2023 Mid-Year Threat Review

Rapid7 Research

RAPID7

CONTENTS

EXECUTIVE SUMMARY

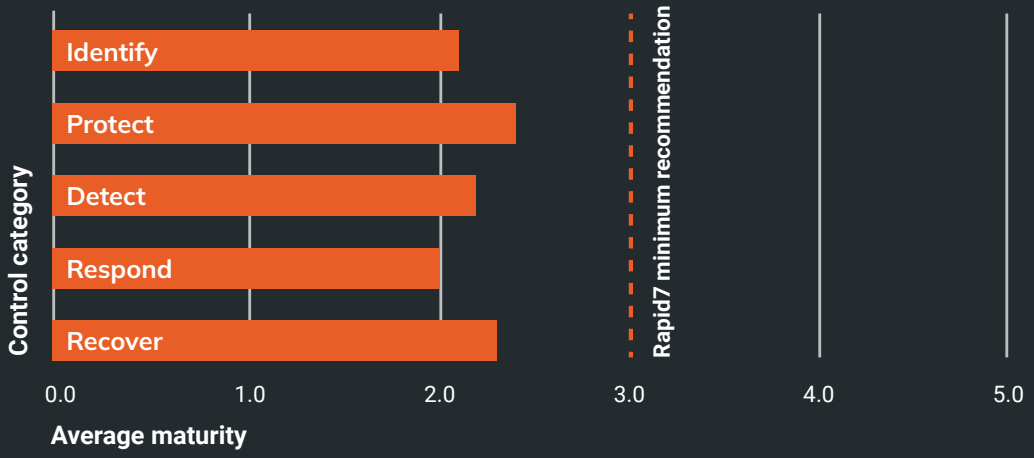
Rapid7's research and managed services teams work side by side during emergent threats and cybersecurity incidents to uncover new forms of risk, shine a light on attacker behavior, and provide timely intelligence that helps our customers and the community strengthen their security posture. Our mid-year threat review draws from Rapid7 threat analytics and underground intelligence data to offer insight on exploit, attack vector, and security landscape trends from the first half of 2023.

- Nearly 40% of incidents Rapid7 managed services teams saw in the first half of 2023 were the result of missing or lax enforcement of multi-factor authentication, particularly for VPNs and virtual desktop infrastructure.
- Ransomware gangs claimed at least 1,500 victims worldwide in the first half of 2023, cementing their status as the dominant threat to global businesses.
- Rapid7 researchers have tracked more than a dozen widely exploited vulnerabilities so far in 2023. Both ransomware groups and APTs continue to exploit vulnerabilities in public-facing applications, particularly in security appliances, business email technologies, and enterprise file transfer products.
- Dark web marketplaces are thriving, often offering a full menu of options to financially motivated threat actors — from zero-day exploits and stolen files to domain-level access to corporate networks.

A Note on Security Maturity

Rapid7 security advisory services consultants conduct a number of security maturity assessments over the course of any given year. Most of these assessments are requested by organizations whose security programs are nascent, and therefore whose initial maturity is expected to be lower than that of businesses with more established programs. Even so, Rapid7 consultants have observed significant programmatic gaps across most assessments conducted over the past 18 months, with only a single organization so far in 2023 meeting our minimum recommendations for security maturity, as measured against CIS and NIST benchmarks.

1H 2023 Average Security Maturity (NIST Benchmark)



Growing cloud adoption and the reality of today's mature, complex cybercrime ecosystem highlight the pressing need for global businesses to establish and measure foundational security program elements, such as inventory and asset management capabilities and a baseline vulnerability risk management program. As some of this report's findings show, basic security hygiene (for example, enabling and enforcing multi-factor authentication) goes a long way toward mitigating risk from a wide range of threats, including attacks levied by highly motivated adversaries.

Vulnerability Intelligence: 1H 2023

Rapid7 researchers tracked more than a dozen new vulnerabilities that were widely exploited over the first half of this year. Overall, more than a third of widespread threat vulnerabilities were used in zero-day attacks, which remain prevalent among exploited 2023 CVEs.

Significant widespread threats from 2023 so far include (but are not limited to):

- **CVE-2023-0669**: Fortra GoAnywhere MFT command injection
- **CVE-2023-29059**: 3CX DesktopApp backdoor (supply chain incident)
- **CVE-2023-34362**: Progress Software MOVEit Transfer SQL injection
- **CVE-2023-2868**: Barracuda ESG appliance command injection
- **CVE-2023-27350**: PaperCut MF/NG remote code execution
- **CVE-2023-28771**: Zyxel ZyWALL/USG remote command execution
- **CVE-2022-47966**: Zoho ManageEngine remote code execution
- **CVE-2022-36537**: ConnectWise R1Soft Server Backup Manager remote code execution
- **CVE-2023-3722**: Avaya Aura Device Services remote code execution

Rapid7 managed services teams have directly observed exploitation of most of the above vulnerabilities in customer environments. Our team has also observed multiple instances of Adobe ColdFusion CVE-2023-26360 exploitation, which may indicate that the vulnerability is being exploited more broadly than the "very limited attacks" Adobe disclosed in their advisory.

Other Exploited CVEs

- **CVE-2023-26360**: Adobe ColdFusion improper access control
- **CVE-2023-20887**: VMware Aria Operations for Networks command injection
- **CVE-2022-21587**: Oracle E-Business Suite remote code execution
- **CVE-2023-47986**: IBM Aspera Faspex remote code execution
- **CVE-2023-27997**: Fortinet Fortigate heap-based buffer overflow
- **CVE-2023-27532**: Veeam Backup & Replication remote code execution
- **CVE-2022-44877**: CentOS Web Panel remote code execution
- **CVE-2022-46169**: Cacti command injection

As expected, Rapid7 managed services teams also continue to see exploitation of older vulnerabilities that remain unpatched. Two notable examples from 1H 2023 are CVE-2021-20038, a Rapid7-discovered vulnerability in SonicWall SMA 100 series devices, and CVE-2017-1000367, a vulnerability in the sudo command that allows for information disclosure and command execution. Rapid7 researchers also disclosed vulnerabilities in Adobe ColdFusion and Fortra Globalscape Enhanced Managed File Transfer products, both of which are likely to be future targets for attackers.

Incident Response Trends: 1H 2023

Rapid7 incident responders have seen a 69% increase in caseload year over year in the first half of 2023. Anecdotally, we aren't alone — industry partners and peers have mentioned similarly noticeable upticks in the number of incidents they've taken on.

While continued ransomware prevalence and high-profile attacks play a part in this trend, plenty of the initial access vectors Rapid7 services teams have observed this year are old classics, like brute forcing or credential stuffing attacks on internet-exposed systems that don't have multi-factor authentication (MFA) enabled.

H1 2023 Initial Access Vectors

39%
Remote Access

27%
Vulnerability Exploitation

13%
Phishing Payloads

6%
Supply Chain Compromise

4%
Insider Threat

11%
Other

Source: Rapid7 MDR Incident Response

Nearly 40% of incidents Rapid7 managed services teams saw in the first half of 2023 were the result of missing or lax enforcement of multi-factor authentication, particularly for VPNs and virtual desktop infrastructure (VDI). Vulnerability exploitation has also been a prevalent vector, and phishing attacks remain a reliable scourge of corporate networks.

Eleven percent of incidents arose from a mish-mash of initial access vectors, including (but not limited to):

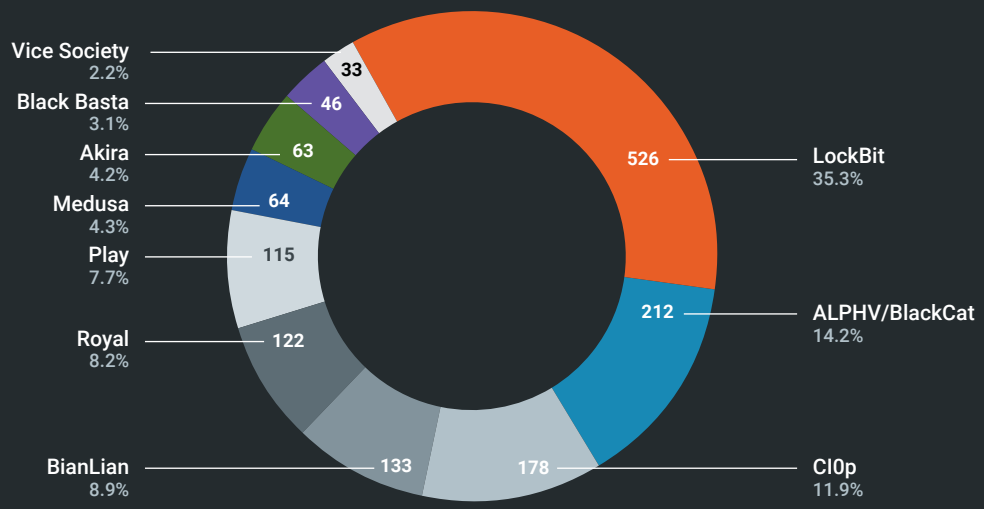
- Cloud misconfigurations
- SEO poisoning
- Failure to eradicate threat actors during previous compromises

A small percentage of engagements concluded without a clearly defined attack vector, often because of missing logs or prematurely wiped data. The end of this report contains practical security guidance to mitigate against the most common types of attacks Rapid7 incident responders see.

Ransomware: 1H 2023

The ransomware landscape during the first half of 2023 has been largely stable as far as the top groups operating in the space. The below diagram shows the number of ransomware incidents attributed to each of the top players as of late June 2023, based on leak site communications, public disclosures, and Rapid7 incident response data.

Incident Response Data



Note: The number of incidents attributed to Cl0p in this chart is likely to be (significantly) low, since the group is still actively claiming new victims from their May 2023 zero-day attack on MOVEit Transfer.

Notably, this data does not take into account all the downstream organizations and individuals that have been indirectly compromised by ransomware incidents at upstream providers or partners. With groups like Cl0p habitually targeting file transfer technologies, which often means exposure of third-party customer or client data, we can expect that downstream victims will significantly outpace primary or direct victims in these types of attacks.

While the top ransomware players have remained stable over the first half of the year, new groups are also continuing to emerge. The Akira ransomware gang, which appears to have launched around the end of Q1, is one of this year's more salient examples, having garnered more than 60 known victims despite only being active for a few months.

EXPLOIT BROKERS AND THE DARK WEB

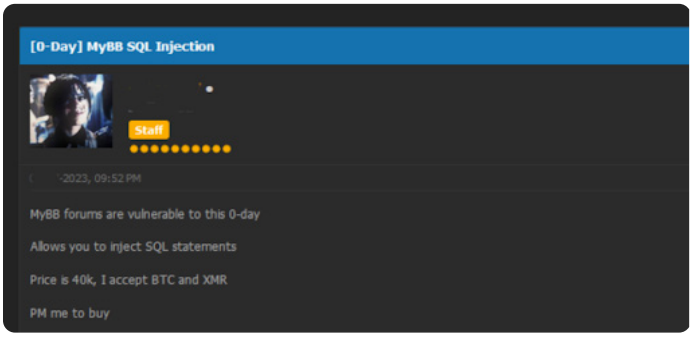
The prevailing demand for remote exploits in security appliances and network edge devices is evident in broker prices for zero-days in common enterprise brands. Below are the going rates for zero-day exploits on a well-known broker site (vulns-sec.com) as of July 2023:

Network Devices

Juniper (RCE)	$75,000+
Cisco (RCE)	$75,000+
FortiNet (RCE)	$75,000+
Citrix (RCE)	$75,000+
Sophos (RCE)	$75,000+
Sonicwall (RCE)	$75,000+
F5 (RCE)	$75,000+
HP (RCE)	$50,000+
IBM (RCE)	$50,000+
Huawei (RCE)	$50,000+
ASUS (RCE)	$5,000+
ZyXEL (RCE)	$5,000+

Source: vulns-sec[.]com

Even if exploit brokers hypothetically demanded 10x returns on these investments — say, by selling a zero-day exploit in one of these devices for $750,000 after acquiring it for a mere $75,000 — ransomware-as-a-service (RaaS) outfits like Cl0p, who have reportedly extorted victims for hundreds of millions of dollars, could easily cover that cost with a single victim payment.



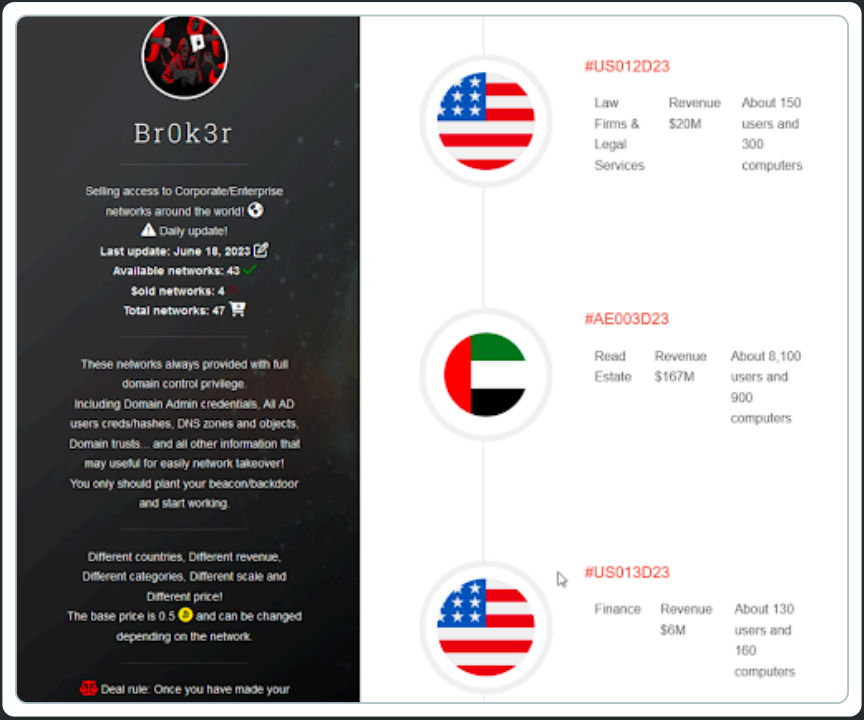
A dark web post offering a zero-day exploit

The potential profit margin for successful RaaS operations, in other words, is staggering. In all likelihood, a threat actor like Cl0p would easily be able to afford a bevy of zero-day exploits for vulnerable enterprise software — enabling the group to hoard and hone proprietary capabilities while they conduct reconnaissance on high-revenue targets. It's not a theoretical use case, either; there are indications that Cl0p tested their zero-day exploit for MOVEit Transfer (CVE-2023-34362) for nearly two years before deploying it in a highly orchestrated attack over Memorial Day weekend this year.

Initial Access as a Service

Buying zero-day exploits isn't the only way for threat actors to gain access to target environments, of course. Business is booming for dark web marketplaces that sell access to compromised networks. Some of these marketplaces advertise revenue and size of victim companies alongside a guaranteed level of access — making it simple for ransomware groups to calculate how much a victim organization can afford to pay.

The site below, for instance, is a relative newcomer to the dark web ecosystem:



The takeaway, once again, is that profit-motivated cybercriminals stand to make outsized profits from even a single successful ransom negotiation.

APT and State-Sponsored Activity: 1H 2023

Rapid7 researchers gather, analyze, and vet data from a wide range of sources for inclusion in a central threat library that supports Rapid7 products and services. The statistics and insights in this section are based on threat data from dark web forums, private messaging platforms (e.g., Telegram), and public reports in addition to intelligence from Rapid7's own managed services teams.

State-Sponsored Threat Activity

Rapid7 researchers tracked 79 known state-sponsored threat actor attacks in 1H 2023, at least 24% of which leveraged exploits against public-facing applications to target governments, critical infrastructure, and corporate networks. 23% of the state-sponsored attacks Rapid7 tracked used spear phishing to gain access to victim environments, and 22% involved the abuse of valid accounts.

Motives across the groups we tracked include:

- Cyber warfare: Campaigns where threat actors conducted attacks against infrastructure in the ongoing conflict in Ukraine
- Cyber espionage: Campaigns aimed at gathering intelligence or intellectual property for political or economic advantage
- Financial: Campaigns that target the private sector in order to evade economic sanctions and/or fund state regimes

The table below shows the most common MITRE ATT&CK techniques used in state-sponsored attacks over the first half of the year:

Rank	Initial Access	Execution	Persistence	Defense Evasion
1	T1190: Exploit Public-Facing Application	T1059.001: PowerShell	T1574.002: DLL Side-Loading	T1574.002: DLL Side-Loading
2	T1566.001: Spear Phishing Attachment	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1140: Deobfuscate / Decode Files or Information
3	T1566.002: Spear Phishing Link	T1059: Command and Scripting Interpreter	T1078: Valid Accounts	T1036: Masquerading
4	T1078: Valid Accounts	T1204: User Execution	T1505.003: Web Shell	T1055: Process Injection

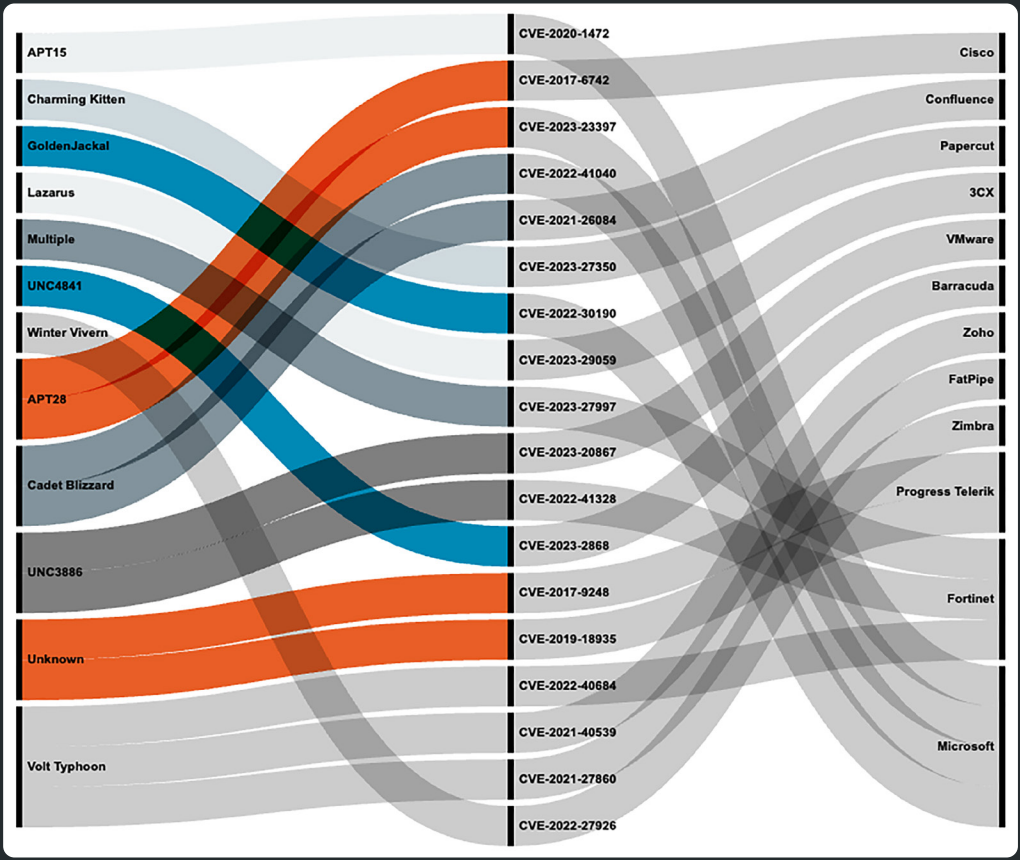
APT Vulnerability Exploitation

Much like financially motivated and commodity threat groups, advanced persistent threat (APT) actors targeted both new (zero-day) and known vulnerabilities in commonly deployed enterprise technology across the first half of the year.

Unsurprisingly, major targets included routers, security appliances, print management software, and Voice Over IP (VOIP) solutions — in other words, all the usual network edge suspects in addition to business email and virtualization platforms. VOIP technologies in particular seem to be an underappreciated attack vector in traditional network security reporting; we expect to see these targeted more in the future.

Older vulnerabilities have remained a functional part of many threat actors' arsenals. While APTs have deployed exploits for newer vulns such as CVE-2023-2868 (Barracuda ESG) and CVE-2023-27997 (Fortinet) thus far in 2023, the majority of attacks our team tracked have leveraged older vulns, including years-old flaws in Cisco IOS and Telerik UI.

Mapping Threat Groups to CVEs and Products



While APT attacks tend to garner more media and industry coverage, nearly all of the CVEs and techniques used in advanced attacks have also been used more broadly. For timely information on emergent threats and widespread attacks, see the Emergent Threat Response section of Rapid7's blog.

Practical Security Guidance

The vulnerabilities, attack vectors, and threats detailed in this report can be considerably mitigated with basic security hygiene, including rigorous MFA enforcement and well-defined, risk-based vulnerability management procedures.

A particular learning from the first half of 2023, however, is this: One of the most important ways organizations can mitigate catastrophic data theft and extortion risk in the face of a mature, highly motivated threat ecosystem is to put measures in place to prevent data exfiltration wherever possible.

This includes (but is not limited to):

- Alerting on or restricting unusually large file uploads; looking for large volumes of traffic to a single IP or domain
- Monitoring for unusual access to cloud storage (ex: Google Drive, SharePoint, ShareFile)
- Monitoring for or adding firewall rules to block known file sharing sites (ex: filetransfer[.]io, anonfiles[.]com, mega[.]nz)
- Monitoring for data transfer utility presence or usage (ex: Filezilla, WinSCP/Putty, MegaCMD, BITS, etc.)
- Monitoring for data archiving utility presence and usage (ex: 7zip, WinRAR, WinZip, etc.)
- Implementing egress filtering
- Restricting local admin privileges on hosts

Additional Security Guidance

Implement and harden MFA. Nearly 40% of incidents during the first half of 2023 were the result of missing or inconsistent enforcement of MFA, particularly on VPN, VDI, and SaaS products. Rapid7 MDR has also observed an uptick in MFA push fraud as a result of notification fatigue. Many MFA vendors offer number matching as a way to prevent MFA fatigue.

Block .one at the perimeter or email gateway. Microsoft OneNote has been abused to spread malware and credential stealers, predominantly through phishing emails. This was the root cause of the majority of phishing incidents our team observed in 1H 2023. Read more here.

Put network edge devices, including VPNs and file transfer appliances, on a high-urgency patch cycle. Network perimeter devices like VPNs, routers, switches, internet-facing load balancers, and more have been primary targets for attackers of all skill levels. These business-critical technologies are often an adversary's doorway to corporate networks, and they frequently provide a jumping-off point for threat actors to pivot deeper into compromised environments. Critical vulnerabilities in these products should ideally be patched urgently, within hours or days wherever possible.

Focus on vulnerability management fundamentals. Today's threats often demand that businesses invoke emergency patching and incident response procedures, but it's impossible to clarify what qualifies as an emergency without an understood, accepted definition of normal. Clearly defined routine patch cycles should have measurable deadlines and results, and ideally should prioritize patching actively exploited vulnerabilities in addition to applying OS-level and other important updates.

Additional Resources

Rapid7 researchers and community members publish vulnerability analysis in Rapid7's open vulnerability research platform, AttackerKB. These analyses often include sample proof-of-concept code and indicators of compromise in addition to exploitation timelines and attack chain analysis. To contribute or subscribe to Rapid7 notifications in AttackerKB, create a free account here.

Rapid7 zero-day vulnerability research is published on a regular basis here.

When a new threat arises, Rapid7 guidance can be found in the emergent threats section of the Rapid7 blog, along with corresponding information for Rapid7 customers. If you are a customer, we'd love to hear your feedback. You can contact your customer success manager (CSM) or technical account manager (TAM), or contact us at research@rapid7.com.

PRACTITIONER-FIRST SECURITY SOLUTIONS ARE HERE

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/