-source projects and using tools to monitor dependencies for issues helps stay ahead of threats. Finally, limiting who can create repositories within your organization adds an extra layer of security. By combining these measures, organizations can significantly reduce the risk of vulnerabilities lurking in the open-source world.

References:

1. https://www.darkreading.com/application-security/millions-of-malicious-repositories-flood-github
2. https://www.arnica.io/blog/malicious-code-campaign-on-github-repos
3. https://www.developer-tech.com/news/2024/jun/26/waf-vs-traditional-firewalls-protecting-your-web-applications/
4. https://securitylab.github.com/advisories/
5. https://openssf.org/wp-content/uploads/2023/12/openssf_annual_report_2023_122323a.pdf
6. https://www.helpnetsecurity.com/2024/06/26/git-exposed-secrets/

Recommendations

In today's dynamic cybersecurity landscape, organizations are bombarded with ever-more sophisticated threats. Critical Start CISO, George Jones emphasizes, "compliance frameworks tend to remain stable, but what changes are the specific artifacts required to demonstrate compliance." This highlights the need for adaptable security strategies that go beyond mere adherence to static frameworks.

Building a strong **security culture** is paramount. "I often emphasize that while I oversee internal security, I'm not the sole security officer," says Jones. "We have 300 others across the organization, and each person shares the responsibility for safeguarding our platform and internal network." This sentiment is echoed by Randy Watkins, CTO, who underlines the importance of extending security awareness beyond your organization: "The principle of 'six degrees of separation' applies—if a vendor with access to our financial data isn't secure, it affects us directly."

User education and training are crucial in this endeavor. Jones reiterates this point: "Regularly conduct phishing tests and security training sessions." By equipping employees to identify and report suspicious messages or activities, you create a sustainable approach to strengthening your organization's security. Ultimately, these trainings should help employees understand their role in the broader security framework, transforming best practices from a mere duty into second nature." Regular phishing simulations and security awareness training sessions empower employees to identify suspicious messages and understand their role in maintaining a secure environment.

Technical measures are equally important. Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) solutions, as recommended by Jones, provide comprehensive coverage to swiftly identify and address vulnerabilities. Additionally, patch management is critical. Critical Start CSO, Jordan Mauriello highlights, "the majority of successful attacks stem from older, known vulnerabilities that could have been prevented with timely patching." Organizations should prioritize applying updates to third-party applications within a month of release.

The threat landscape is constantly evolving. Social engineering attacks, for instance, are becoming increasingly sophisticated. Mauriello observes a rise in attackers' ability to craft "highly convincing communications, often indistinguishable from legitimate correspondence." Organizations must adapt their defenses accordingly, with ongoing training to help employees identify these attempts.

Collaboration is another key element. "Engage with internal and external peers and cybersecurity organizations for threat intelligence sharing, proactive threat hunting, and cyber threat research," advises Jones. Sharing knowledge and best practices strengthens everyone's defenses.

Finally, remember that security is an ongoing process. As Mauriello concludes, "effective cybersecurity starts with robust processes. When these are in place and performing optimally, decisions around resource allocation become clearer." By continuously evaluating and improving their security posture, organizations can stay ahead of cybercriminals and protect their critical data.

CRITICALSTART®

About Critical Start CTI

To stay ahead of emerging threats, the Critical Start Cyber Threat Intelligence (**CTI**) 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), CTI will continue to monitor emerging threat developments and work closely with the Security Engineering and RSOC 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