FORESCOUT RESEARCH | VEDERE LABS

2023H1 Threat Review

Vulnerabilities, Threat Actors and Malware

Author: Daniel dos Santos

Date: September 6, 2023

Contents

1. Executive summary

In the first half of 2023, Forescout Vedere Labs has published numerous blog posts and reports sharing analyses of prominent vulnerabilities, threat actors and malware. We also published a 2022 threat roundup summarizing our data from last year and highlighting the emergence of mixed IT/IoT threats, such as botnets that allow lateral movement from an infected IoT entry point to a vulnerable IT network.

In this report, we look back at the research we published in the period of January 1 to July 31, 2023 (2023H1) as well as other important events and data that we have not covered in the same period to emphasize the evolution of the threat landscape.

Key findings of this report include:

- There were 16,556 new vulnerabilities published, an average of 78 new CVEs per day or 2,365 per month. That is 2,220 more than in the same period of last year, an increase of 15%. Most of these new vulnerabilities had either medium (41%) or high (40%) CVSS scores, while 17% (2,879) had a critical score.
- There were 113 CVEs added to CISA's Known Exploited Vulnerabilities (KEV) catalog, which brought the catalog to a total of 981 vulnerabilities (a 13% increase). An average of 16 new vulnerabilities were added per month. Most of these newly exploited vulnerabilities (52%) were not published in 2023. There was a vulnerability added from 2004 and four vulnerabilities added that affect end-of-life products.
- There were updates about 182 threat actors. These are mostly cybercriminals (51%), including ransomware groups, followed by state-sponsored actors (39%) and hacktivists (8%). These actors come mostly from Russia (25%), China (16%) and Iran (13%).
- These threat actors have targeted more than 150 countries. The top targets were the U.S. (67% of actors), the U.K. (35%) and Germany (32%). The top targeted industries were government (53% of actors), financial services (49%) and technology (43%).
- We observed 2,809 ransomware attacks, up from 2,526 in the same period last year (an increase of 11%). That is an average of 401 attacks per month or 13 per day.
- Some well-known ransomware gangs remain very active even after one year, such as LockBit, Cl0p and ALPHV, but other groups that were relevant last year have disappeared, such as Conti and Hive, due to internal conflicts, law enforcement takedowns or by rebranding to stay under the radar. Entirely new groups now also figure among the most active, such as Malas and 8Base. Overall, the ransomware landscape is more fragmented this year with 53 groups reporting attacks, 36% more than the 39 groups in the same period last year.
- Ransomware victims were located in more than 100 countries, but almost half (48%) are in the U.S., followed by several European countries (26% in total). The other roughly 25% are spread across the world. The services industry was the top target, with 16% of attacks, followed by manufacturing (13%) and technology (11%). Other top targets include healthcare, retail, financial services and education.
- State-sponsored actors have been busy with growing geopolitical tensions. They are showing a preference for network infrastructure devices such as routers, firewalls and VPN appliances to carry out initial access and espionage operations. State-sponsored ransomware operations also continue to be active.
- Hacktivist groups continue operating with many of the same methods we reported as growing in 2022: geopolitical motivations, communication over X (formerly known as Twitter) or Telegram channels and a split between DDoS-focused groups and those intending to cause physical damage by leveraging unmanaged devices, such as IoT and OT.
- IoT botnets such as Mirai have been adding a host of new exploits to take over vulnerable devices. That includes traditional DVRs and routers, but also firewalls, solar power generation monitoring systems, building automation systems and even IT software such as web servers.
- Adversary infrastructure relies heavily on repurposing legitimate tools, such as Cobalt Strike and Metasploit. Many recently popular tools, such as Sliver and Mythic C2s and the xmrig cryptominer, are open source.

2. Vulnerabilities

In the first half of 2023, Forescout Vedere Labs disclosed eight new CVEs:

- On February 13, two CVEs affecting Schneider Electric Modicon PLCs. These vulnerabilities were used as part of a systematic study into how attackers can move laterally between different network segments and types of networks at the controller level of OT networks, which we called Deep Lateral Movement.
- On May 2, three CVEs affecting the FRRouting Border Gateway Protocol (BGP) implementation. These vulnerabilities showed that modern BGP implementations still have low-hanging fruit that can be abused by attackers.
- On June 15, three CVEs affecting industrial controllers and power meters. These vulnerabilities concluded the year-long OT:ICEFALL project, which in total disclosed 61 CVEs affecting OT devices. The project also concluded with lessons about OT security design and patch quality.

Beyond our own research, there were 16,556 new vulnerabilities published during the study period. That is an average of 78 new CVEs per day or 2,365 per month. That is also 2,220 more vulnerabilities than in the same period of last year, which represents an increase of 15%. Figure 1 shows a breakdown of new vulnerabilities published per month in 2023 and 2022.

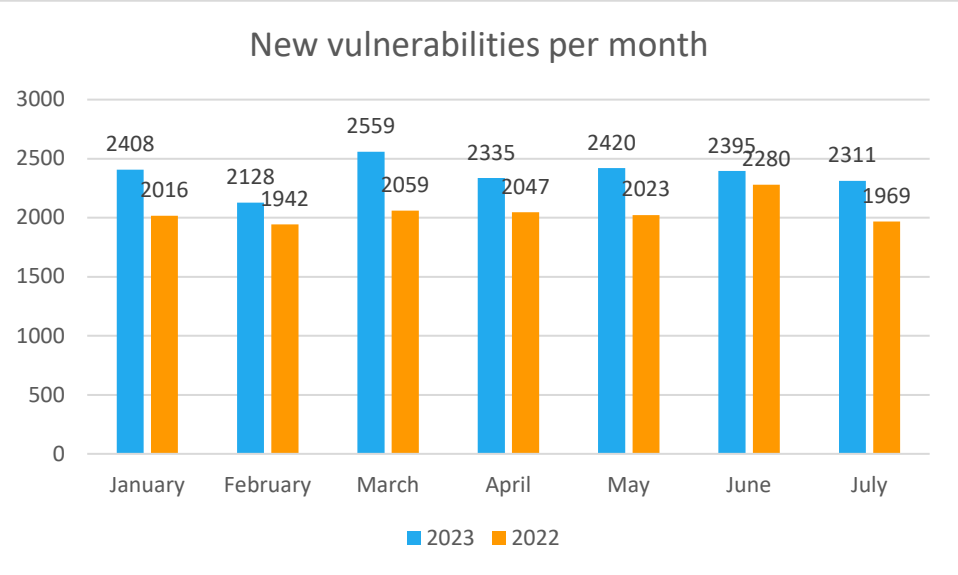


Figure 1 – New vulnerabilities per month

Most of these new CVEs had either medium (41%) or high (40%) CVSS scores, while 17%, a total of 2,879, had a critical score. Figure 2 shows the distribution of new vulnerabilities per CVSS score.

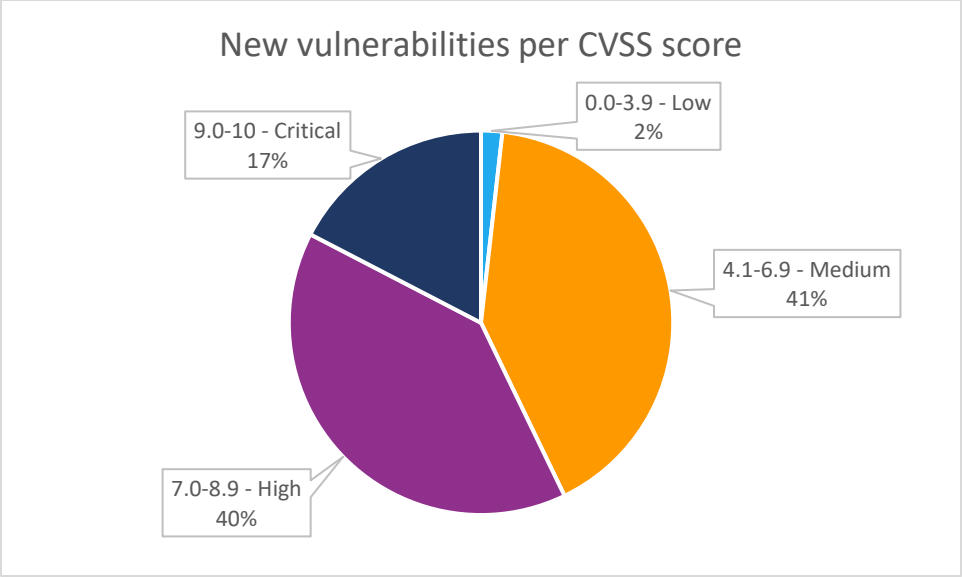


Figure 2 – New vulnerabilities per CVSS score

CVSS scores do not directly indicate likelihood of exploitation, though. In the same period, 113 CVEs were added to CISA's Known Exploited Vulnerabilities (KEV) catalog, which brought the catalog to a total of 981 vulnerabilities (a 13% increase). Figure 3 shows a breakdown of new vulnerabilities added to KEV each month. An average of 16 new vulnerabilities were added per month.

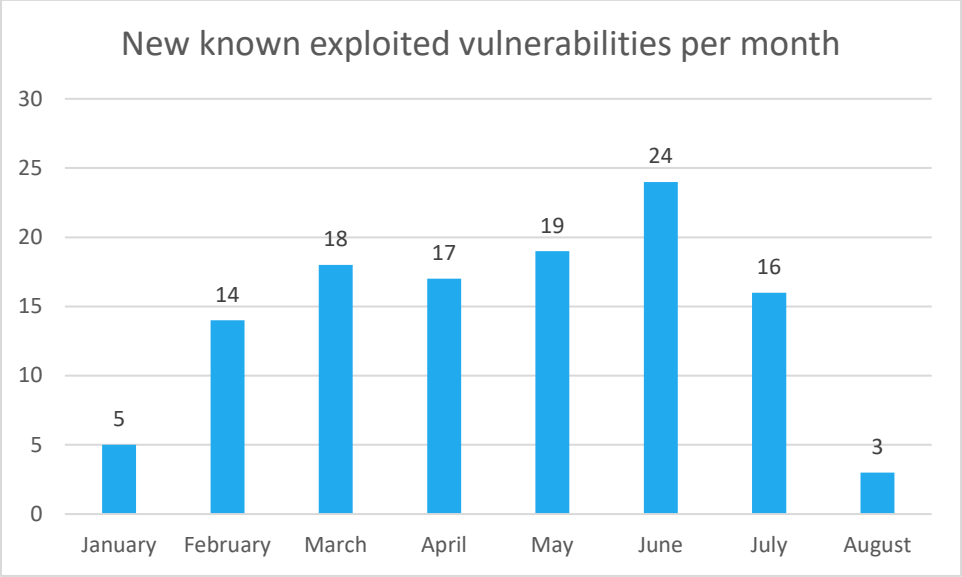


Figure 3 – New known exploited vulnerabilities per month

Figure 4 shows that although many of these newly exploited vulnerabilities were published in 2023 (48%), most were not. In fact, there was even a vulnerability added from 2004: CVE-2004-1464, a denial of service affecting routers running Cisco IOS. Four vulnerabilities also affect products that are end-of-life: CVE-2013-3163 affecting Internet Explorer, CVE-2023-25717 affecting multiple Ruckus Wireless products and two CVEs affecting the Linux Kernel, which means that there are no patches available for these products.

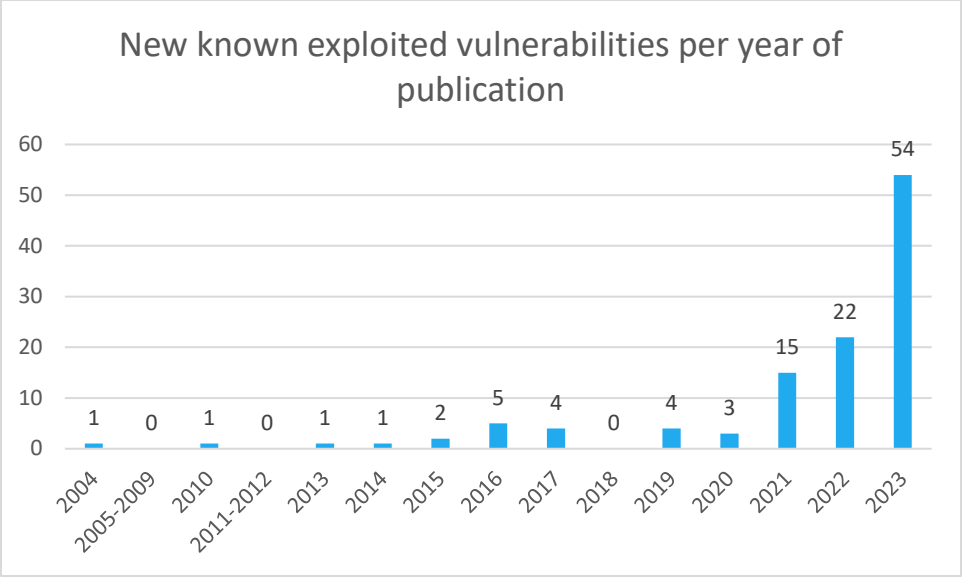


Figure 4 – New exploited vulnerabilities per year of publication

Figure 5 shows that the new vulnerabilities in the KEV affected 47 different vendors, with 21 (45%) having more than one vulnerability added to the catalog and the top 10 being responsible for 54% of the new vulnerabilities.

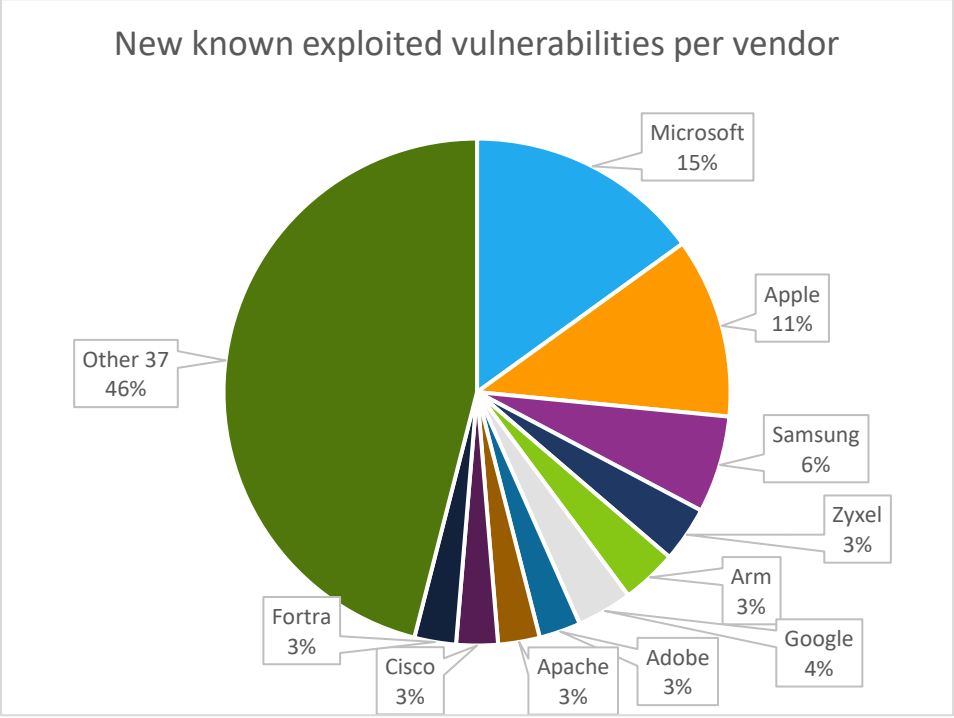


Figure 5 – New known exploited vulnerabilities per vendor

Although most new vulnerabilities in the KEV affect traditional IT software, such as Microsoft Windows, Office and Exchange, 13 CVEs (11%) affect network infrastructure devices such as routers, firewalls and gateways. The latter includes CVE-2023-27997 which impacts Fortinet VPN devices and was added to the KEV in June. That vulnerability alone is expected to affect more than 300,000 exposed devices worldwide.

This is representative of an ongoing wave of exploitation of network infrastructure devices. CISA also released an advisory in August listing the most exploited vulnerabilities in 2022. The advisory shows that CVE-

2018-13379, also affecting Fortinet VPN devices, continues to be exploited consistently since at least 2020. Other routinely exploited CVEs affecting networking infrastructure include:

- F5BIG-IP – CVE-2022-1388 and CVE-2020-5902
- SonicWALL – CVE-2021-20016, CVE-2021-20038 and CVE-2021-20021
- Fortinet – CVE-2022-42475 and CVE-2022-40684

Beyond networking equipment, another type of device being routinely exploited is network attached storage (NAS). CVE-2022-27593 affecting QNAP NAS devices figured on the 2022 most exploited list and CVE-2023-27992 affecting Zyxel NAS devices was added to the KEV.

3. Threat Actors

Forescout Vedere Labs tracks information about 464 threat actors, of which 182 (39%) had updates in 2023H1. Figure 6 shows that these 182 actors are mostly cybercriminals (51%) – including ransomware groups – followed by state-sponsored actors (39%) and hacktivists (8%). Figure 7 shows that these actors come mostly from Russia (25%), China (16%) and Iran (13%).

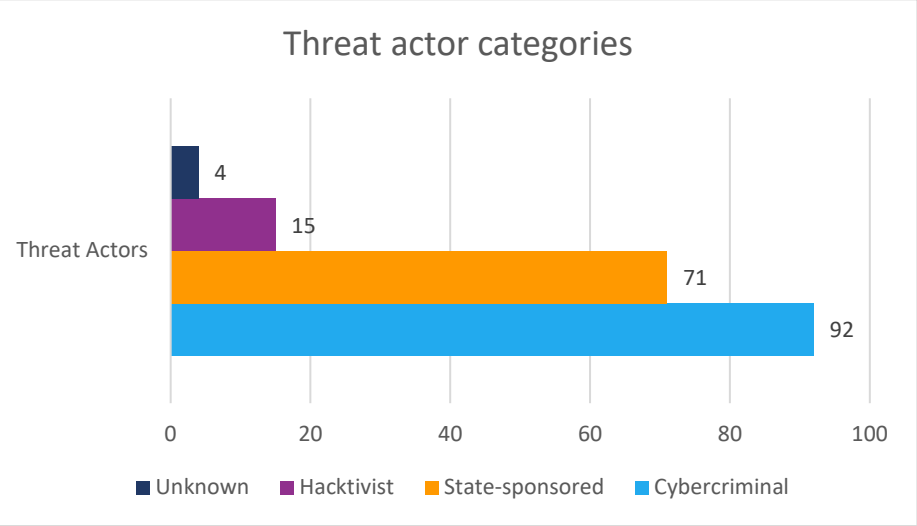


Figure 6 – Threat actor categories

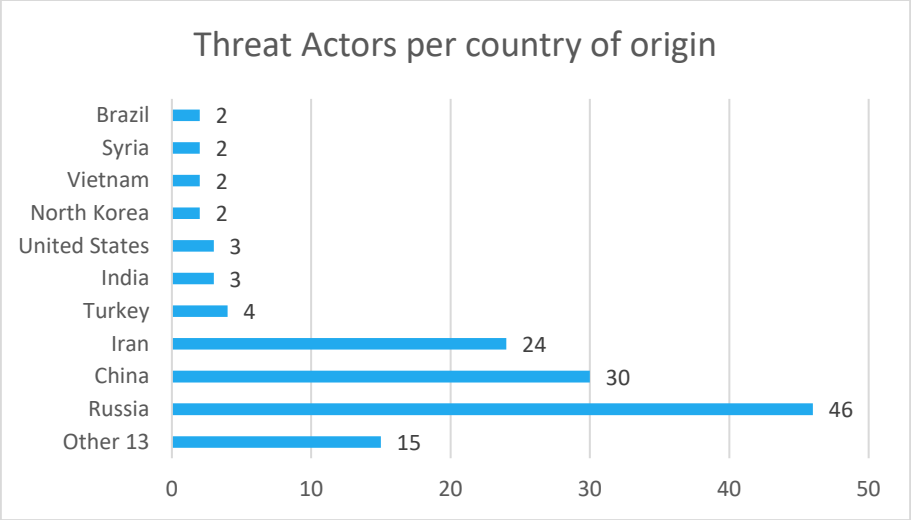


Figure 7 – Threat actors per country of origin

These threat actors have targeted more than 150 countries, but Figure 8 shows that the top targets were the U.S. (67% of actors), the U.K. (35%) and Germany (32%). At the same time, the top targeted industries – shown in Figure 9 – were government (53% of actors), financial services (49%) and technology (43%).

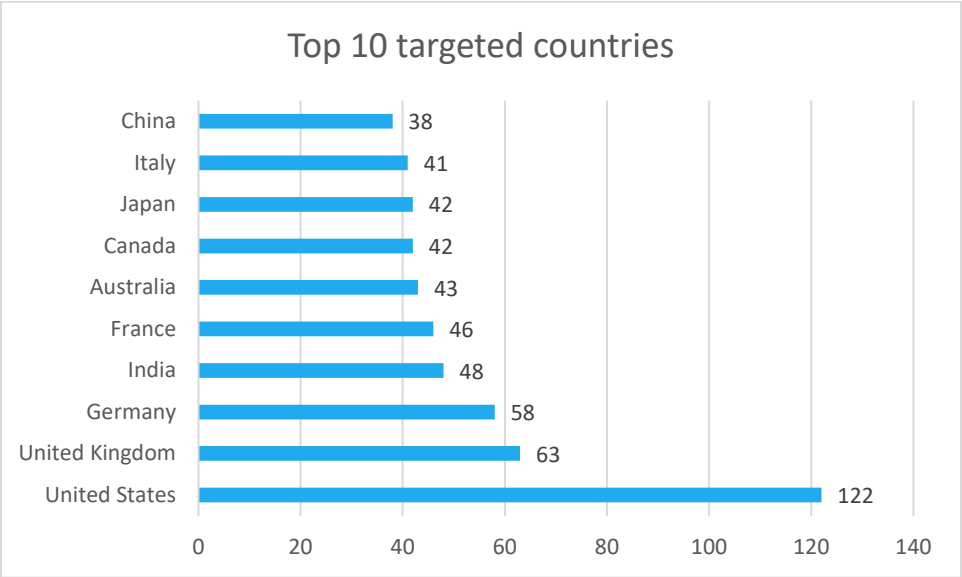


Figure 8 – Top 10 targeted countries (by number of threat actors)

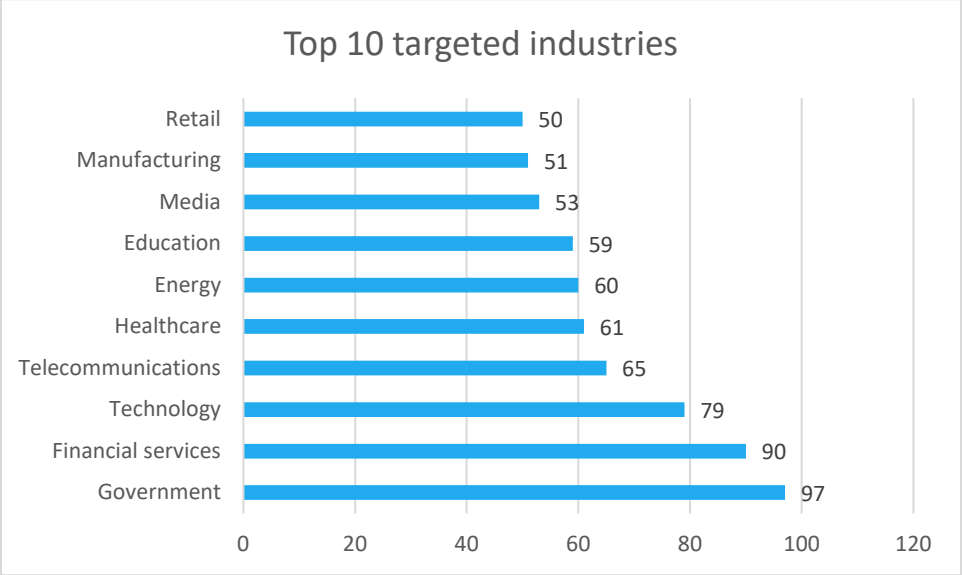


Figure 9 – Top 10 targeted industries (by number of threat actors)

Below we discuss in more detail some of the relevant activities for each category of threat actor.

3.1. Cybercrime/Ransomware

Two ongoing trends in cybercrime are the use of residential proxies and infostealers, while ransomware continues to be a top threat.

Residential proxies are services that allow a user to connect to a network and use a residential device running "proxyware" as an exit node. Proxyware can be either distributed as a legitimate application, where a user chooses to share their network bandwidth ,or it can be installed without the user's knowledge, effectively as malware that allows malicious actors to proxy their connections. Proxyware typically runs on computers, but the

most notable discovery of 2023H1 was AVrecon, a botnet infecting small office and home routers with malware to enlist them as residential proxies for the SocksEscort service. Another interesting discovery was a campaign targeting vulnerable SSH servers to deploy Docker containers that enroll victims in proxy networks such as Peer2Proxy and Honeygain.

Infostealer malware is used to harvest login items such as cookies, credentials and session tokens as well as cryptocurrency wallets and credit card information from victims, which are then typically packaged as "logs" and sold in dark web marketplaces. This type of malware is usually distributed as a service, sold via a monthly subscription that provides access to command-and-control servers. Infostealers have been around for years, but they became very prominent in 2022 and continued to grow in 2023. The most popular infostealers are Raccoon, RedLine and Vidar, but in 2023H1 we observed rising popularity of infostealers developed more recently, such as Mystic, Aurora, Misha and Titan. An interesting newcomer was the RedEnergy stealer, which combines infostealer capabilities with a ransomware module.

Ransomware continues to be among the most lucrative and active cybercriminal activities. In 2023H1, Forescout Vedere Labs reported on the activities of emerging ransomware groups such as Royal, discussed popular ransomware targets such as virtualization servers and analyzed vulnerabilities being massively exploited by these groups, such as CVE-2023-34362, used by Cl0p to breach into hundreds of organizations, exfiltrate sensitive data and publish it. Finally, we analyzed the most common TTPs of ransomware groups and how these groups tend to follow similar patterns while allowing for evolution, such as an increased use of vulnerability exploitation for initial access, including 0-days.

Via open-source tracking of ransomware leak sites, we observed 2,809 attacks in 2023H1, up from 2,526 in the same period last year (an increase of 11%). That is an average of 401 attacks per month or 13 per day.

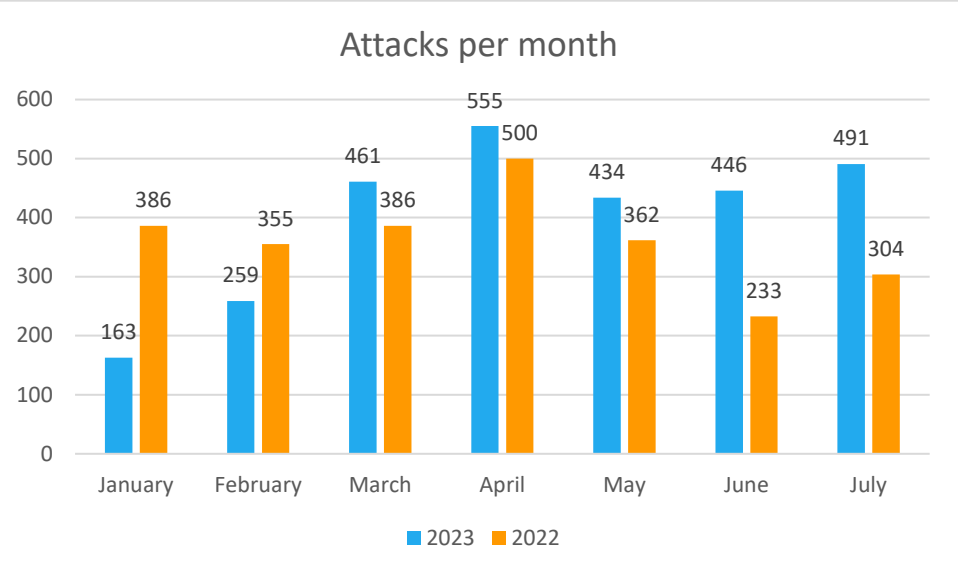
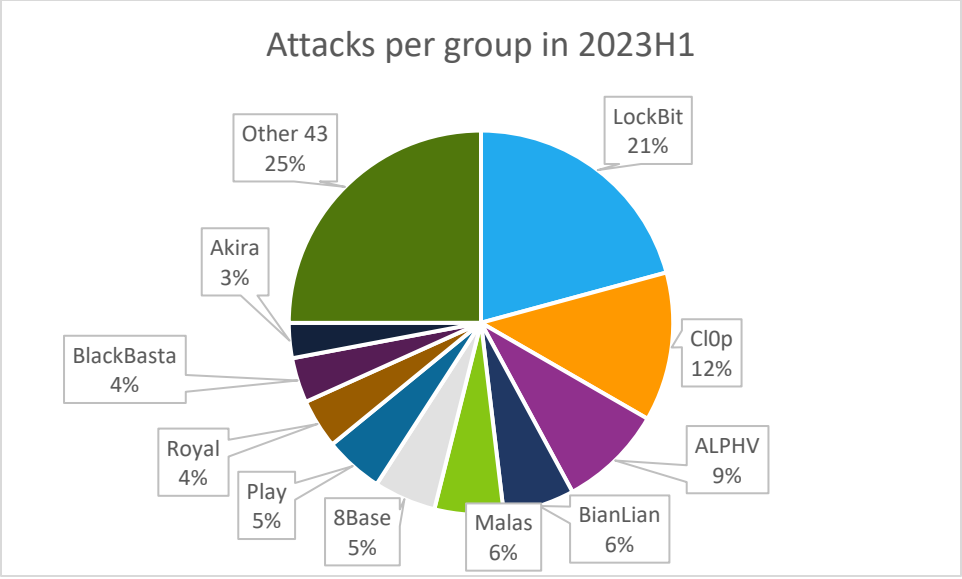


Figure 10 – Ransomware attacks per month in 2023H1

Figure 11 shows the number of attacks per ransomware group in 2023H1 and 2022H1. Some well-known names remain at the top even after one year, such as LockBit, Cl0p and ALPHV, but other groups that were very relevant last year have disappeared, such as Conti and Hive, due to internal conflicts, law enforcement takedowns or by rebranding to stay under the radar. At the same time, entirely new groups figure among the most active, such as Malas and 8Base. Overall, the ransomware landscape is more fragmented this year with 53 groups reporting attacks, 36% more than the 39 groups in the same period last year.



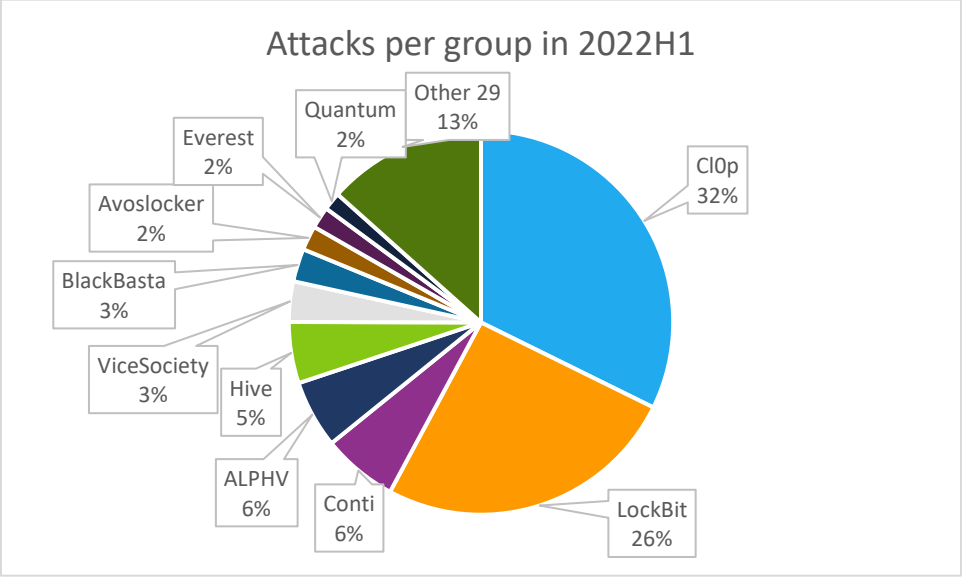


Figure 11 – Attacks per ransomware group in 2023H1 and 2022H1

Figure 12 shows the distribution of countries where the organizations targeted by ransomware are located. Ransomware victims were located in more than 100 countries, but almost half (48%) are in the U.S., followed by several European countries (26% in total). The other roughly 25% are spread across the world.

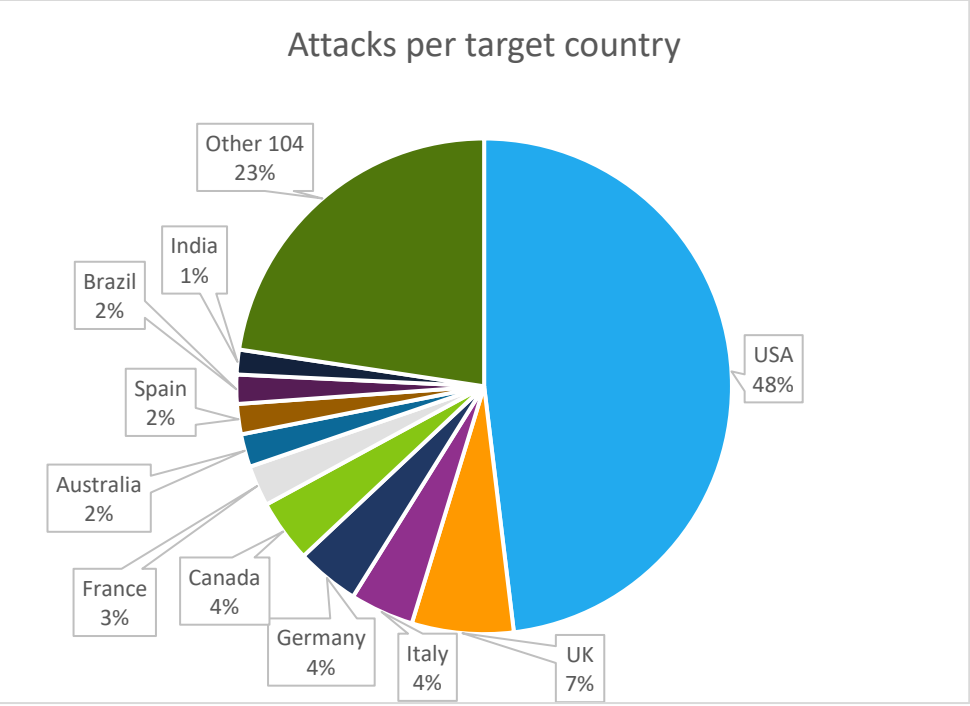


Figure 12 – Ransomware attacks per target country

Figure 13 shows the industries most targeted by ransomware in 2023H1. The services industry was the top target in the period, with 16% of attacks, followed by manufacturing (13%) and technology (11%). Other top targets include healthcare, retail, financial services and education.

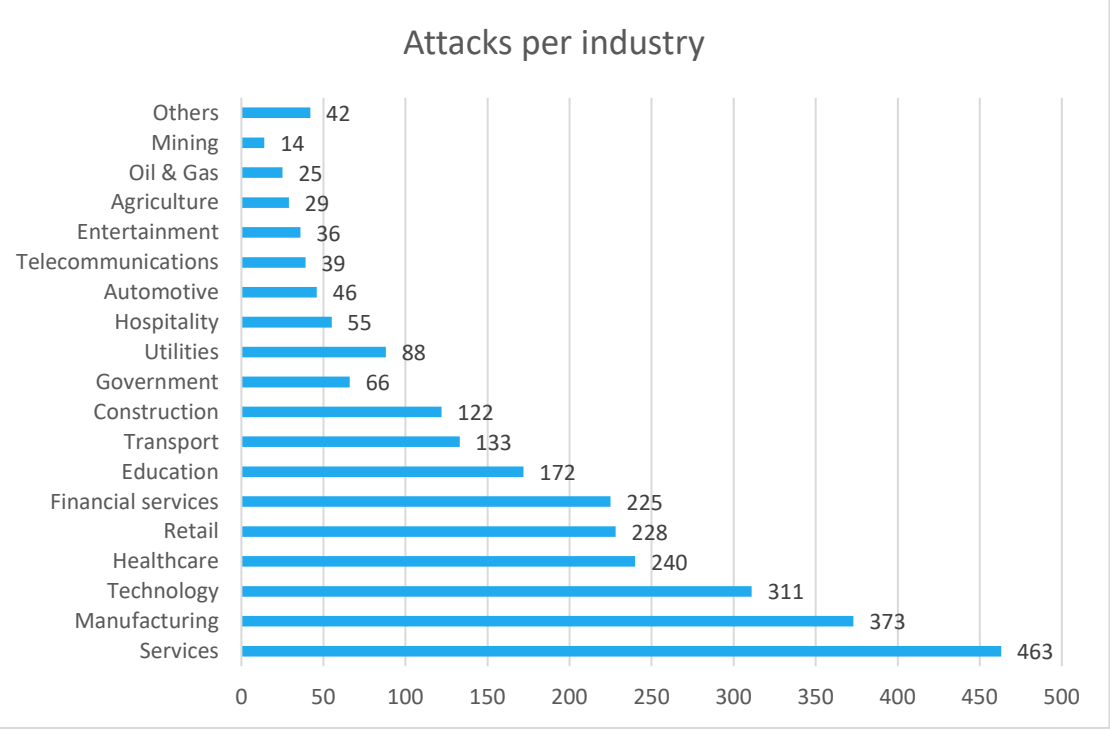


Figure 13 – Ransomware attacks per industry

3.2. State-sponsored

As geopolitical tensions grow around the world due to ongoing or potentially upcoming conflicts, state-sponsored actors have been busy. Below are some of the most relevant state-sponsored activities in 2023H1, categorized by APT origin:

Russia

- In April, CISA, the NCSC-UK, the NSA and the FBI revealed a campaign by APT28 exploiting Cisco routers via CVE-2017-6742 to deploy malware for espionage in Europe, the U.S. and Ukraine. The deployed malware was dubbed Jaguar Tooth.
- In May, the same agencies alongside others around the world unveiled the Snake implant, a malware used by the FSB to create a peer-to-peer network of infected computers around the world and collect intelligence from high-priority targets.
- Also in May, researchers discovered a new OT-focused malware designed to disrupt industrial control systems using the IEC-104 protocol. The malware, dubbed CosmicEnergy, was found on a sharing platform, not as part of an incident, and appears to be a training tool rather than something developed for exploitation against a real target. The development was tied to "Rostelecom-Solar," a Russian cybersecurity company.

China

- In May, a Chinese cluster of activity named Volt Typhoon was discovered infecting networks across U.S. critical infrastructure. Volt Typhoon's most relevant TTPs include the use of VPN devices for initial access, living off the land on Windows targets, and compromising routers to proxy traffic. The most troubling finding, however, is that military bases were also targeted; this could represent preparation work for disruptive attacks in the case of war.
- Also in May, researchers uncovered a new router implant by Chinese APT Camaro Dragon, which enables persistence and lateral movement.
- In June, it was revealed that an APT of probable Chinese origin has been exploiting a recent vulnerability in Barracuda Email Security Gateways with advanced malware that allows for data exfiltration and lateral movement.
- In July, CISA published an advisory about Chinese actors obtaining Microsoft privileged keys and forging authentication tokens to access e-mail accounts of government agencies.

Iran

- In March, Israel's leading technology university was the victim of a DarkBit ransomware attack attributed to Iran's MuddyWater APT.
- In April, a similar approach of state-sponsored ransomware was reportedly used to cover a destructive attack.
- In May, there were reports of Iran accelerating the use of cyber influence operations to achieve its geopolitical goals.

North Korea.

- In February, CISA released an update to an advisory about North Korean actors deploying state-sponsored ransomware for financial gains. The new advisory mentions the use of custom malware such as Maui and H0lyGh0st as well as publicly available variants such as BitLocker, Deadbolt and others against critical infrastructure organizations to demand ransom payments.
- In late March, the Lazarus APT leveraged a trojanized version of the 3CXDesktopApp, a popular voice and video conferencing software as the first stage in a multi-step attack that affect several organizations across the globe. Lazarus has historically been involved in espionage and financially motivated attacks.

3.3. Hacktivists

Hacktivist groups continued operating in 2023H1 with many of the same methods we reported as growing in 2022: geopolitical motivations, communication over X (formerly known as Twitter) or Telegram channels and a split between DDoS-focused groups and those intending to cause physical damage by leveraging unmanaged devices, such as IoT and OT.

One of the groups that gained the most notoriety in 2022 for supporting Russia by attacking western organizations was Killnet. The group is known for DDoS operations targeting critical infrastructure. Between January and March 2023, they attacked more than 90 U.S. healthcare organizations causing "service outages to vulnerable systems lasting several hours or even days." In June, Killnet attacked financial institutions in Europe alongside a newer hacktivist group called Anonymous Sudan.

Another active group, which became notorious for attacks against Russian critical infrastructure leveraging operational technology, is GhostSec. In January, the group announced that it had managed to run ransomware on and encrypt a remote terminal unit (RTU). The specific model was a TELEOFIS RTU968V2, which is a cellular router that can connect to serial devices. The claimed initial access method was brute-forcing the SSH service on the device, which allowed the group to manually run a Go-based ransomware developed specifically for this attack.

Outside the Russia-Ukraine nexus, Israel continued to be a favorite target for hacktivism. As in every year since 2013, #OpIsrael was launched in April to target Israeli organizations. This operation was initially coordinated by Anonymous from 2013 until 2021, but this year a myriad of groups joined in, especially those based in Southeast Asia. Most attacks were traditional DDoS and defacement, but hacktivists also targeted water irrigation systems and wastewater treatment control systems. The attackers located exposed web-based human-machine interfaces controlling these devices and modified their parameters directly.

4. Malware

The Mirai botnet and its variants continued to add new IoT exploits to their arsenal and to leverage them for DDoS attacks. In 2023H1, Mirai variants were observed exploiting firewalls, web servers, solar power generation monitoring systems, cameras, DVRs, building automation systems and other devices. A variant of Gafgyt exploited a vulnerability impacting end-of-life Zyxel routers. At least three entirely new botnets have been observed: Condi has been exploiting TP-Link routers; HinataBot has been exploiting Realtek SDK, Huawei routers and Hadoop servers; and Andoryu has been exploiting Ruckus Wireless routers.

Besides the now traditional DDoS botnets, two pieces of malware caught our attention in 2023H1:

- Raspberry Robin, a malware which has been distributed via compromised QNAP NAS devices since 2022 and used to drop other malicious software on victims, was observed in campaigns against financial institutions in Europe. A new analysis also showed that the botnet has a second layer of infrastructure composed of Linode VPS servers that are contacted by the compromised QNAP and that the botnet could be repurposed by other threat actors.
- HiatusRAT, a new malware targeting end-of-life DrayTek Vigor routers. The malware passively captures email and file transfer traffic, allows attackers to run commands on compromised devices, and can be used to proxy traffic. The malware has been operating since at least July 2022 and is reminiscent of ZuoRAT, which was discovered less than a year ago and attributed to Chinese actors. The actors behind HiatusRAT originally deployed the malware on organizations in Europe, South and North America, but have since shifted to targets in U.S. and Taiwan, which align which Chinese strategic objectives.

While continuously monitoring adversary infrastructure, we observed the distribution of unique IPs shown in Figure 14. The figure shows a combination of C2s, RATs, stealers, miners and other malicious tools. The top six tools observed are legitimate applications developed for pentesting, most of them open source except for the top one. The top two tools, Cobalt Strike and Metasploit, have been used by malicious actors for a long time. Cobalt Strike specifically is one of the most used tools by ransomware gangs. The most interesting observations are the rising popularity of Sliver, an open-source "adversary emulation framework" with a C2 and implants that support Windows, Linux and macOS, and GoPhish, an open-source phishing toolkit that can "quickly and easily setup phishing engagements."

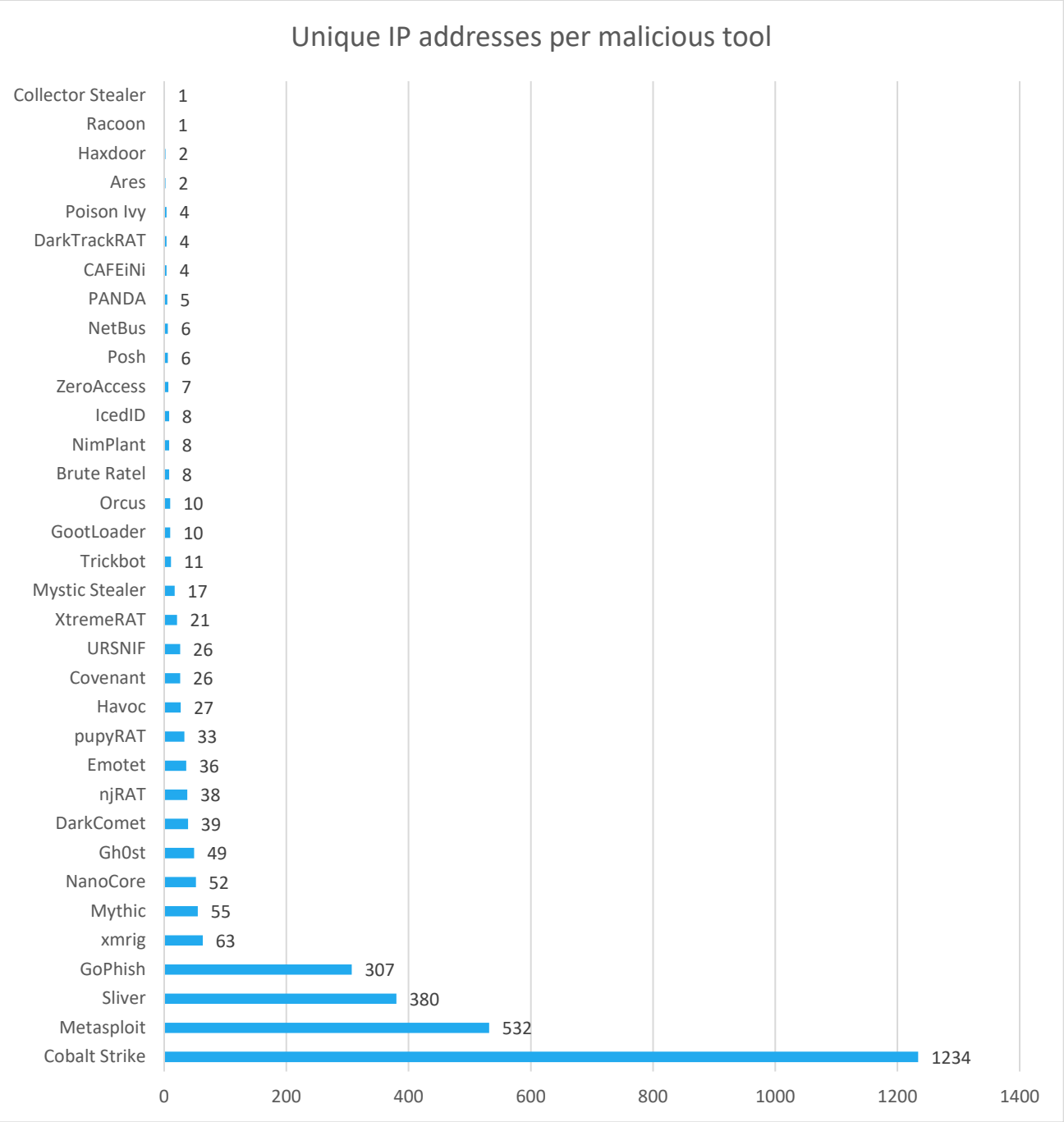


Figure 14 – Unique IP addresses per malicious tool

5. Conclusion

The activities and data we saw in 2023H1 confirm trends we have been observing recently about threats to unmanaged devices, such as:

- **Network infrastructure has become a favorite target for initial access and traffic proxying.** Several Russian and especially Chinese state-sponsored actors have been focusing on exploiting vulnerabilities on and developing custom malware for routers and VPN devices, while cybercriminals are leveraging routers and other compromised devices for residential proxies. Increased activity targeting network

infrastructure has led CISA to issue a specific operational directive about reducing the risks from these devices in June.

- **NAS devices often host malware other than traditional DDoS botnets**. In a report in July, we showed how NAS had recently become the riskiest IoT device on organizations networks partly because of targeted ransomware campaigns that compromised thousands of devices and partly because of how often they are exposed online. In 2023H1, we also saw new vulnerabilities being exploited (such as CVE-2023-27992), vulnerabilities ranking among the top exploited (such as CVE-2022-27593) and advanced malware such as Raspberry Robin, which targets traditional IT, being distributed via compromised NAS on the internet.
- **Building automation devices are becoming increasingly easy targets.** Mirai botnet variants in 2023H1 have been exploiting a new vulnerability on an access control device that was already a target in the past as well as vulnerabilities on devices used for solar power generation monitoring in small facilities. Additionally, Schneider Electric published an advisory in April about publicly available exploits targeting vulnerabilities from 2020 and 2022 in their KNX devices and linking back to a previous advisory about attacks on these systems. Looking into Shadowserver statistics, we see 13 vulnerabilities on building automation devices from nine vendors that are being exploited (as shown in Table 1), while none of them is present on CISA's KEV.

Table 1 – Exploited vulnerabilities affecting building automation devices

Vendor	Product	CVEs
APsystems	Altenergy Power Control Software	CVE-2023-28343
Carel	pCOWeb	CVE-2019-11370
CONTEC	SolarView Compact	CVE-2023-23333, CVE-2022-29303, CVE-2023-29919
ECOA	Building Automation System	CVE-2021-41293
Emerson	Dixell XWEB-500	CVE-2021-45420
KevinLAB	Building Energy Management System	CVE-2021-37291
Linear	eMerge	CVE-2019-7254, CVE-2019-7256, CVE-2022-46381
Loytec	LGATE-902	CVE-2018-14918
Schneider Electric	SpaceLogic C-Bus Home Controller	CVE-2022-34753

On the other hand, some developments were more surprising, such as:

- **Most vulnerabilities added to CISA KEV are from before 2023.** Although new vulnerabilities are dangerous because usually there hasn't been enough time to patch, organizations tend to dismiss older vulnerabilities believing that they present lower risk. Currently on CISA's KEV not only is there evidence of exploitation of older vulnerabilities on IT software, but even on building automation devices – as shown in Table 1, there are exploited vulnerabilities that are more than five years old.
- **Attackers are increasingly using open-source tools as part of their infrastructure.** The trend of commoditization of attack tools continues strongly. Malicious actors now have a wide range of choice of open-source tools developed as legitimate applications to use as part of their campaigns, from phishing attacks to command-and-control infrastructure.
- **The ransomware landscape never stops changing.** Although ransomware has probably been the most prominent threat for at least the last five years, groups continue to change, appearing and disappearing quickly, sometimes being used as disguise for state-sponsored activities. It seems like ransomware

innovation never stops, with 2023H1 showing new families distributing ransomware packaged with infostealers, hacktivists using custom ransomware on OT devices and established families experimenting with ransomware on embedded devices.

Overall, 2023H1 pushed forward the trend of an increasingly diverse attack surface being exploited by threat actors. This period also brought more evidence of the type of "cross-device" attacks we first demonstrated with R4IoT and then observed with botnets such as Chaos. Some threat actors are now routinely mixing traditional endpoints with unmanaged devices, such as VPN appliances, routers, NAS and building automation devices, as part of their attack campaigns.

Based on all the observations during this period, we recommend the following concrete risk mitigation actions:

- **Prioritize extending visibility, risk mitigation and network segmentation for the increased attack surface being exploited.** Some of the devices being leveraged in attacks, such as network infrastructure, may already be in your radar but other types, such as NAS and building automation, are more likely to be forgotten during risk assessments. These, and other risky devices, are all now relevant for attackers, so you need to ensure that you proactively secure them. That means you should, at a minimum: have the proper visibility into these devices in terms of their presence on the network, the software they run, and who they communicate with; understand their risk in terms of vulnerabilities, weak configurations, exposure and other factors; segment them properly to prevent threats from moving between network segments of different criticalities.
- **Do not overlook older vulnerabilities and end-of-life systems.** Although there are new CVEs being published all the time, the old ones that still work against your devices will get exploited just as well. Part of the risk assessment mentioned in the point above is prioritizing which vulnerabilities to patch and which devices to replace. Pay attention to vulnerabilities that may have been forgotten in previous patching cycles but are now being leveraged by threat actors.
- **Ensure that threat detection covers every device in the whole organization.** As threats now move from one type of device to another, it is imperative to ensure that you can detect them across the organization, from an entry point that may be a vulnerable router to a pivot point that may be a misconfigured workstation and finally to a target that may be an insecure OT device. You need threat detection to cover all types of devices and multiple sources of data, including firewalls, intrusion detection systems, endpoint detection and response and others.
- **Follow the latest threat intelligence about ransomware and other actors.** As threat actors continue to evolve and their targets change, you need to be up to date by consuming the latest threat intelligence, whether that is machine-readable indicators of compromise or strategic reports about threat trends.
- **Hunt for threats using emerging tools.** After ensuring that you can detect threats in your environment that use the most traditional tools, such as Cobalt Strike, and you understand how these threats are evolving, you need to extend detection and include threat hunting for emerging tools, such as Sliver. Threat actors move fast when using new tools, so you need to keep up the pace.