Weekly Summary Activity Report – June 5th, 2020

The weekly summary cybersecurity news report is a snapshot of cybersecurity news in Canada and across the globe. The report highlights topical cybersecurity news and analysis of network scanning activity as observed from CCTX SOC sensors over the reporting period, (Wednesday to Wednesday).

Noteworthy Security News

Canadian

June 2, **Canadian hospitals 'overwhelmed' by cyberattacks fuelled by booming black market**

CBC News published a report that Canadian hospitals are under siege from unrelenting cyber attacks. According to industry experts, a growing list of healthcare institutions have fallen victim to data breaches over the last year, exposing sensitive patient information. Cybersecurity professionals believe that health data is more valuable than credit card data since it includes health and date of birth, personal information that does not change over time and can be used to steal identities... Read more at cbc.ca

June 2, **Fewer Canadians willing to disclose personal information**

Insurance Business Canada published details from a report released by the Canadian Internet Registration Authority (CIRA). The report revealed that fewer Canadians are willing to share their personal information in exchange for better content and services online. About 52% of Canadians surveyed understand the need for privacy and are sharing less of their personal information with online platforms and service providers. In addition, 83% of Canadians surveyed believe that personal information used by the Government of Canada should be stored and transmitted only within Canada... Read more at insurancebusinessmag.com

June 1, **Privacy watchdog doubts current law completely protects Canadians for COVID-19 apps**

IT World Canada published a report that Canada's federal privacy commissioner, Daniel Therrien, is not confident that current privacy laws will protect the rights of Canadians if the provincial governments approve the use of COVID-19 contact tracing apps. According to the commissioner, he would prefer that PIPEDA (The Personal Information Protection and Electronic Documents Act) is updated to give Canadians the right to privacy. Specifically modifying the law to cover for public-private transfers of personal data... Read more at itworldcanada.com

Global

June 2, **Octopus scanner sinks tentacles into GitHub repositories**

Threat Post released an article regarding a new malware called the Octopus scanner. The malware was used to target Apache NetBeans Java Integrated Development Environments (IDE) on at least 26 GitHub source-code repositories. Once a repository containing the malware is downloaded, it scans for a new NetBeans build process and then installs a remote access trojan (RAT) malware. Read more at threatpost.com

June 1, **Coronavirus campaigns lead to surge in malware threats, Labs report finds**

Malwarebytes published their analysis of the cyber threat landscape for the first three months of 2020 in a report titled “Cybercrime tactics and techniques: Attack on home base”. The report shows that adversaries are using old malware alongside coronavirus themed phishing campaigns to target users. Older malware families such as NetWiredRC, AveMaria, DanaBot increased their activities between February and March 2020. Phishing campaigns still appear to be the most popular type of attack vector. Read more at malwarebytes.com

May 28, **NSA warns Russia's 'Sandworm' group is targeting email servers**

Dark Reading published an article with details of a threat advisory issued by the United States’ National Security Agency (NSA) regarding cyber attacks linked to the Russian-state threat actor group, ‘Sandworm’. The threat group had been exploiting vulnerable Exim mail transfer agent (MTA) email servers since late 2019, using exploits for a patched remote code vulnerability (CVE-2019-10149), to gain access to corporate networks. The hackers are sending maliciously crafted emails to vulnerable Exim mail servers. When an unpatched server receives the malicious email, the server will download and execute malicious shell scripts from an attacker-controlled domain. Read more at darkreading.com

May 28, **Cyber-criminals impersonating Google to target remote workers**

Info Security Magazine released an article about a new phishing campaign impersonating Google and targeting remote workers. According to an analysis conducted by Barracuda Networks, remote workers have been hit by over 65,000 cyber attacks leveraging the Google brand. About 65% of nearly 100,000 malicious form-based cyberattacks came from Google’s file sharing and storage websites. Read more at Infosecurity-magazine.com

May 27, **OpenSSH to deprecate SHA-1 logins due to security risk**

ZDNet reported on OpenSSH’s announcement that it will no longer be supporting the SHA-1 authentication scheme due to security concerns with the SHA-1 hashing algorithm. This decision was due to recent research reports showing that the cost of creating a SHA-1 collision attack is now as low as $50,000. Threat actors such as nation-state or cybercriminal groups can easily afford this cost and may already possess capabilities to launch attacks against systems secured using the SHA-1 algorithm. Read more at zdnet.com

Top Network Probe Activity Report

Every week, millions of packets of potentially malicious traffic are detected by CCTX SOC sensors. This week's analysis of the traffic is provided below. Figure 1 shows the top ten destination ports with the highest number of network alarms observed on CCTX sensors for the last week.

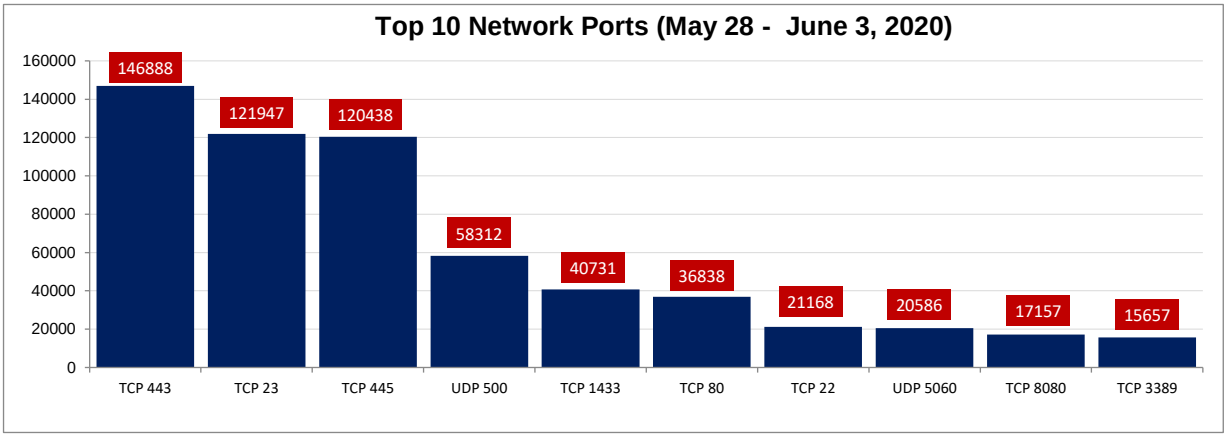

Figure 1: Top 10 Destination Ports (May 28 – June 3, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 443	1	-	-12.3% ↓
2	TCP 23	2	-	-16.2% ↓
3	TCP 445	3	-	2.8% ↑
4	UDP 500	4	-	-0.3% ↓
5	TCP 1433	5	-	-9.9% ↓
6	TCP 80	6	-	-6.0% ↓
7	TCP 22	7	-	-15.4% ↓
8	UDP 5060	8	-	-4.3% ↓
9	TCP 8080	9	-	-8.7% ↓
10	TCP 3389	10	-	-9.8% ↓

This week's data from our top ten most targeted ports show no significant upward trends. We observed a decline in scan volumes across all the major ports except traffic to TCP port 445, which increased marginally by 2.8%. As part of our deeper dive this week, we investigate probe scans targeting TCP port 8545 (a port associated with Ethereum cryptocurrency applications). Recently, scan probes targeting this port (TCP/8545) has been on the rise and is now ranked 11th, just outside our top ten list.

TCP 8545

TCP port 8545 is the default port associated with the Application Programming Interface (API) service for Ethereum clients. Ethereum is one of the most popular cryptocurrency platforms available today outside Bitcoin's platform. According to Ethereum's recommended deployment architecture, internet access to its API should be deactivated by default. However, some Ethereum clients requiring additional operations on their wallets have internet access to the API enabled for third-party applications. Enabling internet access may expose the miner's information and wallet details if not appropriately configured with access restrictions [1]. Hence, threat actors, using malware bots, are regularly scanning the internet to identify mis-configured APIs.

Bots are constantly scanning for open TCP port 8545 (Ethereum nodes) and will attempt to exploit them. On May 27, a user post on reddit confirmed his Ethereum account was hacked when a hacker accessed his private key [2].

As shown in Figure 2, our sensors are seeing increased network scans targeting services hosted on TCP port 8545. We observed a sharp increase in scanning targeting TCP port 8545 between 31st May and 1st June. This may indicate that some threat actors may be trying to identify internet-exposed cryptocurrency wallets. In April, the FBI issued a warning about possible increases in "cryptocurrency-related fraud schemes" [3]. Similarly, a report by CipherTrace estimated that about $1.4B in crypto funds were stolen in the first five months of 2020 [4]. We assess that cryptocurrency related attacks are highly likely to rise as its use and wider acceptance increases. Below are the top hits from our data:

- 51.161.12.231 (OVH, Canada),
- 67.227.152.142 (Liquid Web, US),
- 165.22.39.92 (Digital Ocean, US),
- 178.62.47.158 (Digital Ocean, UK),
- 139.59.211.245 (Digital Ocean, Germany)

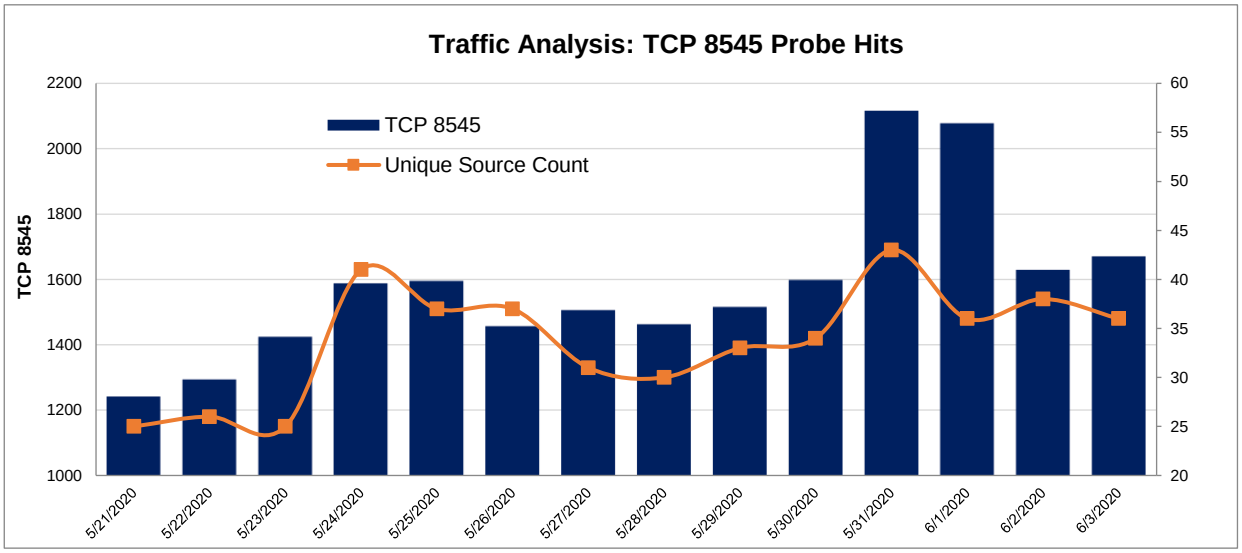

Figure 2: TCP Port 8545 Analysis (May 28 – June 3, 2020)

References

[1] Blockchain Blunders: Exposing Digital Pickpockets in the Ethereum Ecosystem - https://blog.rapid7.com/2018/07/09/blockchain-blunders-exposing-digital-pickpockets-in-the-ethereum-ecosystem/

[2] Reddit User's Ethereum Wallet Compromised and Ether Coins Stolen - https://www.reddit.com/r/CryptoCurrency/comments/gr73wu/i_lost_1200_in_100_seconds/

[3] Crypto Holders Being Targeted by COVID-19 Scammers — FBI Warning - https://cointelegraph.com/news/crypto-holders-being-targeted-by-covid-19-scammers-fbi-warning

[4] $1.4B in Crypto Stolen in First Five Months of 2020 - https://cointelegraph.com/news/14b-in-crypto-stolen-in-first-five-months-of-2020-says-ciphertrace