CATO NETWORKS

SOMMITA TECHNOLOGY GROUP, LLC

Cato Networks SASE Threat Research Report

Q1/22

Executive Summary

The Cato Networks SASE Threat Research Report highlights cyber threats and trends based on more than 328 billion network flows that passed through Cato Cloud. The convergence of networking and security provides unique visibility into both enterprise network usage as well as the hostile network scans, exploitation attempts, malware communication to C&C servers, and other malicious activity occurring across enterprise networks.

The report provides insight and a behind-the-scenes look into how Cato Networks analyzes and identifies new threats. It also highlights important breach reports and cybersecurity news from the past quarter.

Key Quarterly Findings

1/ Log4j continues to be the overwhelming leader in vulnerability exploit attempts. New vulnerabilities such as Spring4Shell (CVE-2022-22965) did not come close to Log4J numbers in Q1 of 2022.

2/ New in the Cato Networks SASE Threat Research Report – MITRE ATT&CK statistics.

3/ Reputation based threats, an event triggered by inbound or outbound communication to destinations known to have bad reputation, more than doubled.

4/ Incidents researched by Cato Network's security teams show MITRE ATT&CK techniques for data exfiltration and application layer protocol rank at the top of threat actors TTPs.

Section 1

The Data

Network

This quarter's total network flows count is slightly higher than Q4 of 2021 and while the total number of high-risk flows continued to grow the total verified security threats increased by only 10%.

Network Flows 350B — Any sequence of packets sharing a common source IP and port, destination IP and port and protocol

Events 26B — Any network flow that is triggered by one of Cato Networks' security controls

Cato Threat Hunting System

Cato Networks automated threat hunting system identifies high risk events using proprietary machine learning models and based on multiple network and security indicators

Threats 300K — High-risk flows based on machine learning and data correlation

Incidents 20K — A verified security threat

Top 5 Threat Types

Q1 of 2022 is the first quarter in which there has been a decline in the number network scans (a roughly 33% decrease), however, other threat categories have significantly increased in numbers. The most notable change was in reputation-based threats – an over 100% increase! Policy violations and web application attacks showed a smaller increase in numbers while the overall vulnerability scanning numbers fell.

It is worth noting that while malware numbers are steady, crypto mining numbers are continuing their steady quarter over quarter growth and brute force attacks and RCE have more than tripled.

Network Scan **10,784,912,994**

Reputation **1,509,239,467**

Policy Violation **539,742,953**

Web Application Attack **253,840,195**

Vulnerability Scan **109,803,080**

Worth Noting

7,367,220
Brute Force

5,995,569
Remote Code Execution

8,691,506
Crypto Mining

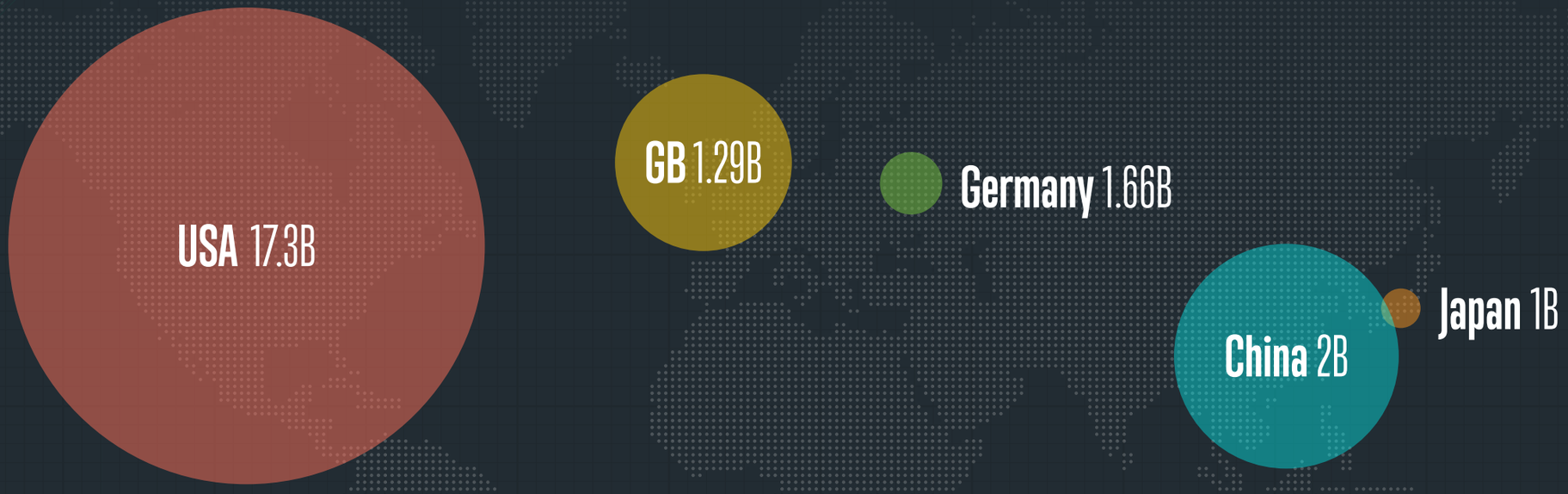
70,130,903
Malware

Top 5 Attack Origin Countries

This map shows the top five countries from which malicious activity was initiated. Most of the malicious activity is related to malware C&C communication, thus this map shows the countries hosting the most C&C servers.

While it is no surprise that the US remains in the first spot, the UK and JP traded places while numbers from Germany slightly increased. India, which was in 8th place in Q4 of 2021, has completely dropped off the Top 20 while Singapore numbers are continuing to grow and get closer to the 1B mark with France, Korea, Ireland and Brazil right behind.

Understanding where attacks originate from or where the destination of malware communicates is a crucial part of any organization's visibility to threats and trends. Attackers know that some outbound communication to certain countries may be blocked or inspected and accordingly – they make sure their C&C (command and control) infrastructure is hosted in what may be perceived as "safe" countries.



Top 5 Most Used Cloud Apps

1 Microsoft

2 Google

3 RingCentral

4 Amazon

5 Facebook

For the second quarter in a row – not much has changed at the top most used cloud apps, at least not in the Top 10. However, looking at places 10-40 we observed a significant increase in usage of consumer applications such as Telegram (which has more than tripled), TikTok (up 10%), and YouTube (up 25%) compared to Q4 of 2021. One possible reason in the conflict between Russia and Ukraine as those applications are common applications for sharing videos of the fighting.

Top 5 CVE Exploit Attempts

Over 24M
CVE-2021-44228

866,916
CVE-2009-2445

287,143
CVE-2018-19629

178,864
CVE-2017-9841

155,470
CVE-2021-31166

The old and the new! Log4j exploitation attempts have dominated the first quarter of 2022. While in Q4 of 2021 we have observed over 3M such attempts, this number increased to 24M in Q1 of 2022 and shows no signs of slowing down. Attack using this vulnerability have been observed around the world, including attacks in the Ukraine.

On the other end of the innovation spectrum, number two on the list is a 13-year-old Java vulnerability (which held the same spot last quarter but has doubled in size). These two extremes highlight the need for immediate virtual patching as well as maintaining actionable and relevant vulnerabilities checked.

Section 2

On the Hunt

To kickoff 2022, the Cato Security report will now include MITRE ATT&CK stats. MITRE offers a lot of information and updates regarding this framework at https://attack.mitre.org/ including roadmap and new releases.

The MITRE ATT&CK framework can be used worldwide across multiple security disciplines such as intrusion detection, threat hunting and intelligence, security engineering, and risk management. Some key benefits or use-cases for the ATT&CK framework can include:

Attacker Emulation

Simulates attack scenarios to test security solutions and verify defense capabilities.

Penetration Testing

Acts as a frame of reference when conducting red team or purple team exercises and studying or mapping adversarial behaviors.

Forensics and Investigations

Aids Incident Response teams in finding missing attacker activity.

Behavioral Analytics

Provides contextual, behavioral information which security teams and vendors can use to identify hidden, unrelated anomalies and patterns.

Security Maturity and Gap Assessments

Helps determine what parts of the enterprise lacks defenses against adversary behaviors and what parts of the organization needs prioritized investments.

Product Evaluations

Acts as a frame of reference when conducting red team or purple team exercises and studying or mapping adversarial behaviors.

Standard For Technology Integrations

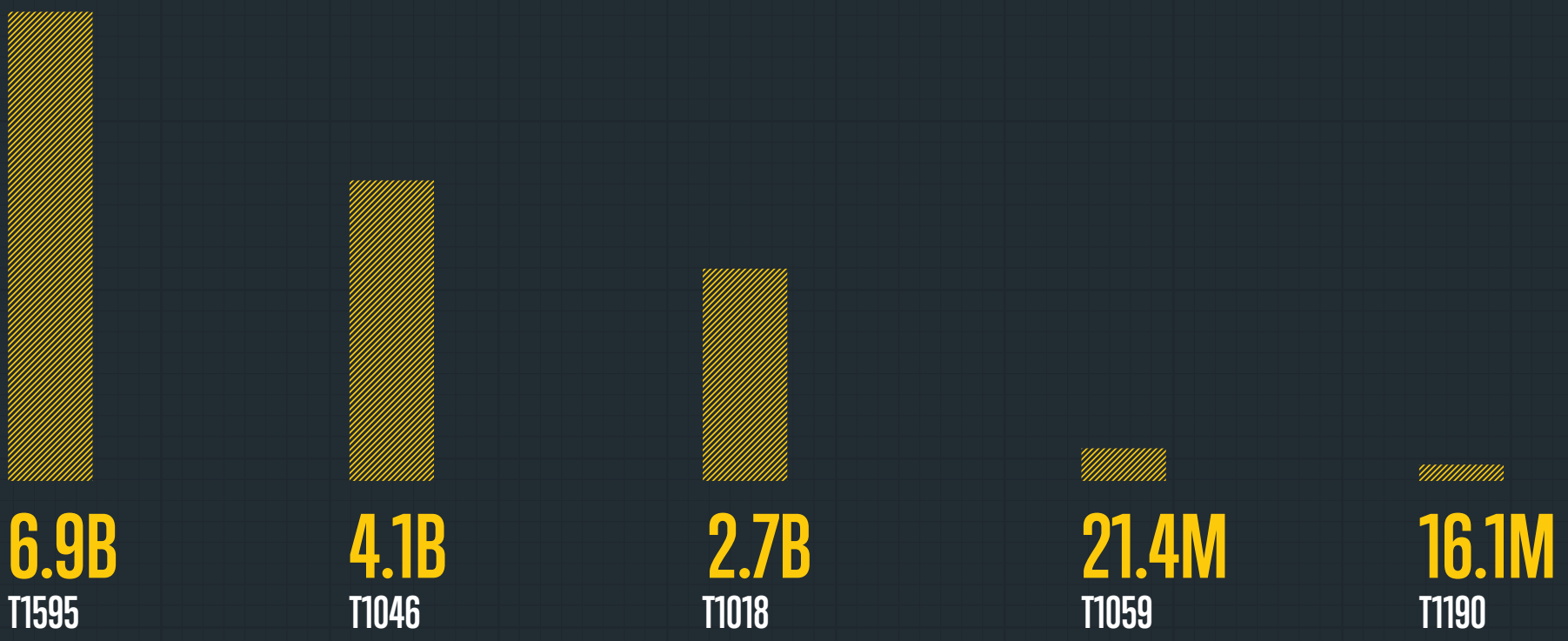
Serves as a common standard that helps connect and communicate disparate security tools, leading to an integrated defense approach.

ATT&CK is truly a gold mine of resources when it comes to adversary techniques and MITRE welcomes contributions from the cybersecurity industry to keep the framework updated with the latest TTPs. Cybersecurity communities worldwide increasingly discuss cyberattack techniques, building defenses and choosing security tools in terms of ATT&CK. Regardless of where you are in your cybersecurity maturity, it is never too late to realign your security, redefine your security processes and rethink your security metrics in terms of the MITRE ATT&CK framework.

As part of our Master Class series, we will also feature an intro to MITRE ATT&CK session in the very near future, but for now let's look at the numbers.

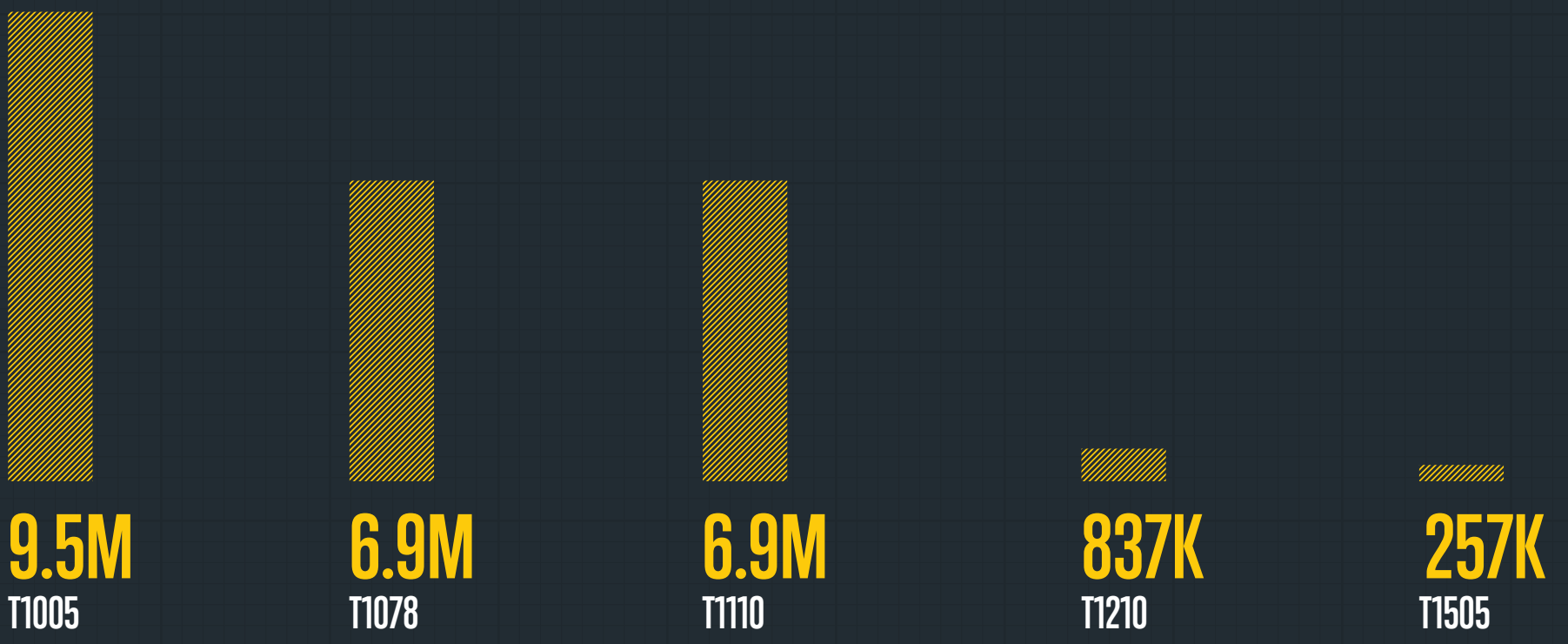
Top 10 number of flows per attack technique

This numbers shows the number of network flows associated with a MITRE ATT&CK technique. When looking at the Top 5 Threat Types tables it is no surprise to see network-based scanning dominating this chart. Active scanning, network discovery and remote system discovery hold the top 3 spots, respectively. Following are command and scripting interpreter and exploitation of public facing application.



Top 10 number of incidents per attack technique

This chart is based on confirmed security events that have been researched by Cato Networks security team and shows the number of times different techniques were used by threat actors. As such, these will usually be more “internal events” when compared to the “Flows per attack technique” chart. The top 3 techniques for Q1 of 2022 are Application Layer Protocol, Exfiltration Over C2 Channel and Automated Exfiltration.



Section 3

In other news...

Critical attacks against critical systems

"President Joe Biden signed a law that requires critical infrastructure entities to report cyber attacks within 72 hours and report ransom payments in 24 hours".

Related:

PYMNTS.com FDIC's new regulation for financial institutions.

Cyber attacks targeting satellites

The conflict between Russian and the Ukraine has introduced a new, even if to be expected, target – satellites. The attack against Viasat as well the operations of Starlink have highlighted how this new vector will now be a central piece in cyberwarfare.

Ukraine Vs Russia – who is who

A list of threat actors and tools observed in the ongoing conflict.

Lapsus$ arrests

Lapsus$ has captured the attention of the security community over the past month by compromising four of the most prominent enterprise technology companies in the world: Nvidia, Samsung, Microsoft, and Okta. The group has appeared to be less financially motivated than traditional ransomware gangs, with Lapsus$ rarely encrypting victim networks and often releasing data before demanding payment.