FORESCOUT RESEARCH | VEDERE LABS

PERILS IN THE PERIPHERY: A 2024H1 THREAT REVIEW

Vulnerabilities, Threat Actors and Ransomware in the Unmanaged Perimeter

August 29, 2024

CONTENTS

1. Executive Summary

In the first half of 2024, Forescout Research – Vedere Labs published a diverse range of blog posts and reports analyzing prominent vulnerabilities, threat actors and ransomware.

Our data shows state-sponsored actors are using hacktivist persona and **are targeting VPN vulnerabilities as entry points**. Attackers have shifted from managed endpoints to the unmanaged perimeter for initial access and impact. Network infrastructure and other high-risk unmanaged devices are becoming more attractive targets due to the challenges in detecting and investigating these attacks, primarily due to a lack of network visibility and security telemetry from these devices. It is crucial to proactively secure them.

This report reviews the period between January 1 and July1 31, 2024 (2024H1) highlighting the evolution of the threat landscape as compared with 2023H1.

Key Findings:

- Published vulnerabilities increased 43%
- More than two thirds of these vulnerabilities had low or medium CVSS scores
- CVEs added to CISA KEV decreased by 23%
- **Roughly 20% of new exploited vulnerabilities in CISA KEV and VL KEV catalogs targeted VPN or network infrastructure appliances**
- 387 threat actors had updates
  - 50% are cybercriminals and include ransomware groups
  - 40% are state-sponsored groups
- Ransomware attacks are up 6%
  - At 3085 attacks, they average 441 attacks per month or 15 per day
  - Active groups grew from 53 to 82 – for a 55% increase
- China has the highest number of threat actors
- The US, Germany and India are the top targeted countries
- Top vertical industry targets are government, financial services and technology

In addition, we provide mitigation recommendations based on our research findings.

2. Key Trends in the First Half of 2024

Two key observations stand out from the cyber threats in 2024H1:

1. State-sponsored actors are increasingly using hacktivist persona as a front for their operations, especially when targeting critical infrastructure.
2. Sophisticated threat actors are heavily targeting VPNs and other perimeter devices exploiting new vulnerabilities for initial access. This supports our recent finding that routers and wireless access points are the riskiest devices in 2024.

2.1. Blurred Lines Between Hacktivists and State-Sponsored Actors Targeting Critical Infrastructure

In 2022, we reported on a trend of hacktivists aligning with geopolitical conflicts and expanding their TTPs from defacements and DDoS to data leaks and disruption of cyber-physical systems. Nearly two years later, the trend has evolved to state-sponsored actors using hacktivist personae to conduct some of their attacks. This shift may be driven by several factors, such as increased visibility of campaigns and plausible deniability for the actors.

Notable early examples include "Predatory Sparrow," which poses as a hacktivist group rebelling against the Iranian state, but is believed to be affiliated with Israel. Similarly, Iranian groups like "Karma Power" and "The Malek Team" have targeted Israeli critical infrastructure and are thought to be affiliated with Iran's Ministry of Intelligence or the Islamic Revolutionary Guard Corps.

Critical infrastructure organizations continue to be disproportionally targeted by this type of threat actor. Notable examples in 2024H1 include:

- The Cyber Army of Russia, believed to be linked to Sandworm, launched an attack against a wastewater treatment plant in the U.S. This attack occurred a month after the White House warned of hackers targeting U.S. water systems.
- The BlackJack group, thought to be affiliated with Ukrainian intelligence, used the custom malware Fuxnet to disable thousands of sensors monitoring Moscow's sewage system.
- The Ikaruz Red Team, believed to be affiliated with China, deployed ransomware created using builders from several known families, such as LockBit, Cl0p and ALPHV to disrupt the government of the Philippines.

Partly due to the increase in attacks like these, OT device manufacturer Rockwell Automation issued an alert in May, warning their users to take internet-exposed devices offline "due to heightened geopolitical tensions and adversarial cyber activity globally".

2.2 Massive targeting of VPN vulnerabilities

The trend of exploits targeting perimeter and network infrastructure devices has only increased in 2024H1. VPNs have been a primary target during this period with threat actors exploiting a series of vulnerabilities in widely used solutions leading to unauthorized access, including:

- Ivanti Connect Secure
- Cisco Adaptive Security Appliance (ASA)
- Firepower Threat Defense (FTD)
- FortiOS SSL VPN

These attacks frequently utilized zero-days or recently disclosed vulnerabilities that had not yet been patched. The motivations behind these attacks typically included espionage, data theft, and sometimes the disruption of critical services, particularly in sectors heavily reliant on remote access. Specific examples include:

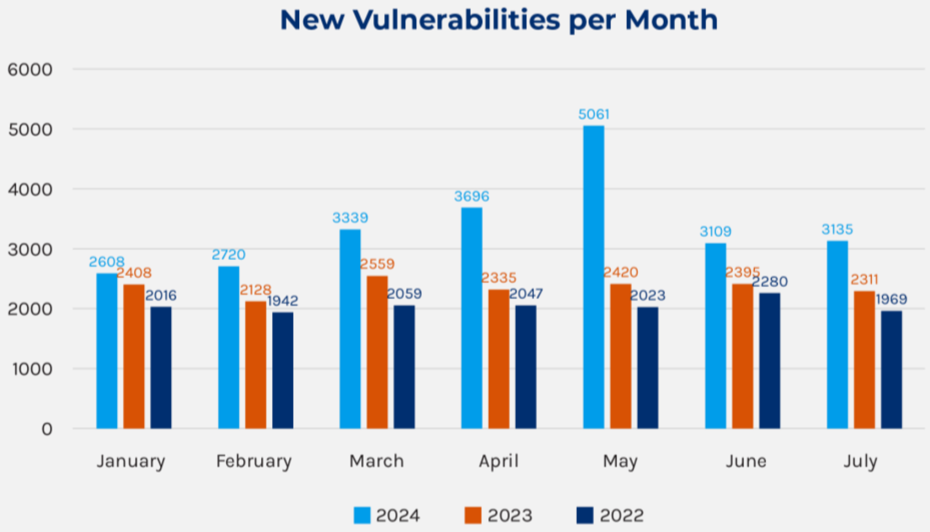
- Chinese APTs, such as Volt Typhoon, exploiting FortiOS SSLVPN vulnerabilities for initial access and deploying custom malware on over 20,000 devices worldwide, including a Dutch military network.
- The ArcaneDoor campaign, attributed to STORM-1849, which gained unauthorized access to government networks worldwide via Cisco's SSL VPN services.
- The Chinese group RedJuliett exploiting known vulnerabilities in firewalls, VPN appliances, and load balancers to gain initial access into Taiwanese organizations for intelligence gathering.

In response to this wave of attacks, CISA released a guide on "modern approaches to network access security" discussing how organizations can replace VPNs with solutions like SASE. Similarly, Norway's cybersecurity center recommended that organizations replace their SSL VPN solutions with alternatives using IPsec.

3. Statistics

3.1. Vulnerabilities

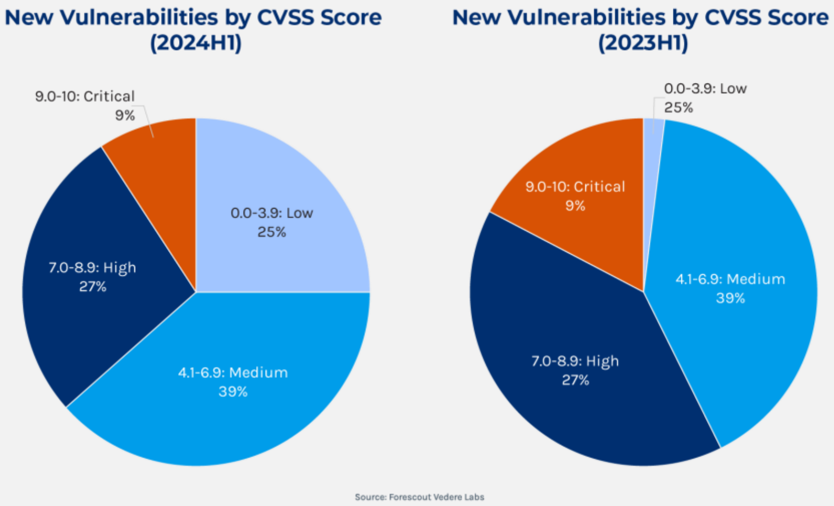
In the first half of 2024, there were 23,668 vulnerabilities published, averaging 111 new CVEs per day or 3,381 per month. This represents an increase of 7,112 vulnerabilities compared to the same period last year, a rise of 43%. Figure 1 provides a monthly breakdown of vulnerabilities published in 2024, 2023 and 2022.



Source: Forescout Vedere Labs

Figure 1 – New vulnerabilities per month

A significant difference compared to last year is that the majority of vulnerabilities in 2024H1 had either a medium (39%) or low (25%) CVSS score, while only 9% had a critical score. Last year, most vulnerabilities had either a medium or high score. Figure 2 illustrates the distribution of new vulnerabilities by CVSS score.



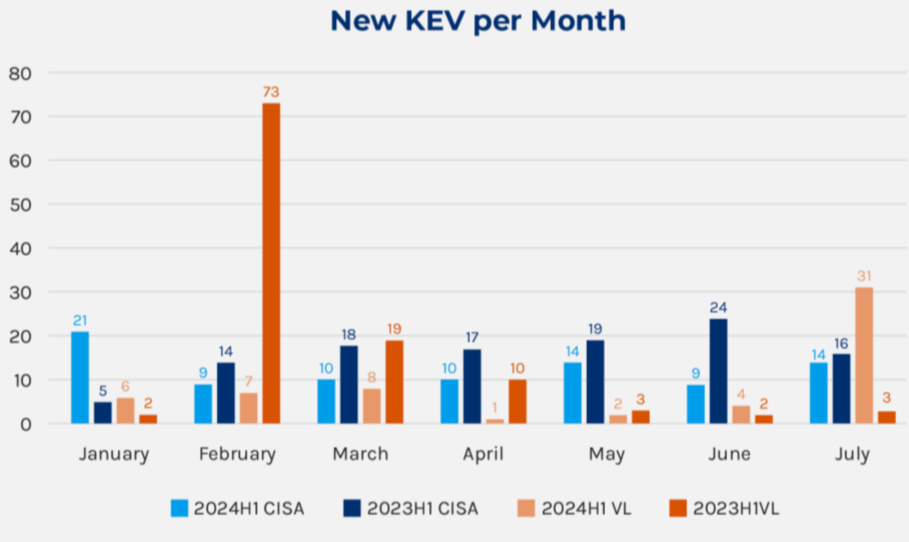
Source: Forescout Vedere Labs

Figure 2 – New vulnerabilities by CVSS score

During the same period:

- 87 CVEs were added to CISA's Known Exploited Vulnerabilities (KEV) catalog, bringing the total to 1,140 vulnerabilities. This marks a reduction of 26 CVEs compared to the same period in 2023, a decrease of 23%.
- 59 vulnerabilities were added to the Vedere Labs KEV (VL KEV) catalog, bringing the total to 338 vulnerabilities. This marks a reduction of 53 CVEs compared to the same period in 2023, a decrease of 47%.

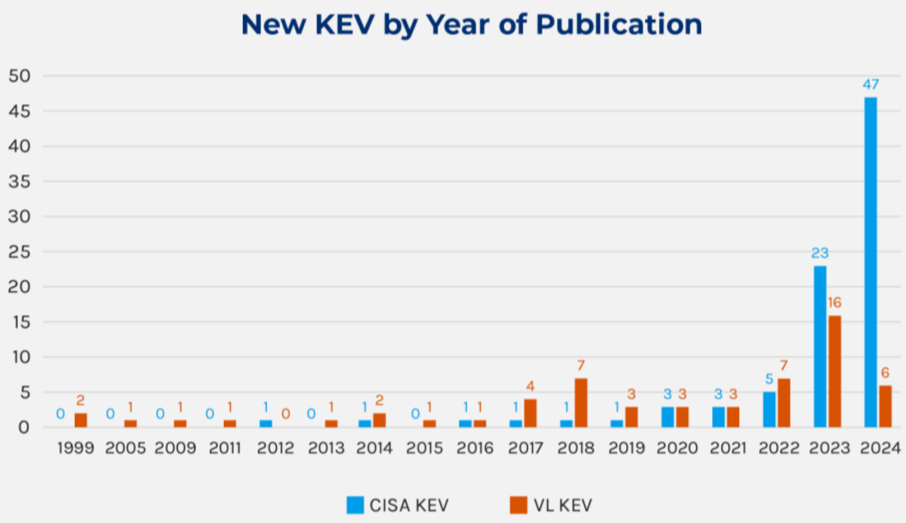
Figure 3 shows a monthly breakdown of new vulnerabilities added to CISA and VL KEV. On average, 12 new vulnerabilities were added to CISA KEV and 8 to VL KEV per month in 2024H1.



Source: Forescout Vedere Labs

Figure 3 – New known exploited vulnerabilities per month

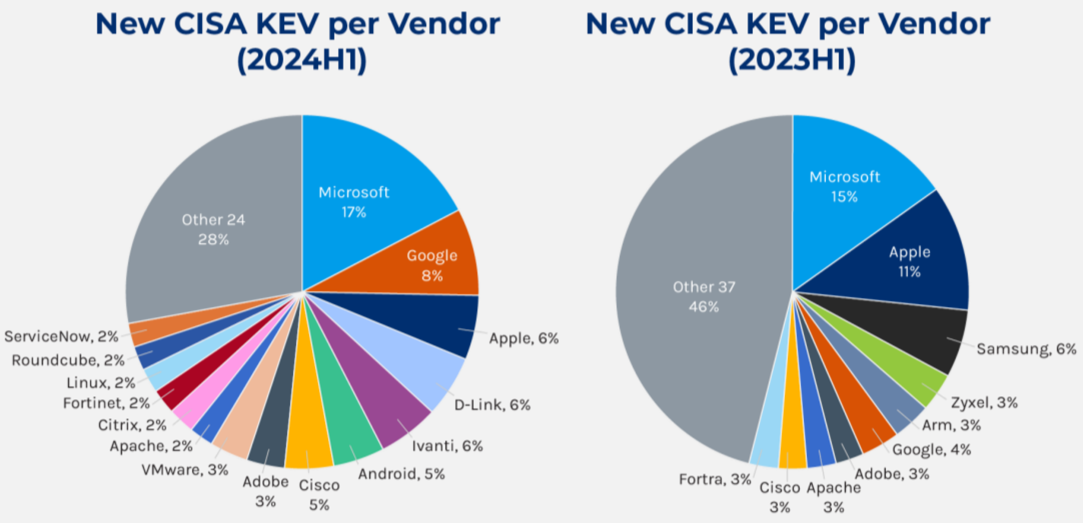
Figure 4 reveals that 46% of the new additions to CISA KEV were vulnerabilities published before 2024. Additionally, five of the new vulnerabilities affect end-of-life products: CVE-2012-4792, CVE-2014-100005, CVE-2021-40655, CVE-2024-3272 and CVE-2024-3273. These vulnerabilities affect Internet Explorer, D-Link routers and network attached storage products, which means no patches are available for this equipment. For VL KEV, 53 vulnerabilities (90%) originated prior to 2024.



Source: Forescout Vedere Labs

Figure 4 – New known exploited vulnerabilities by year of publication

Figure 5 shows that the new vulnerabilities in the CISA KEV catalog affected 39 different vendors, a 17% decrease from the 47 in 2023H1. Out of these, 15 vendors had more than one vulnerability added to the list.



Source: Forescout Vedere Labs

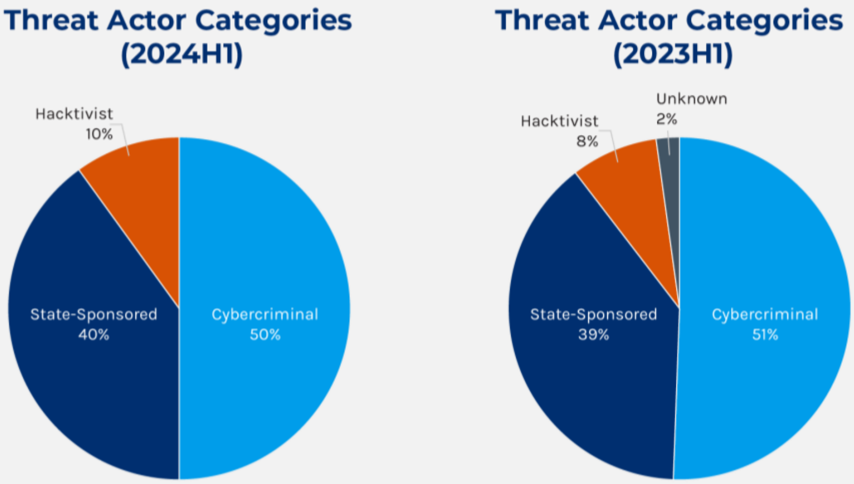
Figure 5 – New known exploited vulnerabilities per vendor

The trend of exploits targeting perimeter and network infrastructure devices, first noted in 2023H1 has increased. In 2024H1, 15 new CVEs in the KEV catalog targeted network infrastructure and security appliances from vendors such as Ivanti, Citrix, Fortinet, Cisco, Palo Alto Networks, Check Point and D-Link. This accounts for nearly one in every five new vulnerabilities added to KEV. This trend also supports our recent finding that routers and wireless access points are the riskiest IT devices in 2024.

Interestingly, a vulnerability we reported as being exploited by botnets in our 2023H1 report, CVE-2019-7256 which affects Linear eMerge physical access control solutions, was only added to CISA KEV almost a year later in March, 2024. Another significant vulnerability added to KEV in 2024H1 was CVE-2023-48788 which affects FortiClient EMS. We tracked the exploitation of this CVE as part of the Connect:fun campaign, which used it to deliver a remote management tool to its targets. Out of the 59 new vulnerabilities in VL KEV, 18 were also added to CISA KEV (30%).

3.2. Threat Actors

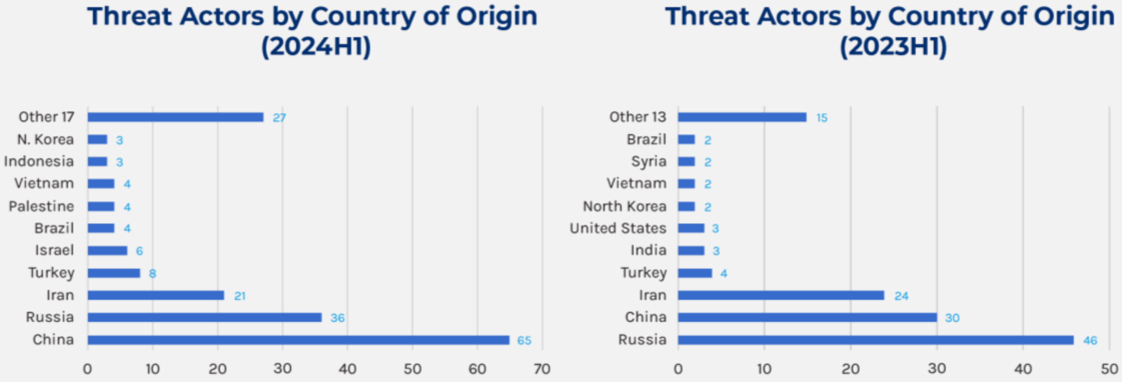
Forescout Research – Vedere Labs tracks information on 740 threat actors, with 387 (52%) having updates in 2024H1. The live information about all threat actors is available on our website. As shown in Figure 6, these 387 actors are predominantly cybercriminals (50%), including ransomware groups, followed by state-sponsored actors (40%) and hacktivists (10%). This distribution remains largely unchanged since 2023H1.



Source: Forescout Vedere Labs

Figure 6 – Threat actor categories. Source – Forescout Research Vedere Labs

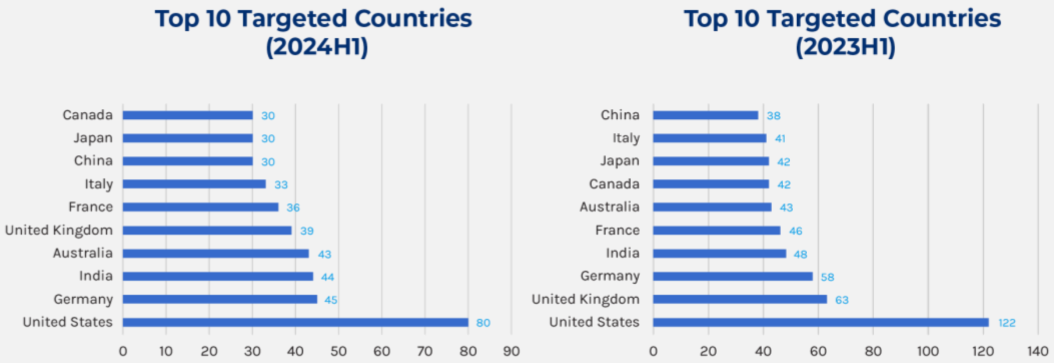
Figure 7 shows that most of these threat actors originate from China, Russia and Iran. Notably, China has surpassed Russia in the rankings, and Palestine and Israel have appeared on the list. In 2024H1, CISA has released four alerts related to Chinese actors, highlighting their targeting of small office and home (SOHO) routers, their use of living-off-the-land techniques, and two alerts concerning the Volt Typhoon group's access to US critical infrastructure. In contrast, the agency only issued one alert about Russian actors, one for North Korean and none for Iranian actors.



Source: Forescout Vedere Labs

Figure 7 – Threat actors by country of origin

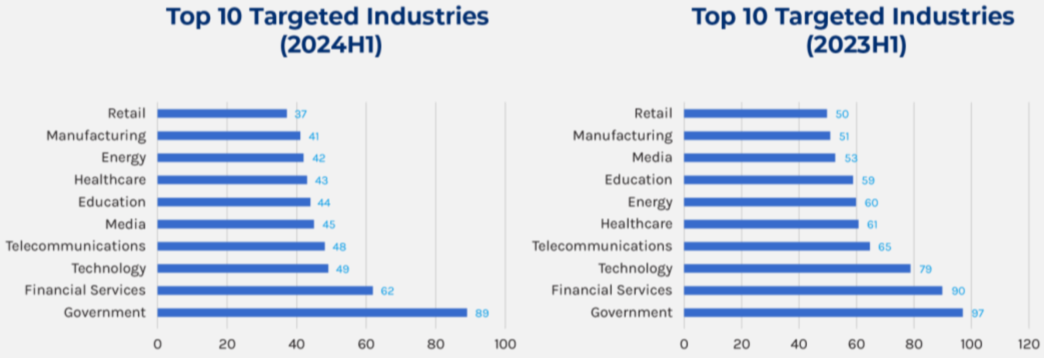
These threat actors have targeted over 150 countries, with the US, Germany and India being the primary targets, as shown in Figure 8. While these countries were also in the top 10 last year, a noticeable change is that the UK, previously the second most popular target, has now dropped to fifth place.



Source: Forescout Vedere Labs

Figure 8 – Top 10 targeted countries (by number of threat actors)

The top 10 targeted industries, shown in Figure 9, remain the same as last year, with minor shifts in ranking (for instance, healthcare used to be fifth and is now seventh).

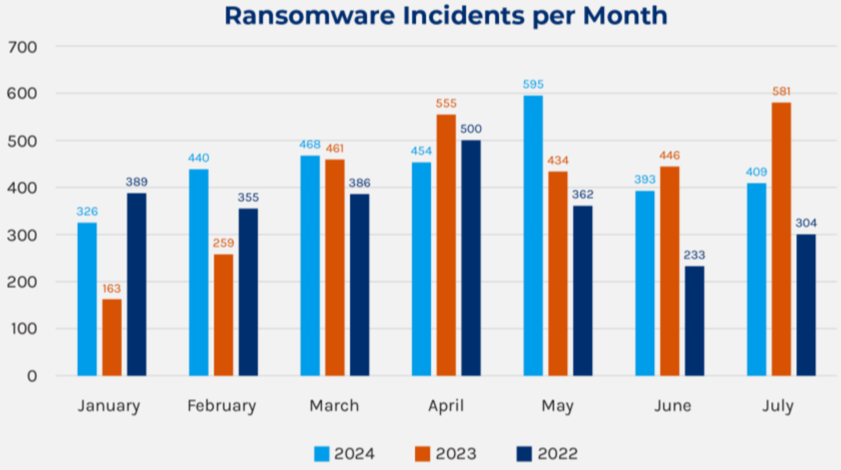


Source: Forescout Vedere Labs

Figure 9 – Top 10 targeted industries (by number of threat actors)

3.3. Ransomware

Through open-source tracking of ransomware leak sites, we observed 3,085 attacks in 2024H1, an increase from 2,899 during the same period last year (an increase of 6%). This averages to 441 attacks per month or 15 per day.

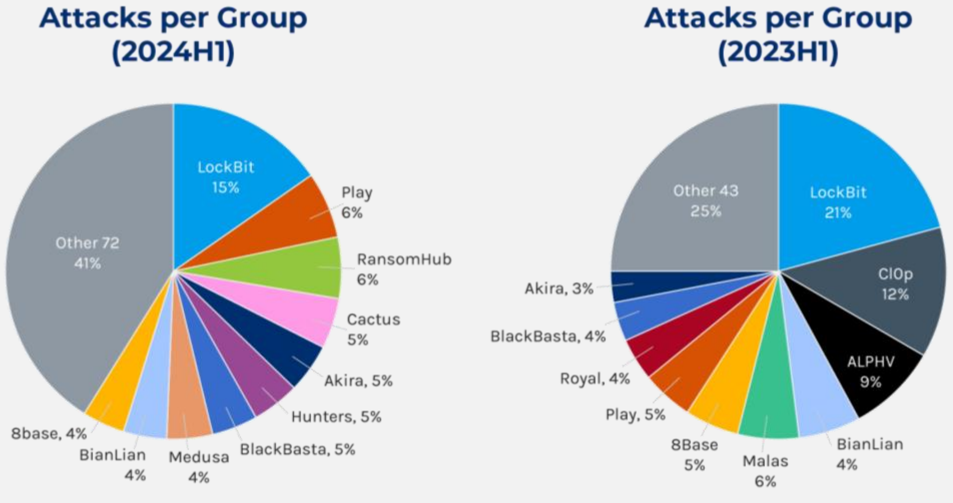


Source: Forescout Vedere Labs

Figure 10 – Ransomware incidents per month

Figure 11 shows the number of attacks per ransomware group in 2024H1 and 2023H1. LockBit remains the most active group, despite a significant law enforcement operation in February this year. Other groups remaining in the top 10 are Play, BlackBasta, 8Base, Akira and BianLian. Among the new groups in the top 10, RansomHub has experienced rapid growth and was recently analyzed by our team.

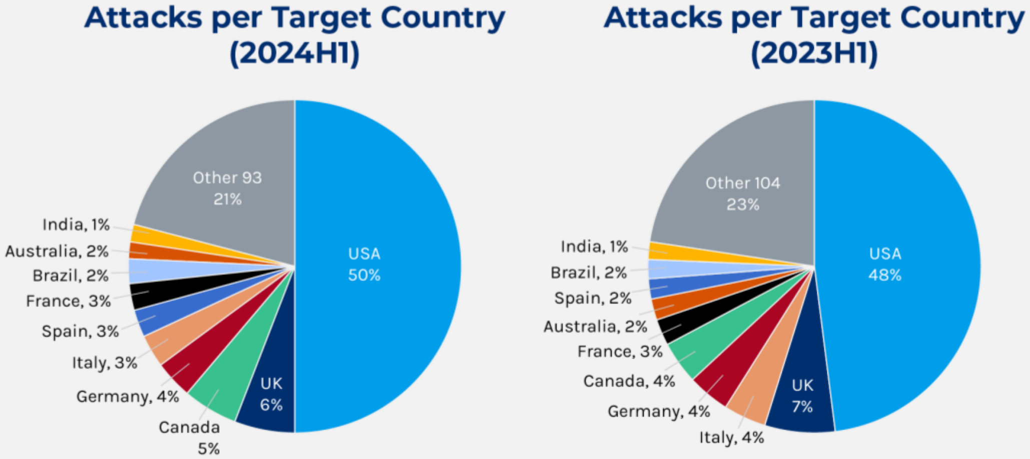
Overall, the ransomware landscape has continued to fragment and expand. While last year the top 10 groups accounted for three-quarters of attacks, they now only represent 59%. Concurrently, the number of active groups increased from 53 to 82, marking a 55% rise.



Source: Forescout Vedere Labs

Figure 11 – Ransomware incidents per group

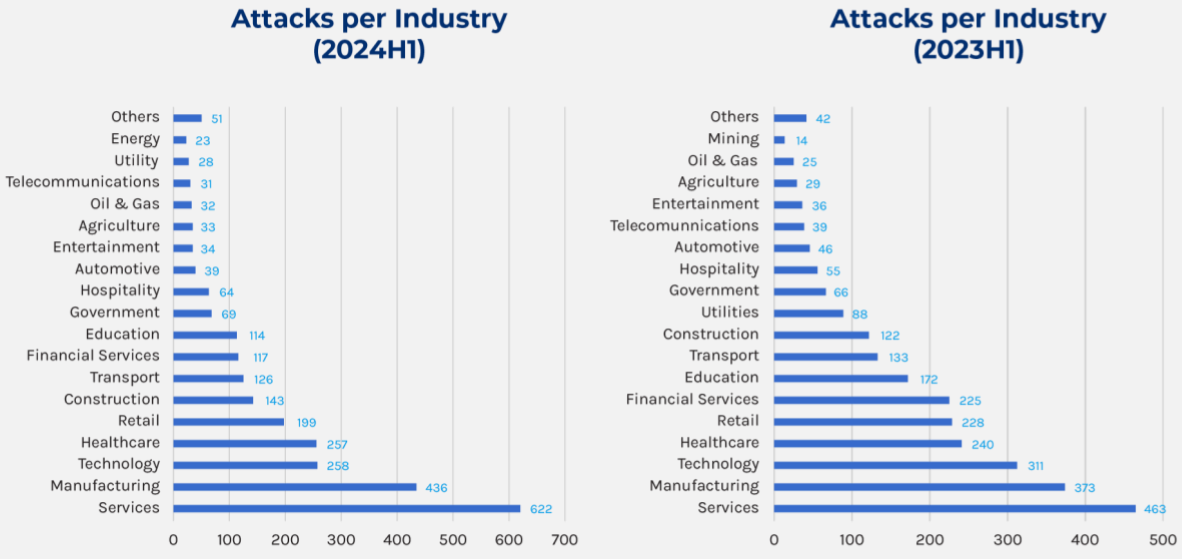
While ransomware perpetrators are increasing and fragmenting, the list of countries where ransomware victims are located is decreasing and consolidating. In 2024H1, the top 10 targeted countries suffered 79% of all attacks, up from 77% last year. The U.S. alone accounted for half of all attacks, an increase from 48% the previous year. Overall, there were ransomware victims in 103 countries, a 10% decrease from the 114 countries in 2023H1. All the countries that were in the top 10 last year remained on the list this year.



Source: Forescout Vedere Labs

Figure 12 – Ransomware incidents per target country

Figure 13 illustrates the industry verticals most targeted by ransomware in 2024H1, showing little change from the previous period. The top 5 industries remained identical and in the same order: services, manufacturing, technology, healthcare and retail.



Source: Forescout Vedere Labs

Figure 13 – Ransomware incidents per target industry

4. Mitigation Recommendations

We encourage organizations to **prioritize extending** visibility, risk assessment **and proactive controls to cover the increased attack surface of VPNs and network perimeter assets and appliances being exploited.** In addition, we urge organizations to follow specific recommendations for disconnecting internet-exposed operational technology and replacing SSL VPNs**.**

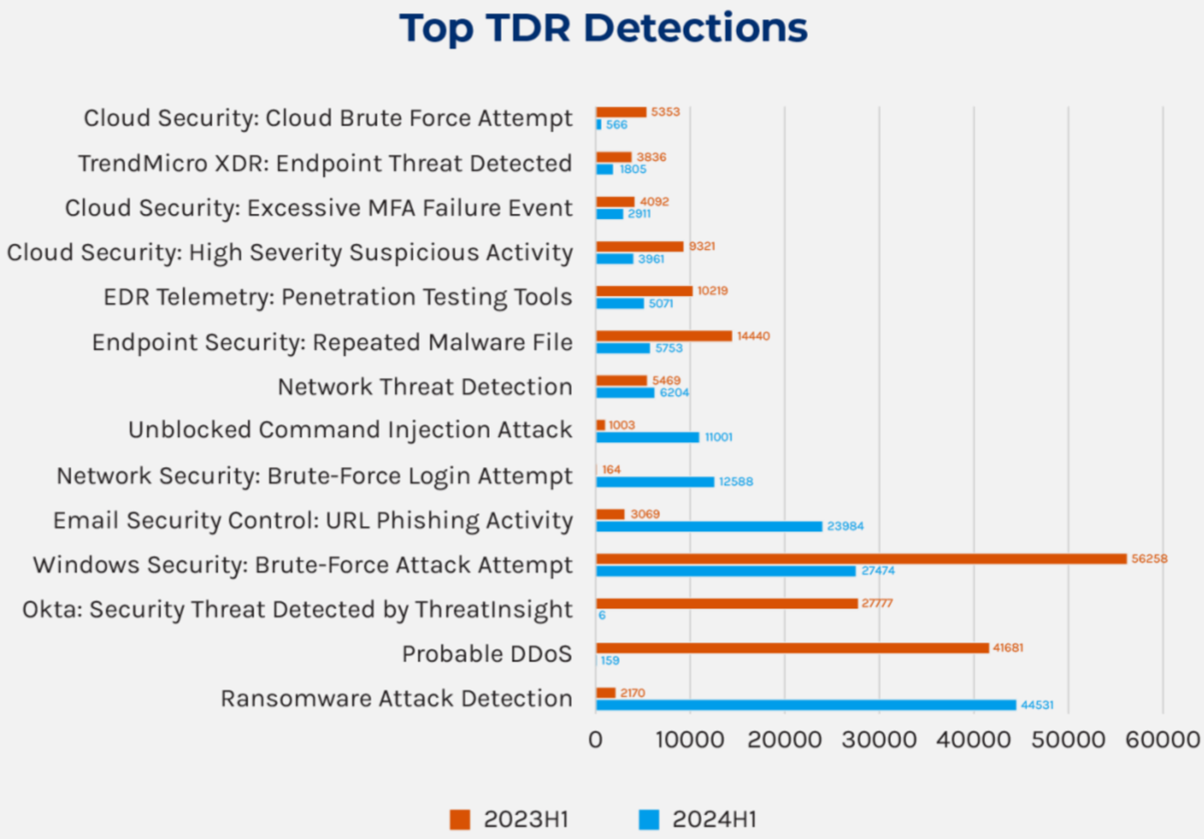
At a minimum, you should:

- Ensure proper visibility into these devices, including their presence on the network, the software they run, and their communication patterns. This can be achieved with agentless solutions.
- Understand their risk profile concerning vulnerabilities, weak configurations, exposure and other factors.
- Disable unused services and patch vulnerabilities to prevent exploitation.
- Change default or easily guessable credentials and use strong, unique passwords for each device.
- Enforce Multi-factor Authentication (MFA) whenever possible to add an additional layer of security, especially for VPN authentication processes.
- Avoid exposing unmanaged devices directly to the internet, except in rare cases. Ensure administrative interfaces (such as web UIs and engineering ports) on connected devices require authentication and are secured behind IP-based access control lists or a VPN-protected management VLAN.
- Enable IP-based access control lists for specific protocols, such as Modbus for OT networks.
- Segment the network to isolate IT, IoT and OT devices, limiting network connections to only authorized management and engineering workstations or among unmanaged devices that need to communicate.

After implementing these proactive controls, ensure that threat detection and response systems encompass every device within the whole organization. Since threats now move from one type of device to another, it is crucial to detect them throughout the entire organization – from an entry point such as a vulnerable router, to a pivot point, like a misconfigured workstation, and finally to a target such as an insecure OT device. Ensure your threat detection solution covers all device types and ingests multiple data sources, including firewalls, intrusion detection systems, endpoint detection and response (EDR), and other security tools.

Forescout Threat Detection & Response (TDR) collects telemetry and logs from a wide range of sources, some of which contain indications of possible malicious activity. TDR correlates these attack signals to generate high-fidelity detections for analyst investigation and enables automated response actions across the enterprise.

Figure 14 shows the most common Forescout TDR detections in customer networks in 2024H1 and 2023H1, based on nearly 400,000 individual detections. While many of the detections remained consistent, such as brute force attempts, there was a notable decrease in DDoS and credential-based detections (such as Okta-related incidents). Conversely there was an increase in command injection detections, reflecting the shift in threat actors' focus towards exploiting vulnerabilities in unmanaged devices.



Source: Forescout Vedere Labs

Figure 14 – Top 10 malicious activity detections

© 2024 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products or service names may be trademarks or service marks of their respective owners.