Cato Networks:

Cato CTRL
SASE Threat Report

Q2 | 2024

Table of Contents

Foreword 3

Executive Summary 5

Chapter 1: Top Threat Intelligence Trends 7

Chapter 2: Top Enterprise Security Trends 18

Top 10 Spoofed Brands 19

Top 10 AI Applications Used 21

Top 10 Anonymizer Applications Used 23

Chapter 3: Top Network Security Trends 25

Suspicious Activity Monitoring (SAM) 27

Secure vs. Insecure Protocols 31

Mitigated Vulnerabilities 38

Chapter 4: Key Recommendations 41

Chapter 5: Conclusion 44

Methodology 45

About Cato CTRL 45

About Cato Networks 45

Foreword

Cato CTRL (Cyber Threats Research Lab) is the cyber threat intelligence (CTI) team at Cato Networks.

Cato CTRL protects organizations by collecting, analyzing and reporting on external and internal threats, utilizing the data lake underlying the Cato SASE Cloud Platform.

Through this data lake, Cato CTRL has granular data on every traffic flow from every device communicating with the Cato SASE Cloud Platform. This data lake is further enriched with hundreds of security feeds and analyzed by proprietary AI/ML algorithms and human intelligence (HUMINT). The result is a unique data repository that provides Cato CTRL with insights into the threat landscape and network characteristics for all traffic, including inbound, outbound and WANbound traffic.

For those unfamiliar with these terms, here is an explainer:

- **Inbound:** Traffic that doesn't originate from within a network, but attempts to enter the perimeter of a network

- **Outbound**: Traffic that originates from inside a network and is destined for services on the internet or outside networks.

- **WANbound:** Traffic that resides within a Wide Area Network (WAN). For example, between a branch and a datacenter.

Cato's ability to provide a holistic view of inbound, outbound and WANbound threats, as well as external data, is exceptionally unique in the industry. Without such a holistic view, it's difficult to accurately evaluate the threat landscape for organizations.

Additionally, Cato CTRL utilizes HUMINT to investigate the dark web and hacking communities. This enables Cato CTRL to understand what threat actors are buying, selling, discussing and planning.

With the release of the Q2 2024 Cato CTRL SASE Threat Report, Cato CTRL is delivering threat intelligence that enables organizations to stay ahead of emerging threats and keep their environments secure. The Q2 report provides insights into:

- **Threat intelligence trends**, particularly within hacking communities and the dark web.
- **Enterprise security trends,** including the top 10 spoofed brands, the top 10 AI applications used and the top 10 anonymizer applications used.
- **Network security trends,** including key stats on Suspicious Activity Monitoring (SAM), secure vs. insecure protocols and mitigated vulnerabilities.

We hope you find the Q2 2024 report informative.

Etay Maor
Chief Security Strategist at Cato Networks
Founding Member of Cato CTRL

Executive Summary

The Q2 2024 Cato CTRL SASE Threat Report provides insights into the threat landscape across several key areas: hacking communities and the dark web, enterprise security and network security. These insights are gathered from Cato CTRL's analysis of 1.38 trillion network flows across more than 2,500 customers globally between April and June 2024.

Key findings include:

IntelBroker is a highly active threat actor selling data and source code

In its investigation of hacking communities and the dark web, Cato CTRL came across a threat actor named IntelBroker, who is a prominent figure and moderator in the BreachForums hacking community.

IntelBroker's illicit activities encompass a wide range of cybercriminal tactics. In recent months, IntelBroker has offered to sell data and source code from AMD, Apple, Facebook, KrypC, Microsoft, Space-Eyes, T-Mobile and U.S. Army Aviation and Missile Command.

Amazon is the top spoofed brand - thanks to cybersquatting

Cybersquatting involves using a domain name with the intent to profit off another brand's registered trademark. Threat actors leverage cybersquatting to harvest user credentials through various techniques, including malware distribution or phishing attacks.

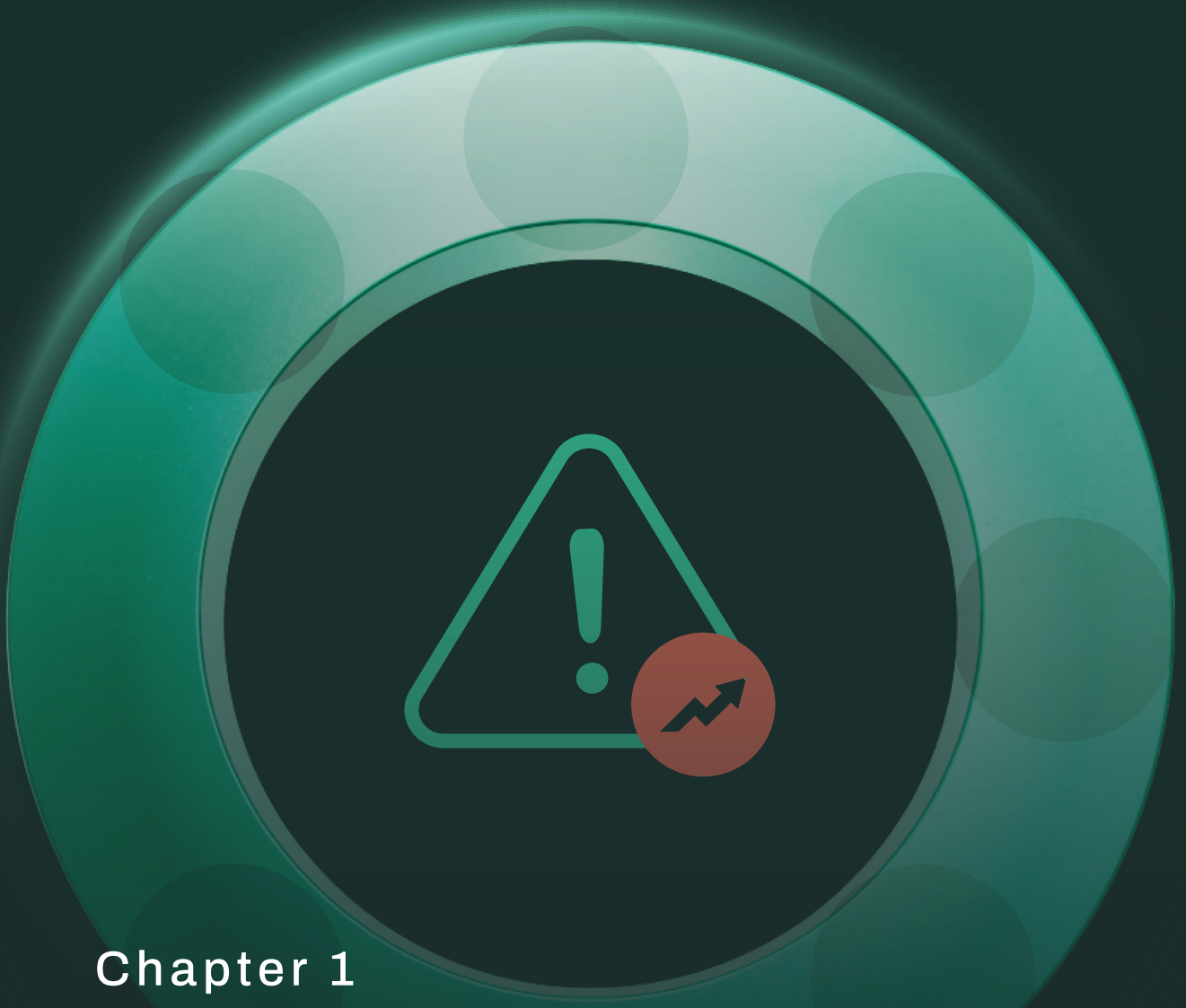
In Q2 2024, Cato CTRL observed that Amazon was the top spoofed brand by a significant margin (66% of domains), with Google ranked second at 7%. Given the popularity of Amazon, users should be wary of threat actors creating counterfeit websites that ask to submit sensitive information. Users could be putting themselves or their organizations at risk.

Log4j remains a popular vulnerability that threat actors attempt to exploit

Three years after its discovery in 2021, Log4j remains one of the most used vulnerabilities leveraged by threat actors. From Q1 2024 to Q2 2024, Cato CTRL observed a 61% increase in the attempted use of Log4j in inbound traffic and a 79% increase in the attempted use of Log4j in WANbound traffic.

The Oracle WebLogic vulnerability, which originated in 2020, is another popular exploit leveraged by threat actors. From Q1 2024 to Q2 2024, Cato CTRL observed a 114% increase in the attempted use of the Oracle WebLogic vulnerability in WANbound traffic.

Inbound traffic is traffic that doesn't originate from within the network, while WANbound traffic resides within a WAN environment. For threat actors, these are different potential entry points to infiltrate organizations and conduct attacks.



Chapter 1

Top Threat Intelligence Trends

In each quarterly edition of the Cato CTRL SASE Threat Report, we focus on a trend that is drawing increased demand in hacking communities and the dark web. In the Q1 2024 Cato CTRL SASE Threat Report, we focused on artificial intelligence (AI) including the use of enhanced attack tools, deepfakes and talent recruitment to develop AI-based systems for threat actors. In Q2 2024, we noticed an increase in the release and sale of breached company data.

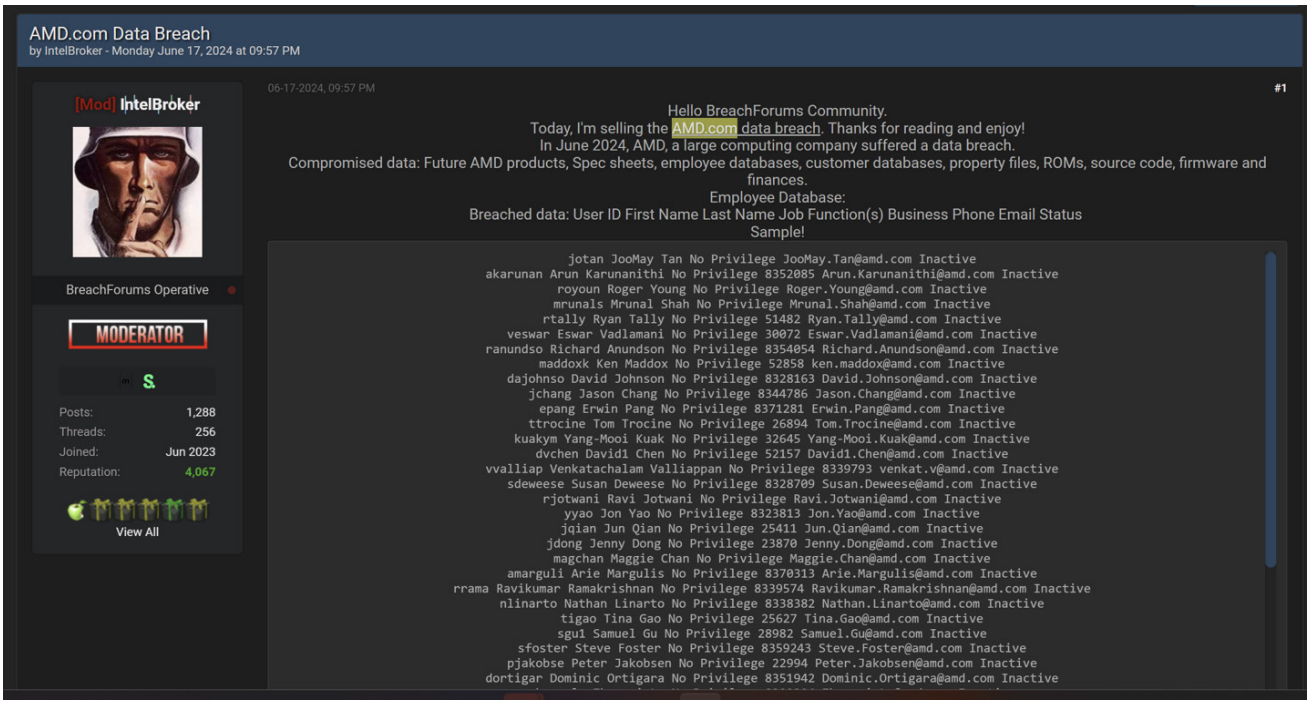


Figure 1. IntelBroker sells AMD data including source code

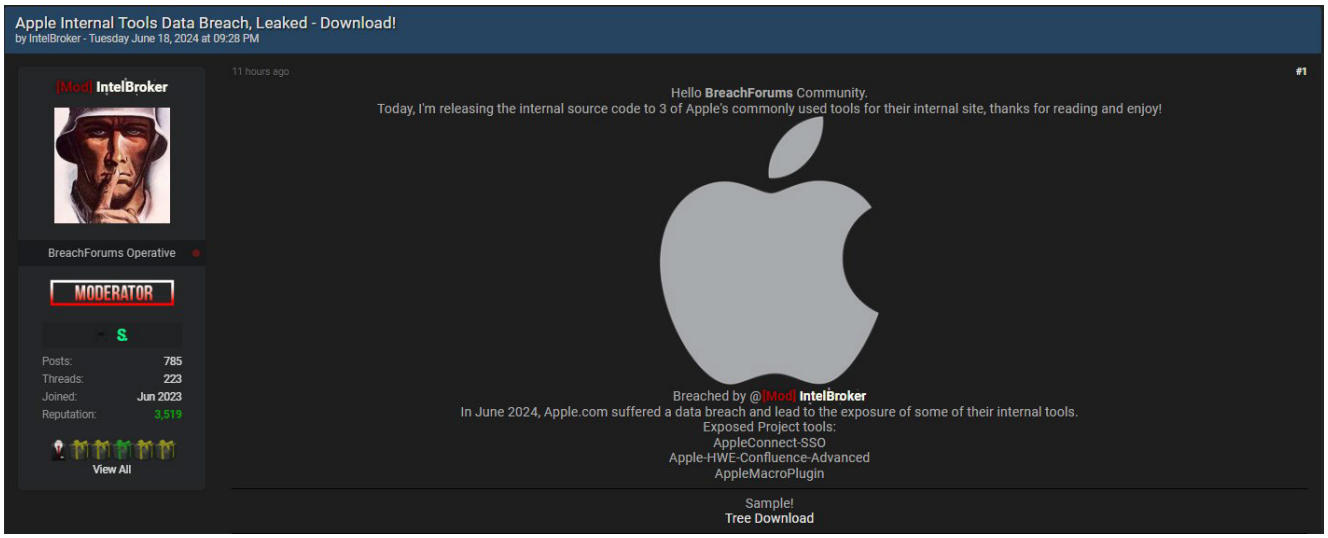


Figure 2. IntelBroker sells Apple source code

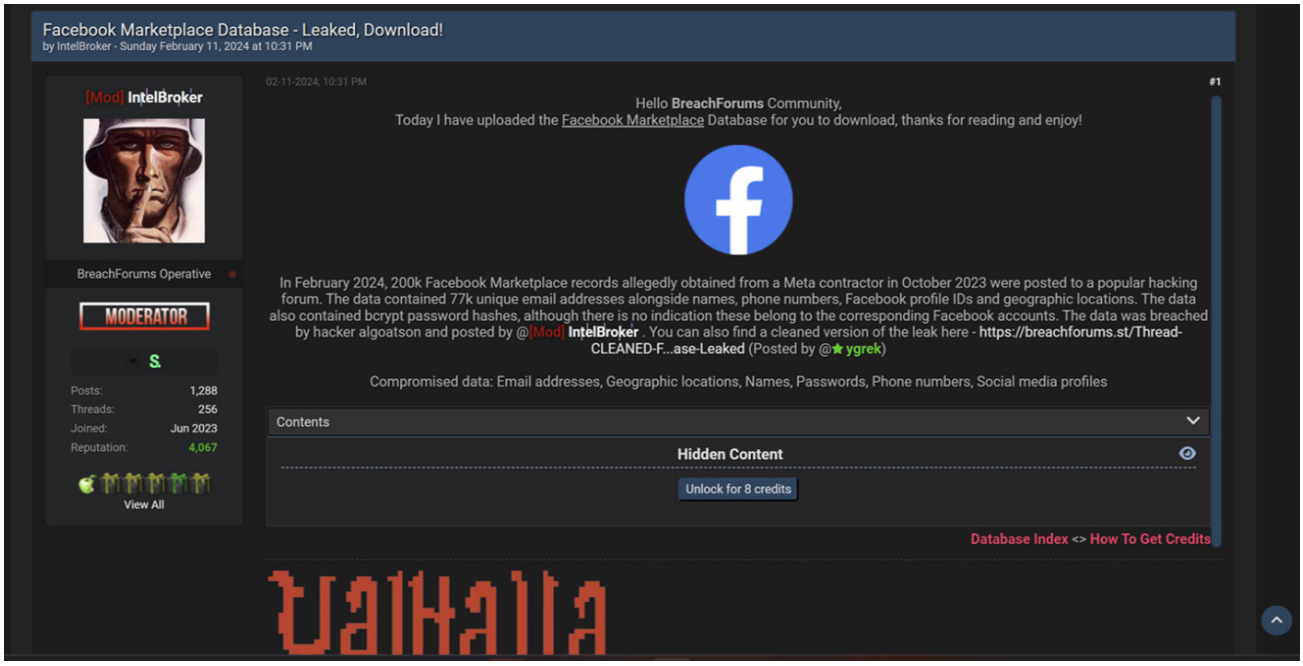


Figure 3. IntelBroker sells Facebook Marketplace data

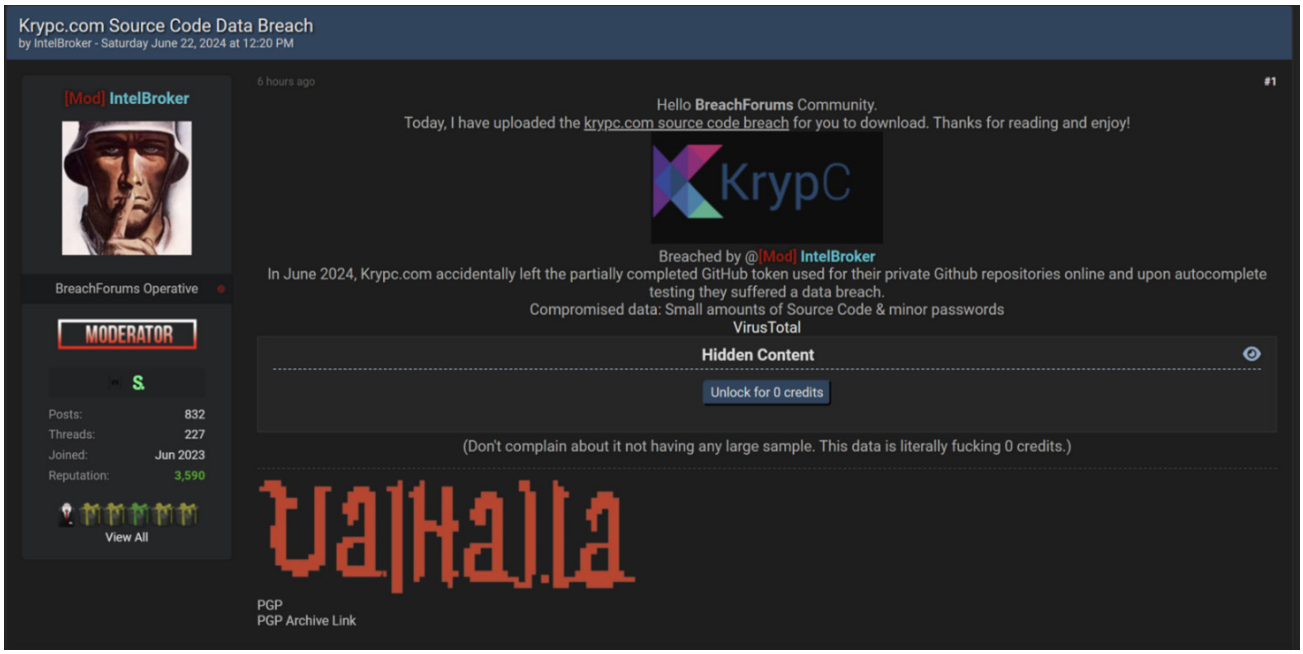


Figure 4. IntelBroker sells KrypC source code

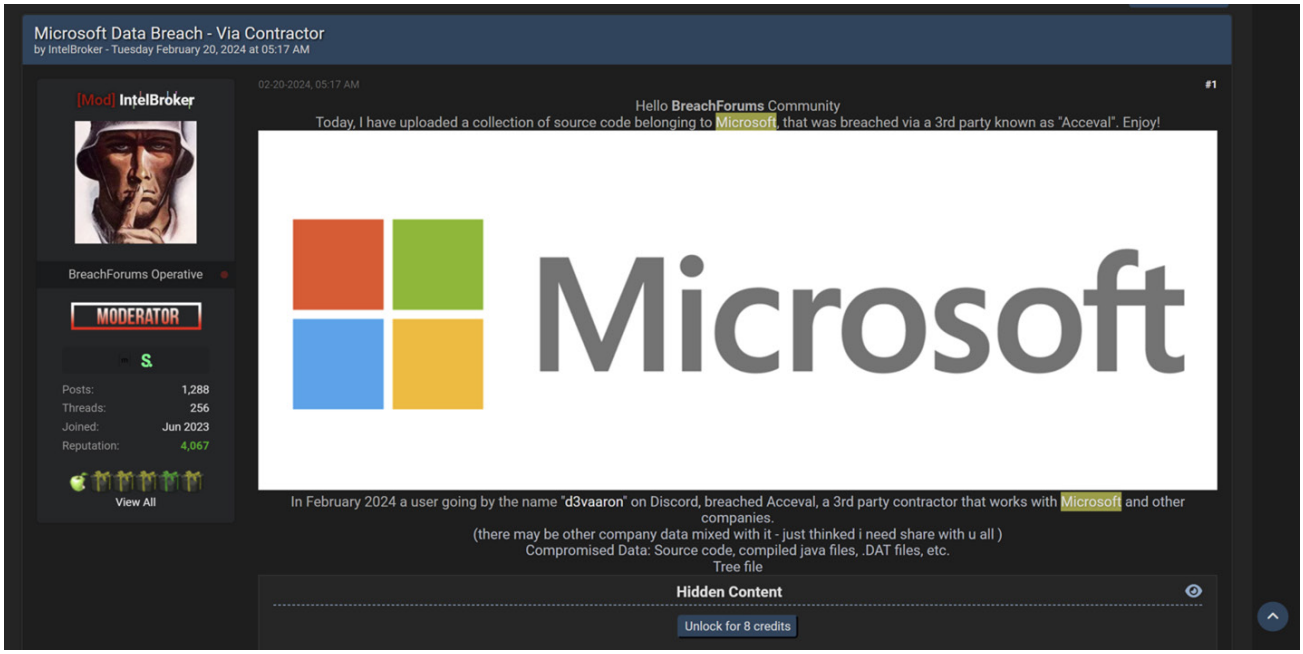


Figure 5. IntelBroker sells Microsoft data that was breached via a third-party

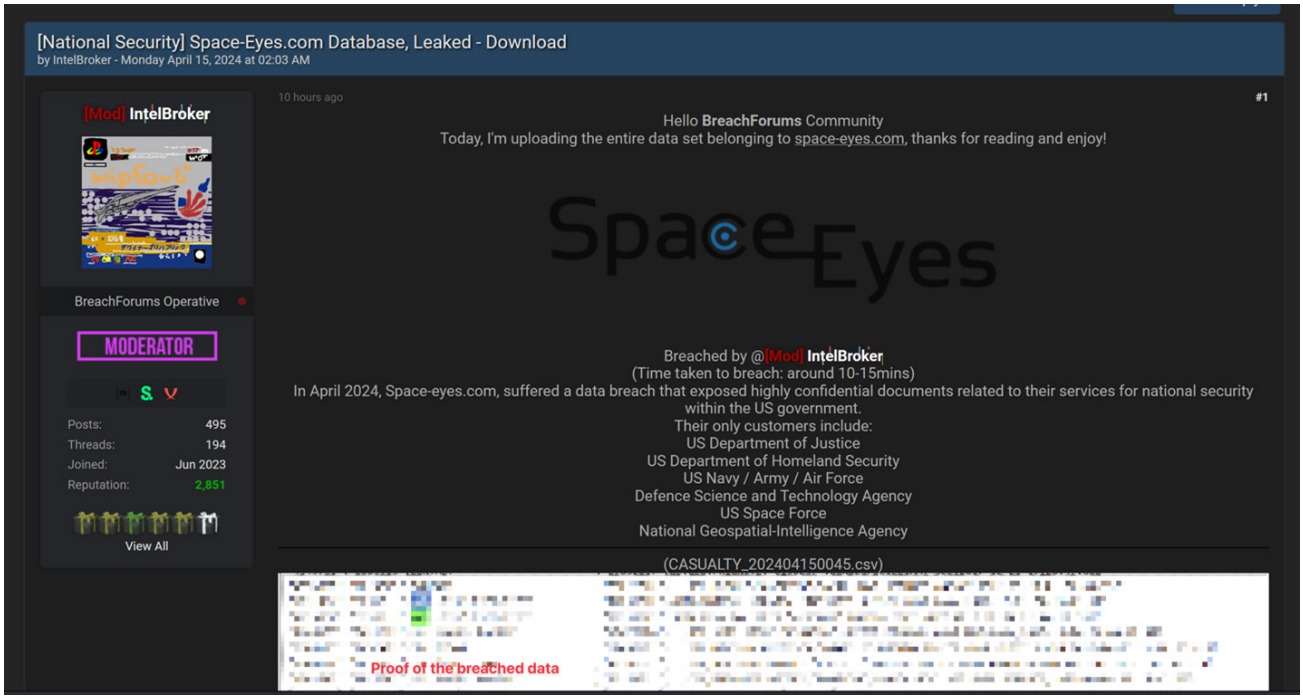


Figure 6. IntelBroker sells Space-Eyes documents

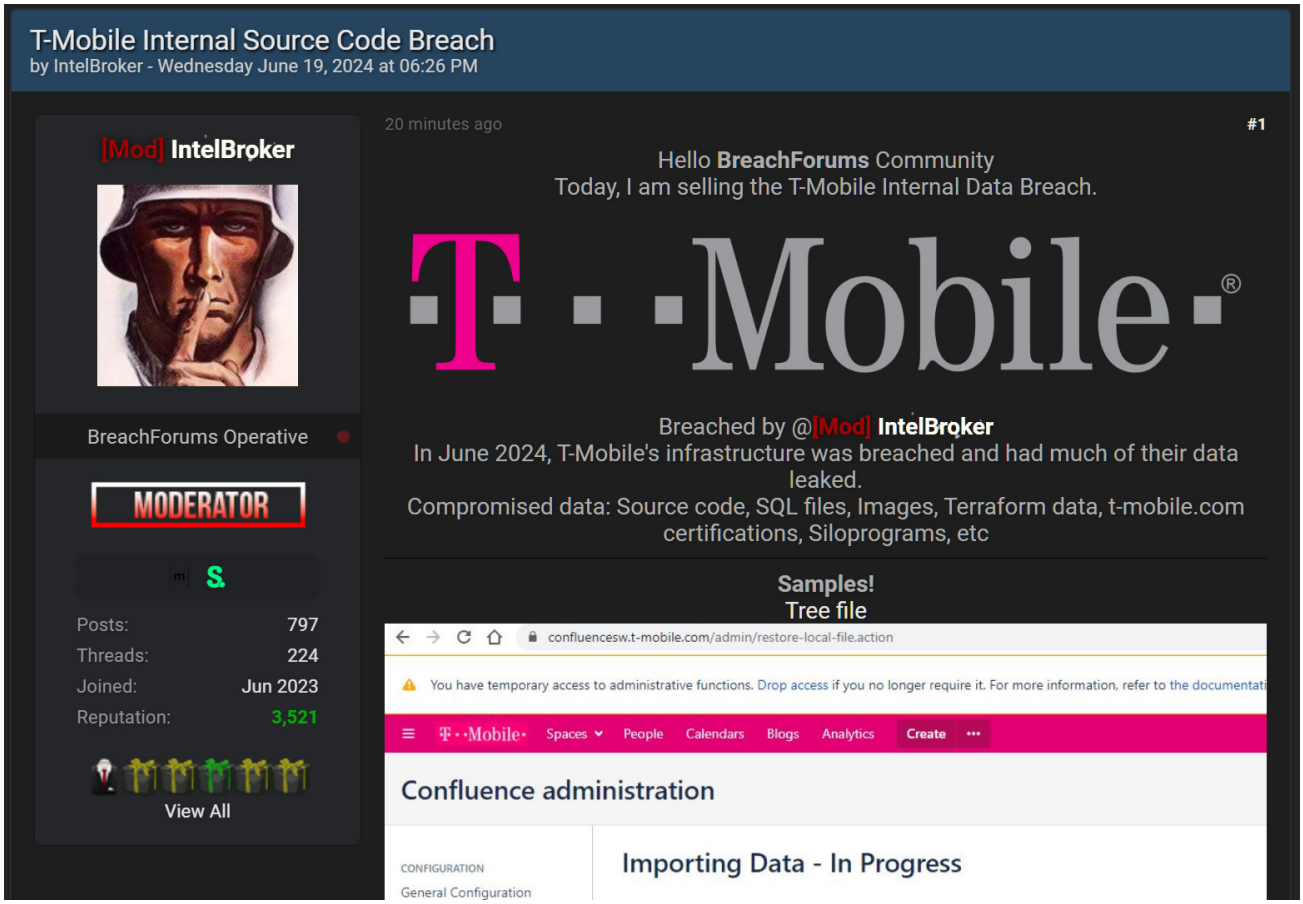


Figure 7. IntelBroker sells T-Mobile data

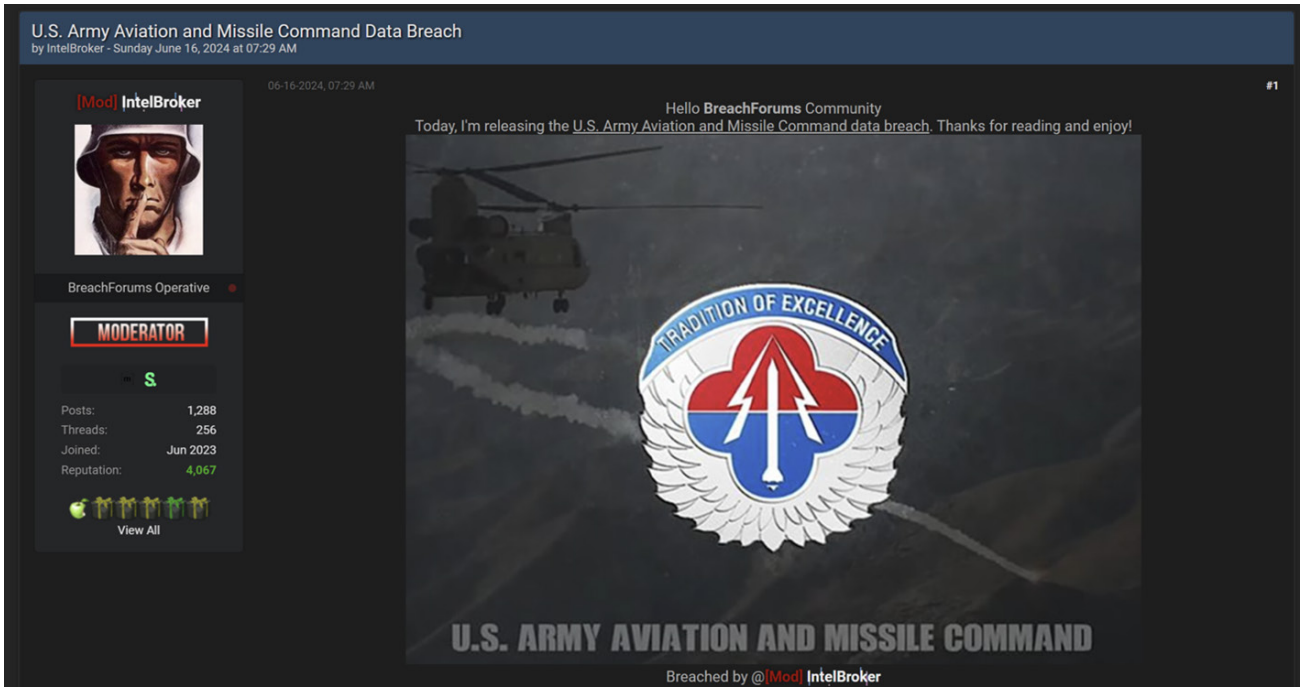


Figure 8. IntelBroker sells U.S. Army Aviation and Missile Command data

Meet IntelBroker, a moderator and highly active threat actor in the hacking community BreachForums. In recent months, IntelBroker has been offering up data and source code from top brands and organizations such as: AMD, Apple, Facebook, Microsoft, KrypC, Space-Eyes, T-Mobile and U.S. Army Aviation and Missile Command. IntelBroker does not target a specific industry. He targets them all.

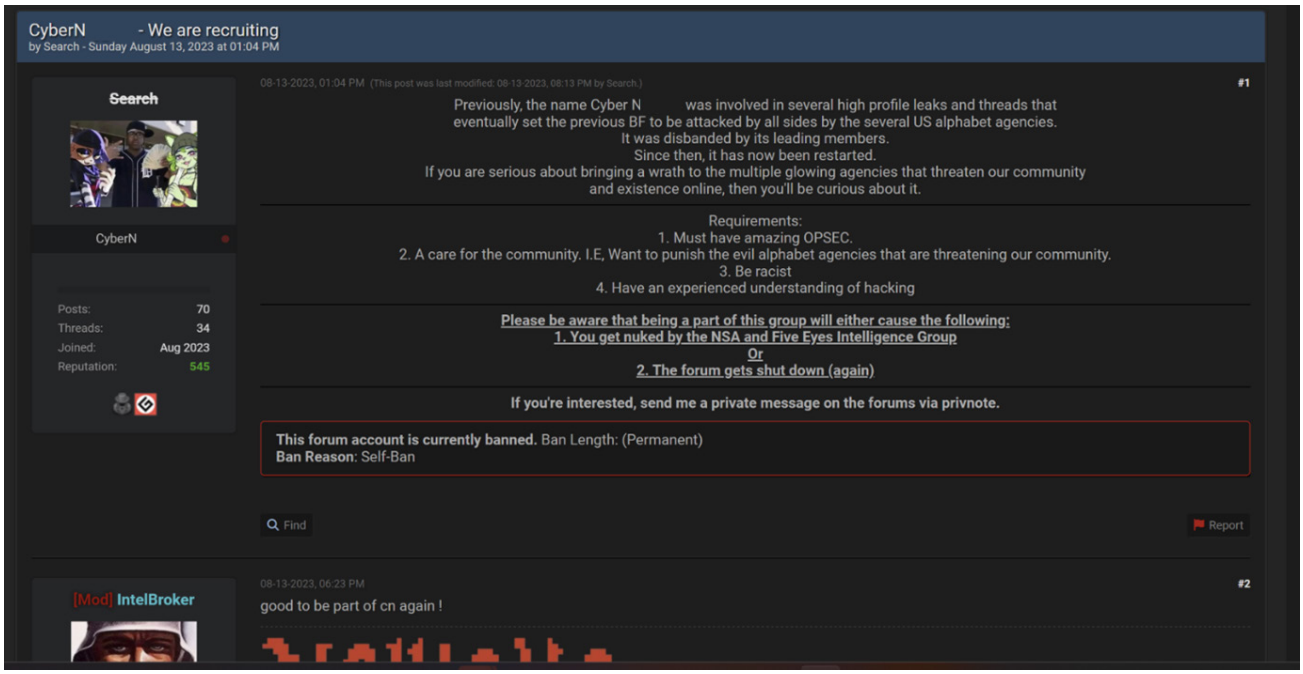


Figure 9. IntelBroker joins CyberN******** hacking group

Based on a post from BreachForums, IntelBroker is associated with the hacking group CyberN*****. It's still unclear what specific role he plays in the hacking group, but it is likely a significant one based on his activity.

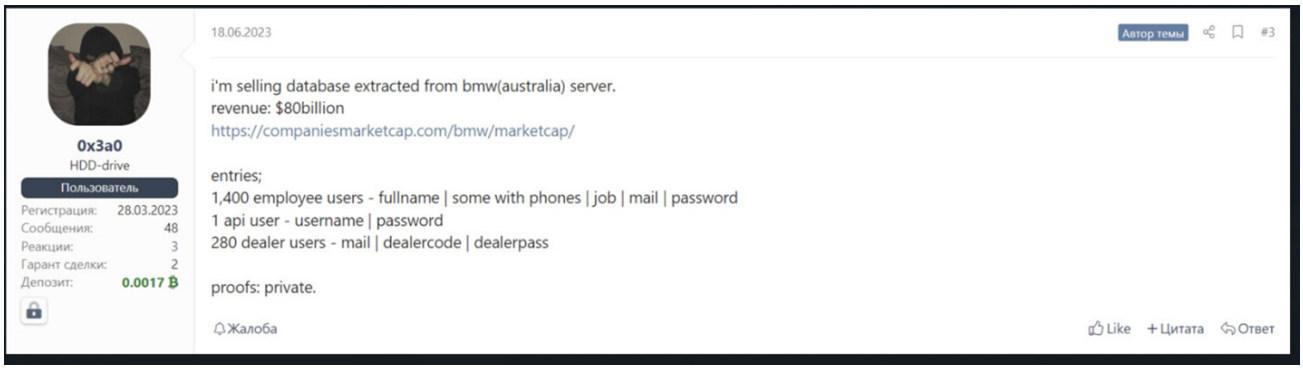


Figure 10. 0x3a0 AKA mont4na sells BMW Australia data

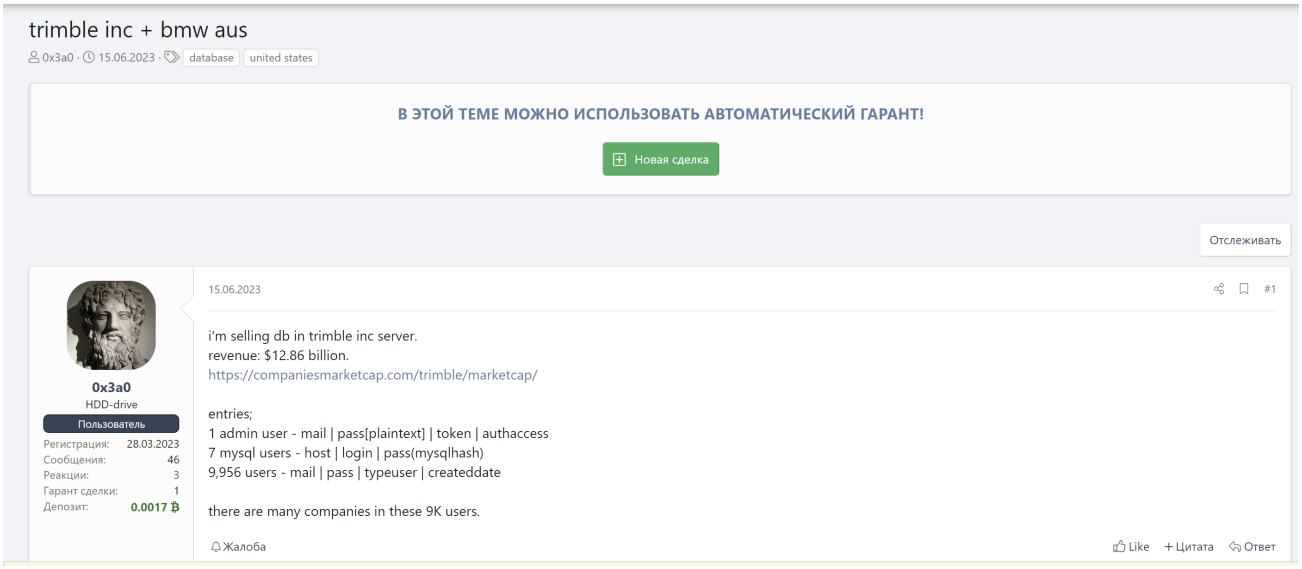


Figure 11. 0x3a0 AKA mont4na sells Trimble data

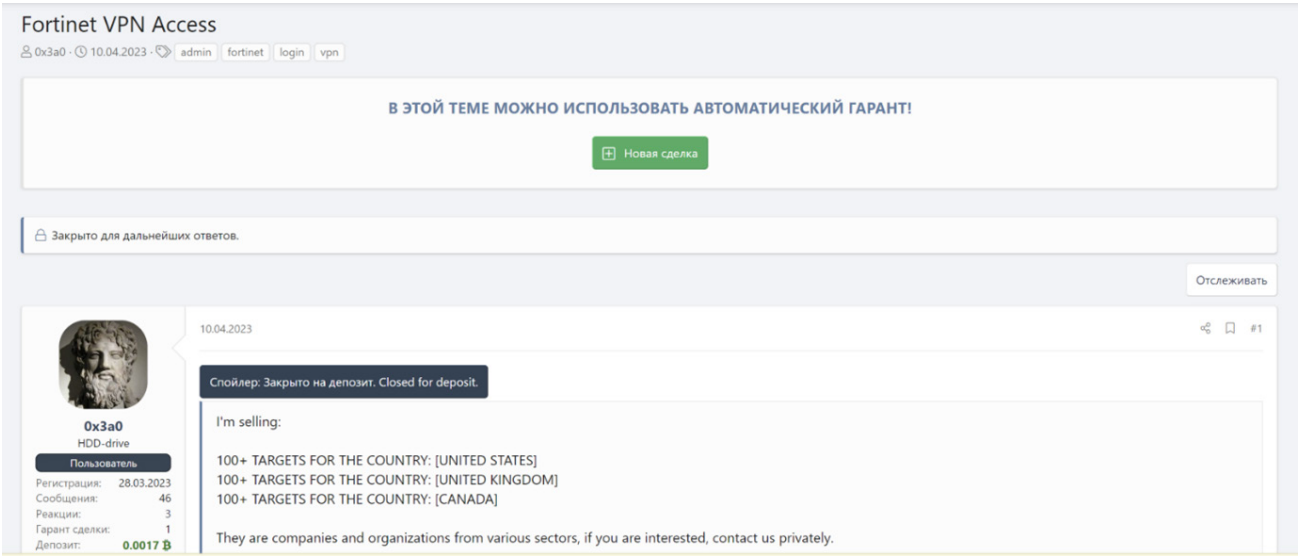


Figure 12. 0x3a0 AKA mont4na sells Fortinet VPN access

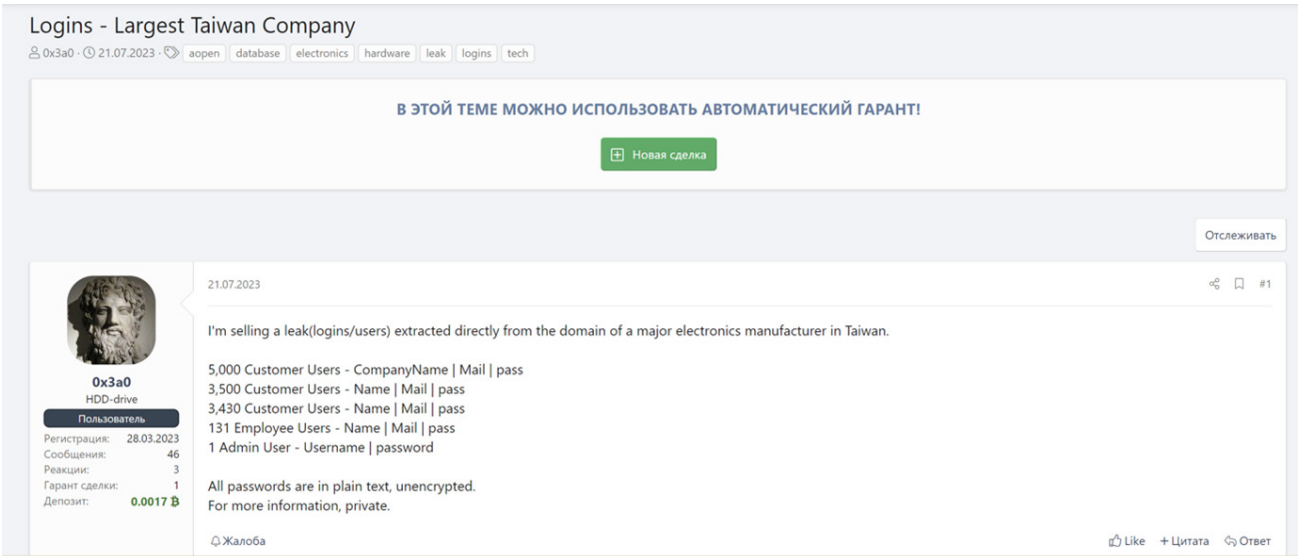


Figure 13. 0x3a0 AKA mont4na sells credentials to an electronics manufacturer in Taiwan

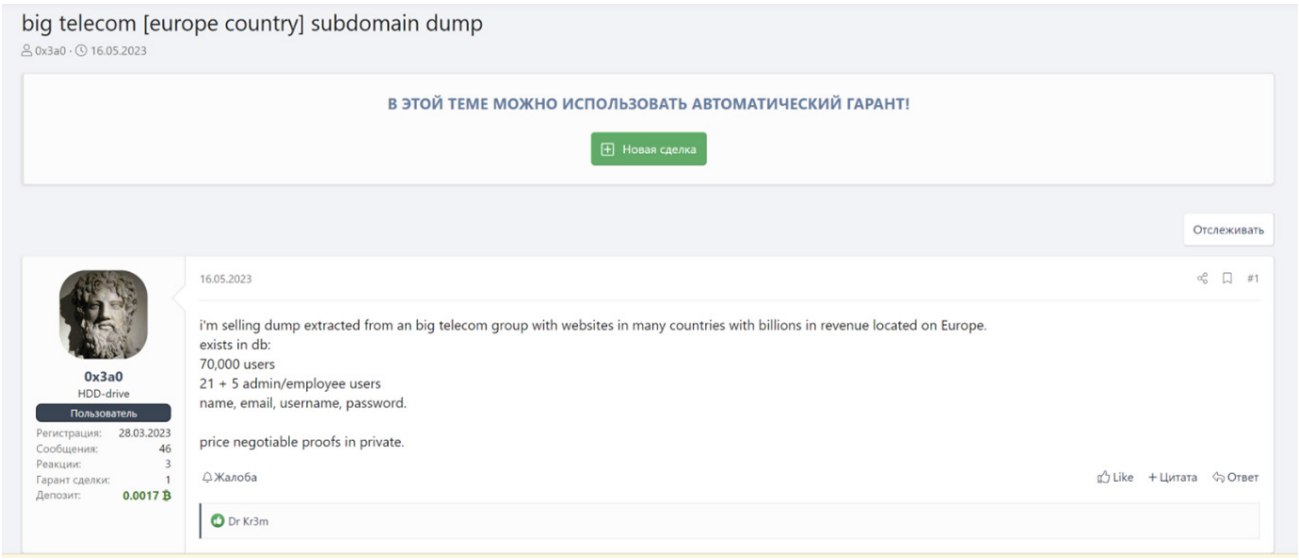


Figure 14. 0x3a0 AKA mont4na sells credentials for a telecommunication group in Europe

Another notable threat actor for hire is 0x3a0, also known as mont4na. 0x3a0 has been actively involved in selling compromised access and sensitive data from various targets across a variety of industries including technology, telecommunications and transportation.

Highlights from 0x3a0's "sales portfolio" include:

- **A database with admin and user credentials.**
  - BMW Australia (nearly 1,700+ users)
  - European telecommunications group (70,000+ users)
  - Trimble (nearly 10,000+ users)

- **A database with customer and employee credentials, including plaintext passwords.**
  - Electronics manufacturer in Taiwan (12,000+ total users)

- **A database with Fortinet VPN credentials.**
  - 300+ companies in the U.S., U.K. and Canada

While IntelBroker and 0x3a0 are leading "salesmen" in various hacking forums, we've observed other threat actors selling access to organizations. These threat actors are more commonly referred to as initial access brokers or IABs. Here are some examples of the IAB threat actors we've discovered.

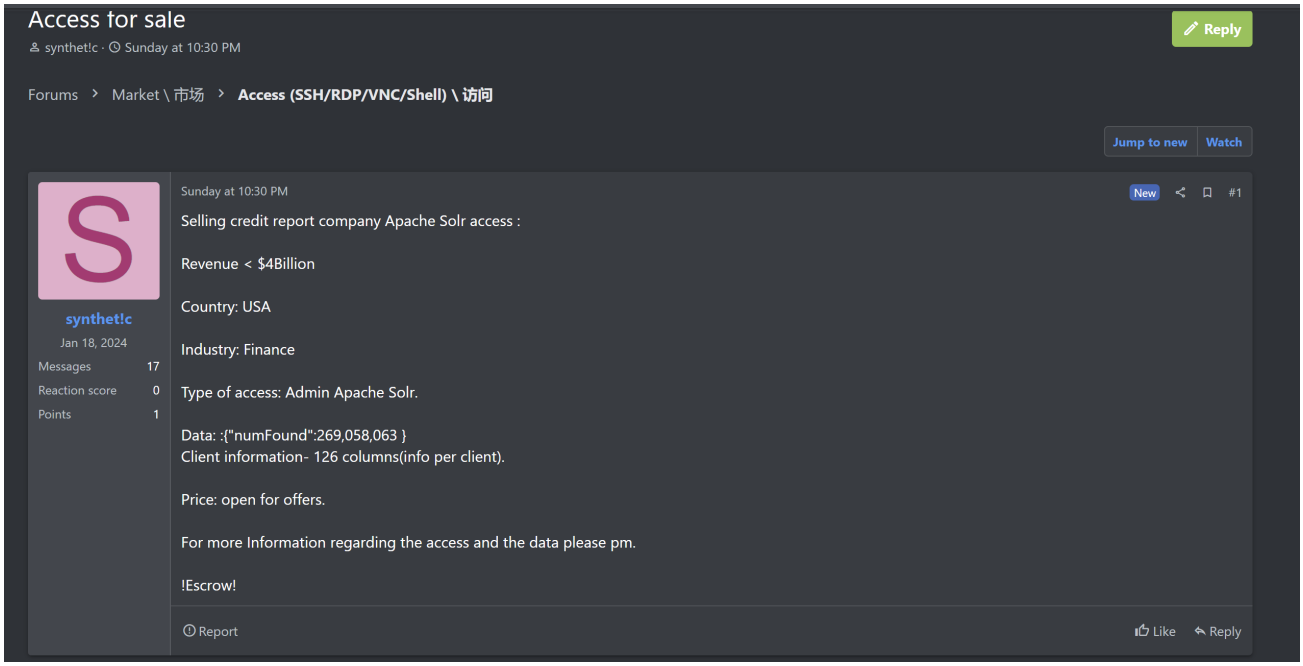


Figure 15. synthet!c sells credit reports from a U.S. financial company

A new name on the IAB scene is synthet!c, who was observed selling credit reports from a U.S. financial company on a dark web forum called RAMP (Russian Anonymous Marketplace). The access is via Apache Solr, which is an open-source enterprise search platform written in Java.

It's worth noting that synthet!c recently joined RAMP in 2024. Although it's possible that this post may be a one-time "business venture," it's more likely that synthet!c is creating multiple aliases across different hacking forums in an attempt to sell the stolen data to a wider audience

Figure 16. shrinbaba sells access to a Swiss business services company via AnyDesk

On June 22, 2024, a threat actor named shrinbaba posted on the Exploit.in hacking forum, offering local admin (LA) access to a Swiss-based business services company which contained admin privileges via AnyDesk. The access featured 76 domain computers. Payment terms are set as an auction. There is a fixed bidding system, which begins at $800 USD, with bid increments of $400 USD and a blitz (buyout) option at $1,500 USD.

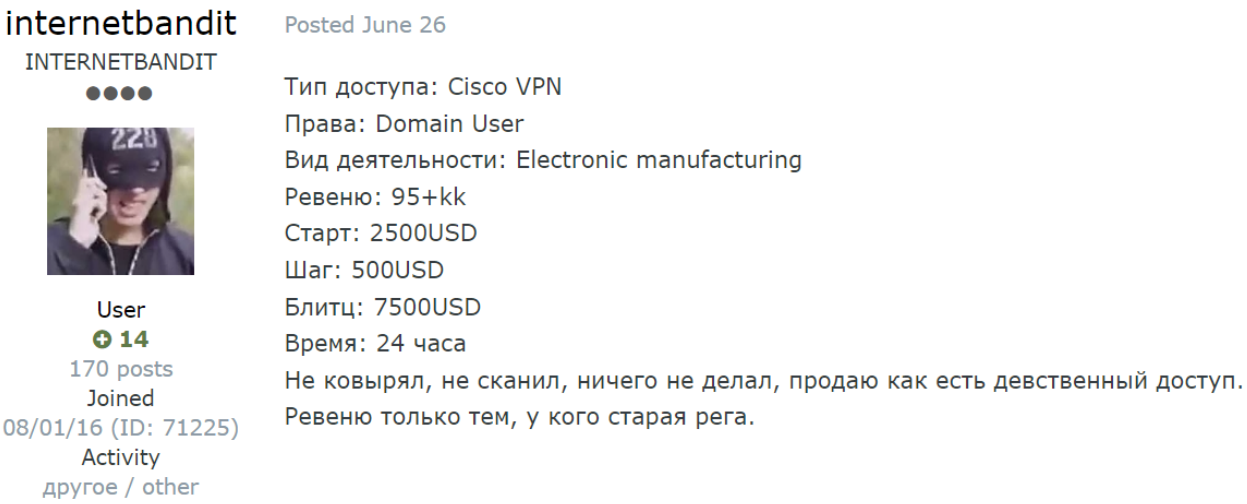


Figure 17. internetbandit sells Cisco VPN access to an electronic manufacturing company

On June 26, 2024, a different threat actor named internetbandit posted on the same hacking forum, offering Cisco VPN access with domain user rights for an electronics manufacturing company.

The access auction had a starting bid of $2,500 USD, with increments of $500 USD and a blitz (buyout) option at $7,500 USD. The auction was live for only 24 hours.

Chapter 2

Top Enterprise Security Trends

Top 10 Spoofed Brands

Well-known brands are often the prime target of cybercriminals, and for good reason. Cybersquatting, also known as domain squatting, involves using a domain name where threat actors can profit from using the recognition of a widely known trademark. Masking themselves using popular brand names, threat actors can conduct phishing attacks, host pirated software, distribute malware and commit fraud with almost no limits.

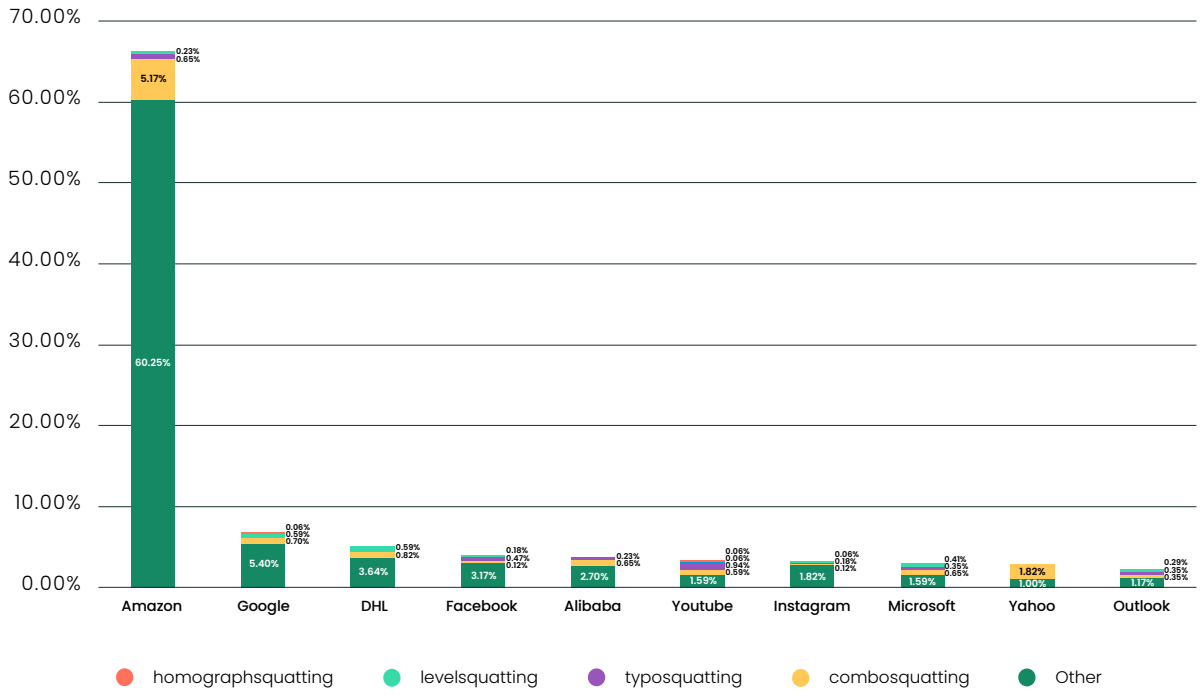


Figure 18. The percentage of domains for the top 10 spoofed brands

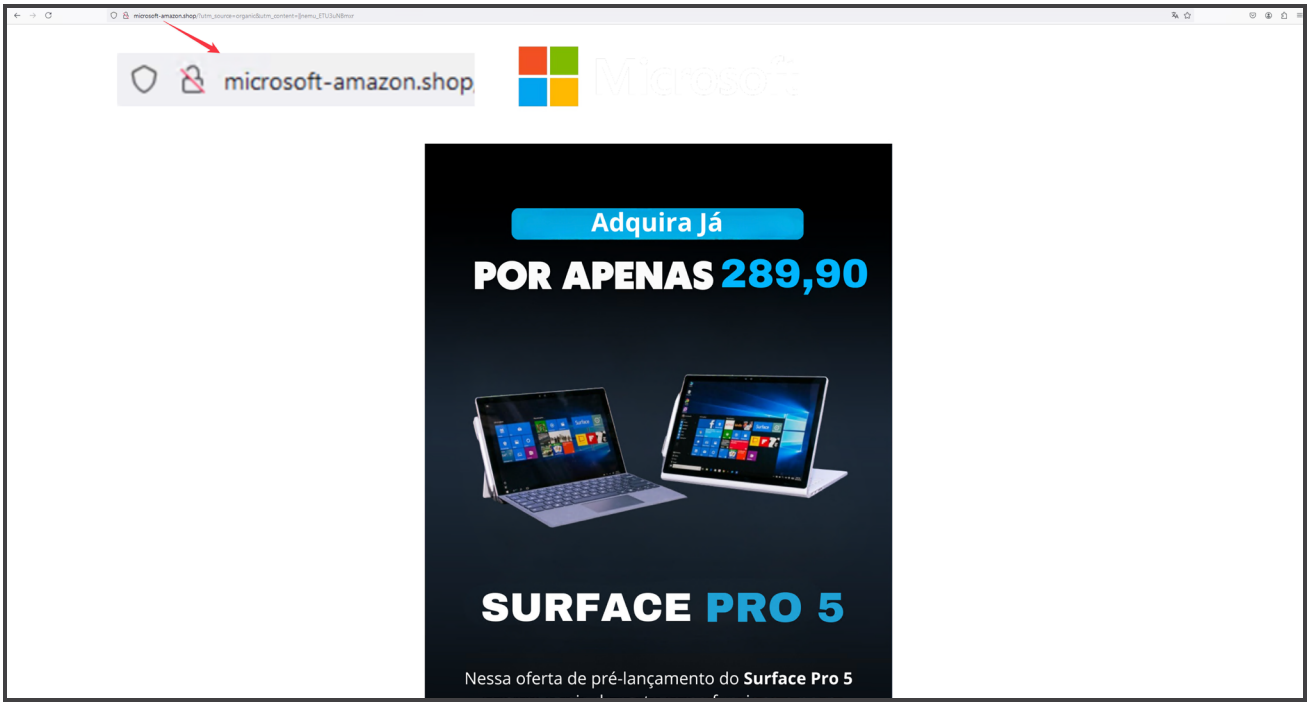


Figure 19. Example of brand spoofing with Amazon (fake domain) and Microsoft (fake advertisement)

In Q2 2024, Amazon was the most spoofed brand (66% of domains) ahead of Google. We are observing an increase in the use of "Amazon" in phishing, fraud and brand impersonation attacks.

Threat actors leverage various “squatting” techniques to mask their domains:

- **Combosquatting** involves creating a domain that combines legitimate domain with additional words or letters, such as “cato-networks.com,” which adds a hyphen to Cato’s URL catonetworks.com.
- **Homographsquatting** uses various character combinations that resemble the target domain visually, such as 'catonet0rks.com, which substitutes a zero to mimic the letter "o."

- **Levelsquatting** inserts the target domain into the subdomain of the cybersquatting URL. A good example of levelsquatting would be login.catonetworks.fake.com - where an unsuspecting user might miss the "fake.com" part and enter.

- **Typosquatting** creates domain names that incorporate typical typos users input when attempting to access a legitimate site. A perfect example of typosquatting would be 'catonetwrks.com', which omits the 'o' in networks.

- **Other** includes other techniques, such as using the brand name within the domain.

Top 10 AI Applications Used

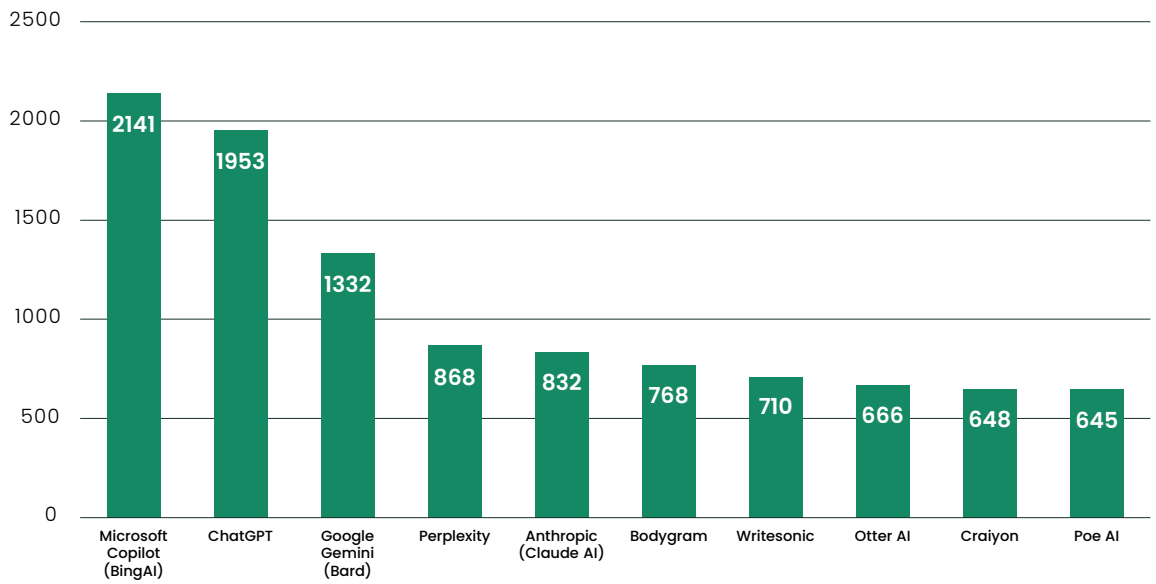
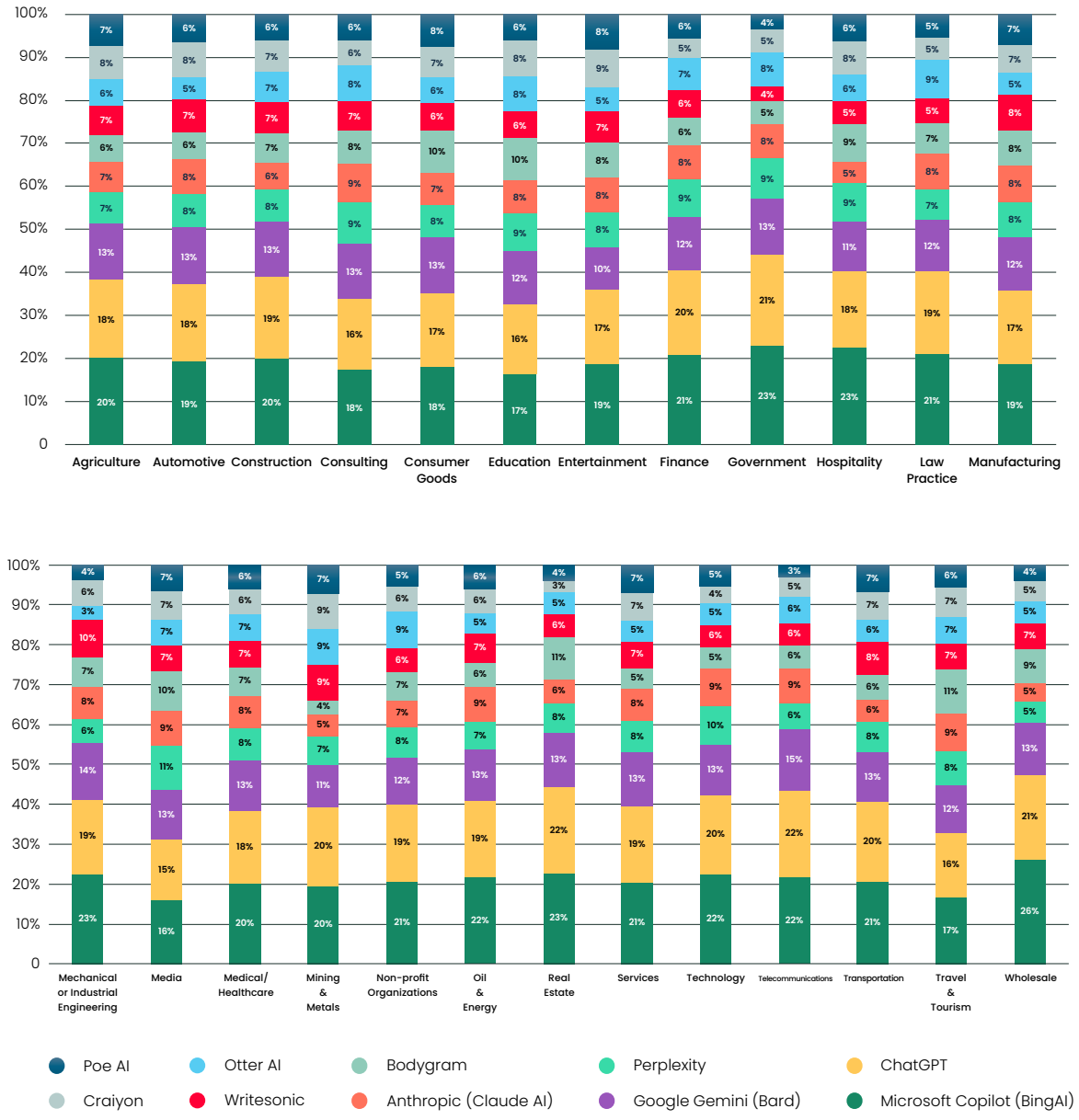


Figure 20. Top 10 AI applications used by unique accounts

In Q2 2024, Microsoft Copilot was the most widely used AI application on our top 10 list, followed by ChatGPT and Google Gemini.

We also observed an increase in the usage of Bodygram, an AI company that claims to produce accurate measurements of body size and body composition with just two photos. This application did not make our top 10 list in Q1 2024.



Figures 21 and 22. Top 10 AI applications used by industry verticals

Top 10 Anonymizer Applications Used

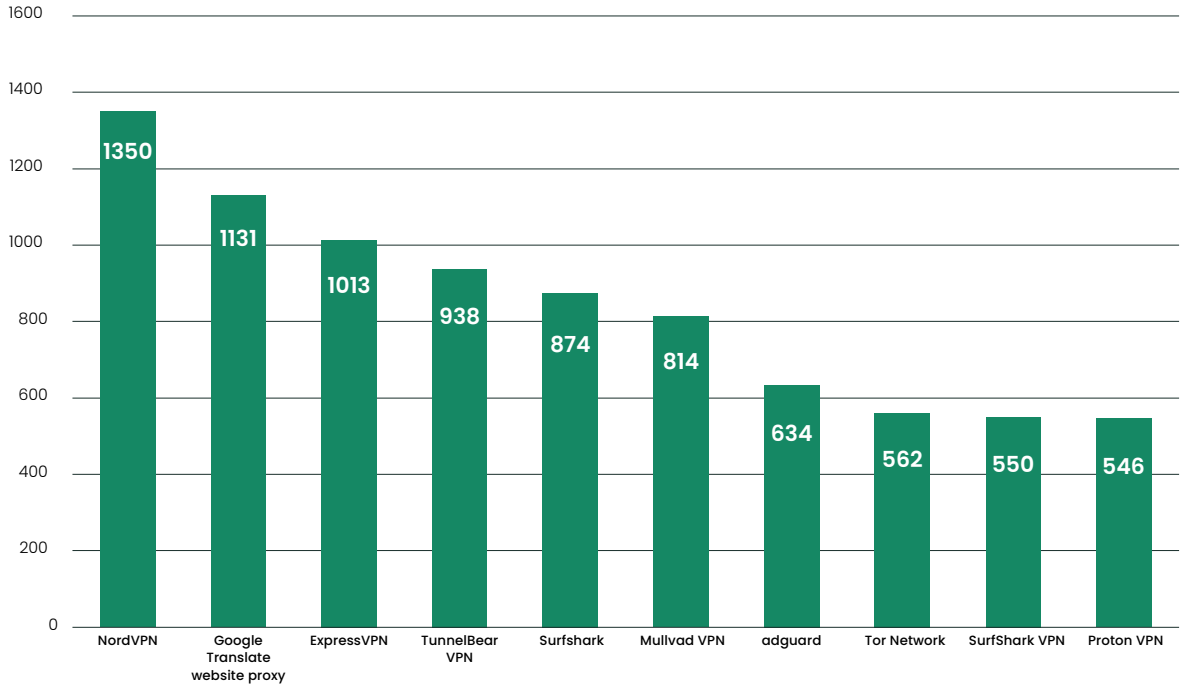
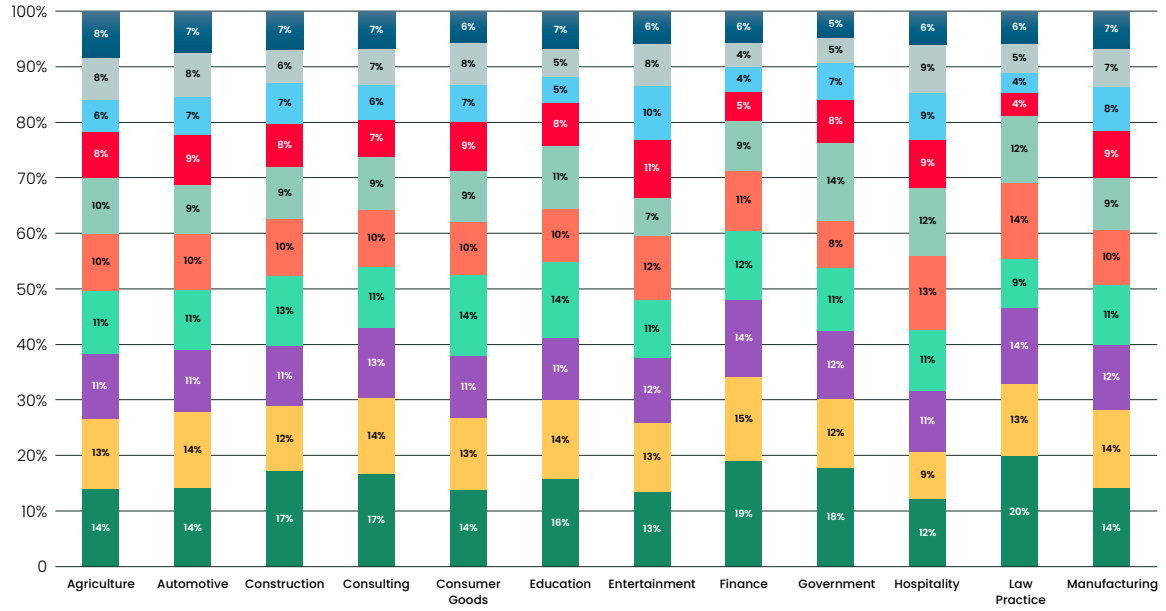


Figure 23. Top 10 anonymizer applications used by unique accounts

NordVPN was the top anonymizer application used in Q2 2024. NordVPN is a popular application to encrypt internet traffic and hide the IP of a physical location.



Figures 24 and 25. Top 10 anonymizer applications used by industry verticals

Chapter 3

Top Network Security Trends

Organizations have traditionally relied on legacy multiprotocol label switching (MPLS) networks to transmit data without encryption, while trusting edge firewalls for protection.

The Zero Trust security model has redefined access authentication by emphasizing the importance for organizations to assume that threat actors may already be present within their networks. The aim is to make it more difficult for threat actors to carry out malicious activities and plan advanced attacks.

Yet despite the advanced security benefits of implementing a Zero Trust approach, recent data indicates that organizations still rely on Wide Area Networks (WAN) and continue to use insecure protocols.

Cato Networks developed SAM (Suspicious Activity Monitoring), a suite of capabilities that can identify suspicious behavior and alert an organization using Cato XDR. Each SAM signature is categorized by risk levels: Low, Medium or High. SAM signatures have also been mapped to their respective MITRE ATT&CK tactics.

Threat actors can remain undetected by exploiting common tools that are used by organizations daily. Through SAM, Cato offers visibility into an organization's utilization of common tools, techniques and operations. SAM can remove the blind spots when it comes to uncovering poor security practices and identifying elusive threat actors.

Suspicious Activity Monitoring (SAM)

Outbound traffic

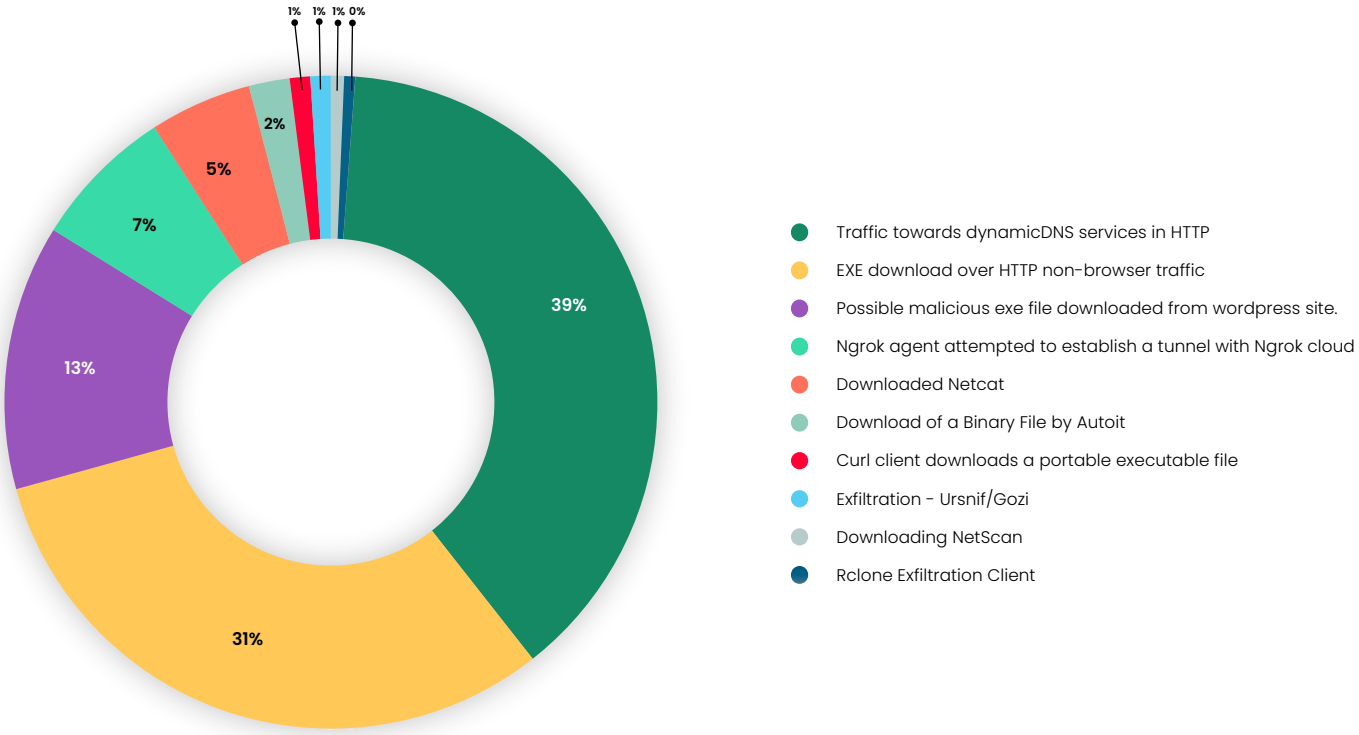
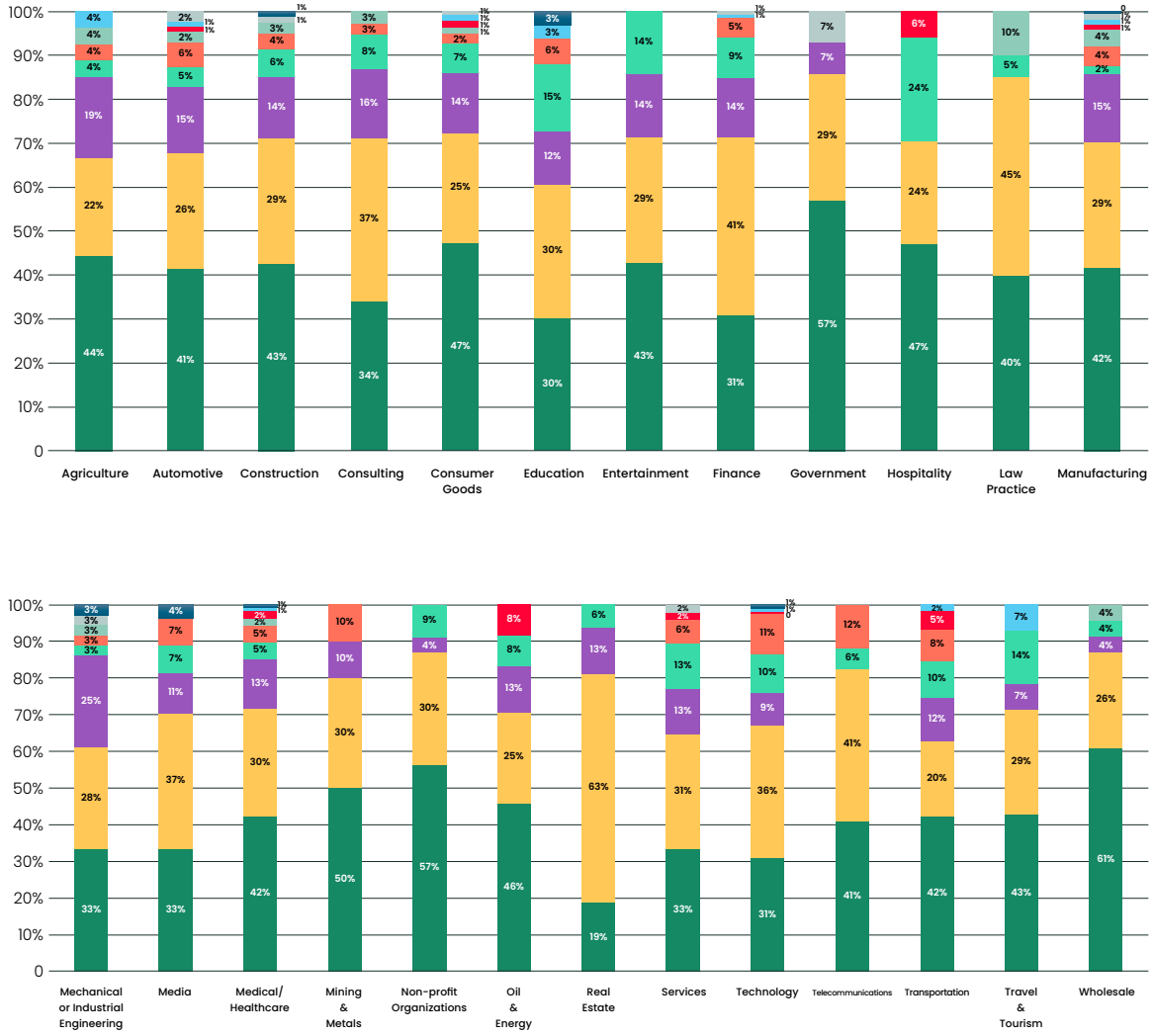


Figure 26. Top 10 high-risk suspicious activities in outbound traffic by unique accounts

We did not observe a noticeable change in outbound traffic activity in Q2 2024 compared to Q1 2024.

It's worth noting that Dynamic DNS (DDNS) topped the list of high-risk suspicious activities in outbound traffic. While this does not necessarily mean that an attack is happening, there are known attacks that use this technique. For example, APT28 (Fancy Bear) and the Mirai botnet use DDNS to communicate with its command-and-control (C2) infrastructure.



Figures 27 and 28. Top 10 high-risk suspicious activities in outbound traffic by industry verticals (unique accounts)

WANbound traffic

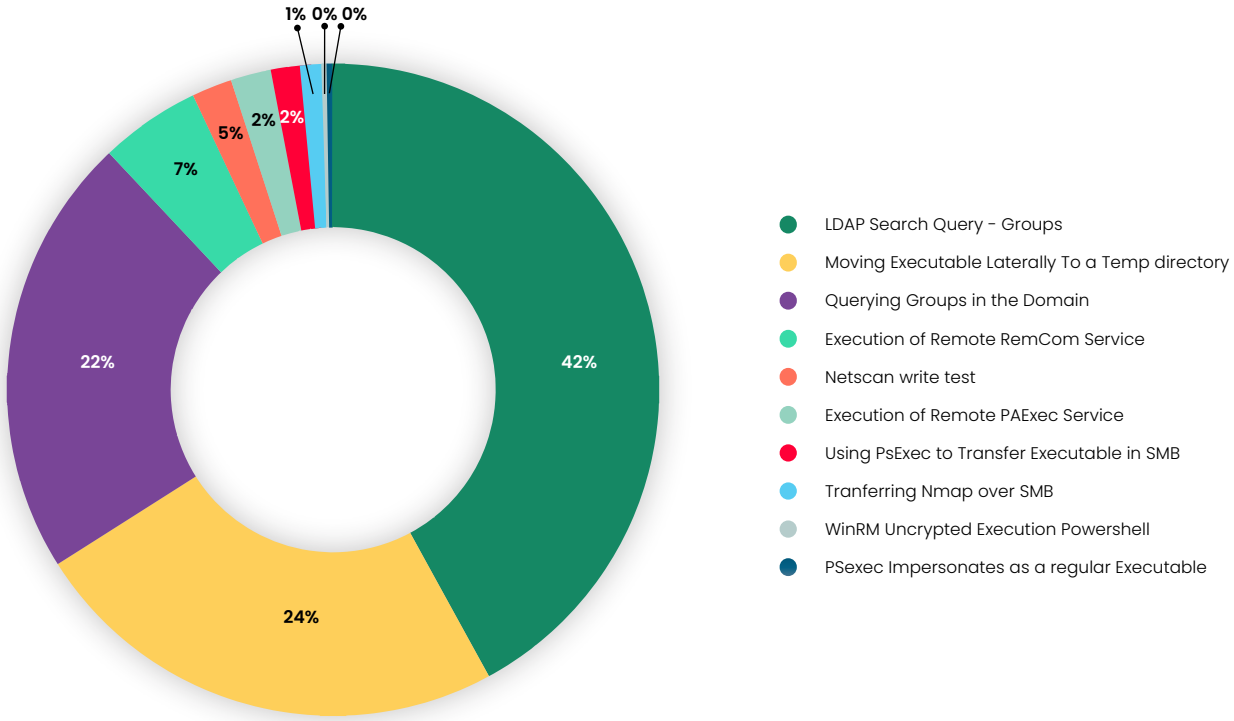


Figure 29. Top 10 high-risk suspicious activities in WANbound traffic (unique accounts)

We observed a noticeable change in WANbound traffic activity in Q2 2024 compared to Q1 2024.

"Moving Executable Laterally to a Temp Directory" increased 200% (from 8% in Q1 to 24% in Q2). Threat actors leverage this technique to move tools between systems, which typically occurs during lateral movement. "Temp" directories usually have permissions for reading, writing and executing by all users. Threat actors leverage them to download and run tools/scripts.

Figures 30 and 31. Top 10 high-risk suspicious activities in WANbound traffic by industry verticals (unique accounts)

Secure vs. Insecure Protocols

Implementing secure protocols can drastically reduce the attack surface. In this section, Cato CTRL explores the use of such protocols within an organization.

HTTP vs. HTTPS

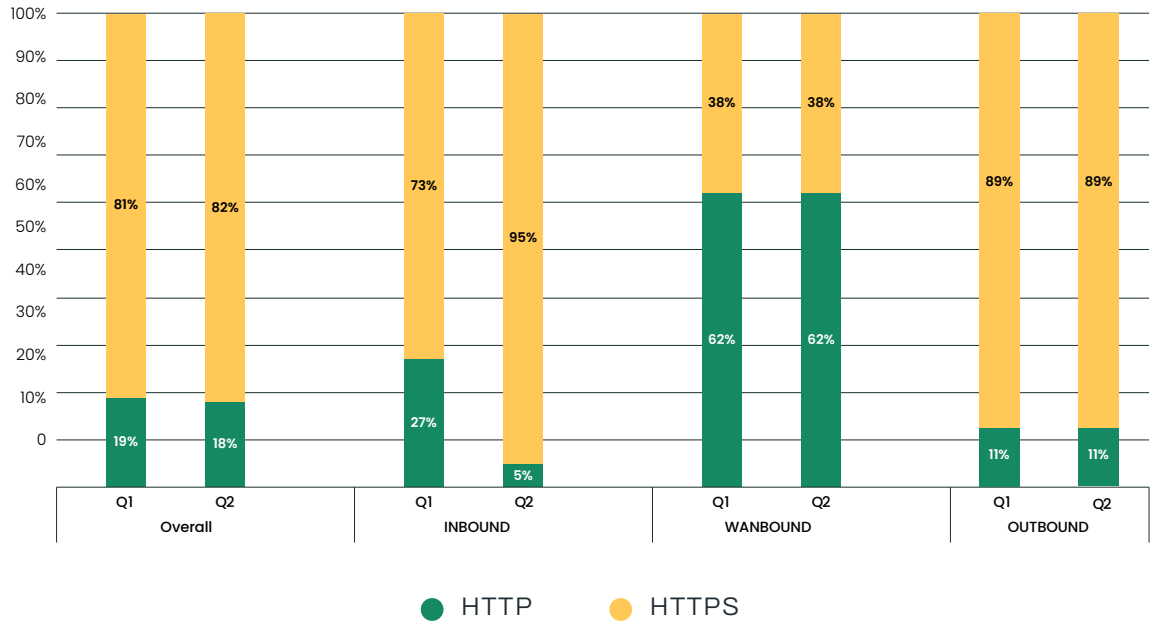
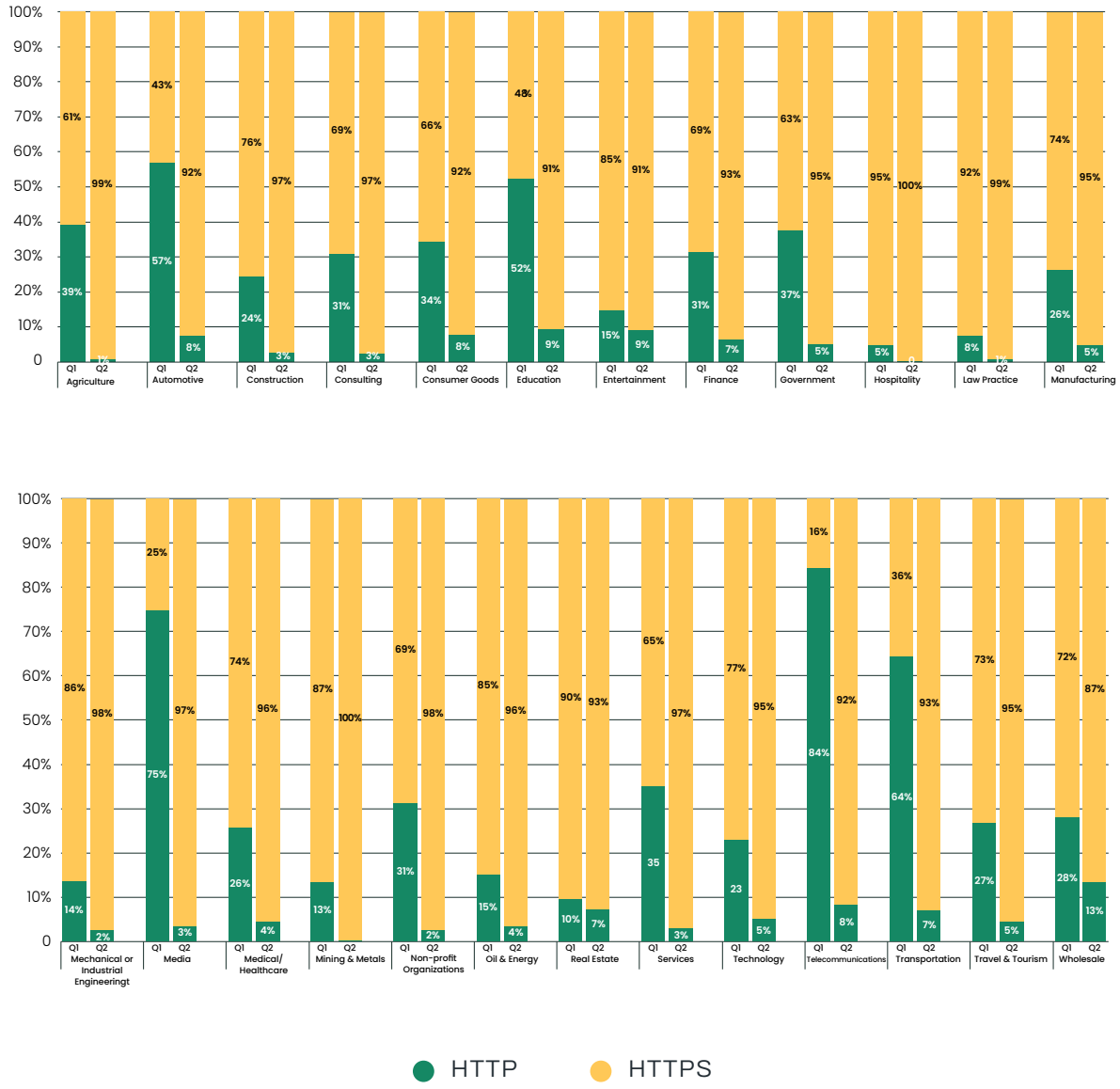


Figure 32. HTTP vs. HTTPS traffic comparison by traffic direction

We observed a noticeable change in inbound HTTP vs. HTTPS traffic activity in Q2 2024 compared to Q1 2024.

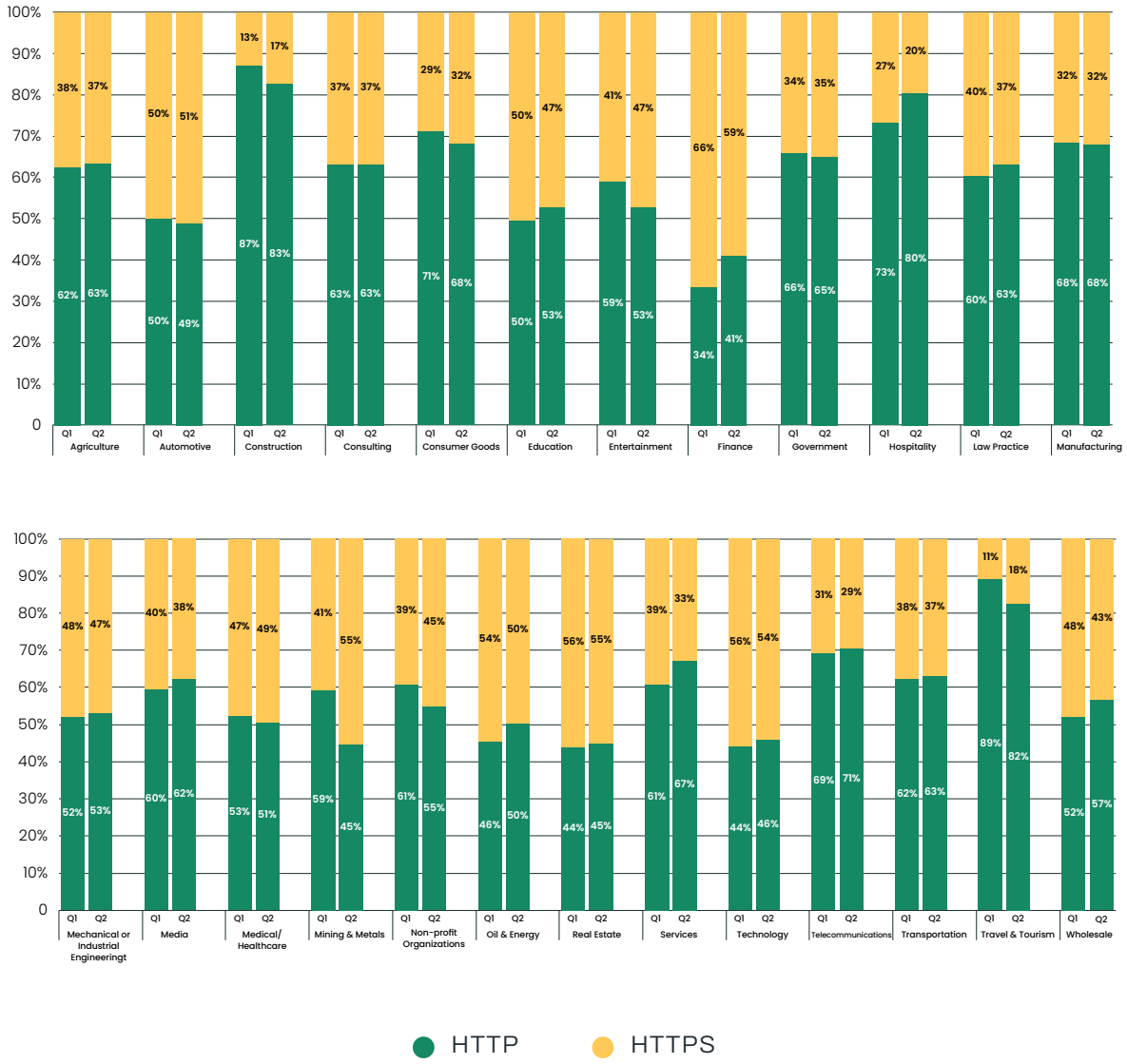
Of note, there was a 30% increase (from 73% in Q1 to 95% in Q2) in inbound HTTPS traffic activity. It's also worth noting there was an 81% decrease (from 27% in Q1 to 5% in Q2) in inbound HTTP traffic activity.



Figures 33 and 34. Inbound HTTP vs. HTTPS traffic by industry verticals

We observed a noticeable change in inbound HTTPS traffic activity by industry verticals in Q2 2024 compared to Q1 2024.

The top three industry verticals with the highest increases in inbound HTTPS traffic activity from Q1 2024 to Q2 2024 were media (288% increase), telecommunications (475% increase) and transportation (158% increase). In other words, these were the verticals that did the most to improve the security of their inbound traffic. The increases were prompted by customers adding TLS certificates to their websites, removing old applications and using HTTPS for new accounts.



Figures 35 and 36. WANbound HTTP vs. HTTPS traffic by industry verticals

We did not observe a noticeable change in WANbound HTTP traffic vs. HTTPS traffic activity by industry verticals in Q2 2024 compared to Q1 2024.

SSH vs. Telnet

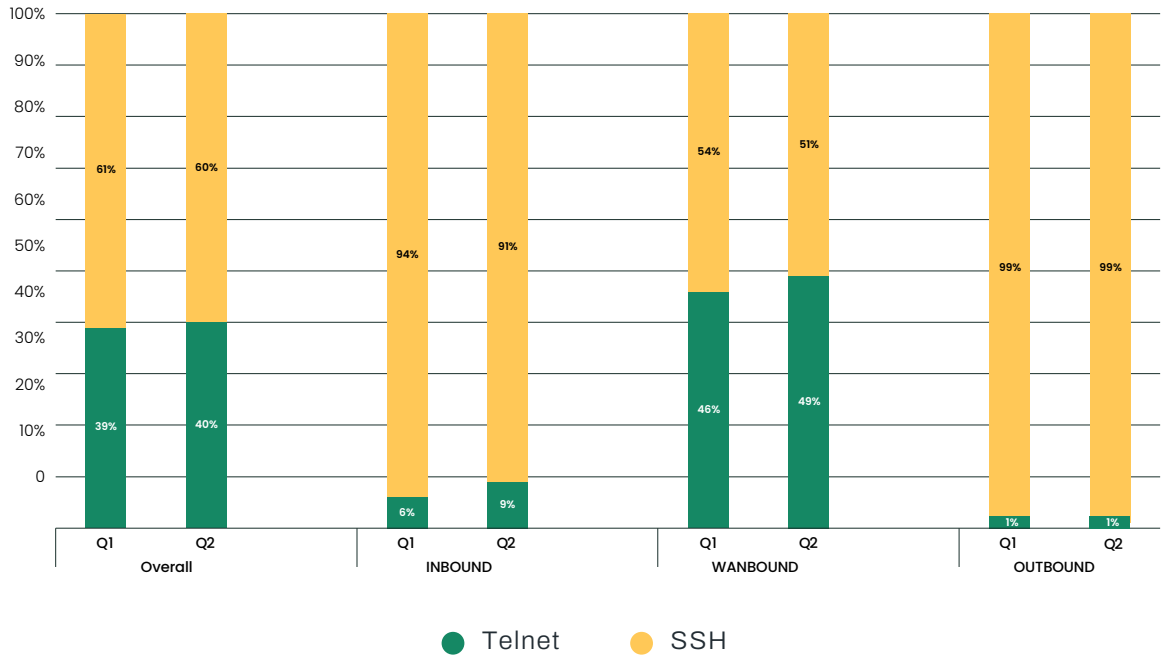
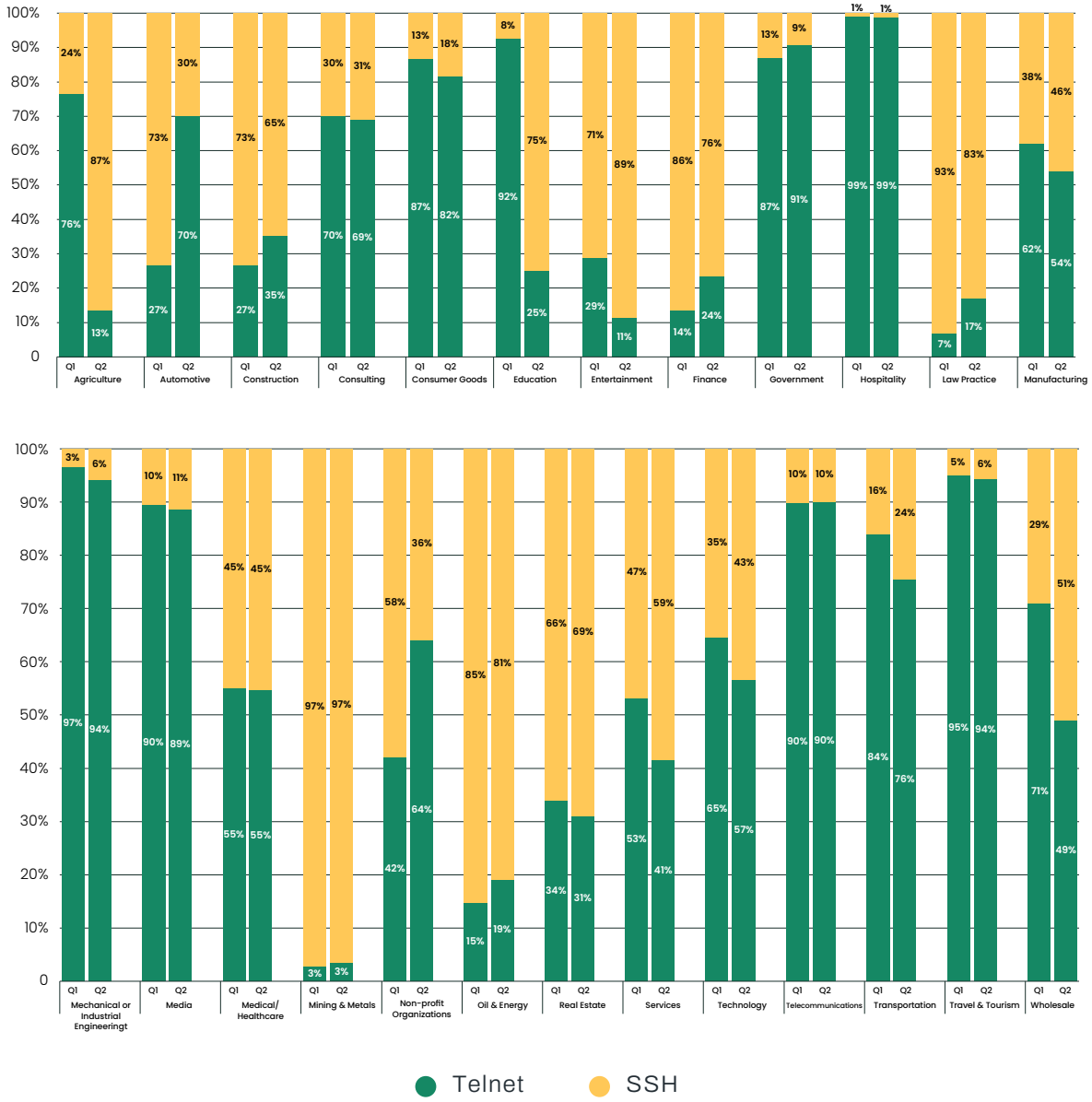


Figure 37. Telnet vs. SSH traffic comparison by traffic direction

We did not observe a noticeable change in Telnet vs. SSH traffic activity in Q2 2024 compared to Q1 2024.



Figures 38 and 39. WANbound Telnet vs. SSH traffic by industry verticals

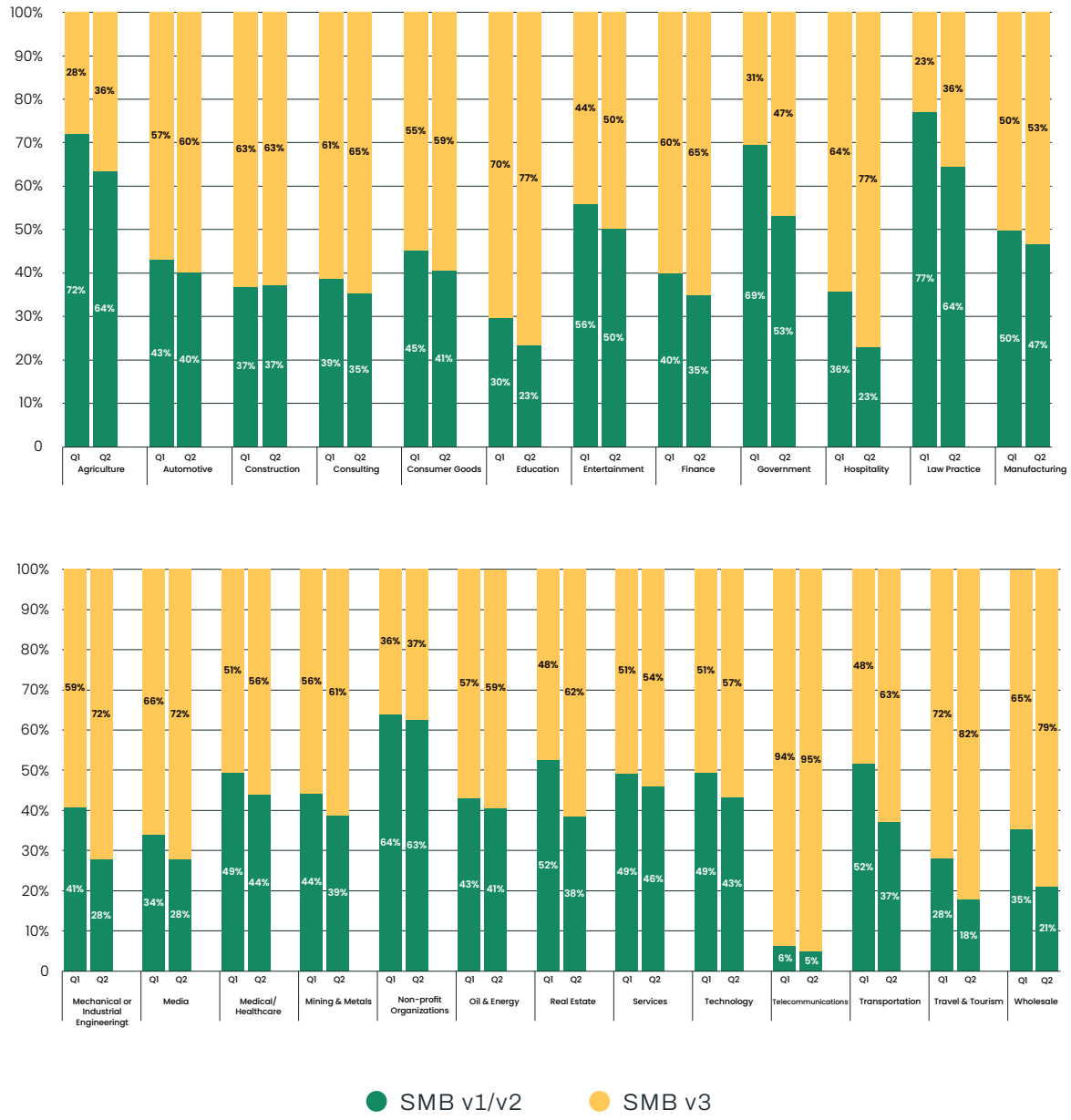
We observed a noticeable change in WANbound Telnet vs. SSH traffic activity by industry verticals in Q2 2024 compared to Q1 2024.

The agriculture and education verticals had the largest increases in WANbound SSH traffic activity (263% increase and 838% increase, respectively). SSH can encrypt traffic in both directions, which helps organizations stay more secure.

SMBv1 and SMBv2 vs. SMBv3

Figure 40. SMB v1 and v2 vs. SMB v3 traffic comparison by traffic direction

We did not observe a noticeable change in SMBv1 and SMBv2 vs. SMBv3 traffic activity in Q2 2024 compared to Q1 2024.



Figures 41 and 42. SMB v1 and v2 vs. SMB v3 WANbound traffic by industry verticals

We did not observe a noticeable change in WANbound Telnet vs. SSH traffic activity by industry verticals in Q2 2024 compared to Q1 2024.

Mitigated Vulnerabilities

We've analyzed mitigated Common Vulnerabilities and Exposures (CVEs) across different traffic directions: inbound, outbound and WANbound. Here's what we found.

SMBv1 and SMBv2 vs. SMBv3

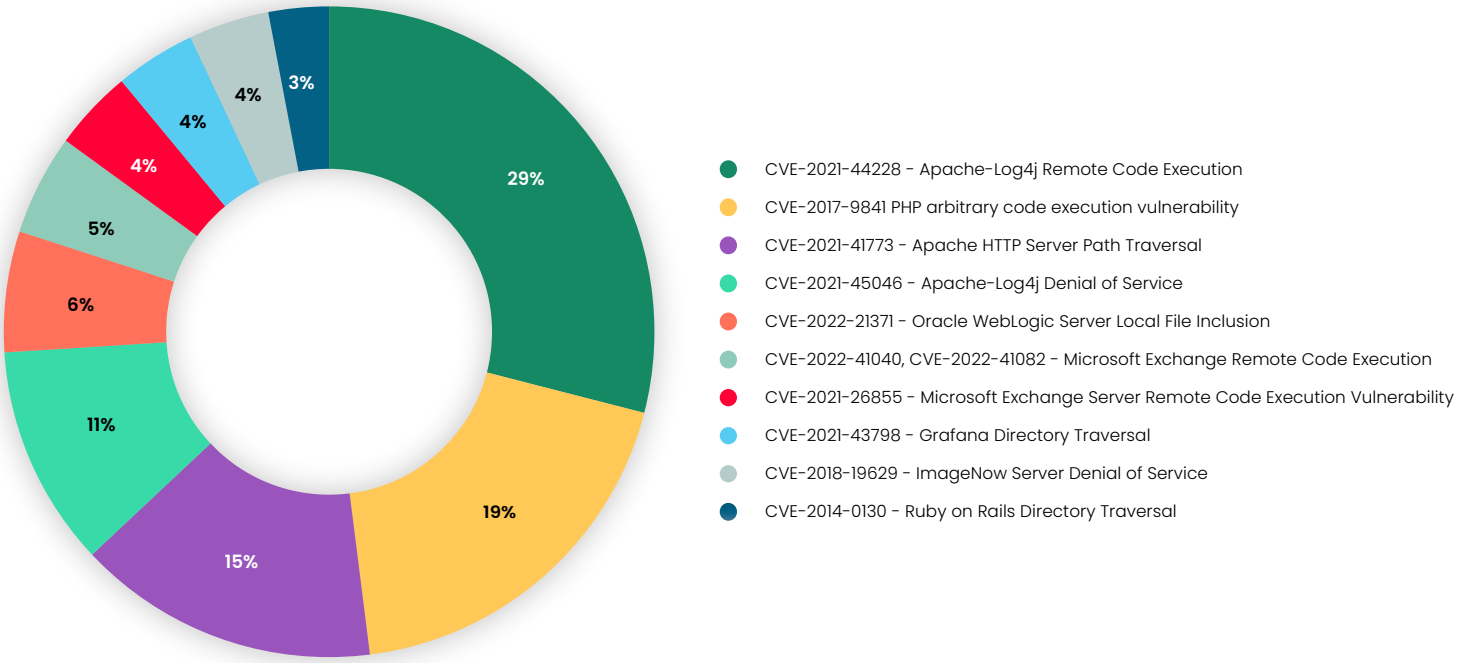


Figure 43. Top 10 mitigated CVEs in inbound traffic by traffic volume

We observed a noticeable change in the attempted use of vulnerabilities in inbound traffic in Q2 2024 compared to Q1 2024.

In inbound traffic, we observed a 61% increase (from 18% in Q1 to 29% in Q2) in the attempt for CVE-2021-44228 (Apache Log4j remote code execution) to be exploited. In fact, it became the most popular exploit for threat actors to attempt to use in inbound traffic in Q2 2024. This exploit ranked second in Q1 2024.

Upon further inbound traffic analysis, we observed attempts to exploit Log4j to deploy the RedTail cryptomining malware in the services and manufacturing industries. We also noticed an attempt to deploy the XMRig cryptomining malware in the manufacturing industry.

Additionally, we observed a 200% increase (from 5% in Q1 to 15% in Q2) in the attempt for CVE-2021-41773 (Apache HTTP Server Path Traversal) to be exploited.

Outbound traffic

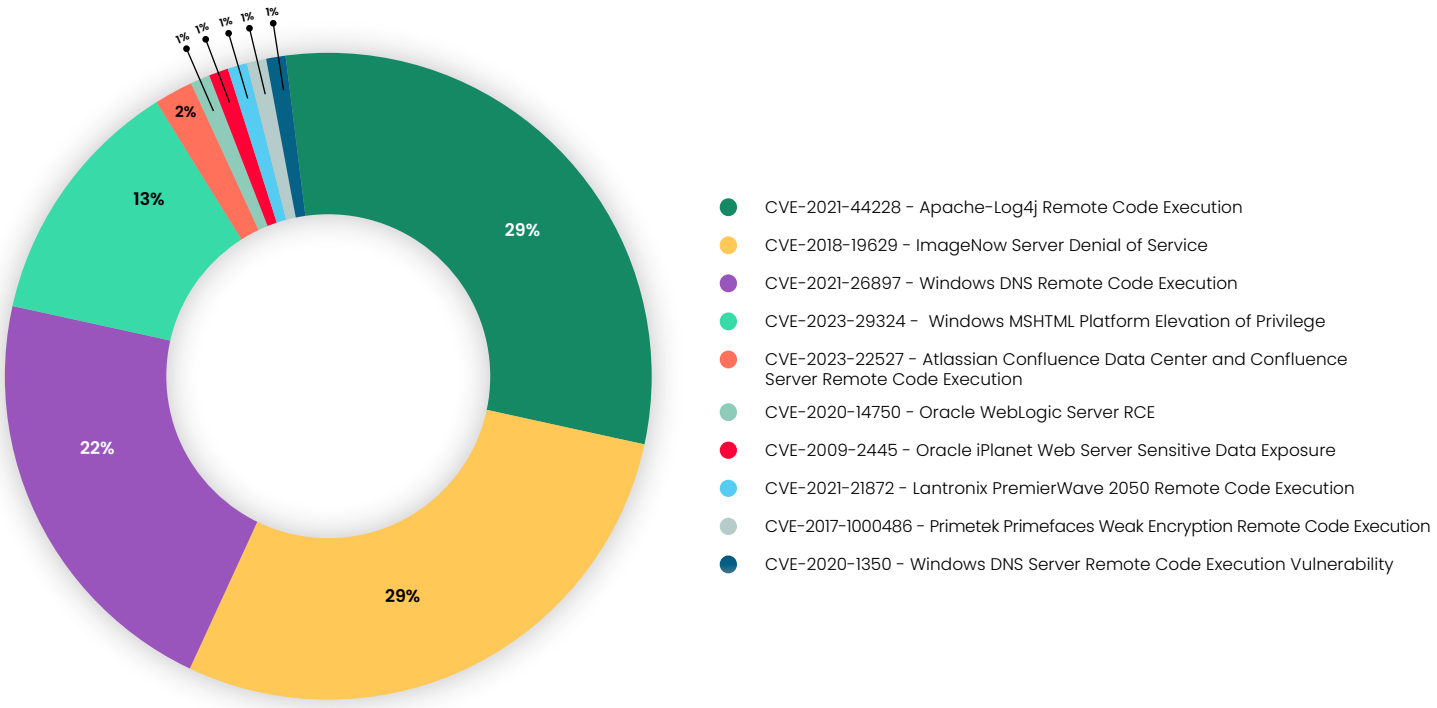


Figure 44. Top 10 mitigated CVEs in outbound traffic by traffic volume

We observed a noticeable change in the attempted use of exploited vulnerabilities in outbound traffic in Q2 2024 compared to Q1 2024.

In outbound traffic, we observed a 190% increase (from 10% in Q1 to 29% in Q2) in the attempt for CVE 2018-19629 (Denial of Service Vulnerability in ImageNow Server) to be exploited. Notably, we also observed a 61% decrease (from 33% in Q1 to 13% in Q2) in the attempt for CVE 2023-29324 (Windows MSHTML Platform Security Feature Bypass Vulnerability) to be exploited.

WANbound traffic

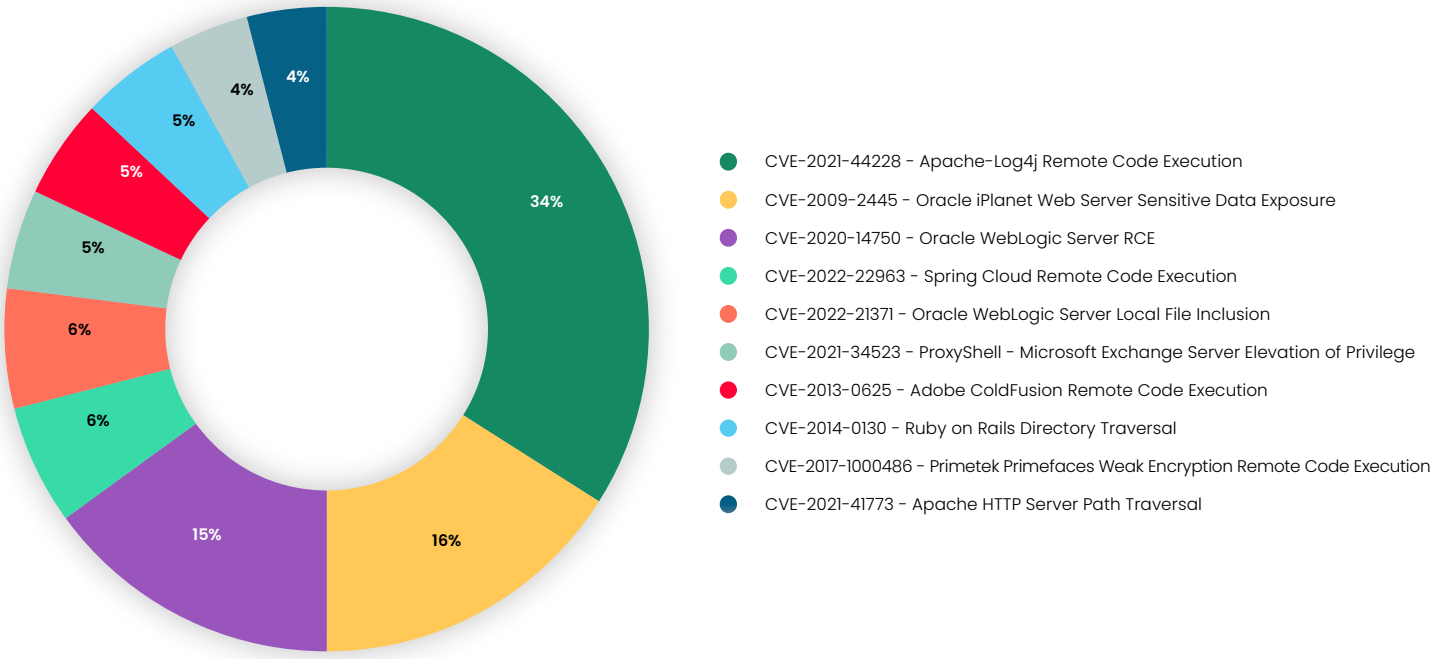


Figure 45. Top 10 mitigated CVEs in WANbound traffic by traffic volume

We observed a noticeable change in the attempted use of exploited vulnerabilities in WANbound traffic in Q2 2024 compared to Q1 2024.

In WANbound traffic, we observed a 79% increase (from 19% in Q1 to 34% in Q2) in the attempt for CVE-2021-44228 (ApacheLog4jRCE) to be exploited. This is a similar increase to what we observed for Log4j in inbound traffic.

Additionally, we observed a 129% increase (from 7% in Q1 to 16% in Q2) in the attempt for CVE 2009-2445 (Oracle iPlanet Web Server sensitive data exposure) to be exploited and a 114% increase (from 7% in Q1 to 15% in Q2) in the attempt for CVE 2020-14750 (Oracle WebLogic Server RCE) to be exploited.

Chapter 4

Key Recommendations

Based on our key findings, Cato CTRL recommends that organizations take the following actions:

Implement Continuous Threat Intelligence Monitoring

- Set up a system to monitor dark web forums and marketplaces for any mention of your company's data or credentials being sold.

Develop a Comprehensive Data Breach Response Plan

- Create a detailed, step-by-step plan for responding to a confirmed data breach.
- Include procedures for containment, assessment, notification (to affected parties and regulators) and remediation.
- Regularly test and update this plan through tabletop exercises.

Adopt an "Assume Breach" Mentality

- Implement strong security measures, such as Zero Trust Network Access (ZTNA), Data Loss Prevention (DLP) and Extended Detection and Response (XDR).
- Conduct regular penetration testing and red team exercises to proactively identify vulnerabilities before attackers do.

Educate Yourself on the Perils of Cybersquatting

- Incorporate cybersquatting tools and techniques for detecting phishing and other attacks that use this method for nefarious purposes.

Develop an AI Governance Strategy

- Create policies and guidelines for the use of AI tools within the organization, and consider security, privacy and compliance implications.
- Implement monitoring and controls for AI application usage, especially for tools that may handle sensitive data.

Implement Suspicious Activity Monitoring (SAM)

- Regularly update a comprehensive set of detection rules for suspicious activities, with a particular focus on potential lateral movement and data exfiltration attempts.
- Pay close attention to suspicious behaviors, such as unauthorized access attempts or unusual login activity as these are strong indicators of a sophisticated attack.

Prioritize Secure Protocol Adoption

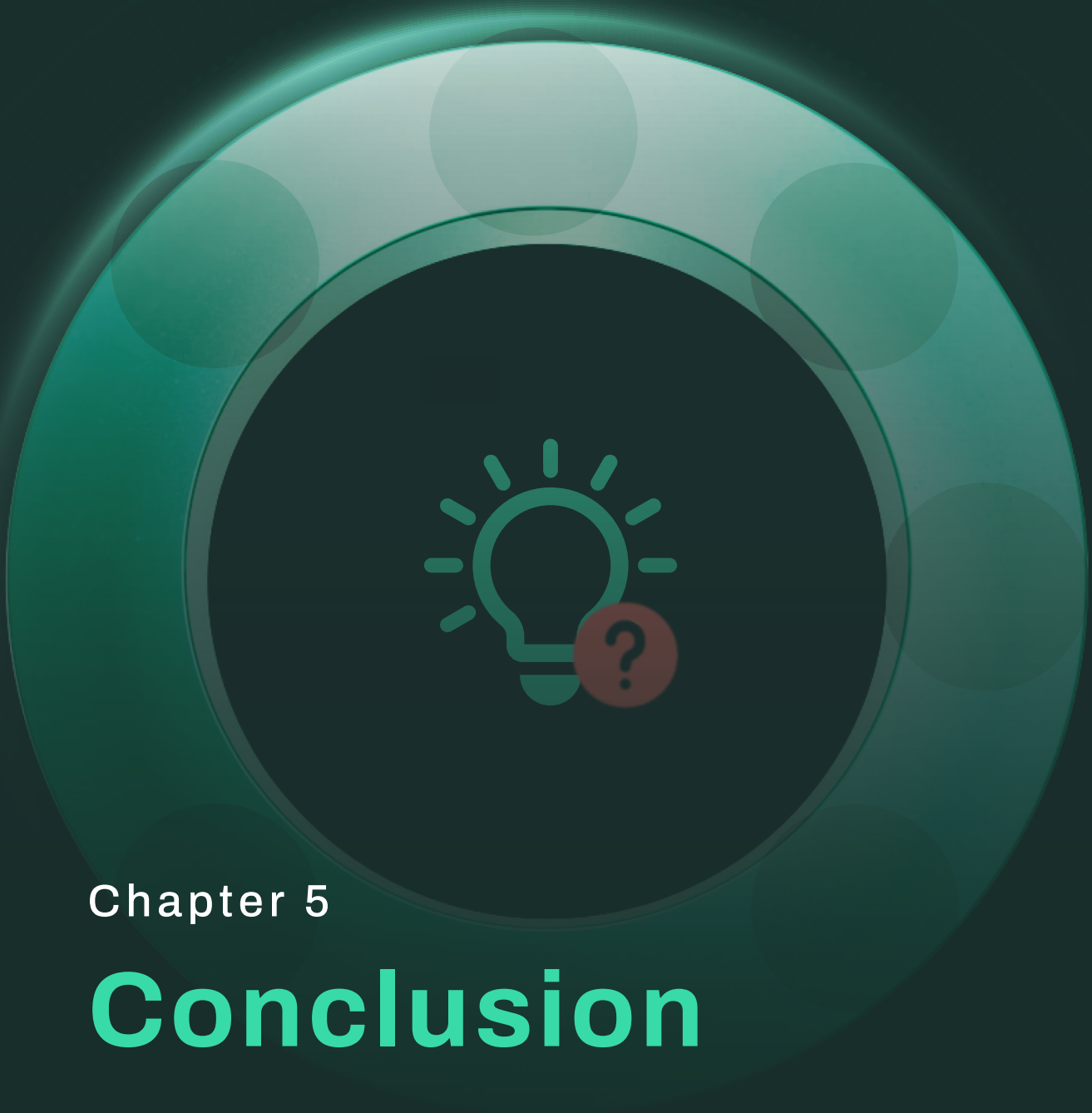
- Conduct an audit of all protocols currently in use across the organization, prioritizing the replacement of insecure protocols (HTTP, Telnet, SMBv1/v2) with their secure counterparts (HTTPS, SSH, SMBv3).
- Implement policy controls to block the use of insecure protocols wherever possible.

Prioritize Patching of Highly Exploited Vulnerabilities

- Implement a proactive patching schedule for critical vulnerabilities, especially those actively exploited (ex: Log4j). Implement policy controls to block the use of insecure.
- Use vulnerability prioritization tools to focus on the most critical and actively exploited vulnerabilities first.

Enhance Monitoring of Public-Facing Services

- Implement continuous vulnerability scanning for all internet-exposed services.
- Use Firewall-as-a-Service (FWaaS) and regularly update security configurations.
- Consider leveraging bug bounty programs to find vulnerabilities in public-facing assets.



Chapter 5

Conclusion

Methodology

The Q2 2024 Cato CTRL SASE Threat Report summarizes findings from Cato CTRL's analysis of 1.38 trillion network flows across more than 2,500 customers globally between April and June 2024.

About Cato CTRL

Cato CTRL (Cyber Threats Research Lab) is the world's first CTI group to fuse threat intelligence with granular network insight made possible by Cato's global SASE platform. By bringing together dozens of former military intelligence analysts, researchers, data scientists, academics and industry-recognized security professionals, Cato CTRL utilizes network data, security stack data, hundreds of security feeds, human intelligence operations, AI (Artificial Intelligence), and ML (Machine Learning) to shed light on the latest cyber threats and threat actors.

About Cato Networks

Cato Networks delivers enterprise security and networking in a single cloud platform. With Cato, organizations replace costly and rigid legacy infrastructure with an open and modular SASE architecture based on SD-WAN, a purpose-built global cloud network, and an embedded cloud-native security stack.

Want to learn why thousands of organizations secure their future with Cato? Visit us at www.catonetworks.com.