CATO NETWORKS

CTRL BY CATO NETWORKS

Cato CTRL SASE Threat Report

Q3 | 2024

Table of Contents

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

Cato CTRL'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 Q3 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 Q3 report provides insights into:

- Threat intelligence trends, including observations on activity for ransomware affiliates.
- Enterprise security trends, including an overview on the threat of shadow AI.
- Network security trends, including a breakdown of TLS attack attempts by country.

We hope you find the Q3 2024 report informative.

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

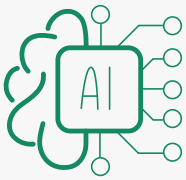
EXECUTIVE SUMMARY

The Q3 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. The insights are collected from Cato CTRL's analysis of 1.46 trillion network flows across more than 2,500 customers globally between July and September 2024.

Threat actors recruiting pen testers for ransomware affiliate programs

In closely monitoring discussions on RAMP (Russian Anonymous Marketplace), Cato CTRL has observed threat actors seeking pen testers to join various ransomware affiliate programs including Apos, Lynx and Rabbit Hole.

Any good developer knows that software needs to be tested before deploying in production environments. This is also true for ransomware gangs. They want to ensure that their ransomware can be deployed successfully against organizations.



Shadow AI lurks in the background for organizations

Shadow AI refers to the unauthorized or unsanctioned use of AI applications and tools within an organization without the knowledge or approval of IT departments or security teams. This phenomenon typically involves employees or departments adopting AI solutions independently and bypassing formal vetting processes and governance controls.

Out of the hundreds of AI applications that Cato CTRL monitors, Cato CTRL tracked 10 AI applications used by organizations (Bodygram, Craiyon, Otter.ai, Writesonic, Poe, HIX.AI, Fireflies.ai, PeekYou, Character.AI and Luma AI) and observed various security risks. The top concern is data privacy.

TLS attack attempts reveal TLS inspection not utilized enough

TLS inspection allows organizations to decrypt, inspect and re-encrypt traffic. However, TLS inspection can break applications and access to some domains. As such, many organizations choose to forgo TLS inspection entirely or bypass inspection for a large portion of their traffic.

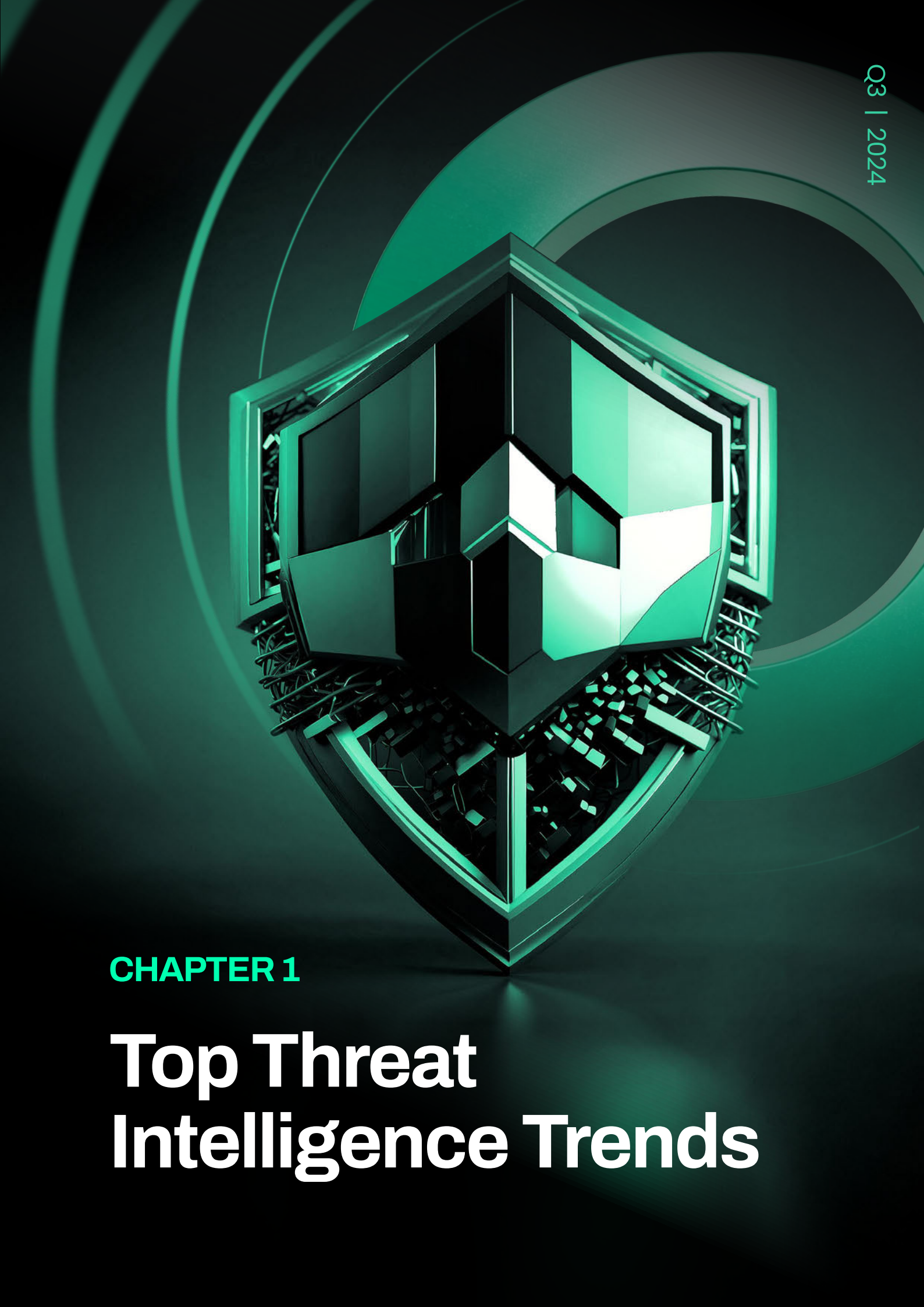
Cato CTRL found that only 45% of participating organizations enable TLS inspection. Even then, only 3% of organizations inspected all relevant TLS-encrypted sessions. This leaves the door open for threat actors to utilize TLS traffic and remain undetected. Organizations must inspect TLS sessions to protect themselves. In Q3 2024, Cato CTRL found that 60% of attempts to exploit CVEs were blocked in TLS traffic. CVEs included Log4j, SolarWinds and ConnectWise.

When TLS inspection is enabled, organizations are better protected. In Q3 2024, Cato CTRL found that organizations who enabled TLS inspection blocked 52% more malicious traffic than organizations without TLS inspection.

New Product Capability

Cato Networks has introduced Safe TLS Inspection to enable organizations to deploy TLS inspection without compromising IT efficiency or user productivity. Cato Safe TLS Inspection uses a unique approach of providing an automated list of applications and domains that are safe to inspect while bypassing everything else. This list includes malicious/suspicious categories like anonymizers, botnets, spam, etc. By using Cato Safe TLS Inspection, organizations improve their overall security posture while at the same time eliminate the complexity and maintenance challenges associated with traditional TLS inspection solutions.

Q3 | 2024



CHAPTER 1

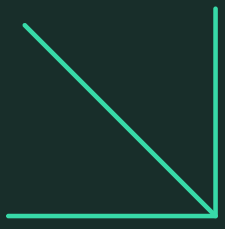
Top Threat Intelligence Trends

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 observed an increase in the release and sale of breached company data by threat actors. In Q3 2024, we are putting the spotlight on ransomware.

Seemingly every week, we hear about a company falling victim to a ransomware attack. Despite advancements in cybersecurity, ransomware remains a pervasive threat for organizations and cybercriminals are increasingly reaping the rewards. Average ransomware payments are millions of dollars according to various industry reports.

In this chapter, we will explore the discussions among threat actors on RAMP. Additionally, we will present a case study on a ransomware incident handled by the Cato MDR (Managed Detection and Response) team.



Ransomware

Development

Threat actors are constantly developing new and more efficient ransomware to stay ahead of security point solutions. Below are noteworthy examples.

Figure 1. helter sells locker source code for $45K (USD) and a GUI builder for an unknown ransomware

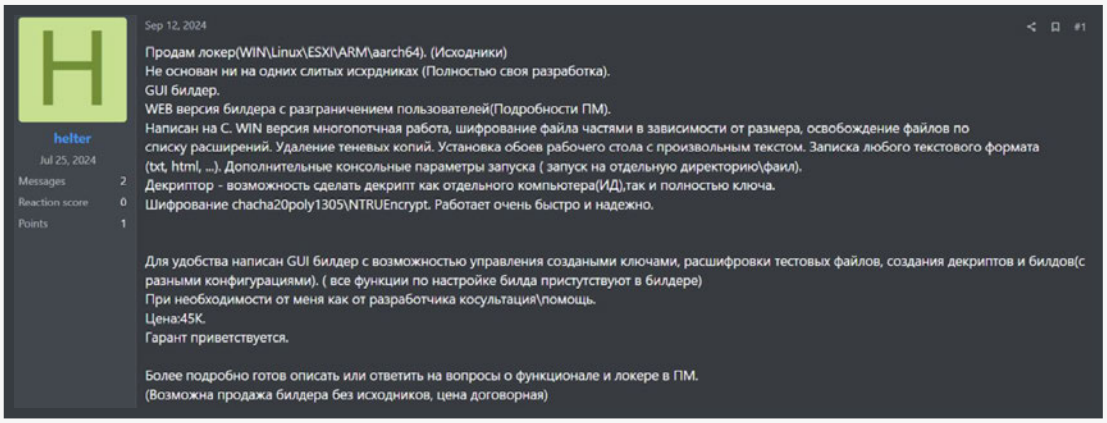
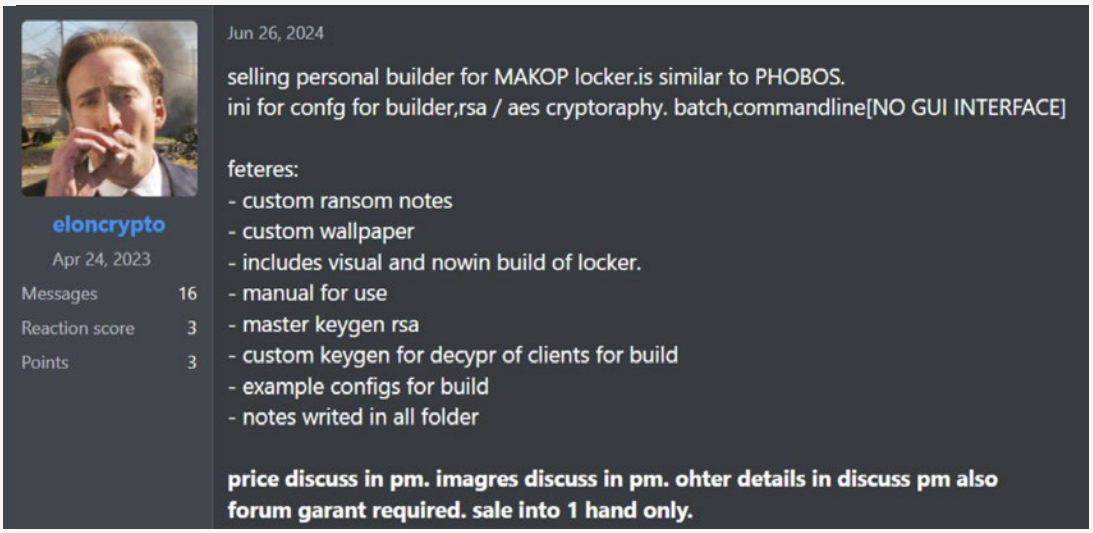


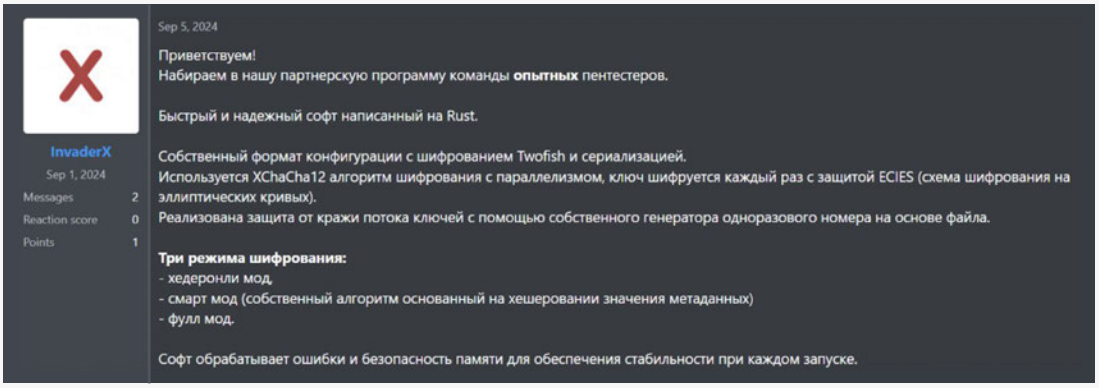
Figure 2. eloncrypto is selling a builder for MAKOP ransomware (an offshoot of the PHOBOS ransomware variant)



Penetration Testing and Affiliate Programs

Any good developer knows that software needs to be tested before deploying in production environments. This is also true for ransomware gangs. We are observing pen testers being recruited to aid in that effort. Below are noteworthy examples.

Figure 3. Pen testers recruited for Rabbit Hole ransomware affiliate program



> *In Figure 3, we observed a threat actor (InvaderX) post that he is seeking experienced pen testers for a ransomware affiliate program. Upon further investigation, we discovered the affiliate program is associated with the Rabbit Hole ransomware gang.*

Figure 4. Pen testers recruited for Lynx ransomware affiliate program

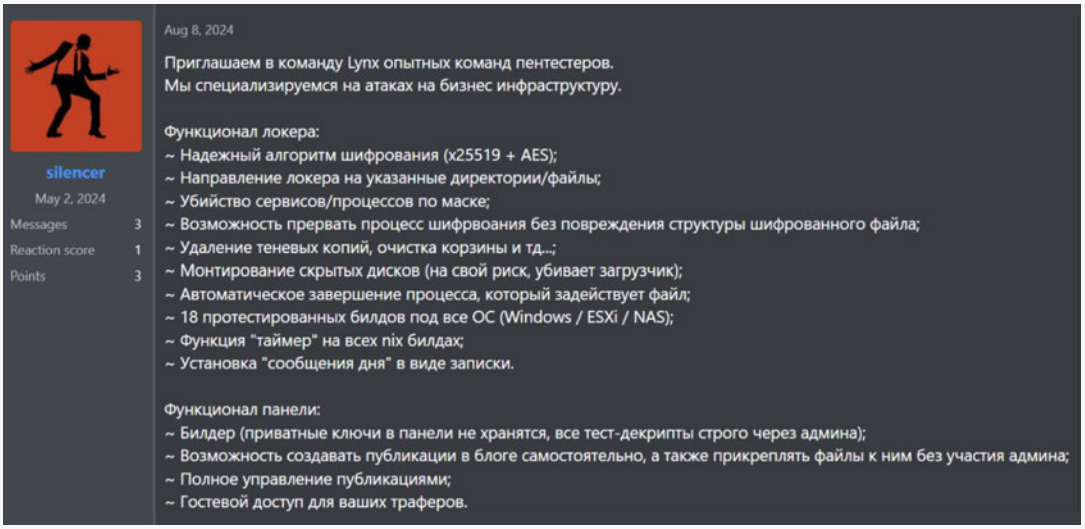
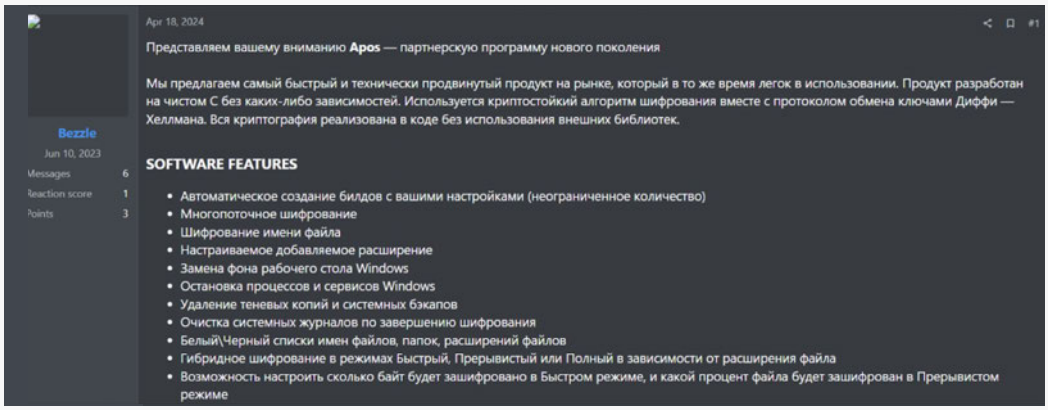


Figure 5. Advertisement for Apos ransomware affiliate program



> *In Figure 5, we observed a threat actor (Bezzle) advertise the Apos ransomware affiliate program. As of writing this report, it is unclear whether the ransomware's build is sold or rented. Based on our observations, the threat actor appears to ignore other users' questions on this subject, possibly only replying in direct messages.*

MDR Case Study

Cato Managed XDR uses a combination of machine learning algorithms that mine network traffic for Indicators of Compromise (IoCs), and human verification of detected anomalies. Cato MDR experts then guide customers on remediating compromised endpoints.

This section will explore a case study on a ransomware attack that the Cato MDR team investigated in July 2024. The case study outlines the kill chain from Hunters International, a ransomware gang, that led to double extortion (i.e. where a threat actor exfiltrates an organization's data before encrypting it).

Case Study – Hunters International

Hunters International is a ransomware gang that emerged in 2023 and is believed to have evolved from the Hive ransomware gang. Hunters International operates on a Ransomware-as-a-Service (RaaS) model.

Target: UK-based technology company

Reconnaissance

- Unknown

Weaponization

- WorkersDev backdoor created for exploitation

Delivery

- Malvertising used to deliver the WorkersDev backdoor

Exploitation

- PSExec and Windows command shell used to execute malicious code

Installation

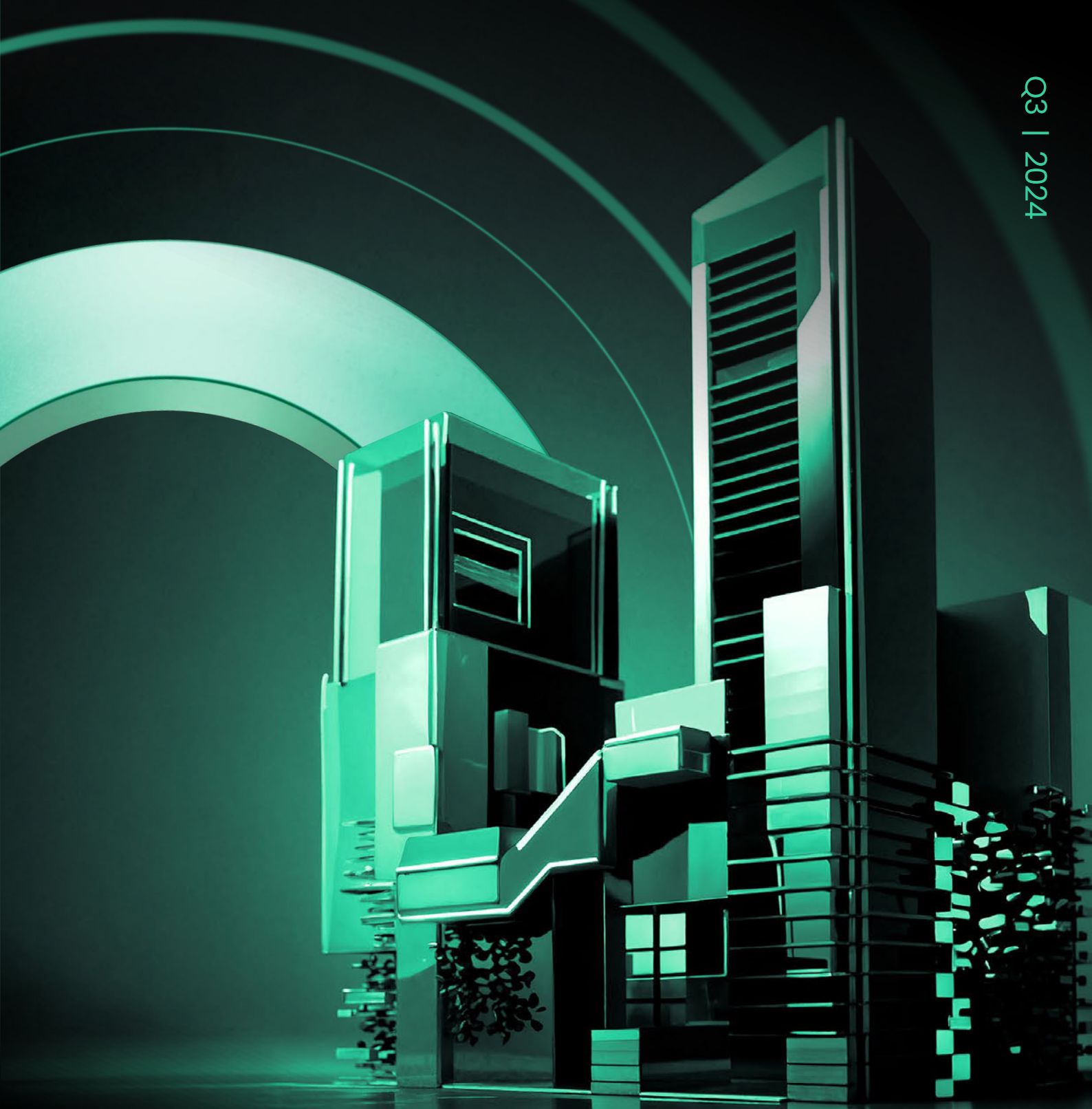
- WorkersDev backdoor and AnyDesk agent installed

Command and Control (C2)

- WorkersDev backdoor used to establish C2

Actions on Objectives

- PsExec and AnyDesk used to move laterally across the network
- Shut down Microsoft Defender for Endpoint and performed network scans for system discovery
- Ransomware attack included data exfiltration and encryption



CHAPTER 2

Top Enterprise Security Trends

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 6. The percentage of domains for the top 10 spoofed brands

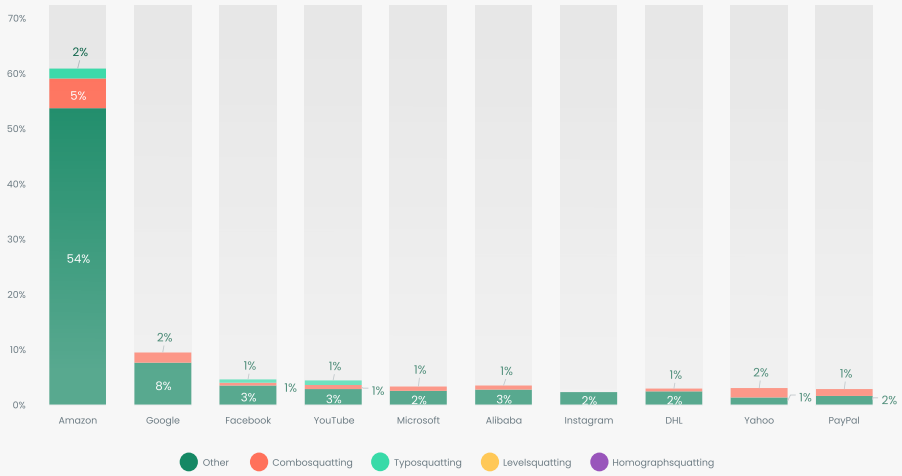


Figure 7. Amazon brand spoofing to increase traffic for a phony website: amazonbama[.]com

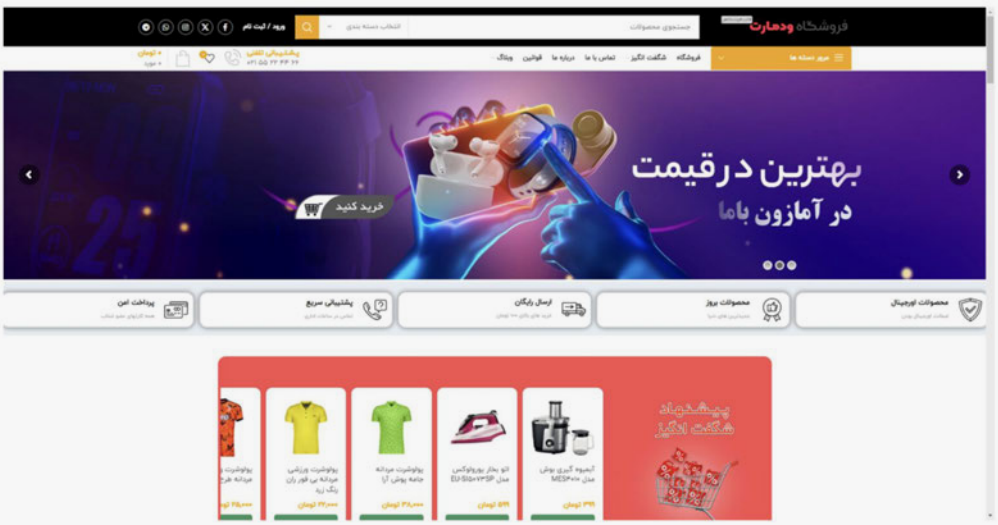
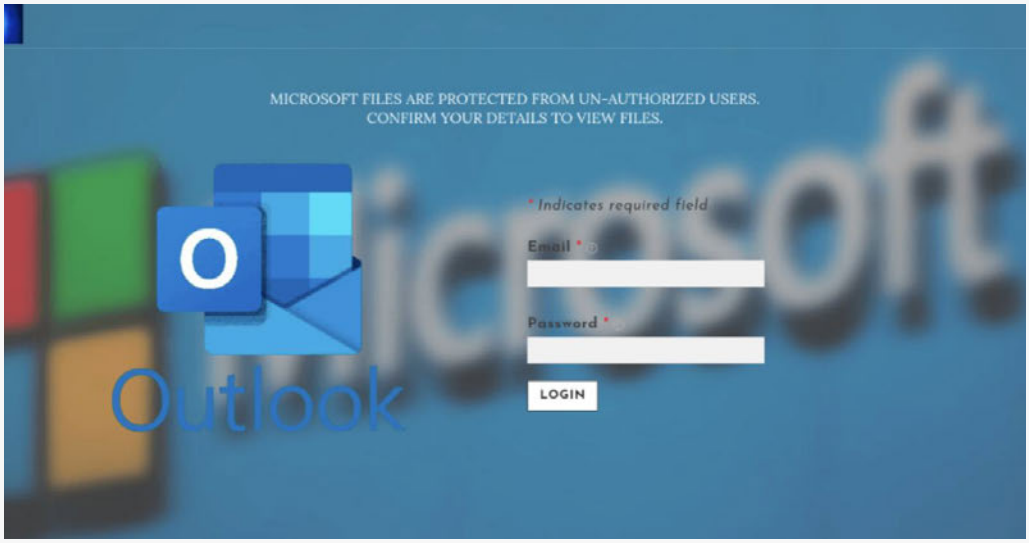


Figure 8. Microsoft phishing website for stealing credentials: microsoft-security-files[.]com



In the Q2 2024 Cato CTRL SASE Threat Report, Amazon was the top spoofed brand (66% of domains). In Q3 2024, Amazon remained the top spoofed brand (61% of domains). We suspect that Amazon Prime Day, which is Amazon's annual deal event held on July 16-17 this year, may have had an impact.

Threat actors leverage various "squatting" techniques to mask their domains:

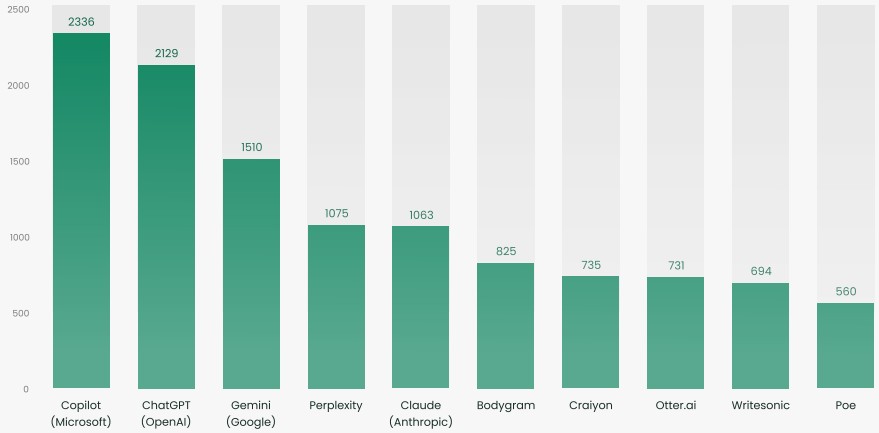
- **Combosquatting** involves creating a domain that combines legitimate domain with additional words or letters, such as "cato-networks.com," which adds a hyphen to Cato's URL catonetworks.com.
- **Homographsquatting** uses various character combinations that resemble the target domain visually, such as catonetw0rks.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.

Shadow AI

Shadow AI refers to the unauthorized or unsanctioned use of AI applications and tools within an organization without the knowledge or approval of IT departments or security teams. This phenomenon typically involves employees or departments adopting AI solutions independently and bypassing formal vetting processes and governance controls.

Cato has visibility into the usage of AI applications within corporate networks. Out of the hundreds of AI applications that Cato CTRL monitors, we provide a breakdown of the top AI applications used by organizations.

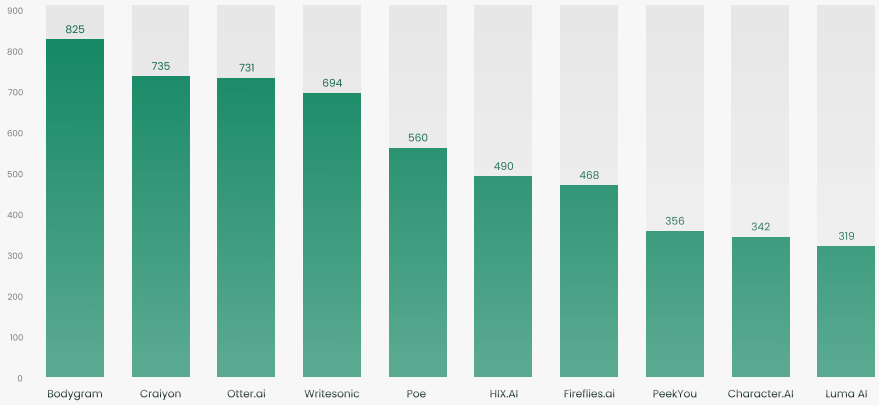
Figure 9. Top 10 AI applications used by unique accounts



In the Q2 2024 Cato CTRL SASE Threat Report, the top five AI applications were Copilot (Microsoft), ChatGPT (OpenAI), Gemini (Google), Perplexity and Claude (Anthropic). In Q3 2024, the top five AI applications remained the same.

Because of the popularity of these AI applications, we believe this list will remain static for the foreseeable future. As a result, we provide a breakdown of the top AI applications used by organizations excluding the previous top five.

Figure 10. Top 10 AI applications used by unique accounts (excluding previous top five)



App Name	Description	AI Usage	Security Risk
Bodygram	A body measurement app using smartphone photos for body measurements and composition data.	Uses AI for photo analysis, 3D avatar generation, and body composition estimates.	Data privacy concerns; potential exposure of employee biometric data.
Craiyon	An AI image generation tool.	Creates images from text descriptions using AI.	Intellectual property risks; potential generation of inappropriate or copyrighted content.
Otter.ai	A voice transcription and note-taking app.	Employs AI for speech recognition and transcription.	Confidentiality breaches; unauthorized recording and transcription of sensitive meetings.
Writesonic	An AI-powered writing assistant.	Generates various types of content using AI.	Data leakage; potential exposure of proprietary information in content generation.
Poe	A chatbot platform by Quora.	Integrates multiple AI models for conversational experiences.	Information security risks; potential sharing of confidential data with external AI models.
HIX.AI	An AI-powered writing tool.	Assists in content creation with AI-driven features.	Data privacy issues; possible exposure of internal documents or strategies.
Fireflies.ai	An AI note-taker and meeting assistant.	Uses AI for transcription and meeting summaries.	Unauthorized data access; potential recording and analysis of confidential discussions.
PeekYou	A people search engine.	Aggregates public information using AI algorithms.	Privacy violations; potential misuse for unauthorized employee background checks.
Character .AI	An AI platform for creating virtual characters.	Leverages AI for character generation and interactions.	Brand reputation risks; potential creation of unauthorized brand representatives.
Luma AI	A 3D capture and AI reconstruction tool.	Creates 3D models from 2D images using AI.	Intellectual property theft; potential unauthorized 3D modeling of proprietary designs.

CHAPTER 3

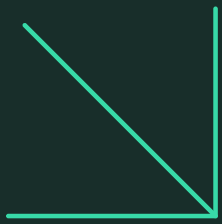
Top Network Security Trends

The threat landscape is constantly evolving, which provides new opportunities for threat actors to exploit and compromise organizations.

Suspicious activities should be monitored, such as non-standard port usage for known protocols, communication with public IPs (often linked to malware) and other unusual behaviors. Those unusual behaviors may include various techniques by threat actors, such as LOLBAS (Living Off The Land Binaries And Scripts) and LOTS (Living Off Trusted Sites).

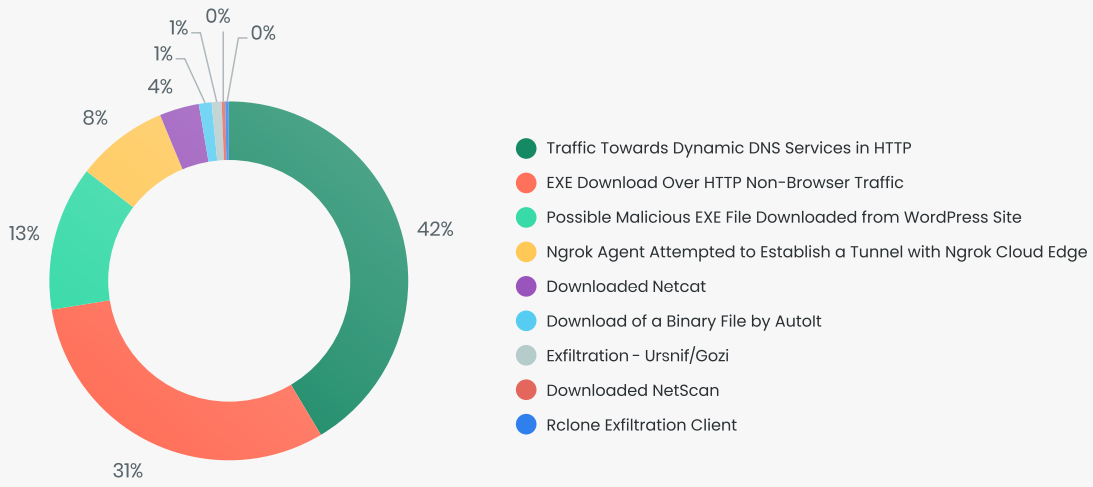
Cato developed SAM (Suspicious Activity Monitoring), a suite of capabilities that can identify suspicious behavior and alert an organization using Cato XDR. Each SAM signature is categorized by risk levels: Low, Medium or High. SAM signatures have also been mapped to their respective MITRE ATT&CK tactics.

Understanding and analyzing suspicious events can help reduce an organization's attack surface. By monitoring suspicious activities, we can trace them back and attribute them to specific threat actors. Honeypots and deception techniques can be deployed based on the activity identified by monitoring these events.



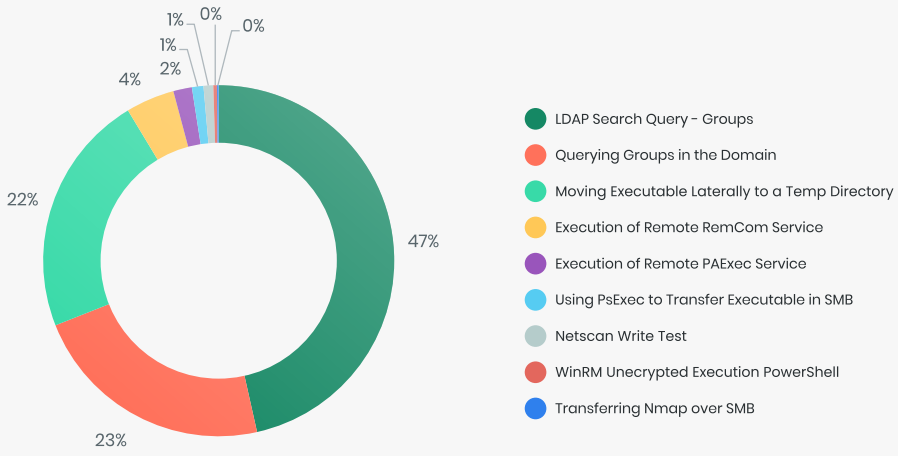
Suspicious Activity Monitoring (SAM)

Figure 11. Top 10 high-risk suspicious activities in outbound traffic (unique accounts)



The top SAM behavior for outbound traffic saw attempts to download Netcat, a utility tool used by threat actors to establish command-and-control (C2) communication. This can lead to file downloads, data exfiltration and more.

Figure 12. Top 10 high-risk suspicious activities in WANbound traffic by unique accounts

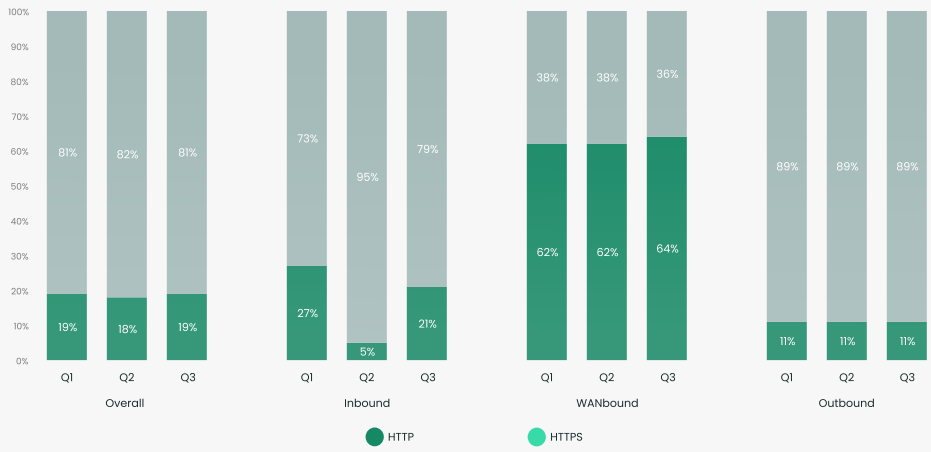


The top SAM behavior for WANbound traffic involves using lightweight directory access protocol (LDAP) to query domain groups. Although these actions are common for legitimate administrative tools, threat actors are employing them to enumerate groups, particularly for the purpose of privilege escalation.

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.

Figure 13. HTTP vs. HTTPS traffic comparison by traffic direction



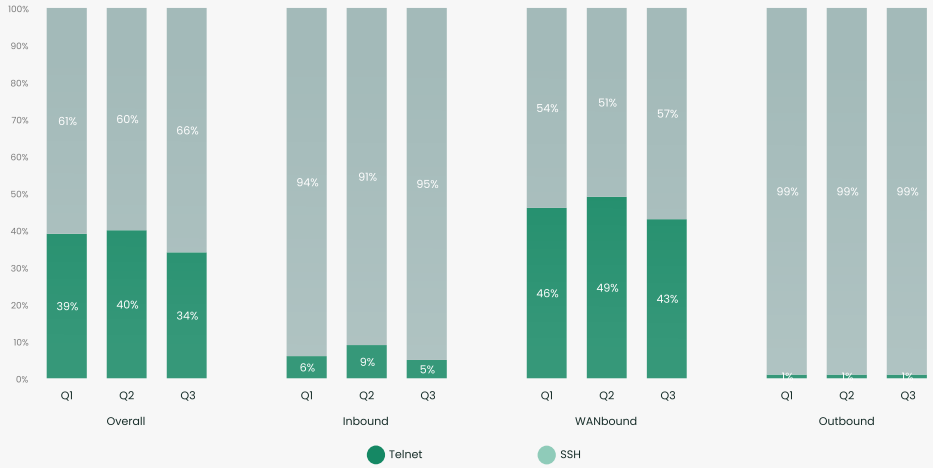
Overall, we didn't observe any significant changes between Q1 2024, Q2 2024 and Q3 2024. However, it is alarming that nearly two-thirds (64%) of WANbound traffic still consists of HTTP, which is far less secure than HTTPS.

Figures 14 and 15. WANbound HTTP vs. HTTPS traffic by industry verticals

When we break down WANbound traffic by verticals, we observed an increase in HTTP traffic in Mining & Metals (69% increase compared to Q2), Oil & Energy (19% increase compared to Q2) and Finance (14% increase compared to Q2).

Also, we saw an increase in HTTPS traffic in Law Practice (25% increase compared to Q2), Real Estate (21% increase compared to Q2) and Construction (8% increase compared to Q2).

Figure 16. Telnet vs. SSH traffic comparison by traffic direction



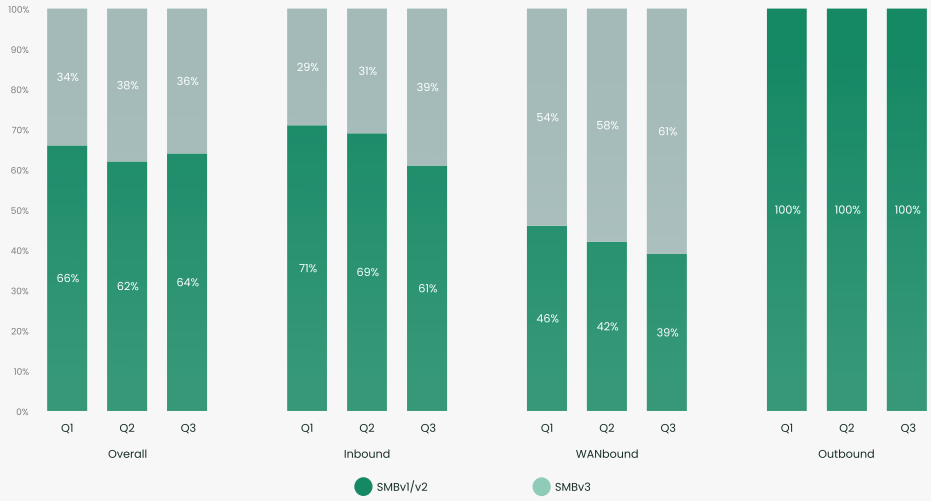
Overall, we didn't observe any significant changes between Q1 2024, Q2 2024 and Q3 2024. However, it is concerning that almost half (43%) of WANbound traffic still consists of Telnet traffic. This is dangerous, as Telnet is a clear text protocol used for connecting to a remote system. Threat actors only need to eavesdrop on the network traffic to capture credentials or any other sensitive information.

Figures 17 and 18. WANbound Telnet vs. SSH traffic by industry verticals

When we break down WANbound traffic by verticals, we observed an increase in Telnet traffic in Agriculture (388% increase compared to Q2), Mining & Metals (671% increase compared to Q2) and Oil & Energy (236% increase compared to Q2).

Also, we saw an increase in SSH traffic in Hospitality (340% increase compared to Q2), Automotive (164% increase compared to Q2) and Consulting (89% increase compared to Q2).

Figure 19. SMB v1/v2 vs. SMB v3 traffic comparison by traffic direction



Overall, we didn't observe any significant changes between Q1 2024, Q2 2024 and Q3 2024. However, we are starting to see a quarterly uptick in the use of SMBv3 for inbound and WANbound traffic. The increase is mainly due to organizations replacing old software, operating systems and devices that used SMBv1/v2. However, this change is slowly growing incrementally because organizations are mostly concerned about possible compatibility issues and downtime.

Figures 20 and 21. SMB v1/v2 vs. SMB v3 WANbound traffic by industry verticals

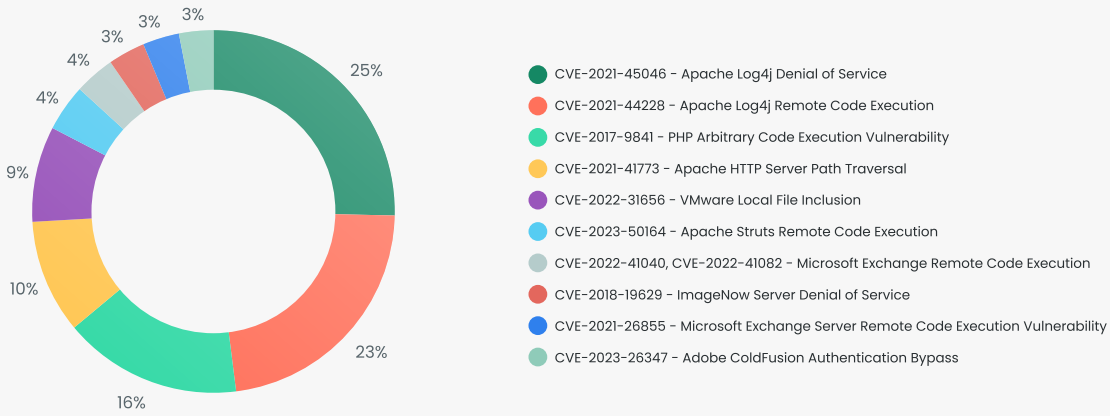
When we break down WANbound traffic by verticals, we observed an increase in SMBv1/2 traffic in Travel & Tourism (77% increase compared to Q2), Media (59% increase compared to Q2) and Transportation (57% increase compared to Q2).

We also saw an increase in SMBv3 traffic in Agriculture (120% increase compared to Q2), Entertainment (120% increase compared to Q2), and Hospitality (120% increase compared to Q2).

Mitigated Vulnerabilities

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

Figure 22. Top 10 mitigated CVEs in inbound traffic by traffic volume



In the Q2 2024 Cato CTRL SASE Threat Report, CVE-2021-44228 (Apache Log4j remote code execution) was the most popular exploit for threat actors to attempt to use in inbound traffic. In Q3 2024, CVE-2021-45046 (Apache Log4j Denial of Service) ranked first.

Although CVE-2016-6277 (Netgear Router RCE) is not in the top 10 inbound threats, we observed an increased number of attempts to deliver Mozi malware, which forms the Mozi botnet to primarily execute Distributed Denial-of-Service (DDoS) attacks. We also observed attempts to exploit CVE-2016-20017 (D-Link DSL-2750B Command Injection) to deliver the Mirai malware, which is also commonly used for DDoS attacks.

Figure 23. Top 10 mitigated CVEs in inbound traffic by traffic volume (US)

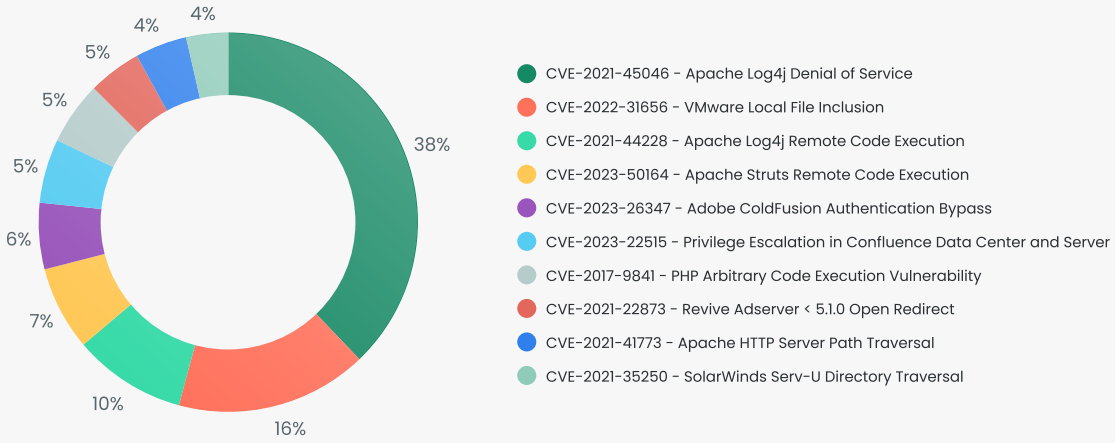


Figure 24. Top 10 mitigated CVEs in inbound traffic by traffic volume (UK)

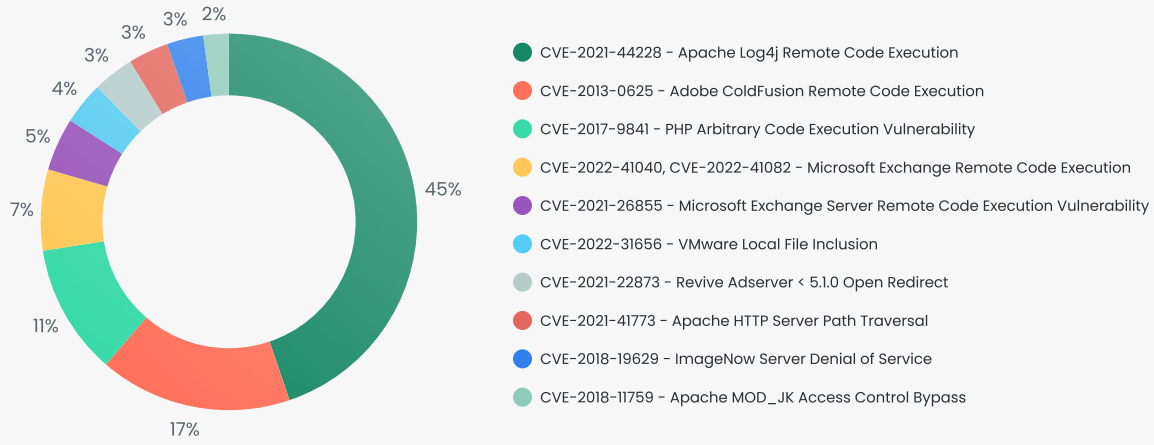


Figure 25. Top 10 mitigated CVEs in inbound traffic by traffic volume (France)

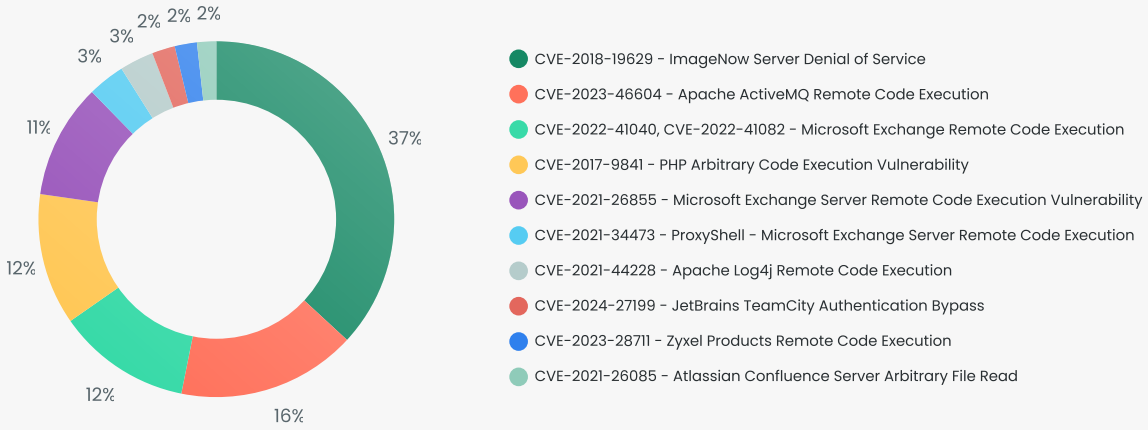


Figure 26. Top 10 mitigated CVEs in inbound traffic by traffic volume (Germany)

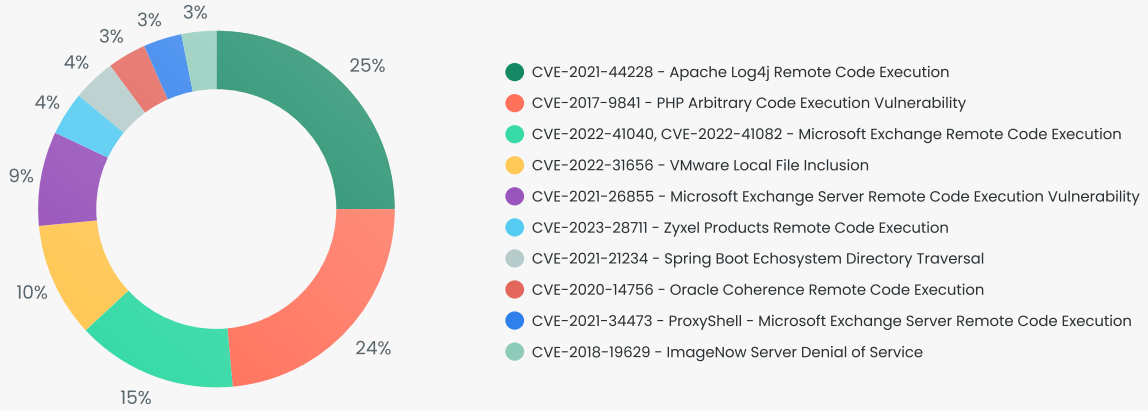


Figure 27. Top 10 mitigated CVEs in inbound traffic by traffic volume (Israel)

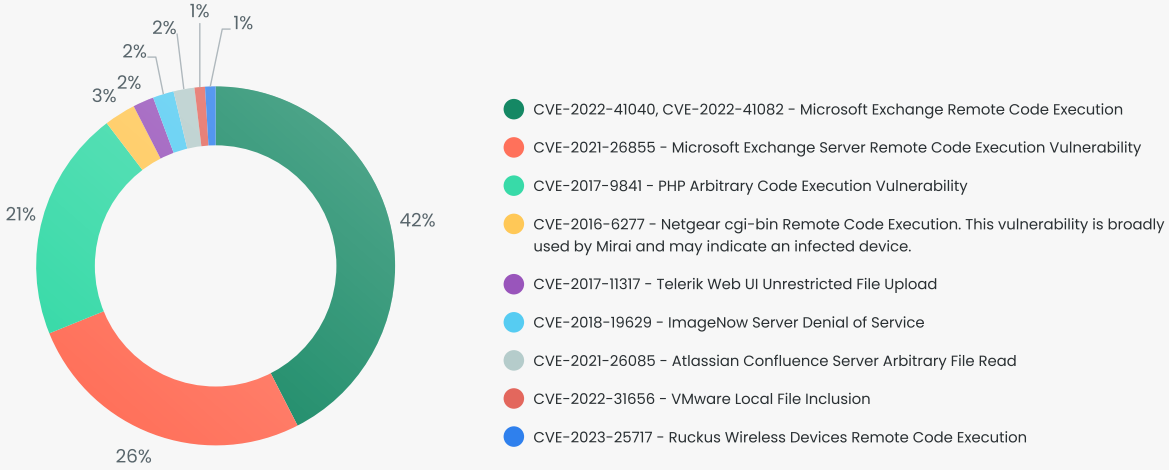
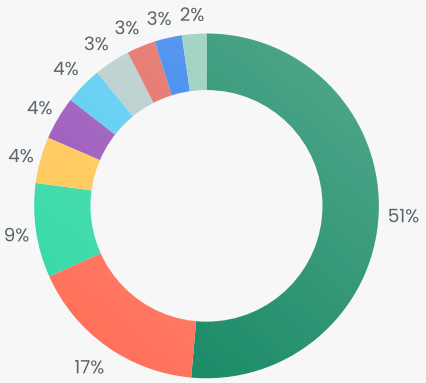
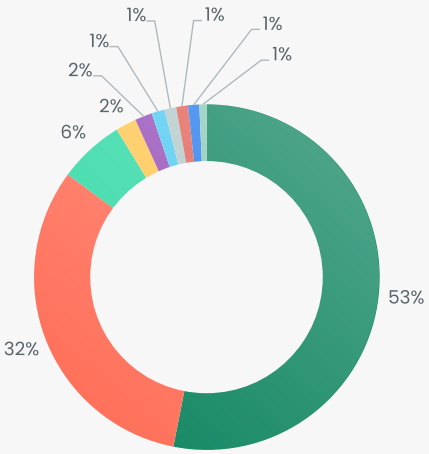


Figure 28. Top 10 mitigated CVEs in inbound traffic by traffic volume (Japan)



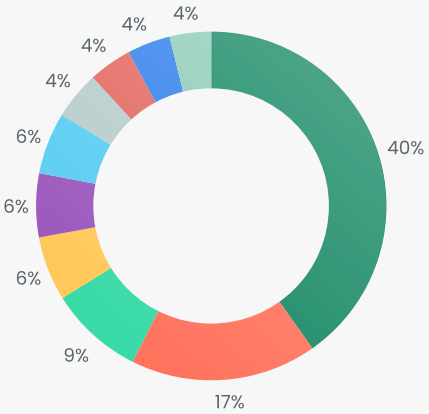
- CVE-2017-9841 - PHP Arbitrary Code Execution Vulnerability
- CVE-2023-46604 - Apache ActiveMQ Remote Code Execution
- CVE-2022-41040, CVE-2022-41082 - Microsoft Exchange Remote Code Execution
- CVE-2018-19629 - ImageNow Server Denial of Service
- CVE-2021-26855 - Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-41773 - Apache HTTP Server Path Traversal
- CVE-2015-2051 - D-Link DIR-645 Router Remote Code Execution
- CVE-2018-10561 - Dasan GPON Home Routers Bypass Authentication
- CVE-2018-10562 - Dasan GPON Home Routers Command Injection
- CVE-2021-26897 - Windows DNS Remote Code Execution

Figure 29. Top 10 mitigated CVEs in outbound traffic by traffic volume



- CVE-2021-44228 - Apache Log4j Remote Code Execution
- CVE-2018-19629 - ImageNow Server Denial of Service
- CVE-2024-38021 - Microsoft Office Remote Code Execution Vulnerability
- CVE-2020-14750 - Oracle WebLogic Server RCE
- CVE-2021-38647 - Open Management Infrastructure Remote Code Execution
- CVE-2017-1000486 - Primetek Primefaces Weak Encryption Remote Code Execution
- CVE-2000-0325 - Detected Attempts to Execute Arbitrary Commands Using the Microsoft Jet Database Engine
- CVE-2009-2445 - Oracle iPlanet Web Server Sensitive Data Exposure
- CVE-2022-22963 - Spring Cloud Remote Code Execution
- CVE-2020-5902 - F5 Big-IP 13.1.3 Local File Inclusion and Remote Code Execution

Figure 30. Top 10 mitigated CVEs in WANbound traffic by traffic volume



- CVE-2021-44228 - Apache Log4j Remote Code Execution
- CVE-2013-0625 - Adobe ColdFusion Remote Code Execution
- CVE-2000-0325 - Detected attempts to execute arbitrary commands using the microsoft jet database vba engine
- CVE-2018-19629 - ImageNow Server Denial of Service
- CVE-2022-35914 - GLPI Project Remote Code Execution
- CVE-2009-2445 - Oracle iPlanet Web Server Sensitive Data Exposure
- CVE-2021-26897 - Windows DNS Remote Code Execution
- CVE-2021-40539 - Zoho ManageEngine Remote Code Execution
- CVE-2020-15505 - MobileIron Core and Connector Remote Code Execution
- CVE-2017-9805-1 - Apache Struts 2 Rest Plugin XStream Remote Code Execution

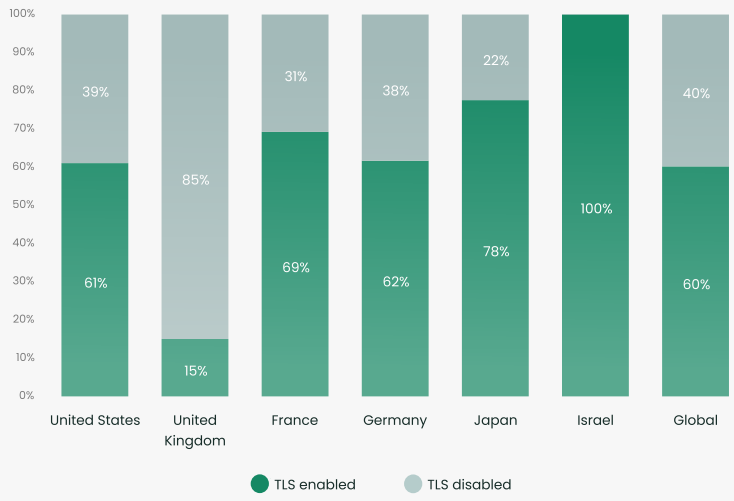
TLS Attack Attempts

TLS inspection allows organizations to decrypt, inspect and re-encrypt traffic. However, TLS inspection can break applications and access to some domains. As such, many organizations choose to forgo TLS inspection entirely or bypass inspection for a large portion of their traffic.

Cato CTRL found that only 45% of participating organizations enable TLS inspection. Even then, only 3% of organizations inspected all relevant TLS-encrypted sessions. This leaves the door open for threat actors to utilize TLS traffic and remain undetected. Organizations must inspect TLS sessions to protect themselves. In Q3 2024, Cato CTRL found that 60% of attempts to exploit CVEs were blocked in TLS traffic. CVEs included Log4j, SolarWinds and ConnectWise.

When TLS inspection is enabled, organizations are better protected. In Q3 2024, Cato CTRL found that organizations who enabled TLS inspection blocked 52% more malicious traffic than organizations without TLS inspection.

Figure 31. Percentage of attempts to exploit CVEs with TLS enabled and TLS disabled by country



New Product Capability

Cato Safe TLS Inspection revolutionizes encrypted traffic analysis by leveraging real-time, crowdsourced data for precise, adaptive inspection. Traditional solutions that inspect all TLS traffic by default require complex and time-consuming bypass lists management to avoid disruptions. Cato inspects only those applications and domains that are known to be safe to inspect, while bypassing everything else.

Cato Safe TLS Inspection offers:

- **Better Protection:**
  Eliminates blind spots in encrypted traffic for enhanced security.
- **Seamless User Experience:**
  Ensures uninterrupted business operations.
- **Operational Efficiency:**
  Automates inspection processes, which reduces IT burden and frees up resources for strategic initiatives.

CHAPTER 4

Key Recommendations

Ransomware

Threat Evolution

Ransomware is continuously being developed with advanced encryption algorithms, and other techniques like multithreading and custom configurations. Early identification of these patterns through advanced threat detection, AI-driven anomaly monitoring and robust endpoint protection is critical to counteract evolving ransomware threats.

Targeted Encryption

Many ransomware variants are designed with the flexibility to target specific directories, file extensions and operating systems. Defensive strategies should include robust segmentation, backup policies and the use of immutable backups to mitigate encryption risks.

Affiliate Programs

Threat actors are recruiting pen testers to test and improve the reliability of their ransomware for affiliate programs. Organizations should engage in red team exercises and pen testing to identify vulnerabilities in their infrastructure before ransomware gangs exploit them.

Shadow AI

Data Privacy

Many AI-powered applications handle sensitive data, including personally identifiable information (PII) and intellectual property (IP). Organizations should be aware of the potential privacy concerns when AI-powered applications are used without proper oversight.

Visibility

The proliferation of shadow AI underscores the urgent need for enhanced visibility into AI usage across an organization. Visibility into which AI tools and applications are being used, by whom and for what purposes is important for organizations to effectively manage risks.

Employee Education

Organizations should prioritize employee education on the risks associated with using unauthorized AI tools and the importance of following company protocols for AI adoption.

Network Security

Legacy Applications

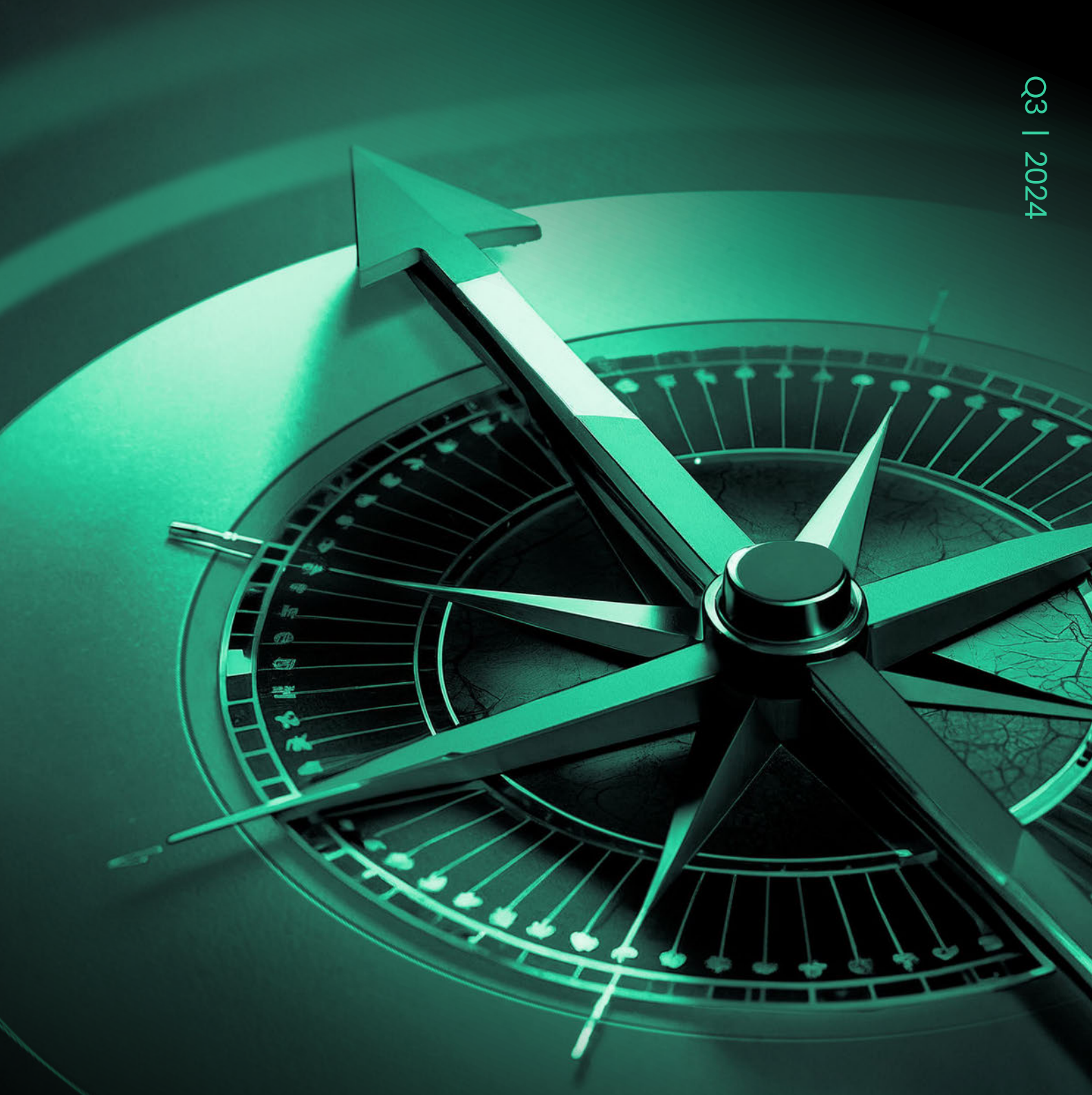
The usage of insecure protocols generally implies the use of legacy systems that rely on these protocols. Organizations should transition to more up-to-date systems to minimize security risks.

Secure Protocols

Organizations should regularly audit the protocols in use by transitioning away from insecure protocols like HTTP, Telnet and SMBv1/v2, and replacing them with secure alternatives such as HTTPS, SSH and SMBv3.

TLS Inspection

Threat actors often use encrypted communication channels to evade detection and exploit vulnerabilities in applications that utilize TLS. Enabling TLS inspection is crucial for effectively monitoring this traffic.



CHAPTER 5

Conclusion

Methodology

The Q3 2024 Cato CTRL SASE Threat Report summarizes findings from Cato CTRL's analysis of 1.46 trillion network flows across more than 2,500 customers globally between July and September 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. The SASE leader creates a seamless and elegant customer experience that effortlessly enables threat prevention, data protection, and timely incident detection and response. 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**.

CATO NETWORKS