FORTINET

2H 2023
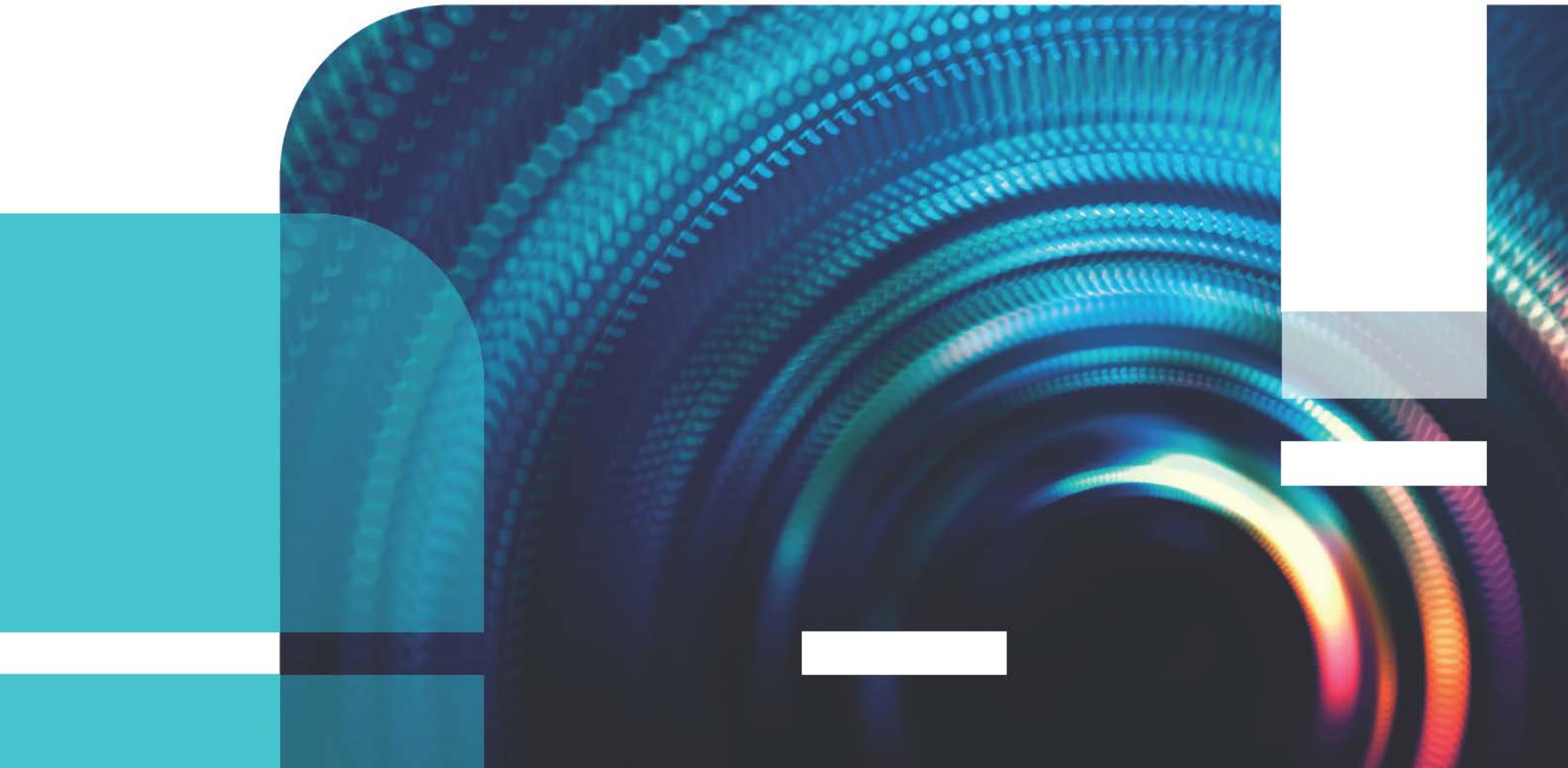
Global Threat Landscape Report

A Semiannual Report by FortiGuard Labs

Executive Summary

In the second half of 2023, the cybersecurity landscape saw a range of significant developments that have considerably impacted the digital attack surface. Notable among these was the rise in sophisticated cyberattacks targeting large-scale entities and essential infrastructure.

If the growing number of attacks weren't enough to keep most CISOs awake at night, the cybersecurity domain is simultaneously grappling with the ongoing challenge of attracting and retaining skilled professionals. The rising demand for qualified cybersecurity experts, coupled with the need for organizations to offer attractive career development opportunities and work environments, continues to highlight the importance of human capital in combating cyberthreats.

The need to understand where your attack surface gaps in detection, mitigation, and response lie is more vital than ever and the most impactful thing we can do is to shed light on how the threat landscape has been shifting and how organizations need to build secure networking systems that can quickly adapt to changing business demands and the evolving threat landscape. That's why we publish this report. Our goal is to help you navigate these changes and understand where to focus your time and energy, using your resources in the most impactful way.

The findings in this report represent the collective intelligence of FortiGuard Labs, drawn from a vast array of network sensors collecting threat events each day observed in live production environments around the world from more than 600K+ environments and 10M+ sensors capturing every detail about threats that hit our detection technology. We've sifted through all that data to find and extract key insights that we hope will help guide you through the cyber challenges of 2024.
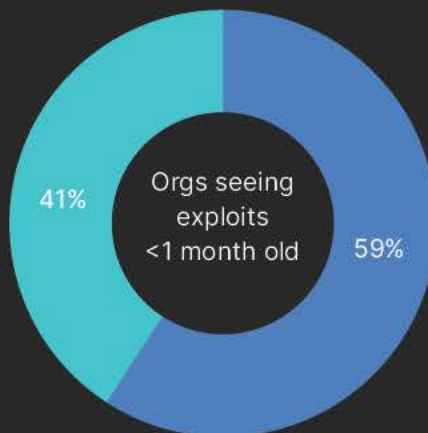
# 2H 2023 Active Threat Landscape at a Glance

Into the Red Zone

8.8%

+0.5% since last half

91.2%
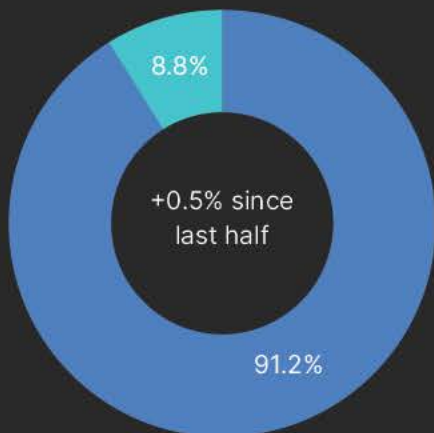
The percent of all endpoint vulnerabilities targeted by attacks remained steady, around 9%.

Exploit Dispersion

Orgs seeing exploits <1 month old

41%

59%

Attacks can spread quickly. 41% of organizations detected activity for exploits less than one month old.

ATT&CK Sightings

32.9%

+0.4% since last half

67.1%
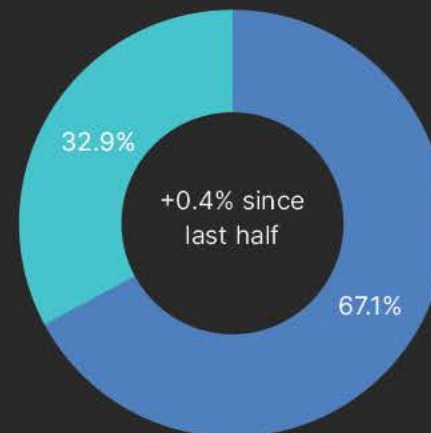
Sandbox and network detection and response (NDR) sensors observed activity for over two-thirds of MITRE ATT&CK techniques.

APT Groups

38/143

FortiRecon intelligence indicates 38 of the 143 advanced persistent threat (APT) groups listed by MITRE were active during this time.

Ransomware

40%+

More than 40% of ransomware and wipers targeted the industrial sector, indicating that cybercriminals are focused on OT and the supply chain.

Time-to-Exploitation

43%

On average, for new exploits identified, attacks occurred in 4.76 days after discovery. That's 43% faster than the prior period.

A Look at Exploit, Malware, and Botnet Trends

FortiGuard Labs monitors a vast array of globally deployed sensors that collect trillions of threat events worldwide each day. This unique vantage point gives us a detailed and comprehensive view of the cyberthreat landscape, including how exploit, malware, and botnet trends change over time.

Exploits	Malware	Botnet
11,030 unique exploit detections, +10% over last half	39,896 unique variants detected, -11% from last half	319 unique botnets detected, -3% from last half
63 exploit detections per organization, +17% over last half	5,962 different active families, -16% from last half	4.3 active botnets per sensor, +/-0% from last half
73% of firms saw severe attacks, +4% over last half	16 families spread to more than 10% of organizations, -11% from last half	85 infection days in average, +2% over last half

This data, outlined in the chart above, shows that the creation and prevalence of exploits are on the rise. Cybercriminals are targeting the ever-increasing number of new vulnerabilities resulting from the exponential growth in the number and variety of connected devices and an explosion in new applications and online services. It's only natural that attacks looking to exploit those vulnerabilities would rise as well. This increase in exploit volume per organization is undoubtedly contributing to the prevalence of overwhelmed security teams.

Interestingly, after rising over the first half of 2023, the volume of malware samples detected by our sensors subsided in the latter half of the year. Unfortunately for defenders, this doesn't mean that malware is falling out of favor among clever attackers. The observed slowdown is likely because certain types of malware, particularly ransomware, are taking a more targeted approach, leading to an increase in cost-per-ransomware incident. This also explains why bot traffic remained steady during this same time.

IoT exploits are on the rise

Exploitation activity captured by the FortiGuard Intrusion Prevention System (IPS) sensors running on our FortiGate Next-Generation Firewalls provides unrivaled visibility into how threat actors find vulnerabilities, exploit their targets, and build malicious infrastructure. These sensors are often the first point of contact with an adversary probing for exposures. Let's start with a view of the technologies attackers are probing most aggressively. Not surprisingly, Internet-of-Things (IoT) devices, shown in red in the corresponding chart, are popular targets, largely because they are often under protected or unprotected.

While we have highlighted outbreak alerts for IoT devices here, our FortiGuard Labs team had their radars filled with all manner of additional vulnerability exploits in 2H 2023. Here's a quick recap of some of those:

- VMware Aria Operations for Networks Command Injection Vulnerability[5]
- IBM Aspera Faspex Code Execution Vulnerability[6]
- Cisco IOS XE Web UI Attack[7]
- Citrix Bleed Attack[8]
- Apache RocketMQ Remote Command Execution Vulnerability[9]
- Progress MOVEit Transfer SQL Injection Vulnerability[10]

Technology platforms targeted most often with exploit attempts

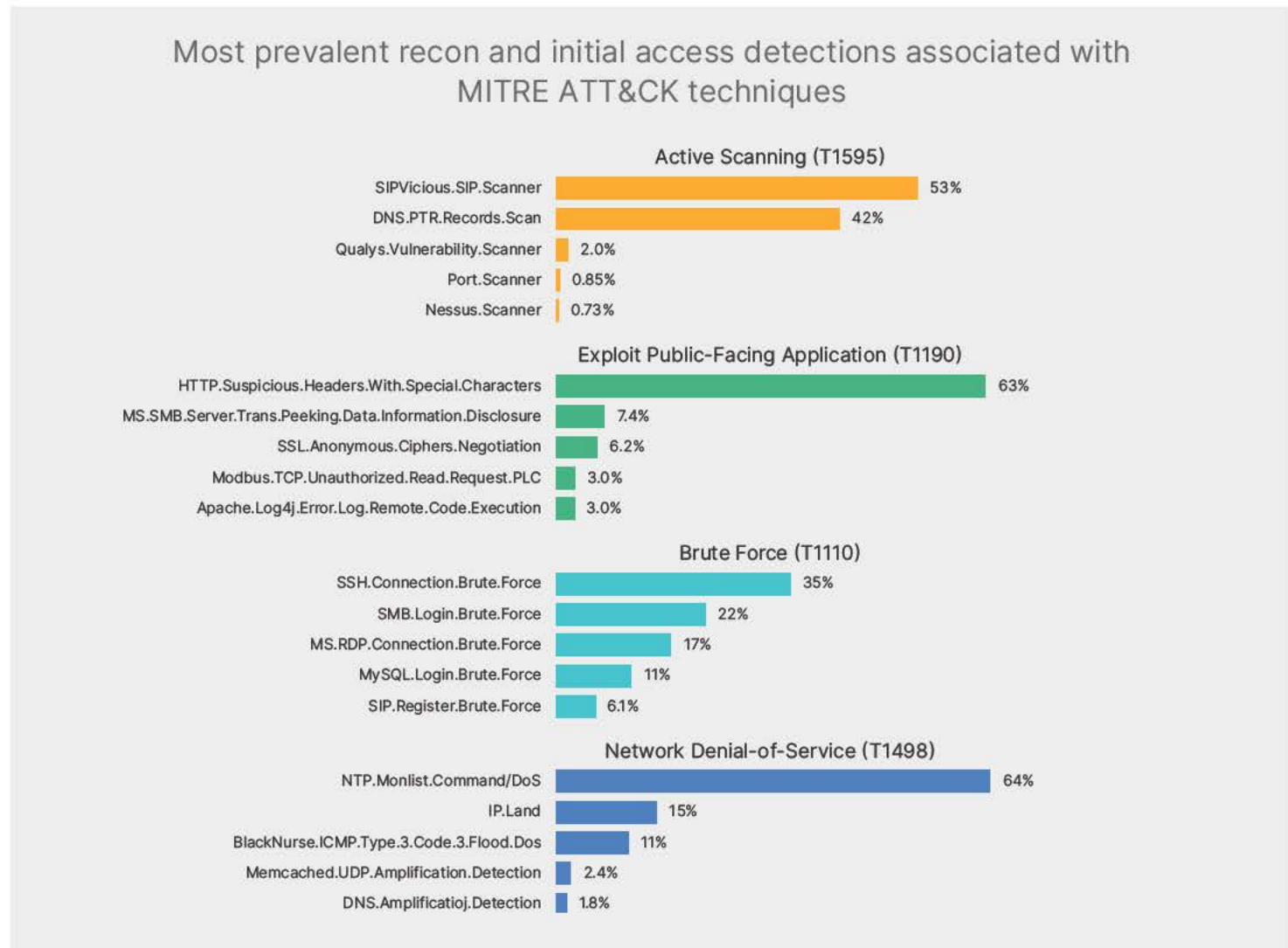|	July	Aug	Sep	Oct	Nov	Dec
1	Zyxel.zhttpd (38%)	Multiple.Routers (40%)	Zyxel.zhttpd (39%)	Apache.Log4j (40%)	Zyxel.zhttpd (37%)	Apache.Log4j (43%)
2	PHP.CGI (37%)	PHP.CGI (37%)	Multiple.Routers (37%)	Zyxel.zhttpd (37%)	Linux.Kernal (36%)	Zyxel.zhttpd (38%)
3	Linux.Kernel (35%)	Zyxel.zhttpd (37%)	PHPUnit.Eval-stdin (36%)	PHPUnit.Eval-stdin (37%)	Multiple.Routers (34%)	Linux.Kernel (35%)
4	D-Link.Devices (35%)	PHPUnit.Eval-stdin (36%)	Linux.Kernal (36%)	Multiple.Routers (36%)	PHPUnit.Eval-stdin (33%)	Multiple.Routers (35%)
5	PHPUnit.Eval-stdin (34%)	Linux.Kernal (35%)	Telerik.Web (34%)	Linux.Kernal (35%)	Telerik.Web (33%)	Telerik.Web (33%)
6	Multiple.Routers (34%)	Dasan.GPON (34%)	Dasan.GPON (33%)	Telerik.Web (32%)	D-Link.Devices (30%)	PHPUnit.Eval-stdin (33%)
7	Dasan.GPON (34%)	D-Link.Devices (34%)	ThinkPHP.Controller (32%)	ZTE.Router (31%)	Dasan.GPON (29%)	D-Link.Devices (30%)
8	Telerik.Web (33%)	Telerik.Web (33%)	Apache.HTTP (31%)	Dasan.GPON (30%)	TP-Link.Home (28%)	Java.Debug (28%)
9	ThinkPHP.Controller (33%)	Apache.Log4j (30%)	JAWS.DVR (29%)	D-Link.Devices (29%)	Apache.Log4j (27%)	Zivif.PR115-204-P-RS (27%)
10	NETGEAR.DGN1000 (31%)	MikroTik.RouterOS (30%)	Backdoor.Cobalt (29%)	PHP.URI (29%)	Bash.Function (25%)	Dasan.GPON (26%)

Vulnerabilities affecting routers, cameras, and other IoT devices were the focus of several outbreak alerts published by FortiGuard Labs throughout 2023.[1]

Zyxel Networks equipment was a favorite target for exploits throughout the second half of the year, with FortiGuard Labs issuing an outbreak alert about the company's firewalls.[2] Perhaps smelling blood in the water, attackers rediscovered and exploited a Zyxel Networks vulnerability relating to an end-of-life router, which was initially published in 2017.[3]

Speaking of old vulnerabilities attracting new attention, exploits targeting Zivif web cameras (CVE-2017-17107) made the top 10 list in December 2023. These exploits appear to be related to ongoing Zerobot attacks we alerted security practitioners to in late 2022.[4] This scenario shows that old vulnerabilities can always be made new (and better) by enterprising threat actors.

We are closing out this exploit review with another chart demonstrating the wide scope of activity detected by our IPS sensors. Here is a look at the top five exploit detections associated with four key MITRE ATT&CK techniques[11] of Active Scanning, Exploit Public-Facing Apps, Brute Force, and Network DoS.

Most prevalent recon and initial access detections associated with MITRE ATT&CK techniques

Active Scanning (T1595)

SIPVicious.SIP.Scanner	53%
DNS.PTR.Records.Scan	42%
Qualys.Vulnerability.Scanner	2.0%
Port.Scanner	0.85%
Nessus.Scanner	0.73%

Exploit Public-Facing Application (T1190)

HTTP.Suspicious.Headers.With.Special.Characters	63%
MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	7.4%
SSL.Anonymous.Ciphers.Negotiation	6.2%
Modbus.TCP.Unauthorized.Read.Request.PLC	3.0%
Apache.Log4j.Error.Log.Remote.Code.Execution	3.0%

Brute Force (T1110)

SSH.Connection.Brute.Force	35%
SMB.Login.Brute.Force	22%
MS.RDP.Connection.Brute.Force	17%
MySQL.Login.Brute.Force	11%
SIP.Register.Brute.Force	6.1%

Network Denial-of-Service (T1498)

NTP.Monlist.Command/DoS	64%
IP.Land	15%
BlackNurse.ICMP.Type.3.Code.3.Flood.Dos	11%
Memcached.UDP.Amplification.Detection	2.4%
DNS.Amplificatioj.Detection	1.8%

Network security appliances provide intelligence on the left side of the MITRE ATT&CK framework, which helps us understand more about the threats that malicious actors are using to try to get inside organizations. Ideally, when applying the ATT&CK framework across your enterprise, we recommend collating ATT&CK sources and creating a consolidated heatmap for using in threat hunting, purple teaming, adversarial emulation, and detection engineering.

Tracking movement across malware families

Once threat actors find an exploitable vulnerability, their next step is often to deploy malware. Samples picked up by our various anti-malware solutions offer insight into popular adversary tools for establishing a foothold, escalating privileges, maintaining presence, and moving laterally within target environments to achieve their goals.

The figure on the next page measures the proportion of organizations in each region that detected variants of the most common malware families during the second half of the year. Malware that gains a foothold in one region of the world, such as the JS/Agent family, gains similar traction across most other geographies.

Top malware families based on regional prevalence

	Africa	Asia	Europe	Latin America	Middle East	North America	Oceania
JS/Agent	40.9%	34.2%	34.0%	37.4%	30.9%	30.0%	35.9%
JS/Phishing	17.6%	15.9%	19.2%	19.8%	12.7%	12.0%	18.5%
MSIL/Kryptik	17.4%	22.6%	19.8%	16.6%	16.9%	4.8%	7.5%
HTML/Phish	16.5%	19.9%	18.6%	15.2%	13.9%	7.9%	12.0%
JS/ScrInject	20.1%	13.1%	11.9%	18.6%	33.4%	10.3%	18.7%
JS/Cryxos	12.8%	28.6%	13.6%	14.7%	12.1%	13.3%	18.7%
MSIL/GenKryptik	14.6%	20.8%	17.9%	16.1%	15.4%	4.3%	7.2%
PDF/Phishing	14.1%	12.8%	14.9%	12.9%	11.2%	8.9%	14.1%
MSIL/GenericKDS	11.8%	19.1%	15.2%	13.6%	12.7%	3.7%	6.1%
HTML/Phishing	12.5%	13.1%	12.0%	9.6%	9.2%	5.6%	7.3%
MSIL/Agent	11.6%	16.1%	14.6%	11.4%	12.1%	3.5%	5.6%
MSOffice/CVE_2018_0798	9.8%	15.0%	15.1%	9.4%	10.2%	3.4%	4.7%
JS/Redirector	13.7%	7.7%	9.6%	8.0%	7.8%	7.5%	10.7%
MSIL/Stealer	9.5%	14.6%	11.8%	10.3%	10.3%	2.8%	4.5%
NSIS/Injector	8.5%	13.4%	13.1%	7.1%	10.1%	2.4%	5.3%
MSOffice/CVE_2017_11882	8.4%	12.1%	11.0%	17.6%	9.5%	2.5%	3.4%
HTML/infObfus	11.8%	5.9%	6.3%	4.2%	10.1%	10.5%	15.7%
BAT/Agent	5.5%	9.1%	6.3%	9.0%	6.7%	3.7%	4.3%
W32/Injector	8.6%	11/9%	8.9%	6.8%	9.0%	2.2%	3.0%
MSExcel/CVE_2017_11882	8.2%	12/3%	8.6%	5.0%	7.4%	2.3%	3.3%

In case you'd like to double-check your antivirus scans for the most common JS/Agent variants, here are the top three to look for, plus a final variant that moved up the popularity ranks quickly in 2H 2023:

- JS/Agent.CY!.tr[12]
- JS/Agent.F022!.tr[13]
- JS/Agent.PIV!.tr[14]
- JS/Agent.NDS!.tr[15]

However, two malware families have bucked the regional uniformity trend: JS/ScrInject and JS/Cryxos. For the former, the variant responsible is JS/ScrInject.B!.tr.[16] This Remote Access Trojan (RAT) has been circulating since 2011 and has a very regular weekly activity cycle.[17] The other is JS/Cryxos and, in particular, the JS/Cryxos.5478!.tr variant.[18] This Trojan, known to have a variety of surreptitious capabilities, appears to be driving the bulk of detections across Asia.

Outside the most prevalent generic families depicted above, four additional malware campaigns caught our attention in the second half of 2023: AndroxGh0st, Apache ActiveMQ ransomware, Lazarus RATs, and Agent Tesla. We cover AndroxGh0st extensively in the botnet section, so we'll summarize the other three here.

Apache ActiveMQ

Apache ActiveMQ is a popular open-source message broker. A vulnerability was disclosed (CVE-2023-46604) in fall 2023 that allowed a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol.[19] Reports emerged in November that attackers were taking advantage of that flaw in the form of the HelloKitty ransomware.[20] FortiGuard Labs released an outbreak alert detailing how threat actors were exploiting this flaw by running ransomware campaigns targeting servers running outdated and vulnerable versions of Apache ActiveMQ.[21]

Lazarus RATs

The Lazarus Group is an APT group sponsored by the North Korean government. In this new campaign, Lazarus was observed employing DLang-based RAT malware in the wild. Lazarus's initial access begins with the successful exploitation of CVE-2021-44228, the infamous Log4j vulnerability discovered in 2021.[22]

Agent Tesla

FortiGuard Labs captured a phishing campaign that spreads a new Agent Tesla variant.[23] This well-known malware family uses a .Net-based RAT and data stealer to gain initial access by exploiting Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2018-0802.[24,25] The Agent Tesla core module can collect sensitive information from the victim's device such as saved credentials, keylogging information, and device screenshots.

Into the Red Zone

14.6%

New botnets
15% of volume

85.4%
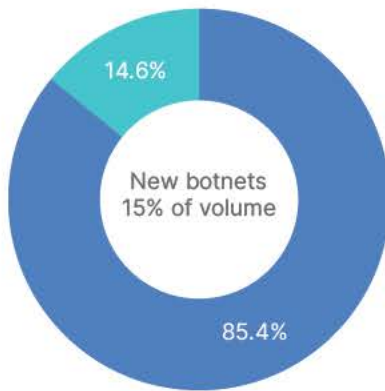
Old versus new bots

New bots on the block: AndroxGh0st, Prometei, and DarkGate

Once infected with malware, systems often attempt to communicate with remote hosts to download additional payloads, establish command and control (C2) channels, and open backdoors into the environment. This makes the analysis of botnet traffic an important part of monitoring the full scope of malicious activity.

A chart of the most active botnets is inevitably filled with many of the same ones we've seen for years, including Gh0st, Mirai, and ZeroAccess. This demonstrates two things:

- Botnets are resilient. They're created to persist and, despite coordinated law enforcement takedowns, can be hard to kill.

- Botnet remediation is a slow process. Much of the botnet traffic we detect comes from infected systems attempting to communicate with botnets that are no longer active.

That said, new botnets do emerge occasionally that warrant attention. In the second half of 2023, three new botnets took the spotlight: AndroxGh0st, Prometei, and DarkGate.
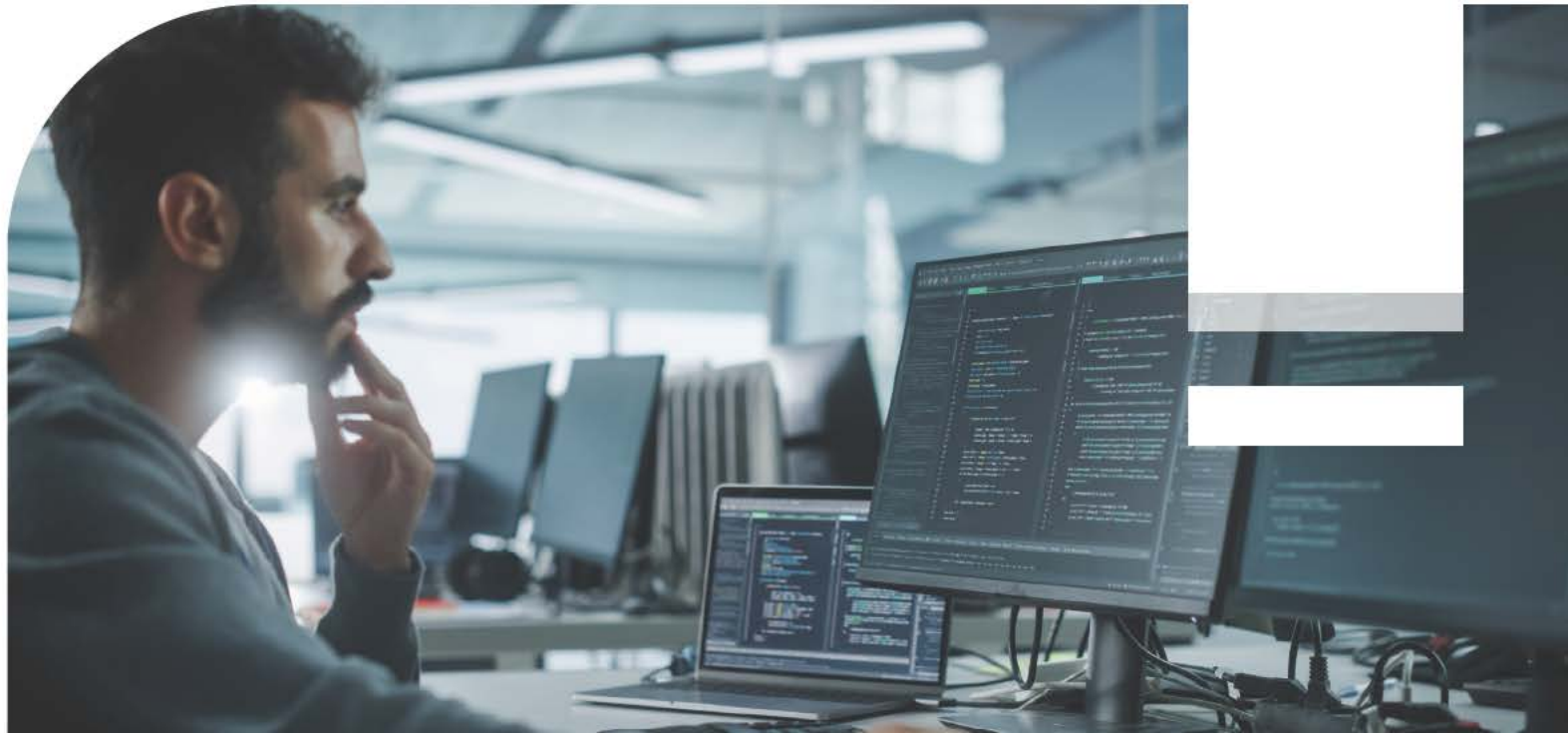
Volume of traffic associated with new botnets emerging in 2H 2023
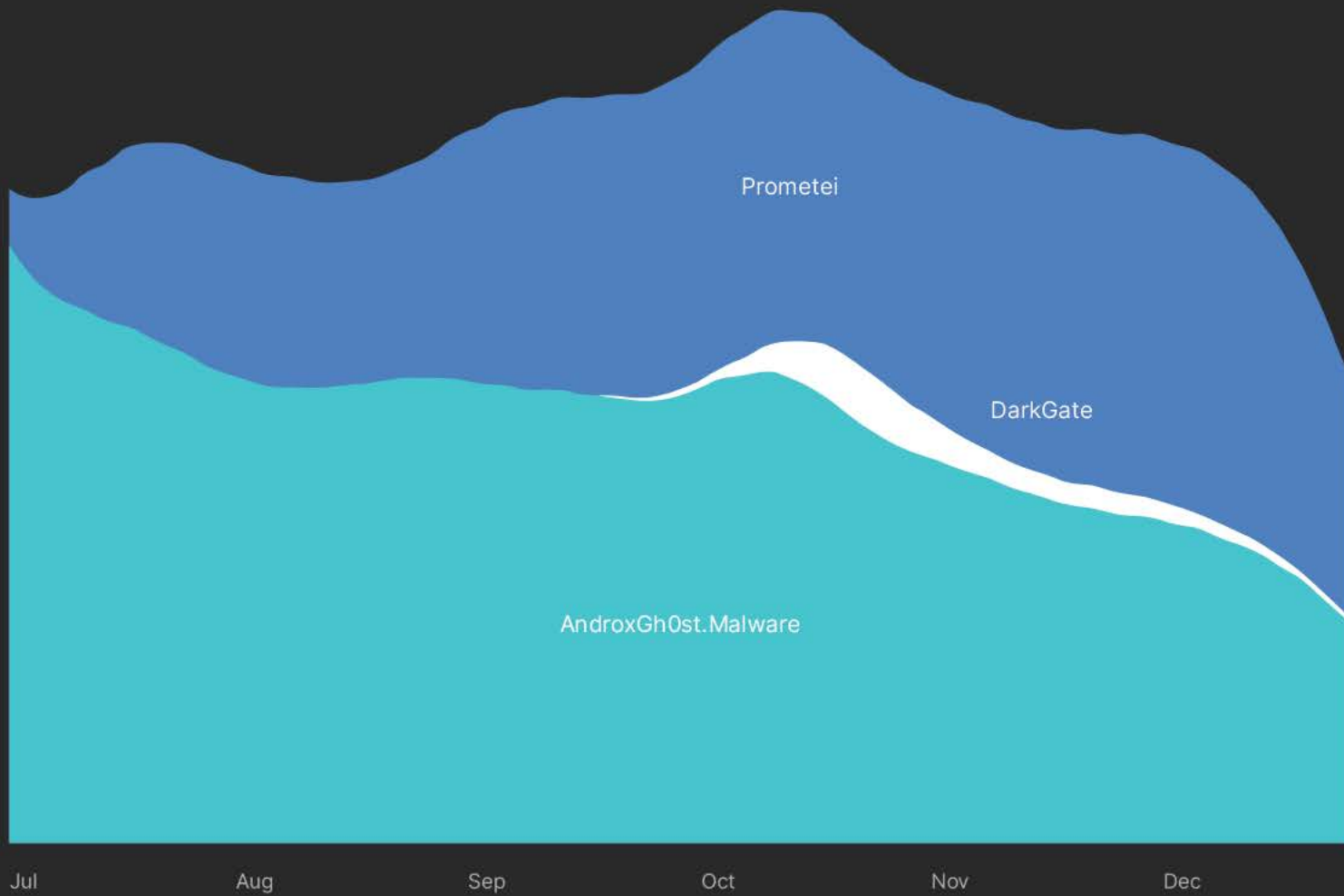
AndroxGh0st

The AndroxGh0st botnet is related to the Python-based malware of the same name. It primarily targets user environment (.env) files, which often contain credentials for a variety of high-profile applications. AndroxGh0st includes numerous malicious functions to abuse Simple Mail Transfer Protocols (SMTP). It also scans and exploits exposed credentials and APIs and deploys web shells to maintain persistent access to systems.

We continue to observe widespread activity of AndroxGh0st malware in the wild exploiting multiple vulnerabilities. It specifically targets the PHPUnit (CVE-2017-9841), Laravel Framework (CVE-2018-15133), and Apache Web Server (CVE-2021-41773) vulnerabilities to spread and conduct information-gathering attacks on the target networks.[26, 27, 28] Fortinet was credited with exposing telemetry on AndroxGh0st, showing over 40,000 devices infected by the botnet.[29]

Prometei

Prometei is malware that can remotely control infected machines. It's capable of spreading laterally across networks, stealing password credentials, executing arbitrary commands, and downloading and executing additional malicious components. Prometei can also perform cryptocurrency mining and has self-updating capabilities.

This malware strain was recently reinvented, and we created new IPS signatures to aid in detection.[30] This retooling worked well, as the Prometei botnet has subsequently been catapulted to the sixth spot on our list for total traffic volume across our sensors in 2H 2023.
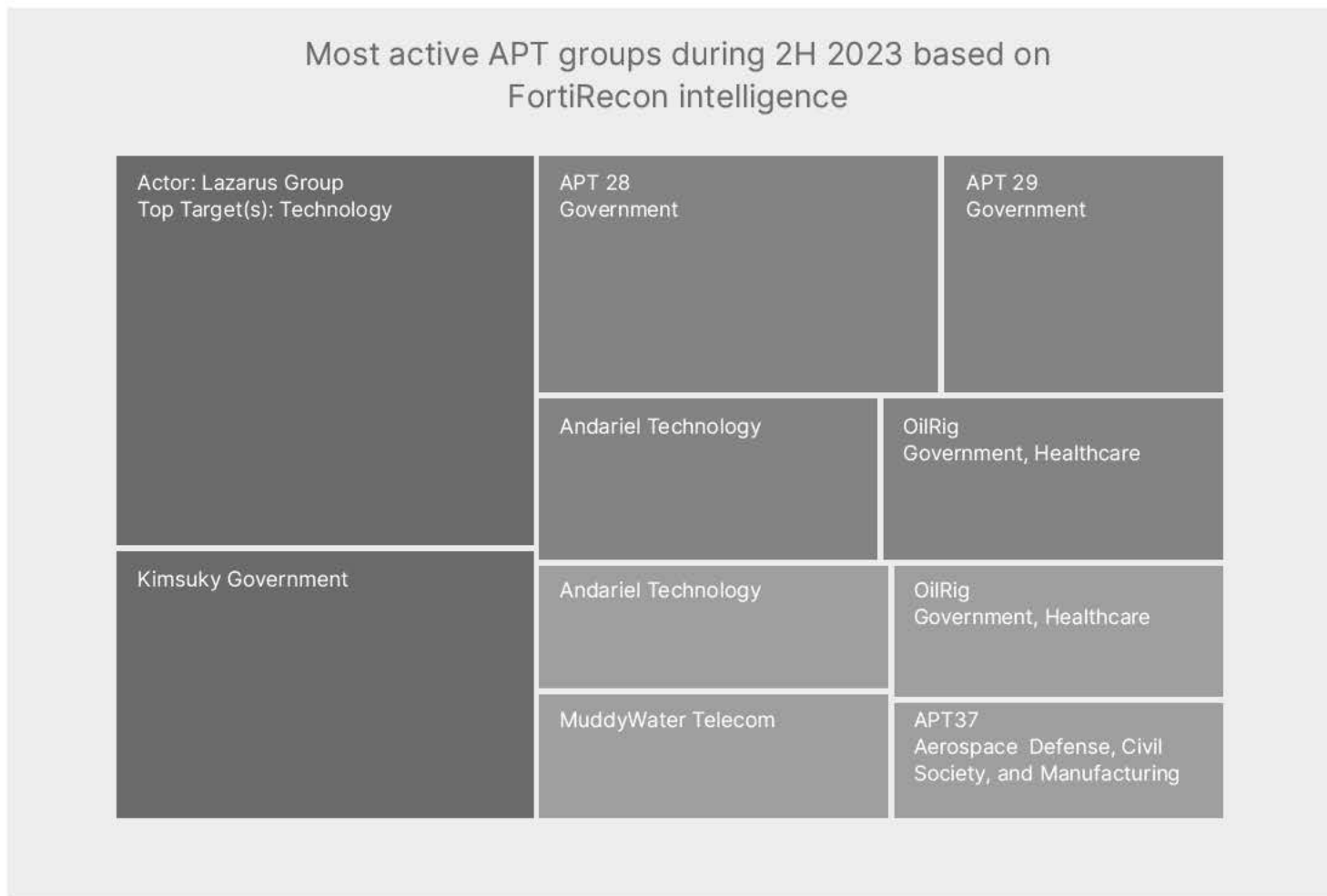
DarkGate

Though it's a distant third to AndroxGh0st and Prometei, the DarkGate botnet warrants mention. The DarkGate malware, which has a range of capabilities from remote access to cryptomining to information stealing, was first reported in 2017. Since then, its creators have used it only for specific campaigns. But in mid-2023, the purported author offered to sell it, and the malware soon began making wider rounds.[31] We saw the DarkGate botnet emerge after the Qakbot takedown as a possible successor.[32] Whether DarkGate has a future as a leading tool for cybercriminals remains to be seen.

Most Active APTs

In the first half of the year, we observed significant activity among APT groups, and that volume has held steady throughout the remainder of 2023. APT groups continue to be highly adaptable to changes in the digital landscape and are increasingly stealthy as they carefully plan and execute attacks. The image below offers a look at the most active APT groups during the second half of the year.

Most active APT groups during 2H 2023 based on FortiRecon intelligence

Actor: Lazarus Group
Top Target(s): Technology

APT 28
Government

APT 29
Government

Andariel Technology

OilRig
Government, Healthcare

Kimsuky Government

Andariel Technology

OilRig
Government, Healthcare

MuddyWater Telecom

APT37
Aerospace Defense, Civil Society, and Manufacturing

Researchers' latest findings indicate a definitive shift in the tactics of the North Korean APT group, Lazarus. Over the past year and a half, they have disclosed three different RATs built using uncommon technologies during development, like QtFramework, PowerBasic, and DLang. This indicates that Lazarus Group is a mature and capable organization, generally using N-Day exploits and known techniques to breach companies in the technology sector, such as blockchain exchanges and software development firms. The group's attacks have been quite lucrative, netting north of $100 million in crypto thefts alone.

Another group that was active these last months of 2023 was APT 28, using N-Day vulnerabilities in Outlook and Winrar to steal New Technology Lan Manager (NTLM) credentials, focusing on breaching government organizations as well as companies in the higher education, manufacturing, and aerospace industries. The group targeted organizations in Eastern Europe, with multiple campaigns aimed at disrupting operations and stealing information from these enterprises. This same group also used previously undisclosed zero days this year to carry on cyberespionage and steal data. APT 28 has also moved away from using backdoors and compromising peripheral devices in the network and is now using legitimate services such as Google Drive and Microsoft OneDrive to exfiltrate sensitive data.

Penetrating the Red Zone

Prioritizing vulnerabilities for remediation is more important than ever given that the rate of discovery and disclosure continues to quicken. As of this report's publication, there are over 222,000 vulnerabilities on the Common Vulnerabilities and Exposures (CVE) list.[33] We witnessed a new record in 2023, with a total of 30,000 new vulnerabilities published—a 17% jump from the previous year.

In 2022, we introduced the concept of the "red zone," which helps readers better understand how likely (or unlikely) it is that threat actors will exploit a specific vulnerability.[34] This allows security teams to focus on the vulnerabilities that present the most risk by prioritizing remediation efforts.

Thankfully, our data shows a small subset (12.5%) of all historical CVEs are present and unremediated on endpoints in live environments. This is depicted in the ratio of blue versus gray squares in the adjacent chart.
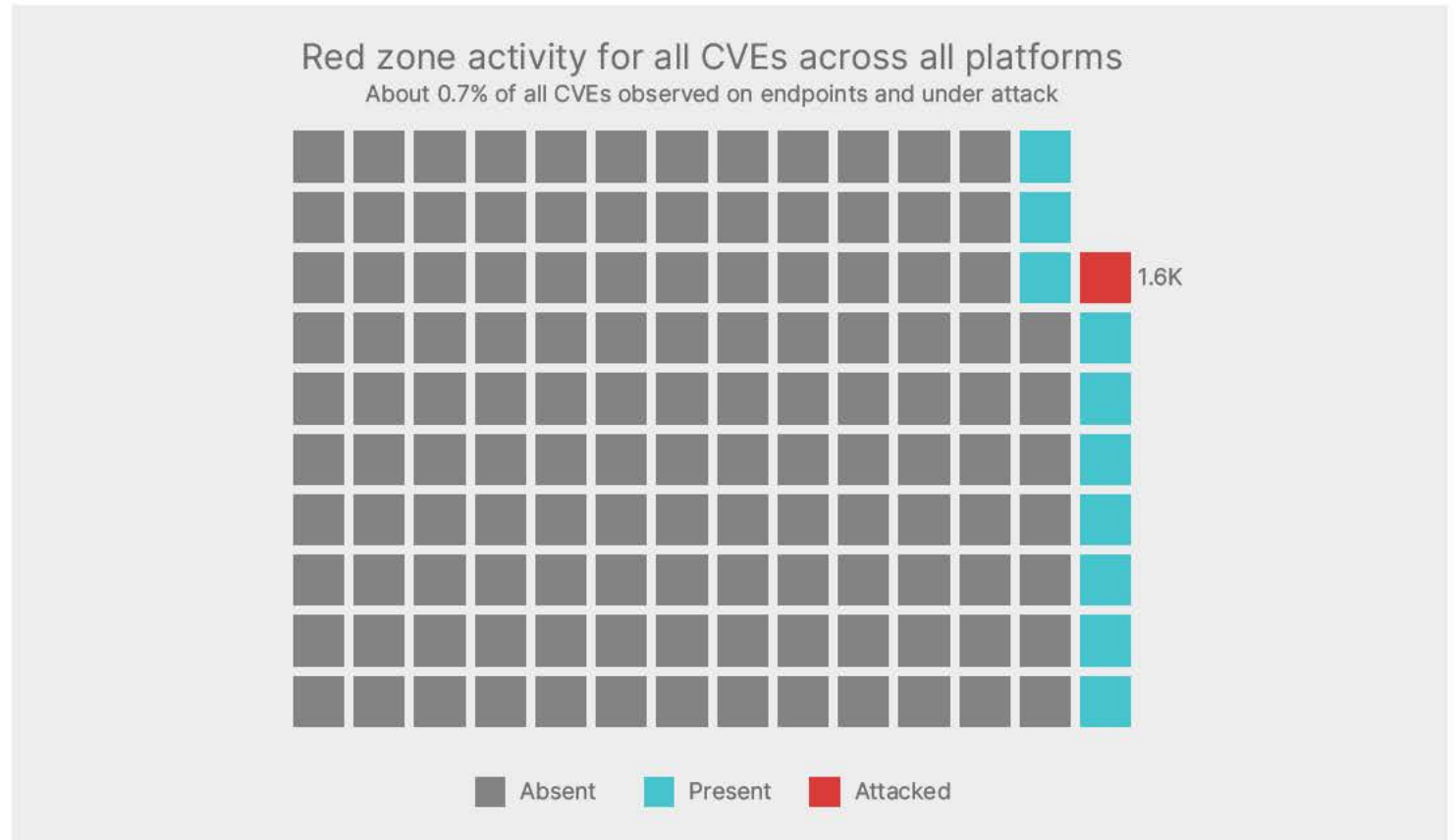
Further, only a fraction (<1%) of all vulnerabilities were exploited in 2H 2023. That proportion has remained remarkably steady over time, which is good news for security teams.
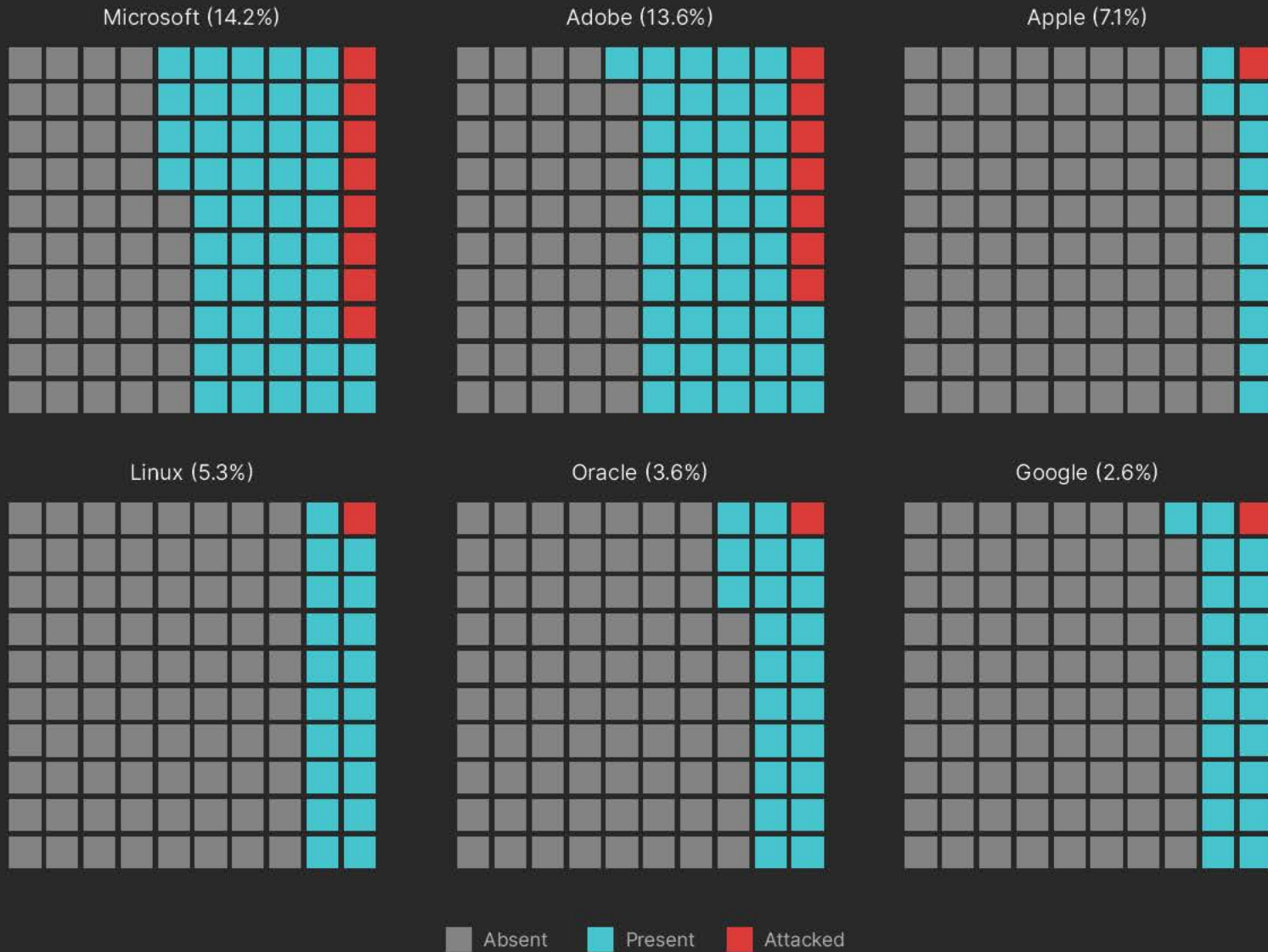
30K

new vulnerabilities across all industries were published in 2023, marking a 17% increase from the prior year.

Of course, the red zone for many prominent software platforms is substantially larger. For example, Microsoft's attack surface is 20x larger than the overall average (14%) and twice that of Apple (7%) and Linux (5%). Practically speaking, the larger the red zone, the more effort and automated patching is required for timely remediation of high-risk vulnerabilities with active exploits.
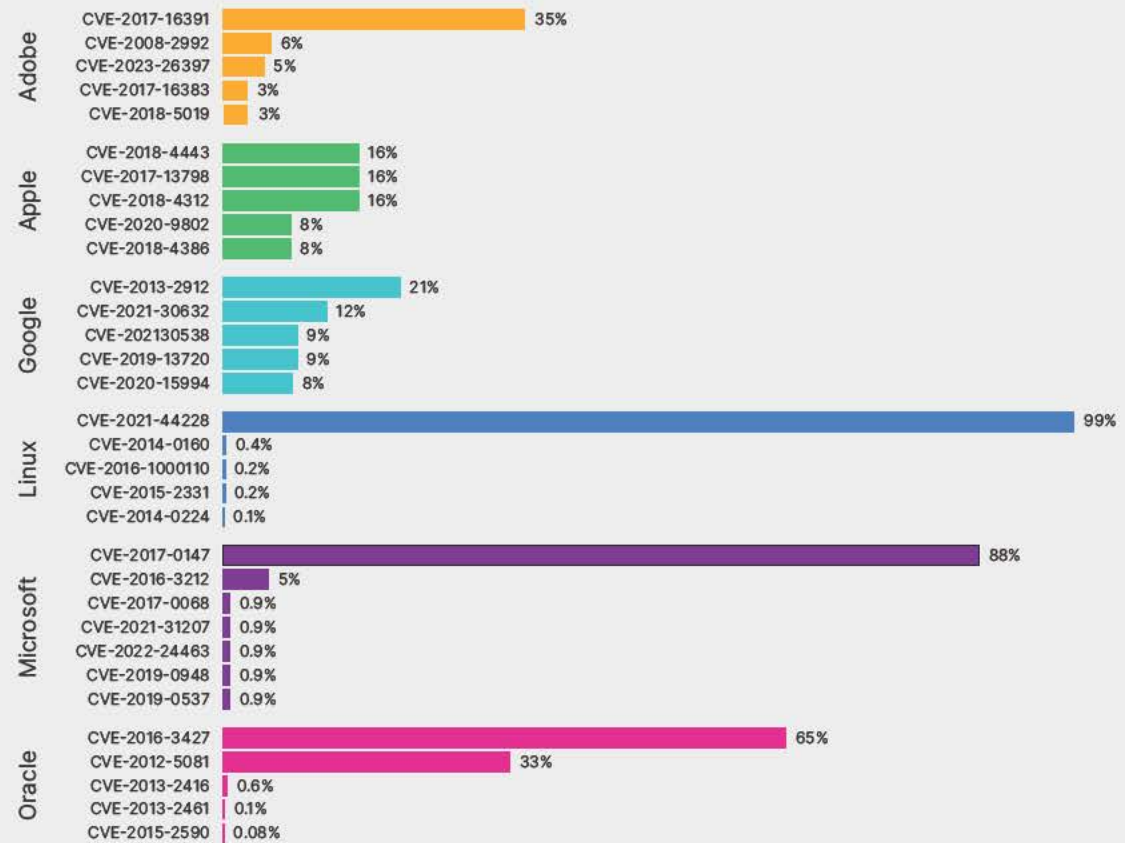
Red zone activity for all CVEs across all platforms
About 0.7% of all CVEs observed on endpoints and under attack

1.6K

■ Absent   ■ Present   ■ Attacked

Red zone activity for CVEs affecting prominent platforms

Microsoft (14.2%)

Adobe (13.6%)

Apple (7.1%)

Linux (5.3%)

Oracle (3.6%)

Google (2.6%)

Absent   Present   Attacked

Here is a look at the top five vulnerabilities that comprise each platform's red zone based on the prevalence of detected exploit attempts:

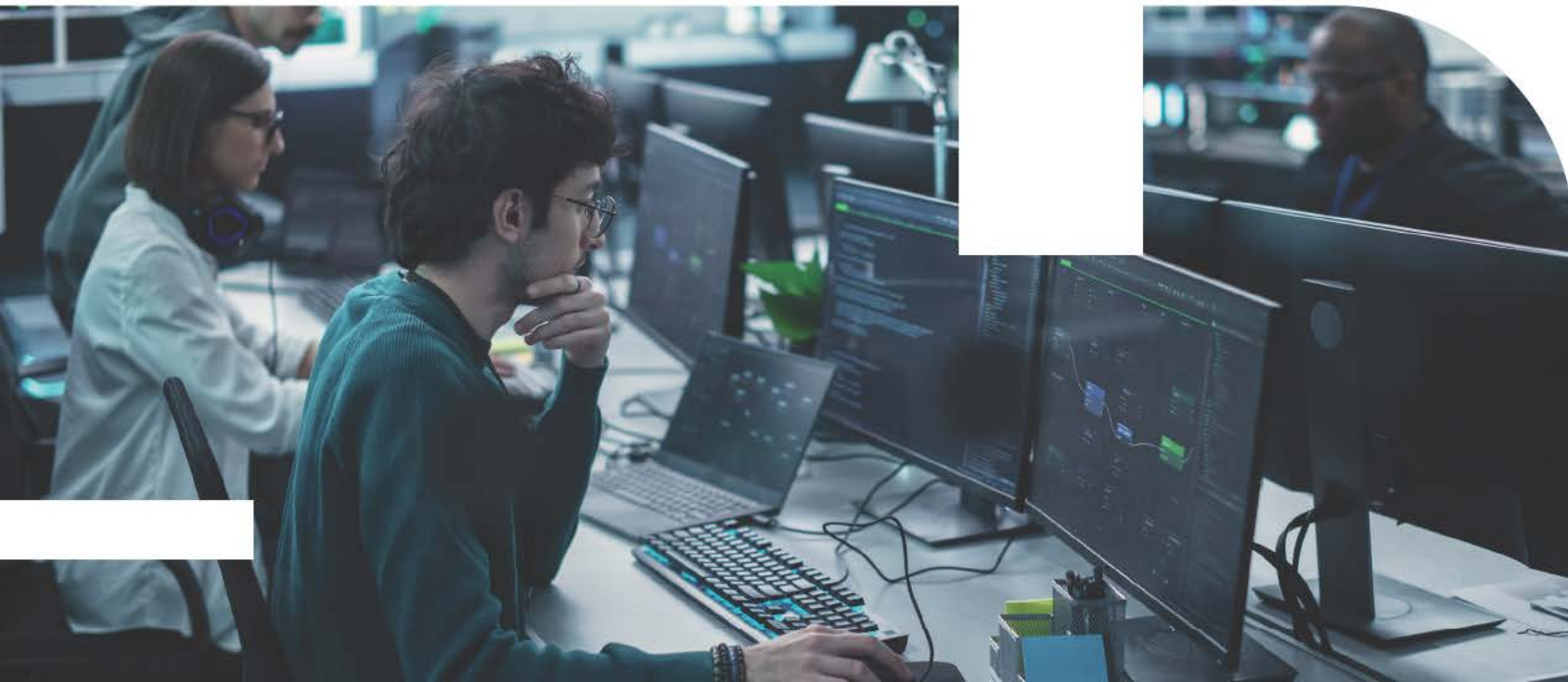CVEs with the highest exploit activity for each prominent software platform

Adobe
- CVE-2017-16391 — 35%
- CVE-2008-2992 — 6%
- CVE-2023-26397 — 5%
- CVE-2017-16383 — 3%
- CVE-2018-5019 — 3%

Apple
- CVE-2018-4443 — 16%
- CVE-2017-13798 — 16%
- CVE-2018-4312 — 16%
- CVE-2020-9802 — 8%
- CVE-2018-4386 — 8%

Google
- CVE-2013-2912 — 21%
- CVE-2021-30632 — 12%
- CVE-202130538 — 9%
- CVE-2019-13720 — 9%
- CVE-2020-15994 — 8%

Linux
- CVE-2021-44228 — 99%
- CVE-2014-0160 — 0.4%
- CVE-2016-1000110 — 0.2%
- CVE-2015-2331 — 0.2%
- CVE-2014-0224 — 0.1%

Microsoft
- CVE-2017-0147 — 88%
- CVE-2016-3212 — 5%
- CVE-2017-0068 — 0.9%
- CVE-2021-31207 — 0.9%
- CVE-2022-24463 — 0.9%
- CVE-2019-0948 — 0.9%
- CVE-2019-0537 — 0.9%

Oracle
- CVE-2016-3427 — 65%
- CVE-2012-5081 — 33%
- CVE-2013-2416 — 0.6%
- CVE-2013-2461 — 0.1%
- CVE-2015-2590 — 0.08%

The share of red zone activity across vulnerabilities differs dramatically among platforms. A full 99% of Linux's red zone is dominated by exploits targeting CVE-2021-44228.35 Compare that to Apple, where the top three vulnerabilities each account for approximately 16% of exploit activity.
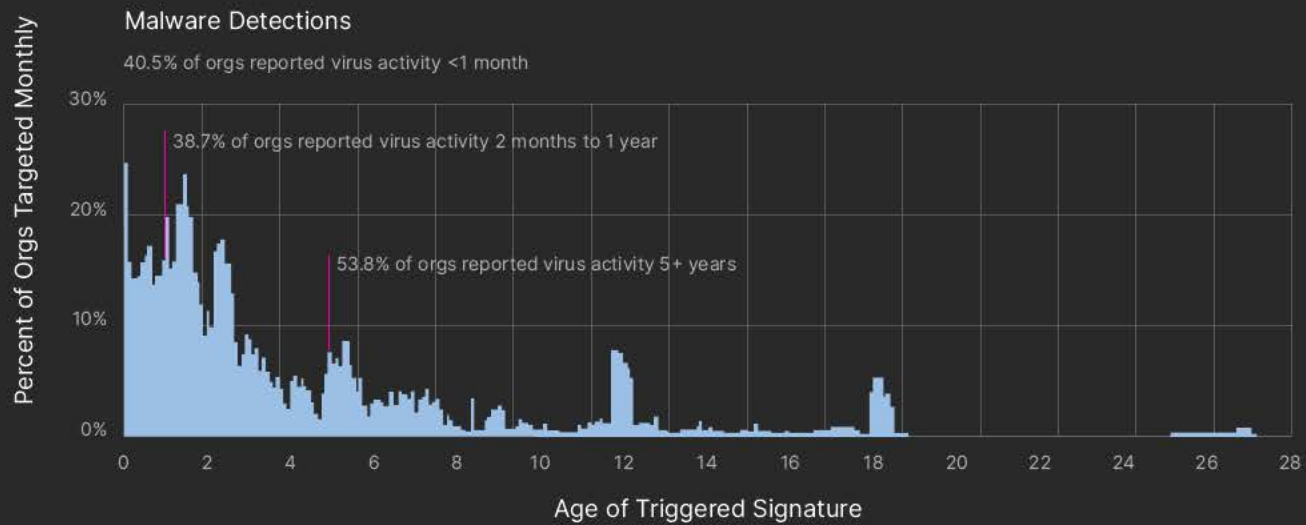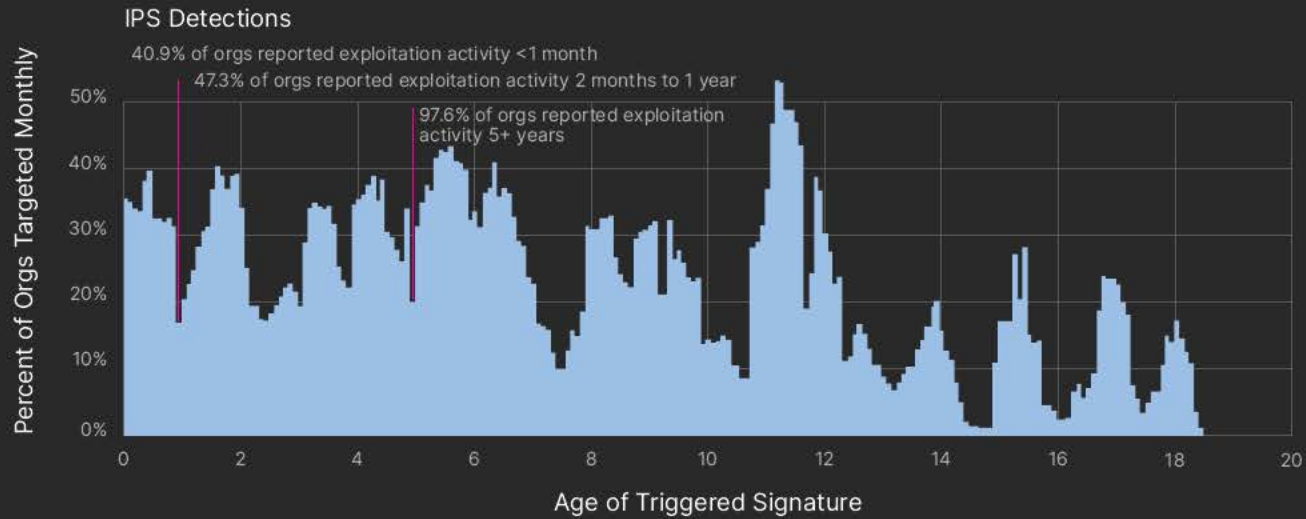
Most of these red zone vulnerabilities aren't new. Only two were published in 2023, and just one of those emerged in the second half of the year (CVE-2023-44487).36 The rest span the last decade. And keep in mind that the exploitation "old" vulnerabilities isn't slowing—the top vulnerability for half the platforms listed was discovered at least five years prior.

From Exploit Prediction to Outbreak

As we've discussed previously, when it comes to vulnerabilities, what's old is still new in the eyes of many attackers. To understand the prevalence of this trend, we identified all vulnerability exploits and malware samples that occurred in 2H 2023 along with the proportion of organizations registering detections. We then charted those signatures according to when they were created and added to Fortinet devices. The charts on the next page measure the active lifespan of exploit and malware threats.

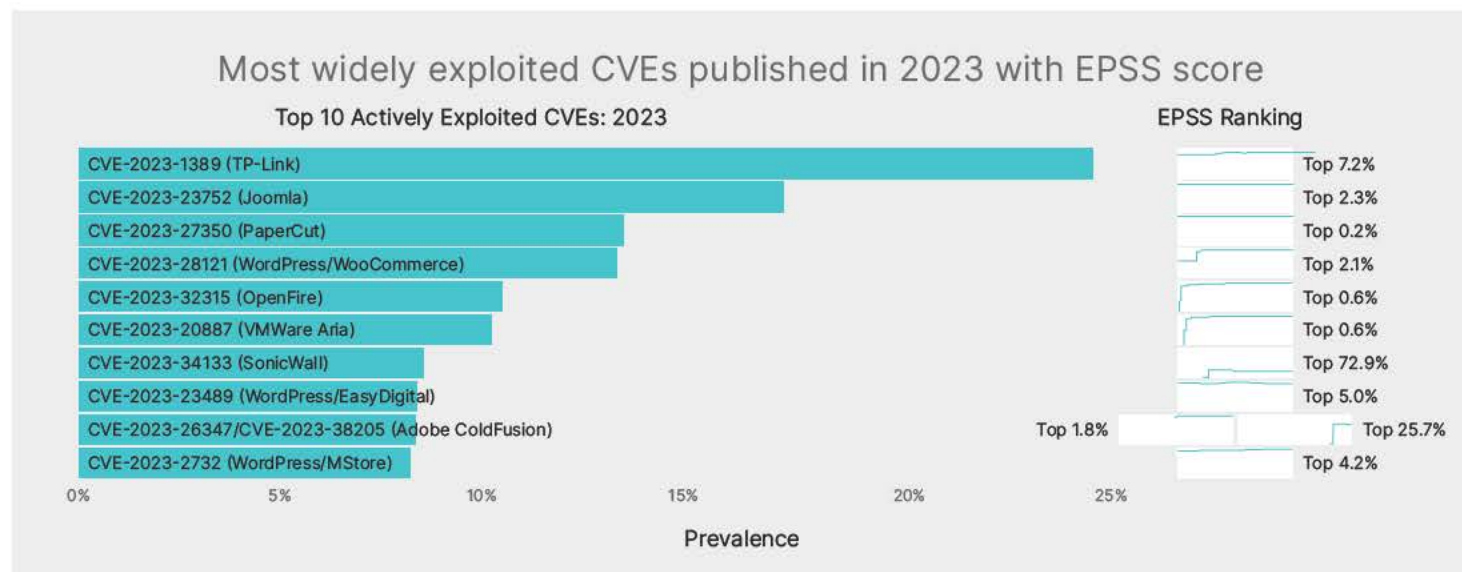# Age and prevalence of exploits and malware detected in 2H 2023

IPS Detections

40.9% of orgs reported exploitation activity <1 month

47.3% of orgs reported exploitation activity 2 months to 1 year

97.6% of orgs reported exploitation activity 5+ years

Percent of Orgs Targeted Monthly

Age of Triggered Signature

Malware Detections

40.5% of orgs reported virus activity <1 month

38.7% of orgs reported virus activity 2 months to 1 year

53.8% of orgs reported virus activity 5+ years

Percent of Orgs Targeted Monthly

Age of Triggered Signature

We continue to observe threat actors exploiting vulnerabilities more than 15 years old. Nearly all organizations (98%) have detected exploits that have existed for at least five years. Yet there's plenty of room for new threats to make their way onto the scene: 41% of organizations also detected exploits from signatures less than one month old. But when it comes to malware, just over half of organizations have detected variants that have been around for five or more years—much less than what we see for exploits.

This analysis yields some critical insights into the cyberthreat landscape. Exploits and malware have very similar speeds and scopes related to their spread, but the longevity of each differs. Malware variants die off more quickly as new code replaces the old. Exploits show a much longer active lifespan because the vulnerabilities cybercriminals target can remain unpatched for years.

Practically speaking, this reinforces the importance of remaining vigilant about security hygiene, as attackers aren't likely to stop exploiting older vulnerabilities. It's also a great reminder to security practitioners to act quickly through a consistent patching and updating program when new vulnerabilities emerge that are likely to be exploited.
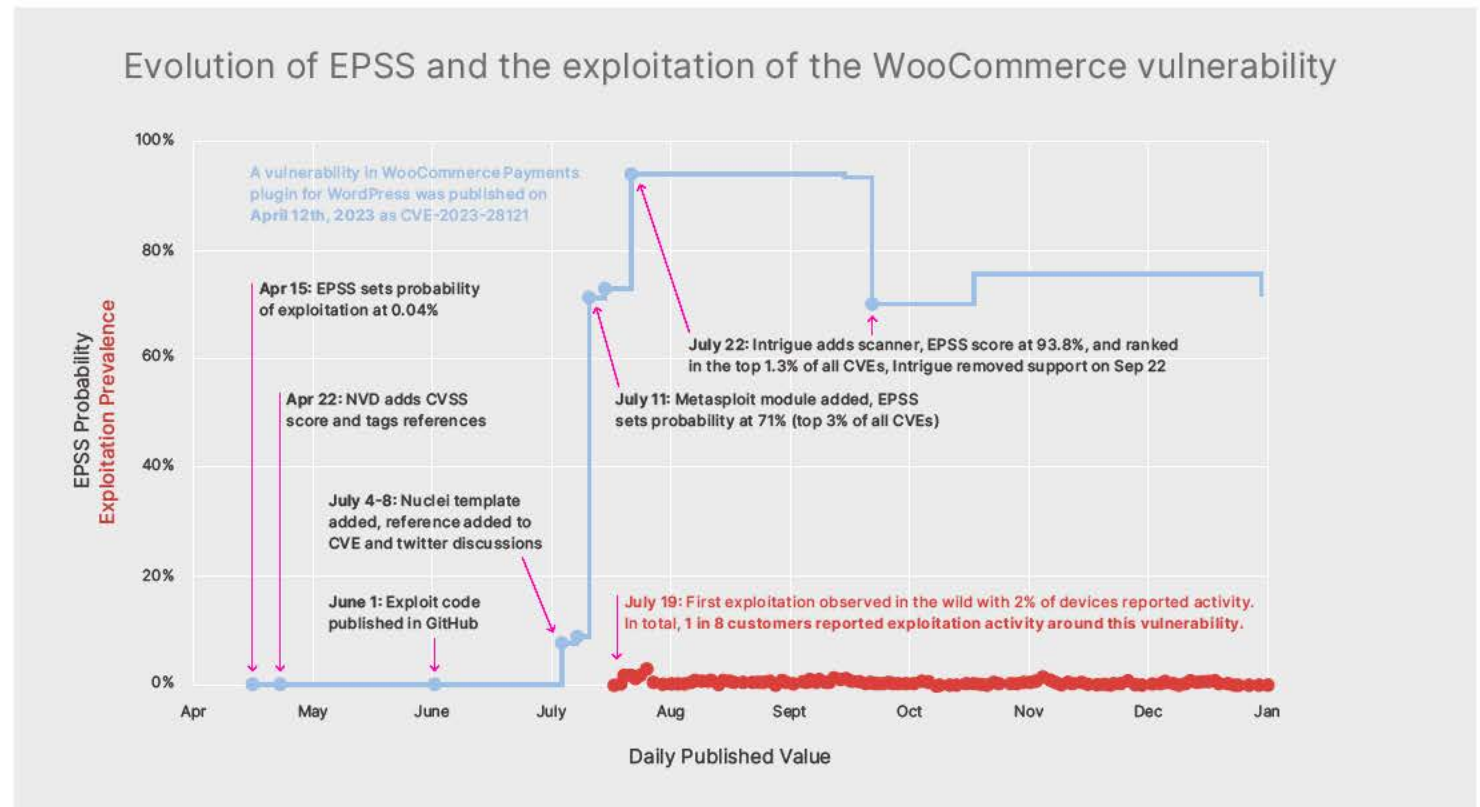
How can you track emerging vulnerabilities that are most likely to be attacked? The Exploit Prediction Scoring System (EPSS) exists for this exact purpose.[37] Fortinet is a major contributor to the exploitation data that drives EPSS. The chart below shows the vulnerabilities released in 202 that were most targeted by exploit activity in the latter half of the year.

Most widely exploited CVEs published in 2023 with EPSS score

Top 10 Actively Exploited CVEs: 2023	EPSS Ranking
CVE-2023-1389 (TP-Link)	Top 7.2%
CVE-2023-23752 (Joomla)	Top 2.3%
CVE-2023-27350 (PaperCut)	Top 0.2%
CVE-2023-28121 (WordPress/WooCommerce)	Top 2.1%
CVE-2023-32315 (OpenFire)	Top 0.6%
CVE-2023-20887 (VMWare Aria)	Top 0.6%
CVE-2023-34133 (SonicWall)	Top 72.9%
CVE-2023-23489 (WordPress/EasyDigital)	Top 5.0%
CVE-2023-26347/CVE-2023-38205 (Adobe ColdFusion)	Top 1.8% / Top 25.7%
CVE-2023-2732 (WordPress/MStore)	Top 4.2%

Prevalence

98%

of organizations have detected exploits that have been in existence for at least five years.

Let's take a closer look at just how accurate EPSS is in identifying vulnerabilities that are likely to be exploited. The chart below highlights EPSS scoring for the vulnerability affecting the WooCommerce Payments plugin for WordPress (CVE-2023-28121).[38] This CVE was published on April 12, 2023, and was initially assessed by EPSS as having a low probability of exploitation. That assessment was revised dramatically after a Nuclei template and Metasploit module were released in early July. Given these changes, the vulnerability rose to the top 3% of EPSS scores with a 71% chance of exploitation in the next 30 days.

Evolution of EPSS and the exploitation of the WooCommerce vulnerability

A vulnerability in WooCommerce Payments plugin for WordPress was published on April 12th, 2023 as CVE-2023-28121

Apr 15: EPSS sets probability of exploitation at 0.04%

Apr 22: NVD adds CVSS score and tags references

July 4-8: Nuclei template added, reference added to CVE and twitter discussions

June 1: Exploit code published in GitHub

July 11: Metasploit module added, EPSS sets probability at 71% (top 3% of all CVEs)

July 22: Intrigue adds scanner, EPSS score at 93.8%, and ranked in the top 1.3% of all CVEs, Intrigue removed support on Sep 22

July 19: First exploitation observed in the wild with 2% of devices reported activity. In total, 1 in 8 customers reported exploitation activity around this vulnerability.

EPSS Probability — Exploitation Prevalence

Daily Published Value

Shortly after this revision of EPSS, our team observed the first signs of exploitation in the wild on July 19. In this case, EPSS provided an effective early warning system prior to the outbreak of attacks, giving defenders a valuable head start on remediation.

With the time-to-exploit decreasing significantly by **43%** to just **4.76** days, the pressure on already stretched cyber-defense resources has intensified. The ability to quickly sift through a prioritized list of vulnerabilities, effectively managing these "ticking time bombs," is now more critical than ever. Integrating this prioritization into your patch management process equips you with a clear, time-sensitive strategy for risk mitigation, enhancing your cybersecurity posture in a rapidly evolving threat landscape.

Ransomware Attacks Increasingly Target Critical Industries

Ransomware continues to keep security teams up at night. According to a recent Fortinet survey, more than 80% of leaders are "very" or "extremely" concerned about ransomware.[39] Across our sensors, ransomware detections surged 13x higher over the first half of 2023. That was followed by a 70% drop during the latter half of the year, during which we also saw fewer organizations detecting ransomware variants.

Weekly prevalence of ransomware detections over 2H 2023
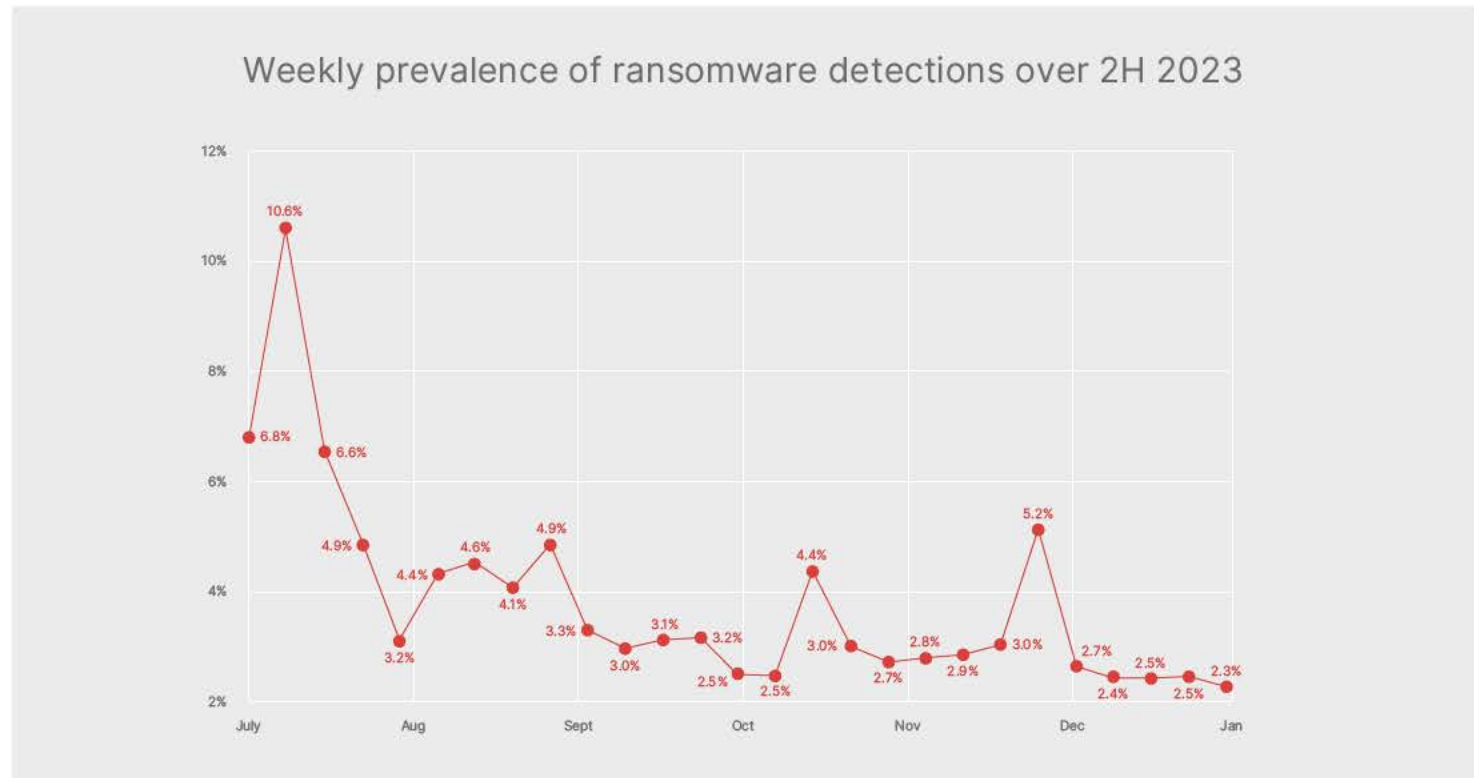
Many of these ups and downs can be traced back to the dynamics of ransomware gangs. Some follow a high-volume, low-margin strategy, which results in a larger number of ransomware variants and victims. Other gangs set their sights on fewer organizations that can pay bigger ransoms using highly targeted attacks.

In our 2024 threat predictions report, we forecast that adversaries looking for bigger payouts would turn their attention to critical industries such as healthcare, utilities, manufacturing, and finance. As predicted, in 2H 2023, we've witnessed a shift away from the traditional "spray and pray" strategy, with cybercriminals taking a more targeted approach combined with ransom demands skyrocketing.[40]

Industries with the highest volume of ransomware and wiper detections

Ransomware		Wiper

Industry	Ransomware	Wiper
Technology	34%	26%
Energy & Utilities	3.5%	31%
Banking/Fin./Insurance	15%	9.3%
Healthcare	6.8%	14%
Manufacturing	15%	4.4%
Transp. and Logistics	6.7%	6.0%
Construction	4.7%	1.8%
Automotive	5.4%	0.24%
Government	0.91%	4.0%
Consulting	2.1%	1.3%
Education	0.77%	1.5%
Retail/Hospitality	1.8%	0.067%
Media/Comms	1.1%	0.048%

The chart above provides an industry breakdown of all ransomware and wiper samples picked up by our sensors over the back half of 2023. The significant presence of industries such as energy, healthcare, manufacturing, transportation and logistics, and automotive offers some evidence of our prediction taking shape. In total, industrial sectors experienced 44% of all ransomware and wiper detections for 2H 2023. This trend is concerning for many reasons, especially because critical industry breaches can have a sizeable and adverse impact on society.

44%

of industrial organizations experienced almost half of all ransomware and wiper detections in the second half of 2023.

Ransomware groups

In the last half of the year, threat actors advertised 23 new malware strains, eight mobile malware strains, 15 Malware-as-a-Service (MaaS) offerings, and six new Ransomware-as-a-Service (RaaS) programs.

A notable example of a new ransomware group that emerged in late 2023 is Ransomed.VC, which initially served as a forum but was later transformed into a ransomware-focused data leak site. The actions of the Ransomed.VC group serves as a testament to the dynamic tactics employed by today's ransomware groups. Their engagement in geopolitical matters, alliances with other groups, participation in data breaches, and promotion of DDoS services has quickly established them as a major player in the ever-shifting realm of cybercrime.

Active ransomware groups and the number of activity reports

Group	Reports
Lockbit 3.0	997
clop-leaks	250
Alphv_BlackCat	240
blackbasta	214
play	211
8base	189
cactus	160
noescape	156
bianlian	124
akira	105
medusa	177
ransomed_vc	68
snatch	63
rhysida	54
losttrust	53
huntersinternational	45
incransom	44
ragroup	40
Nokoyawa	35
mallox	30
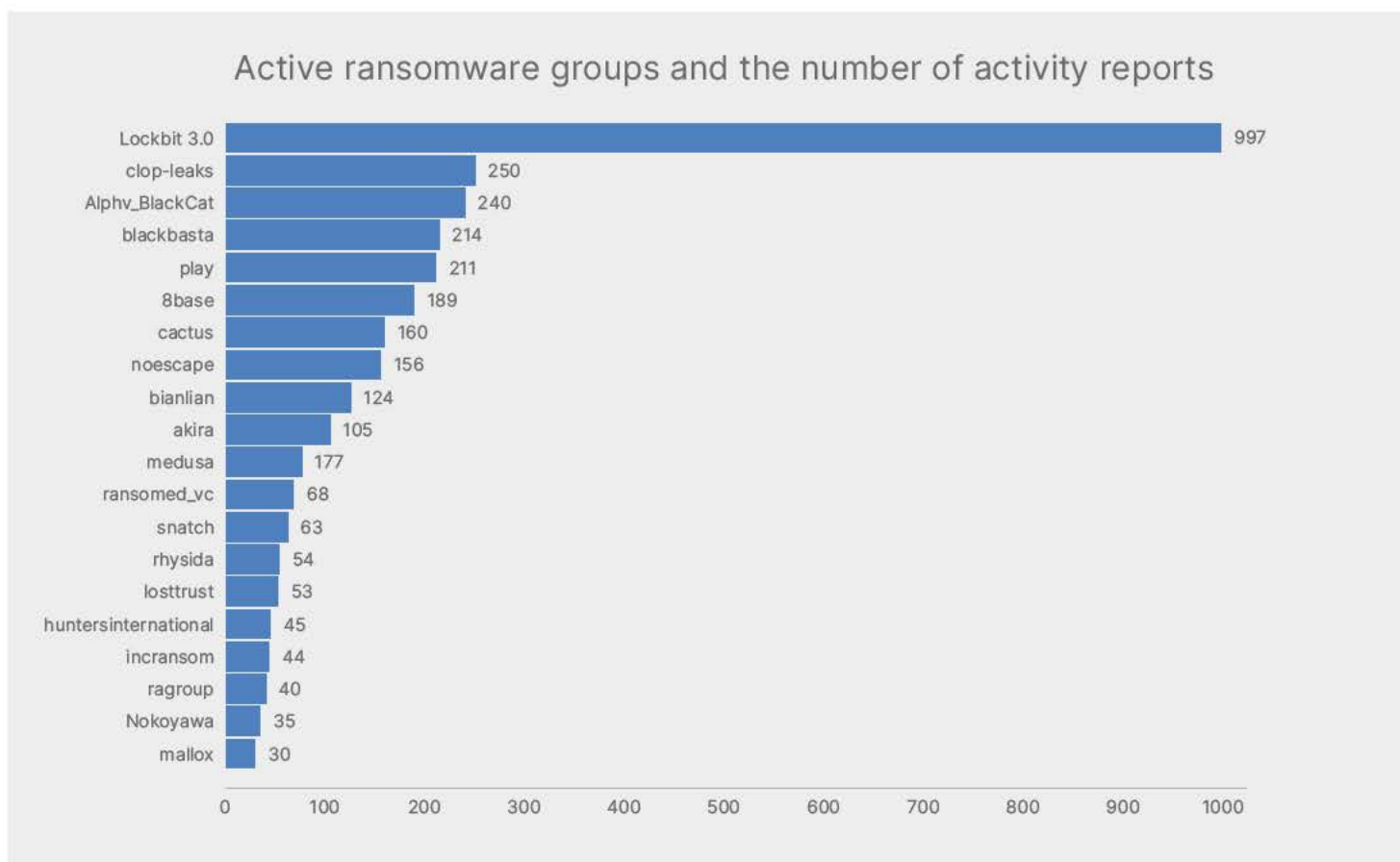
The hacktivist group GhostSec also announced a new ransomware named GhostLocker on the dark web. This announcement signifies the group's expansion into the realm of providing ransomware services, highlighting the ever-evolving nature of the threat landscape and the emergence of new tools within the cybercrime community. GhostSec members primarily use Telegram and X to share their target lists and attack outcomes, which demonstrates how monitoring the dark web can serve as an early warning system for new cybercrime initiatives.

As for the Russian-language cybercrime forum known as XSS, a threat actor using the pseudonym "malwareguy" actively promoted a builder tool designed for the Chaos ransomware version 4.0. The presence of such offerings on underground forums is another example of the ongoing and evolving threats posed by cybercriminals, as well as the need to monitor the dark web for discussions that may give us insight into potential future attack vectors. We expect this trend to intensify as we get deeper into 2024.

Global ATT&CK Heatmap

MITRE ATT&CK is a widely used repository of adversary tactics, techniques, and procedures (TTPs).[41] It offers a common language developed from real-world observations that are used by organizations and cybersecurity teams to build threat models and threat-informed defenses. Many Fortinet solutions offer visibility into ATT&CK TTPs, and we feature two of those in this section.

The first source of discovering ATT&CK techniques is through our sandboxing solutions. Millions of sensors around the world collect suspicious files that are sent through an array of antivirus engines, behavioral analysis, static and dynamic analysis, AI and ML, and intelligence to identify subtle behaviors indicative of their underlying threat. The TTPs identified via this method are best interpreted as capabilities possessed by malware in the wild during 2H 2023.

The image on the following page depicts the most prevalent techniques under each tactic. The percentages correspond to the proportion of organizations that observed malware with capabilities corresponding to each TTP.

Top ATT&CK techniques observed via sandbox solutions

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Replication Through Removable Media: 48%	Exploitation for Client Execution: 27%	Hijack Execution Flow: 33%	Process Injection: 34%	Obfuscated Files/Info: 20%	Input Capture: 43%	System info Discovery: 21%	Replication Through Removable Media: 60%	Data from Local System: 25%	Application Layer Protocol: 44%	Exfiltration Over Alternative Protocol: 96%	System Shutdown/ Reboot: 69%
Phishing: 31%	WMI: 22%	Boot/Logon Autostart Execution: 30%	Hijack Execution Flow: 22%	Masquerading: 15%	OS Credential Dumping: 37%	File and Directory Discovery: 15%	Taint Shared Content: 28%	Input Capture: 25%	Ingress Tool Transfer: 20%	Automated Exfiltration: 3%	Data Encrypted for Impact: 15%
Valid Accounts: 9%	Command and Scripting Interpreter: 19%	Create/Modify System Process: 15%	Boot/Logon Autostart Execution: 20%	Virtualiz./ Sandbox Evasion: 15%	Unsecured Credentials: 15%	Virtualiz./ Sandbox Evasion: 11%	Use Alternate Authentication Material: 4%	Email Collection: 17%	Non-Application Layer Protocol: 18%	Exfiltration Over C2 Channel: 0.4%	Inhibit System Recovery: 5%
Drive-by Compromise: 8%	Shared Modules: 14%	Scheduled Task/Job: 14%	Create/Modify System Process: 10%	Impair Defenses: 11%	Steal Web Session Cookie: 3%	Process Discovery: 11%	Software Deployment Tools: 3%	Automated Collection: 13%	Encrypted Channel: 11%		Service Stop: 4%
Exploit Public-Facing Application: 3%	Scheduled Task/Job: 8%	Office Application Startup: 5%	Scheduled Task/Job: 9%	Process Injection: 10%	Credentials from Password Stores: 0.8%	Software Discovery: 11%	Remote Services: 3%	Browser Session Hijacking: 6%	Non-Standard Port: 6%		Data Destruction: 3%
	Native API: 5%	Event Triggered Execution: 1.0%	Access Token Manipulation: 4%	Hijack Execution Flow: 7%	Network Sniffing: 0.2%	Query Registry: 8%	Exploitation of Remote Services: 0.7%	Clipboard Data: 6%	Proxy: 0.8%		Resource Hijacking: 1%
	System Services: 3%	Browser Extensions 0.6%%	Event Triggered Execution: 1.0%	Modify Registry: 5%	Forge Web Credentials: 0.004%	Remote System Discovery: 8%	Lateral Tool Transfer: 0.7%	Archive Collected Data: 3%	Web Service: 0.5%		Endpoint Denial of Service: 1%
	Inter-Process Comm.: 0.8%	Valid Accounts: 0.3%	Abuse Elevation Control Mechanism: 0.3%	Hide Artifacts: 5%		Application Window Discovery: 6%		Video Capture: 2%	Data Encoding: 0.07%		Data Manipulation: 0.6%
	User Execution: 0.2%	Pre-OS Boot: 0.3%	Valid Accounts: 0.2%	Indicator Removal on Host: 3%		System Network Configuration Discovery: 6%		Screen Capture: 2%	Remote Access Software: 0.05%		Defacement: 0.4%
	Software Deployment Tools: 0.06%	Boot/Logon Initialization Scripts: 0.2%	Boot/Logon Initialization Scripts: 0.1%	Deobfuscate/ Decode Files/Info: 3%		Network Service Discovery: 1%		Data from Info Repositories: 0.5%	Data Obfuscation: 0.04%		Firmware Corruption: 0.2%

Falling ◁────────────▷ Rising

We shared this same chart in our 1H 2023 Threat Landscape Report and wanted to highlight changes over the current period.[42] We layered shading on top to depict whether each technique's ranking remained consistent (gray), increased (red), or decreased (blue). Interestingly, the chart reveals remarkable consistency across TTPs. We do note that quite a few of the techniques sliding down the charts relate to the manipulation, tampering, or obfuscation of information.

As the graphic shows, most tactics had techniques showing increased activity, with the most change coming from "Impact" with "Data Destruction" increasing dramatically. Another technique that warrants attention is "Valid Accounts," rising from sixth in the list to the third spot. This refers to adversaries using compromised credentials, often bought on the dark web, to bypass access controls, create persistent access to remote systems and externally available services, escalate privileges, and evade detection.

We also see some shuffling among positions within "Credential Access" but nothing that constitutes a sea change. The remaining techniques climbing the charts are "Modify Registry" to evade detection, which is expected given the rise of its typical prerequisite, "Valid Accounts," and the use of "Software Deployment Tools" to move laterally. In some high-profile campaigns, we've seen attackers use security software present in victims' environments for their own benefit.

The second source of TTP observations comes via FortiNDR (network detection and response) Cloud sensors. Because these solutions operate at different layers of the stack, you'd expect their visibility of TTPs to differ.

Top ATT&CK techniques observed via FortiNDR

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application: 44%	Command and Scripting Interpreter: 98%	Valid Accounts: 65%	Valid Accounts: 68%	Valid Accounts: 83%	Forced Authentication: 49%	Network Service Discovery: 44%	Remote Services: 54%	Adversary in the Middle: 100%	Application Layer Protocol: 52%	Exfiltration Over C2 Channel: 51%	Resource Hijacking: 100%
System Network Configuration Discovery: 0.2%	WMI: 1%	Scheduled Task/Job: 13%	Scheduled Task/Job: 13%	Indicator Removal on Host: 11%	OS Credential Dumping: 31%	Account Discovery: 27%	Lateral Tool Transfer: 46%		Proxy: 30%	Exfiltration Over Alternative Protocol: 44%	
System Network Configuration Discovery: 0.2%	System Network Configuration Discovery: 0.2%	Boot/Logon Autostart Execution: 12%	Boot/Logon Autostart Execution: 12%	Obfuscated Files/Info: 3%	Steal/Forge Kerberos Tickets: 11%	File and Directory Discovery: 14%			Ingress Tool Transfer: 10%	Exfiltration Over Web Service: 5%	
System Network Configuration Discovery: 0.2%	Exploitation for Client Execution: 0.08%	Create/Modify System Process: 6%	Create/Modify System Process: 6%	Subvert Trust Controls: 3%	Brute Force: 4%	Permission Groups Discovery: 8%			Remote Access Software: 7%		
System Network Configuration Discovery: 0.2%	User Execution: 0.07%	External Remote Services: 4%		Execution Guardrails: 0.3%	Adversary in the Middle: 4%	Network Share Discovery: 5%			Non-Application Layer Protocol: 0.8%		
	System Services: 0.001%	Server Software Component: 0.4%		Deobfuscate/Decode Files/Info: 0.03%		System Network Connections Discovery: 0.7%			Non-Standard Port: 0.4%		
				Rogue Domain Controller: 0.03%		System Info Discovery: 0.6%			Encrypted Channel: 0.007%		
						System Owner/User Discovery: 0.4%			Web Service: 0.005%		
						Remote System Discovery: 0.3%					
						System Network Configuration Discovery: 0.2%					

The differences between the TTPs observed by sandboxes and NDR technology don't mean one is better or worse than the other. Any source reporting on "top" ATT&CK techniques is inherently dependent on the lens through which they're being viewed. The fact that they "see" threats differently makes a compelling case for why security teams need multiple layers of detection to obtain a comprehensive understanding of their organization's risk.

Here are some additional highlights to consider specific to the TTP observations provided by FortiNDR Cloud:

- *C2 techniques:* We detected several techniques in the C2 phase of the MITRE ATT&CK framework, including, but not limited to, Cobalt Strike DNS requests, DNS tunneling, and Long DNS queries. Attackers are increasingly using legitimate services for C2, and in some cases we are already starting to see blockchain used for communications, as this is take-down resistant. Glupteba was the group we saw most recently using this technique.

- *Malware detections:* RATs such as Lokibot and IcedID Banking Trojan continue to trend in detection activity. Loki is an open-source remote access tool with features like file transfer over HTTP or SFTP, launching a local browser, taking screenshots, running a keylogger, and more. Loki is often used as a post-exploitation tool for red team activity or malicious activity. FortiGuard ATR considers Loki to be high severity due to its common usage for lateral movement following a compromise of a single host. IcedID banking Trojan hooks into users' browser sessions and can take screenshots to steal credentials for financial institutions. IcedID is also used to facilitate Access-as-a-Service offerings where access to compromised networks is sold to additional malicious actors. FortiGuard ATR considers IcedID high severity due to the level of access it grants malicious actors to both the environment and information.

- *Defense evasion:* Note that the "Valid Accounts" technique listed in the "Defense Evasion" phase of the MITRE ATT&CK framework is still relevant for possible threat activity that organizations may want to pay attention to. As we have reported from other sources such as FSA and Recon, this technique seems to be abused by threat actors, mainly fueled by Initial Access Brokers on the dark web.

- *Execution:* We detected known malicious portable execution (PE) files seen on the network. A PE file is a specialized file format designed to store executable code, object code, dynamic link libraries (DLLs), and similar resources for use on Windows operating systems. When a PE file becomes malicious, it means that harmful or malicious code has been embedded within it, potentially compromising the security and integrity of any system where the file is executed.

- *Discovery:* Several suspicious Active Directory (AD) and LDAP enumerations (lists of users, groups, and domain trusts) were detected by FortiNDR Cloud. Threat actors can use LDAP and DCE/RPC to enumerate all groups, admins, users, computers, domain controllers, and domain trusts within a domain. After compromising a network, adversaries may query AD to gain a better understanding of an organization's layout and assets.

Shedding Light on Dark Web Activity

While much of our telemetry shows us what actions attackers have taken in the past, darknet intelligence can help us anticipate what adversaries may do next. For the first time in our threat landscape reports, we're sharing insights we've collected from dark web forums, marketplaces, Telegram channels, and other sources during the second half of 2023 that give us a glimpse into emerging threats based on the chatter occurring between threat actors. Using this intelligence, security practitioners can more effectively guard against new and emerging attack techniques and tactics.

Here's a look at some of the most prevalent findings:

- Threat actors discussed targeting organizations within the financial services industry most often, followed by the business services and education sectors.

- The most publicly active threat actors across the dark web were Valerka, Punktir, CoreLab, XXXX, and qwer.

- More than 3,000 data breaches were shared on prominent dark web forums.

- Of these data breaches, threat actors frequently advertised access to organizations through VPN, RDP, and compromised accounts.

- 221 vulnerabilities were actively discussed on the dark web, while 237 vulnerabilities were discussed on Telegram channels.

- 22 significant zero days were advertised, impacting Microsoft Windows, Microsoft Server, Google Chrome, Microsoft Outlook, Adobe Commerce, and BIG-IP.

- Over 850,000 payment cards were advertised for sale, with most being VISA or Mastercard credentials.

Types of access advertised on dark web forums

In the second half of 2023, we observed that threat actors operating in the dark web most often advertise access to organizations via VPN, followed by RDP and compromised accounts:
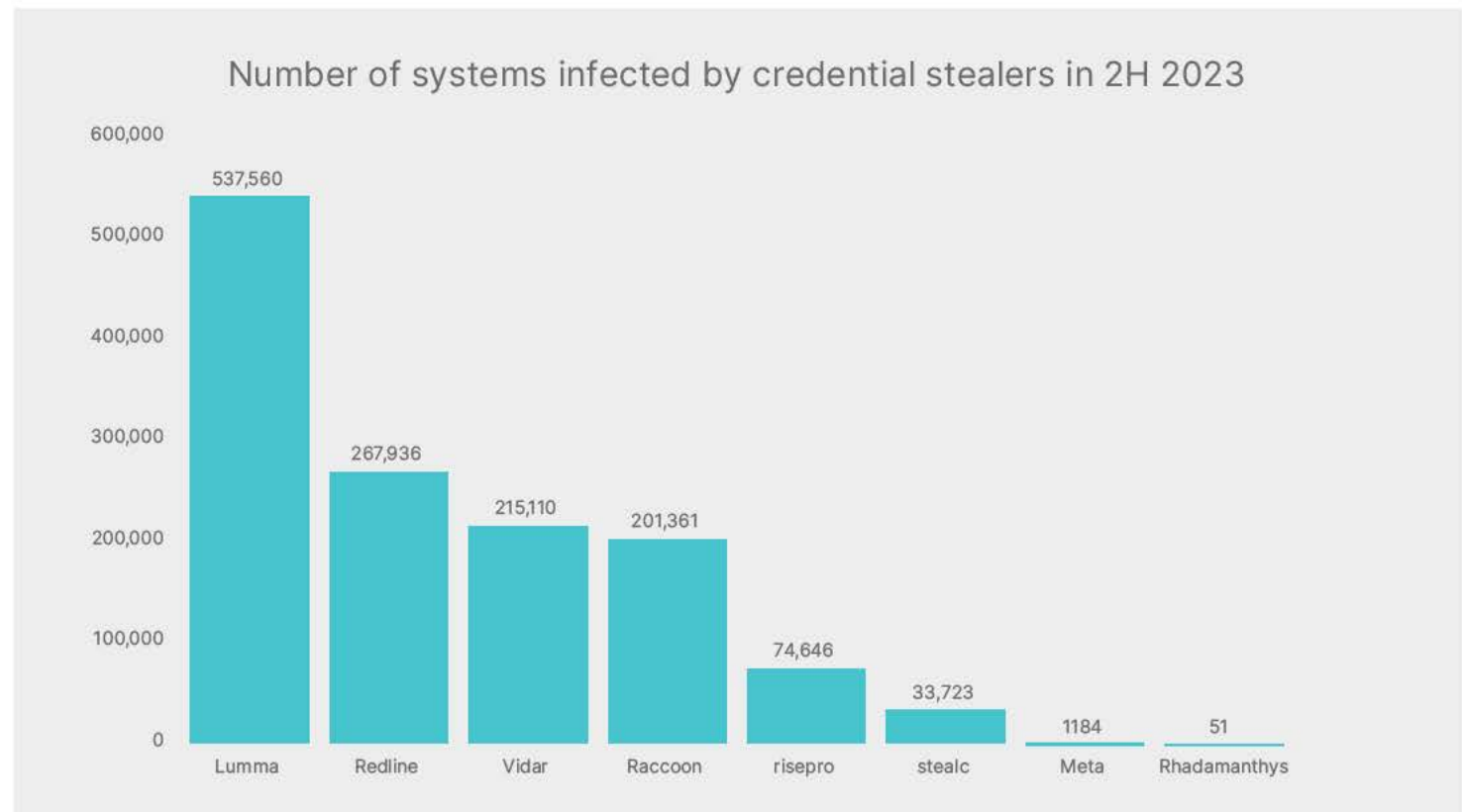
The advertised pricing for access credentials on darknet forums is dynamic and primarily contingent upon the specific targeted organization. Various factors contribute to this pricing structure, such as the valuation of the targeted industry, its scale, the workforce size, and annual revenues. Additionally, the organization's susceptibility plays a pivotal role in determining prices offered by the threat actors. The level of vulnerability exhibited by the organization is another crucial factor that impacts pricing.

Number of advertised credentials seen in H2 2023

Type	Count
VPN	77
RDP	72
Compromised Account	63
Panel Access	58
Webshell	25
Source Code	25
SQL Injection	13
Email Access	13
SSH	12
RDweb	11
Case Management System	11
FTP	8
Exploitation	8
Development System	7
Admin Portal	7
Cloud Access	7
AnyDesk	7
Wordpress	5
Virtualization Environment	4
API	4
Network Devices	3
Storage System	2
SSO	2
Screen Connect	1
VNC	0

Credential stealers

Credential stealers are a type of malware designed to pilfer user account credentials that, if acquired, can help an attacker gain access to secure systems and networks to gather sensitive or critical information. Data from the infected end-user's system is also frequently listed for sale on credential stealer darknet marketplaces.
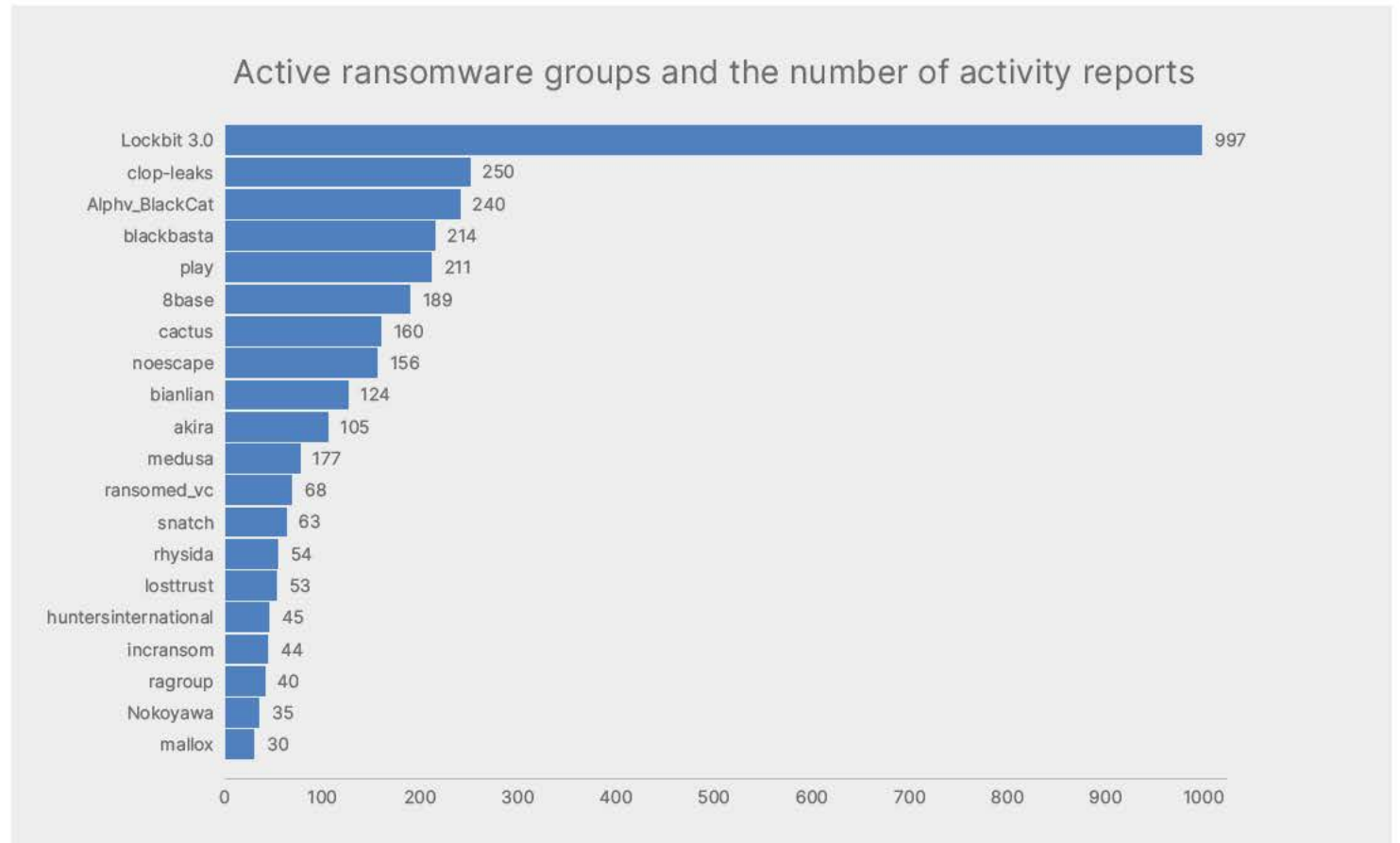
In 2H 2023, we observed over 1,331,571 systems infected by credential stealers, including Lumma, Redline, Vidar, Racoon, Risepro, stealc, Meta, and Rhadamanthys. These stealer logs are available at low prices, enabling large numbers of threat actors to easily acquire them.

Number of systems infected by credential stealers in 2H 2023

Stealer	Count
Lumma	537,560
Redline	267,936
Vidar	215,110
Raccoon	201,361
risepro	74,646
stealc	33,723
Meta	1184
Rhadamanthys	51

We also looked at the types and numbers of credentials being leaked on the dark web:

Number and types of credentials being leaked on the dark web

Type	Count
SSO	938204
GitHub	213071
Webmail	160293
Zoom	146135
ADFS	90929
Cloud Infra	62562
OWA	34730
VPN	30797
Oracle	12818
GitLab	11368
SAP portal	7821
Auth portals	7074
Jira	5665
Zimbra	5509
Okta	4983
Citrix	4295
Salesforce	3044
Admin Portals	2511
Confluence	1861
AnyDesk	1548
Rlogin	1428
SharePoint	820
Admin Portals	735
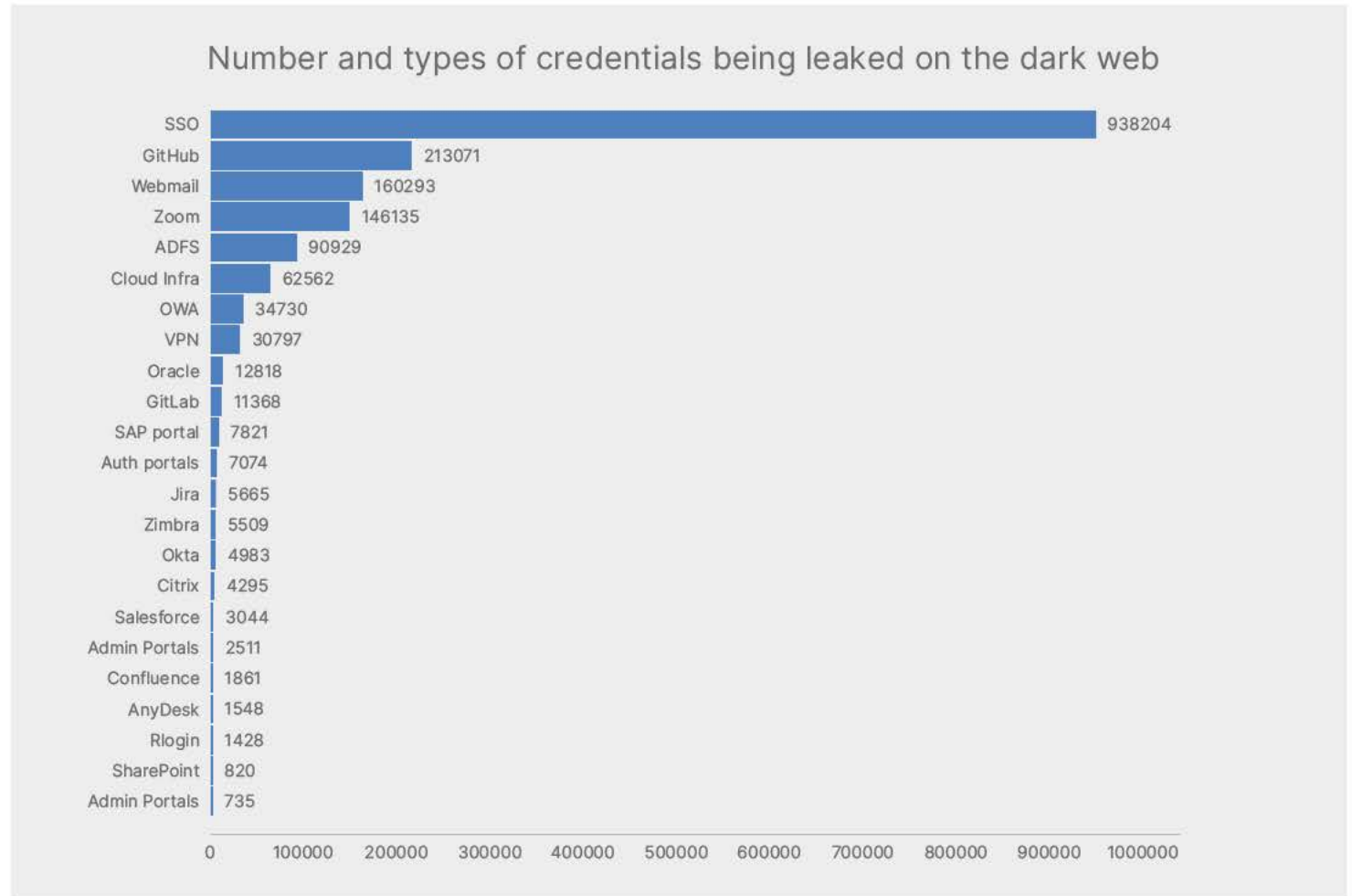
The below chart represents the ransomware groups that have been active in 2H 2023, along with the respective count of victims:

Active ransomware groups and the number of activity reports

Group	Count
Lockbit 3.0	997
clop-leaks	250
Alphv_BlackCat	240
blackbasta	214
play	211
8base	189
cactus	160
noescape	156
bianlian	124
akira	105
medusa	177
ransomed_vc	68
snatch	63
rhysida	54
losttrust	53
huntersinternational	45
incransom	44
ragroup	40
Nokoyawa	35
mallox	30

Trends from the Trenches

The FortiGuard Managed Detection and Response (MDR) team manages endpoint detection and response (EDR) instances on behalf of customers across the globe. Their daily responsibilities give the team a significant snapshot of adversary activities across business verticals and geopolitical regions. Similarly, our intrusion response (IR) team offers proactive and reactive services to support our global customer base. Exposure to customers actively fighting off a security incident provides valuable insight into intrusions initiated by APT groups and financially motivated threat actors.

The following insights come from real-world cases observed by the FortiGuard MDR and IR teams in the second half of 2023. These findings provide practical recommendations for responding to both consistent and emerging features of the threat landscape. They also give us a stronger understanding of how customer actions shape threat trends.

Poorly scoped responses result in unforced errors

Some organizations do not have adequate IR plans or procedures in place, resulting in knee-jerk reactions when a breach occurs. Investigations and remediation actions are often left incomplete. Poorly scoped remediations have resulted in organizations inadvertently "poking the bear," with adversaries responding by rapidly deploying ransomware to cause significant, and wholly unnecessary, damages. This issue also occurs when organizations apply technologies outside their intended use case, for example, practitioners employing legacy, signature-based antivirus solutions in an attempt to eradicate an adversary persisting through in-memory payloads.

Organizations should ensure they have accurate, actionable IR plans and procedures. Teams can improve their security posture significantly by efficiently employing their existing technology through robust procedures.

Failure to patch continues to contribute to intrusions

In 86% of the cases we investigated, where unauthorized access occurred through the exploitation of a vulnerability, the vulnerability was already known at the time and a patch was readily available. Where organizations fail to respond to direct, targeted threat intelligence, it's likely because of a resourcing issue. However, leaders should reassess their security investments given how vital regular patching is to protect against breaches.

Backups connected to production are attractive attacker targets

Our IR team members have worked with some ransomware victims who have invested in backup solutions that authenticate with their main corporate environment and remain connected 24x7. In these cases, the threat actors involved were able to access, manipulate, and encrypt the backup solutions during the intrusions, rendering them worthless. Threat actors often actively search for backups to inhibit system recovery. Organizations should ensure their backups are adequately separated from the network.

Automated deletion processes can hamper investigations

On many occasions, our IR team worked with organizations that had configured their antivirus tools to automatically delete malicious files upon detection, rather than quarantining them. This automatic deletion rule prevents the proper attribution of observed activity, which can slow an investigation. This can also affect security teams who may be unable to properly perform triage once these artifacts have been removed. We recommend that organizations move to a configuration that quarantines samples and stores a copy (or at least collects file hashes) so that IR teams can use alternative retrieval methods if needed.

ESXi servers are cash cows for ransomware operators

ESXi servers are increasingly being targeted during ransomware attacks. (ESXi is a bare metal hypervisor that can partition a server into multiple virtual machines.) ESXi servers offer adversaries a big bang for their buck given the significant impact they can have on an organization's ability to conduct business when compromised. The release of builders such as the Babuk and HelloKitty ransomware, which can be used to target ESXi servers, has made it easier than ever for financially motivated adversaries to target these devices.

Valid accounts continue to provide fast tracks through kill chains

Attackers continue to misuse valid accounts to move laterally across compromised environments. Threat actors use these valid accounts in combination with LoLbins techniques to evade organizations' defenses. As a result, organizations need to monitor for suspicious usage of valid accounts within their environment.

Adversaries are increasingly using Microsoft Windows services to execute RATs

There was a slight increase in the prevalence of Microsoft Windows services being used as the primary execution method for RATs within a victim's environment. Service execution can be used for privilege escalation and can abstract execution in RAT process chains, obscuring malicious activities and increasing complexities for security teams tasked with triaging an incident. This often results in an incomplete investigation by teams lacking the resources to support the in-depth analysis required to link anomalous service activity to compromised accounts and ingress points. Service execution is simple to implement and, given the service-heavy nature of newer versions of Microsoft Windows, adversaries likely view this as another opportunity to evade detection.

Threat actors regularly use open-source administration tools

Threat actors and APT groups continue to use known open-source administration tools to compromise unsuspecting victims. The use of these tools is consistently high for many stages of an intrusion from discovery to lateral movement. Open-source tools are typically lightweight and can often fly under the radar in organizations that don't understand the threat they pose. The issue of identifying suspicious use of these tools is made more complex by the legitimate use of open-source software by system administrators. Organizations should look to characterize the legitimate use of these tools and use application control techniques to block anomalous use.

To get notified when we detect a new or emerging threat, sign up here to receive outbreak alerts from FortiGuard Labs. You can also download the *Outbreak Alerts Annual Report 2023* here.

Conclusion

We hope this edition of the Fortinet threat landscape report provides valuable insights to help you prioritize and implement appropriate security measures within your organization. In summary, here are the three primary trends we observed during the second half of 2023 that stood out most to us. Keep these in mind and adjust your risk management strategy accordingly.

The red zone remains steady. The threat landscape is typically defined by constant change, which is why it's unusual to find something static. The proportion of observed vulnerabilities with known exploits has hovered around 8% since we initially started measuring it nearly two years ago. The vulnerabilities themselves change, of course, but the overall effort required to remediate them apparently does not. Take advantage of this predictability to allocate resources to minimize your organization's red zone.

Keep "old" vulnerabilities on your radar. New exploits and malware can spread far and fast, so if your organization tends to be among the first targeted, it can be only a matter of hours or days before attacks come your way. However, we've also seen that many vulnerabilities, even ones that have existed for years, often remain on threat actors' radar as active targets. Unfortunately, this means you can't be so focused on safeguarding against new vulnerabilities and attacks that you neglect the old ones. Successful security teams need to protect against the entire exploitation life cycle, and this starts with a proactive patching and updating program.

Critical industries are top ransomware targets. The actors behind ransomware campaigns have always been industrious. Whether it's making rapid adjustments to ransom demands based on cryptocurrency market dynamics or creating vast criminal enterprises to minimize cost and maximize scale, they have a penchant for making things happen. That's what makes the ongoing shift to targeting critical industries all the more concerning. These OT-heavy environments are particularly susceptible to costly outages, which greatly increases the pressure to pay high ransoms to restore productivity.

While each of us has a vital role to play in fighting against our collective adversaries, no single organization can single-handedly halt threat actors. Shared intelligence is a crucial part of how we ensure timely and precise responses when attackers strike. The more we collaborate across the public and private sectors, the more effective we can be at disrupting cybercrime.

Footnotes

1   FortiGuard Outbreak Alerts, FortiGuard Labs, accessed February 18, 2024.

2   Zyxel Multiple Firewall Vulnerabilities, FortiGuard Outbreak Alerts, June 6, 2023.

3   Zyxel Router Command Injection Attack, FortiGuard Outbreak Alerts, August 9, 2023.

4   Zerobot Attack, FortiGuard Outbreak Alerts, December 27, 2022.

5   VMware Aria Operations for Networks Command Injection Vulnerability, FortiGuard Outbreak Alerts, June 22, 2023.

6   IBM Aspera Faspex Code Execution Vulnerability, FortiGuard Outbreak Alerts, March 1, 2023.

7   Cisco IOS XE Web UI Attack, FortiGuard Outbreak Alerts, October 20, 2023.

8   Citrix Bleed Attack, FortiGuard Outbreak Alerts, November 2, 2023.

9   Apache RocketMQ Remote Command Execution Vulnerability, FortiGuard Outbreak Alerts, July 5, 2023.

10   Progress MOVEit Transfer SQL Injection Vulnerability, FortiGuard Outbreak Alerts, June 5, 2023.

11   MITRE ATT&CK, accessed February 18, 2024.

12   JS/Agent.CY!tr, FortiGuard Labs Encyclopedia, June 9, 2022.

13   JS/Agent.F022!tr, FortiGuard Labs Encyclopedia, July 10, 2023.

14   JS/Agent.PIV!tr, FortiGuard Labs Encyclopedia, November 1, 2021.

15   JS/Agent.NDS!tr, FortiGuard Labs Encyclopedia, November 7, 2023.

16   JS/ScrInject.B!tr, FortiGuard Labs Encyclopedia, August 30, 2011.

17   Ibid.

18   JS/Cryxos.5478!tr, FortiGuard Labs Encyclopedia, March 30, 2021.

19   CVE-2023-46604, NIST National Vulnerability Database, accessed February 18, 2024.

20   Lucian Constantin, HelloKitty Ransomware Deployed Via Critical Apache Active MQ Flaw, CSO Online, November 2, 2023.

21   Apache ActiveMQ Ransomware Attack, FortiGuard Outbreak Alerts, November 6, 2023.

22   Lazarus RAT Attack, FortiGuard Outbreak Alerts, December 12, 2023.

23   Agent Tesla Malware Attack, FortiGuard Outbreak Alerts, September 7, 2023.

24   CVE-2017-11882, NIST National Vulnerability Database, accessed February 18, 2024.

25   CVE-2018-0802, NIST National Vulnerability Database, accessed February 18, 2024.

26   CVE-2017-9841, NIST National Vulnerability Database, accessed February 18, 2024.

27   CVE-2018-15133, NIST National Vulnerability Database, accessed February 18, 2024.

28   CVE-2021-41773, NIST National Vulnerability Database, accessed February 18, 2024.

29   Cedric Pernet, Androxgh0st Malware Botnet Steals AWS, Microsoft Credentials and More, TechRepublic, January 18, 2024.

30   Ravie Lakshmanan, New Version of Prometei Botnet Infects Over 10,000 Systems Worldwide, The Hacker News, March 10, 2023.

31   The Underground Economist: Volume 3, Issue 12, ZeroFox, June 27, 2023.

32   Kevin Poireault, DarkGate and PikaBot Activity Surge in the Wake of QakBot Takedown, Infosecurity Magazine, November 21, 2023.

33   Common Vulnerabilities and Exposures index, MITRE, accessed February 18, 2024.

34   Douglas Jose Pereira dos Santos, 2H 2022 Global Threat Landscape Report: Key Insights for CISOs, Fortinet, March 3, 2023.

35   CVE-2021-44228, NIST National Vulnerability Database, accessed February 18, 2024.

36   CVE-2023-44487, NIST National Vulnerability Database, accessed February 18, 2024.

37   Exploit Prediction Scoring System, Forum of Incident Response and Security Teams, accessed February 18, 2024.

38   CVE-2023-28121, NIST National Vulnerability Database, accessed February 18, 2024.

39   The 2023 Global Ransomware Report, Fortinet, April 20, 2023.

40   Ransomware Extortion Skyrockets in 2023, Reaching $449.1M and Counting, The Hacker News, July 12, 2023.

41   MITRE ATT&CK, accessed February 18, 2024.

42   FortiGuard Labs 1H 2023 Threat Landscape Report, Fortinet, August 7, 2023.