CATO
NETWORKS

Cato Networks SASE Threat Research Report

Q1/21

Executive Summary

The Cato Networks Quarterly Report highlights cyber threats and trends based on almost 200 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 Network's MDR team analyzes and identifies new threats. It also highlights important breach reports and cyber security news from the past quarter.

Key Quarterly Findings:

1/ There is an uptick in the usage of remote administration tools (RDP, VNC, TeamViewer etc.) as well as attempts by threat actors to brute force passwords to these tools.

2/ Attack source countries are not your usual suspects, banning some regions from accessing your network may lead to a false sense of security while ignoring the true threats.

3/ Network-based threat hunting can help identify previously unknown, unclassified threats.

4/ Remote Code Execution vulnerabilities targeting PHP dominate the observed exploitation attempts.

Section 1

The Data

Network

Network Flows 190B

Any sequence of packets sharing a common source IP and port, destination IP and port and protocol

Events 16B

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 181K

High-risk flows based on machine learning and data correlation

Incidents 19K

A verified security threat

Top 5 Threat Types

Network Scan 5,693,414,033

An event triggered by a network discovery scan (SYN scan, port scanning etc.)

Reputation 229,421,264

An event triggered by inbound or outbound communication to domains, IPs (and more) known to have bad reputation

Vulnerability Scan 74,049,926

An event triggered by a known vulnerability scanner (such as OpenVAS, Nessus and others)

Malware 11,614,484

An event triggered by a malware

Web Application Attack 8,140,518

An event triggered by attacks over http/https

Worth Noting

8,470
Crypto Mining

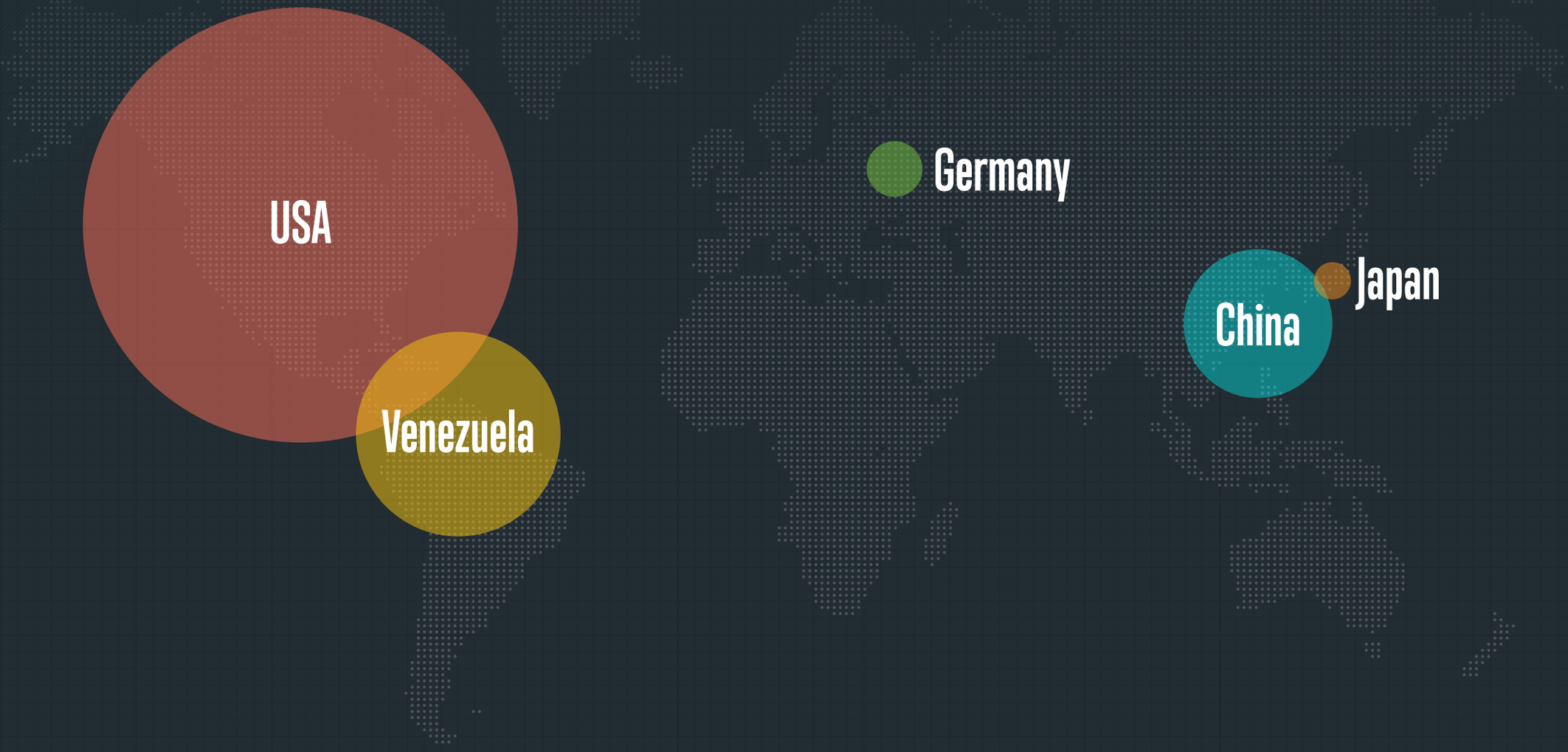
2,027,892
Remote Code Execution

1,763,166
PuP

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 where most of these C&C servers are hosted.

It is worth noting the absence of several countries usually mentioned in relation with cybercrime, fraud, and nation-state actors. At the same time, it is worth noting that the US hosts more C&C servers than any other country. This should be considered when designing firewall rules that completely ban certain countries and regions; these may not be the source of the attacks the organization is experiencing after all.



Top 5 Most Used Cloud Apps

1 Microsoft Office

2 Google Apps

3 Skype/Teams

4 TeamViewer

5 AnyConnect

During the first quarter of 2021 we observed several interesting trends when it comes to the type and frequency of usage of application and services within organizations. One type of heavily used application (as it was in 2020 as well) is remote access software. RDP, VNC, TeamViewer and other such applications generated a noticeable number of networks flows. It is worth noting that some of these applications, when not properly secure, can be a target of threat actors. One such example from this quarter is the attack on one of Florida's water treatment facilities (see Section 3 of this report).

The recent GameStop-Reddit-Wall Street story might have been a contributing factor to the rise in traffic from trading applications. Robinhood and eToro network flows have increased, surpassing previously more popular applications such as the news applications from CNN, New York Times and CNBC.

*Cloud apps are identified based on domains, IPs, and traffic inspection.

Worth Noting

There were more TikTok flows than Gmail, LinkedIn or Spotify flows

A significant rise in Robinhood flows

Significant number of SolarWind flows

Top 5 CVE Exploit Attempts

377,721
CVE-2017-9841

186,275
CVE-2019-9082

125,794
CVE-2017-1001000

43,640
CVE-2020-8515

15,222
CVE-2015-8562

Worth Noting

In the top 10 CVEs observed there are vulnerabilities that are over 20 years old. Threat actors don't attempt to exploit only the most recent vulnerabilities or 0-day. They also scan for EOL, unsupported systems.

Three out of the five most observed CVEs are PHP related (2017-9841, 2019-9082 and 2015-8562) targeting different systems with potential RCE. CVE-2020-8515 got its share of popularity late in 2020 as it was one of 25 CVEs the NSA urged organizations to patch as it was used by nation state actors.

Other notable CVEs are vSphere, Oracle Weblogic and Big-IP vulnerabilities, each with thousands of scans. The exploit attempts were not limited to software, there were multiple hardware exploit attempts, mostly targeting routers with remote administration vulnerabilities. Last on this list but still trending were the Microsoft Exchange targeting HAFNIUM exploits, specifically CVE-2021-26855 and CVE-2021-26857.

Section 2

On the Hunt

Threat actors have been utilizing different techniques to evade detection by security solutions from DGAs (Domain Generation Algorithms) used in combination with Fast Flux networks to malware obfuscation techniques to changing C&C communication characteristics and more.

While tricking end point, on-prem and siloed solutions results in infections and breaches, true SASE providers have the required visibility into security information and network traffic flows to identify new, never-before-researched threats. Cato Networks security researcher Tom Mizrahi has recently used this information to identify a new malware targeting enterprises. The research was performed based on three aspects that alone would seem benign. These three aspects were the **Domain, Payload and Communication Frequency**.

Top 5 Domains Exploit Attempts

The malware analyzed used a DGA to establish communications. Below are some of the domains observed.

4DD551A2A853C411E005795FA6CE640.online

4E4ECDE4BD35A25A212C4387CF55B9.online

A9D5F0F6FF1E417FD0F26A42405A6F5E.online

DEF651313D9BBF292A6C6484E3F076CF.online

A quick analysis of the domains, which does rely on any previously known threat intelligence, resulted in identification of a consistent pattern:

- All the domains consisted of 32 characters
- The domain changes every 2 weeks (with minor deviations)
- All the domains were a HEX string
- All the domains had the same TLD (.online)

Additional data points that may further enhance detection

- All the domains were registered at the same registrar
- All the domains had low reputation (not a well know, frequently accessed domain)
- All the domains were recently registered

Communication Frequency

Researchers and automated tools often attempt to identify a malware communication to its C&C servers. However, what happens if this communication has long intervals? Malware and botnets will try to use a “low and slow” approach in order to evade security controls detection. In our case the malware communicated with its C&C servers every two weeks, with slight deviations in network flow numbers.

11 DEF651313D9BBF292A6C6484E3F076CF.online

2021-01-31

10 4DD551A2A853C411E005795FA6CE640.online

2021-02-10

10 4E4ECDE4BD35A25A212C4387CF55B9.online

2021-02-24

10 A9D5F0F6FF1E417FD0F26A42405A6F5E.online

2021-03-10

Payload

The process of creating a malware signature involves finding network characteristics or behaviors that can be used to uniquely identify the malware in the future. Today’s malware, on the other hand, can be polymorphic and easily change characteristics without changing its behaviors and core capabilities.

In our case, legacy security systems would sign the URI parameters to attempt and identify it. This means that you would ultimately need to create a signature for each and every variant as parameters in the payload can (and will be) changed by the malware operators.

```
/sta.php?
g=148EC3420C03BD80E5D845BB09264CE62FE5FACF1076A746FF&o=6&b=&v=3.0&l=pub1all&i=all&s=EE429A851A25A1B507E57D34FA88CB24
```

In the URI above, which is a malware beaconing communication to the C&C, the ‘g=, o=, b=, v= , l=, l=, s=’ parameters could change with every new variant. Instead, by looking at the URI as a whole and comparing it to other beaconing instances to similar domain structures (as mentioned in the Domains paragraph above), and combining it with an analysis of the communication frequency we can identify this threat.

Domain	URI
A9D5F0F6FF1E417FD0F26A42405A6F5E.online	/sta.php?g=[redacted]&o=6&b=&v=3.0&l=pub1all&i=all&s=[redacted]
DEF651313D9BBF292A6C6484E3F076CF.online	/sta.php?g=[redacted]&o=6&b=&v=3.0&l=pub1all&i=all&s=[redacted]
4DD551A2A853C411E005795FA63CE640.online	/sta.php?g=[redacted]&o=6&b=&v=3.0&l=pub1all&i=all&s=[redacted]
4E4ECDE4BD35A25A212C438F7CFE55B9.online	/sta.php?g=[redacted]&o=6&b=&v=3.0&l=pub1all&i=all&s=[redacted]

By corelating these data points, Tom identified a new malware that would normally have snuck under a legacy security control’s radar.

Conclusion

This example and others that we'll be analyzing in the upcoming reports underscores how network-based threat hunting is a holistic approach to threat detection. As seen above, each technique by itself may not be sufficient to accurately identify threats, in fact, it may generate many false positives. However, by analyzing network behavior rather than only using a known static signature that requires previous knowledge and research, threat hunters can easily identify unclassified, previously undetected threats.

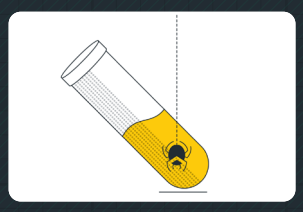
Section 3

In other news...

Critical attacks against critical systems

Researchers discovered credentials for the Oldsmar water treatment facility in the massive compilation of data from breaches posted just days before the attack.

Read more in our blog:



Threat actors are testing the waters with (not so) new attacks against ICS systems

FL reported a breach of their water supply system resulting in a water poisoning attempt that was luckily detected and mitigated.

Malicious browser extensions are on the rise

A company that rents out access to more than 10 million Web browsers so that clients can hide their true Internet addresses has built its network by paying browser extension makers to quietly include its code in their creations.

More covered here:

Researchers Discover Two Dozen Malicious Chrome Extensions

Researchers at Cato Networks have discovered two dozen malicious Google Chrome browser extensions and 40 associated malicious domains that are being used to introduce adware on victim systems, steal credentials, or quietly redirect victims to malware distribution sites.

First it was Jack Daniels, now ransomware attacks are targeting Blue Moon

Molson Coors' March 11 US Securities and Exchange Commission (SEC) filing disclosed that it suffered a "system outage" originating from a "cybersecurity incident".

Another supply chain threat - PHP

The PHP project on Sunday announced that attackers were able to gain access to its main Git server, uploading two malicious commits, including a backdoor. They were discovered before they went into production.