# Weekly Summary Activity Report – May 8th, 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 an analysis of network scanning activity as observed from CCTX SOC sensors over the reporting period, (Wednesday to Wednesday).

## Noteworthy Security News

### Canadian

May 4, **York University suffers cyber attack**

CBC published a story about the recent cyberattack which occurred at York University. According to the University's security officials, the attack began Friday evening and corrupted data on multiple servers and workstations. The University released a statement revealing that the University's internet connection was disconnected, and several online services shut down in order to mitigate the impact of the attack. The University's security experts advised that all passwords must be reset due to the attack. Read more at cbc.ca

May 1, **Coronavirus: Cyber-spies seek coronavirus vaccine secrets**

BBC news published an article about a warning issued by the US government to medical research organizations regarding the potential for increase in targeted cyber attacks. As scientists, researchers, companies and governments are simultaneously working to develop a vaccine for the coronavirus, there is an increased likelihood of foreign intelligence services targeting these research activities. According to a similar warning issued by Canada's Centre for Cyber Security, sophisticated threat actors may attempt to steal intellectual documents related to the research and development of COVID-19. Read more at bbc.com

May 1, **Canadians have lost more than $1.2 million to COVID-19 scams**

CBC published an article with details of scammers exploiting the Coronavirus crisis to lure as many Canadians as possible. According to the Canadian Anti-Fraud Centre, there had been a total of 739 reported attempts to defraud Canadians with Coronavirus themed scams since March 6th. The Canadian Centre for Cyber Security worked to shut down over 2,000 websites that were trying to scam Canadians. Most of these scams mimic websites belonging to agencies actively involved in the Canadian government's response plan to the pandemic. Read more at cbc.ca

April 30, **NTPC confirms 'cyber attack' from unknown source on Thursday, RCMP investigating**

CBC published an article about the Northwest Territories Power Corporation's (NTPC) website which was impacted by a ransomware attack. According to the power corporation, its email system has been temporarily shut down until they can confirm that it has not been compromised. The cybercriminals left a note outlining that the power corporation's files had been encrypted by the Netwalker ransomware and they will not be able to recover their files

unless they contact the hackers. The RCMP are still investigating the cyber breach as the hackers remain unknown. Read more at cbc.ca

## Global

May 6, **Hackers updating EVILNUM malware to target the global financial sector**

Cyberscoop published a story about how cybercriminals are using new techniques to target the financial services sector. Hackers are constantly updating their malware tools to avoid being detected by antivirus applications. The cybercriminals are impersonating CEOs and corporate executives to lure victims. They are also updating various versions of the EVILNUM malware with features to upload and download files, harvest tracking cookies, and execute arbitrary commands without being detected. The malware changes persistence configurations based on the antivirus software running on a victim host. Read more at cyberscoop.com

May 6, **Samsung patches 0-click vulnerability impacting all smartphones sold since 2014**

ZDNet published an article about a critical vulnerability (CVE-2020-8899) that affects all smartphones sold since 2014. The vulnerability resides within how the Android OS handles the custom Qmage image format (.qmg). The flaw was discovered by Mateusz Jurczyk, a security researcher within Google's Project Zero bug-hunting team. According to the Mateusz, an attack exploiting this vulnerability requires around 50 and 300 MMS messages to probe and bypass Address Space Layout Randomization (ASLR), which takes approximately 100 minutes. Read more on zdnet.com

May 6, **Nearly a million WordPress sites targeted in extensive attacks**

HelpNet Security published an article about a threat actor that is actively infecting WordPress based websites with a backdoor to redirect visitors to a malvertising URL. According to Wordfence cybersecurity experts, this threat actor is targeting old vulnerabilities and has compromised over a million individual websites since May 3rd. The cybercriminal actor injects malicious JavaScript code or installs a malicious PHP backdoor. Read more at helpnetsecurity.com

May 4, **New malware jumps air-gapped devices by turning power-supplies into speakers**

The Hacker News published a report detailing a highly sophisticated malware that could be utilized to secretly steal sensitive information from air-gapped and audio-gapped systems that was discovered by a security researcher at Ben Gurion University in Israel. This malware is known as '*POWER-SUPPLaY*' and it leverages electromagnetic, acoustic, thermal, and optical covert channels with power cables to exfiltrate data from a non-networked computer. Once the malicious code is injected, it manipulates the switching frequency of the internal power supply controlling the sound waveforms generated from its capacitors and transformers. Read more at thehackernews.com

April 30, **New Android malware steals banking passwords, private data and keystrokes**

The Hacker News published a report detailing a new mobile banking malware that has been observed by Cybereason security researchers in March 2020. The malware is called "EventBot"

which was first identified on rogue APK stores disguised as a legitimate application. EventBot is a banking trojan that can control numerous banking applications including cryptocurrency digital wallets. The malware can parse SMS messages which makes it possible for the attacker to steal two-factor authentication tokens. Read more at thehackernews.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 events observed on CCTX sensors for the last week.

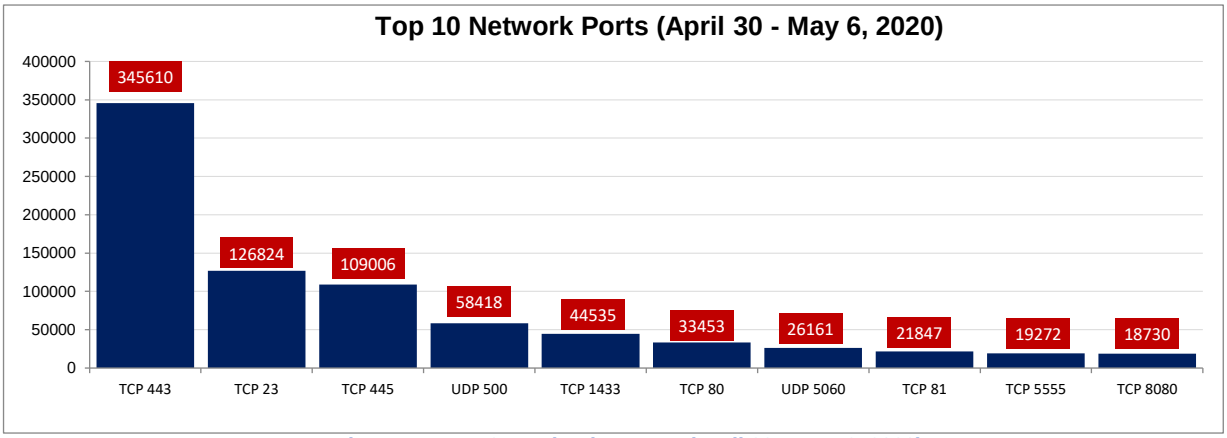


Figure 1: Top 10 Destination Ports (April 30 – May 6, 2020)

***Table 1: Top 10 Network Probe Activity Report***

| *Rank* | Port Number | Previous Week Ranking | Ranking Change (+/-) | % Probe Volume Change (+/-) |
|---|---|---|---|---|
| *1* | TCP 443 | 1 | - | 63.2% |
| *2* | TCP 23 | 2 | - | -6.3% |
| *3* | TCP 445 | 3 | - | 45.9% |
| *4* | UDP 500 | 5 | +1 | 0.1% |
| *5* | TCP 1433 | 4 | -1 | -25.5% |
| *6* | TCP 80 | 6 | - | -2.5% |
| *7* | UDP 5060 | 7 | - | -5.8% |
| *8* | TCP 81 | 10 | +2 | 7.1% |
| *9* | TCP 5555 | 8 | -1 | -17.5% |
| *10* | TCP 8080 | 9 | -1 | -8.5% |

This week's analysis of the top 10 network probe ports is shown in Table 1. We continue to see increases in network scans targeting port TCP/445 which is in continuation of the scanning

trends observed last week. Threat actors continue to target the SMBGhost vulnerability. From data collected this week, we observed about 45% increase in network scans targeting TCP/445. Additionally, we saw increases in traffic targeting TCP/443 and TCP/81. Probe traffic targeting TCP/443 rose by about 63% which is an indication that threat actors are likely targeting vulnerabilities present in exposed web services. This week we take a deeper look into scans targeting port TCP/81.

## TCP 81

According to telemetry retrieved from CCTX sensors, traffic targeting port TCP/81 have been steadily rising over the last couple weeks. While traffic targeting some common ports have been on the decline, we have seen an increase in traffic targeting TCP/81. Malware botnets are known to target vulnerable web services running on port TCP/81. Moobot and Mirai botnets have a history of targeting vulnerable HiSilicon DVR devices or IP cameras. Some scans specifically target vulnerable GoAhead servers [1], which are embedded web servers used on many versions of IoT devices. As shown in Figure 2, we see attackers consistently scanning for open services in TCP/81 over the last two weeks.

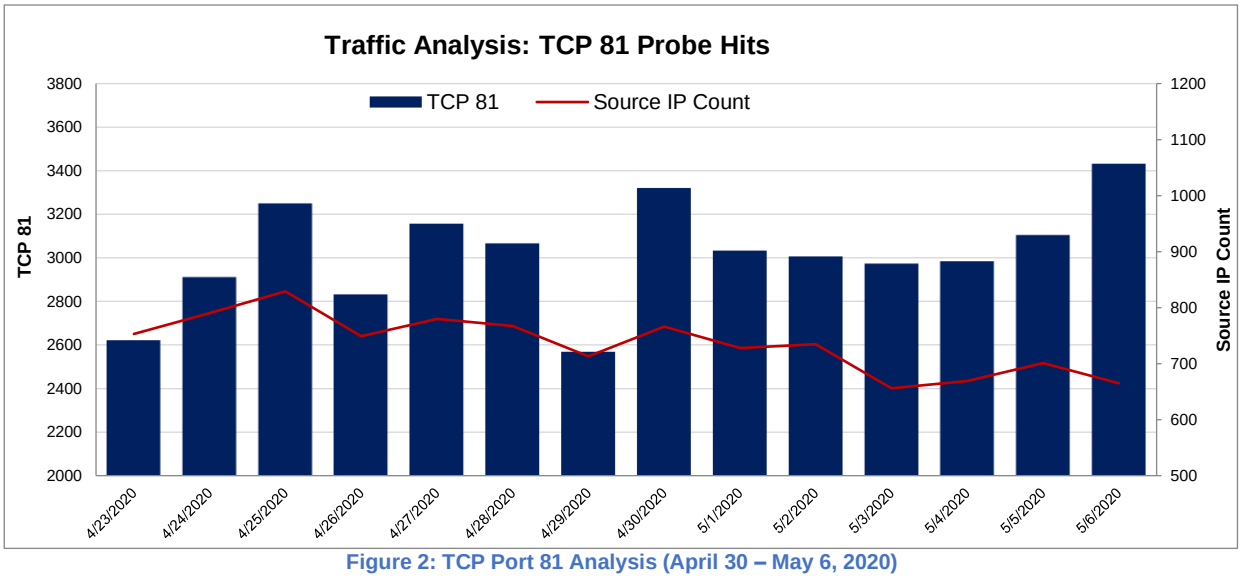


Figure 2: TCP Port 81 Analysis (April 30 – May 6, 2020)

Top talker analysis shows most of the scans we detected originated from the following source IP presented. Aruba Cloud's infrastructure in Italy and United Kingdom were associated with most of the scans observed. Due to limited data, we were not able to ascertain specific vulnerabilities being targeted.

- 195.231.1[.]46 (Italy/Aruba Cloud): Source IP previously linked to Mirai or Hajime botnets and associated with malicious activity. The IP address is listed on the CBL Abuse blacklist.
- 185.172.110[.]230 (Netherlands/Server Hosting Pty): IP address previously linked to IoT botnets and known for malicious activity. The IP address is listed on the CBL Abuse and SpamHaus blacklists.
- 185.43.209[.]214 (United Kingdom/Aruba Cloud): IP address has a poor reputation and known for spam emails. The IP address is listed on the CBL Abuse list.
- 37.49.226[.]4 (Estonia/EstroWeb): No previous records associating IP with IoT botnets. The IP address is listed on the CBL Abuse blacklist.
- 51.15.85[.]14 (Netherlands/ScaleWay): No previous records associating IP with malicious activity. Not on any known public blacklist.
- 14.184.109.95 (Vietnam/Vietnam Posts and Telecoms Network): IP address previously linked to IoT botnets and known for malicious activity. The IP address is listed on the CBL Abuse and SpamHaus blacklists.
- 89.38.145.100 (United Kingdom/Aruba Cloud): IP address previously linked to IoT botnets and known for malicious activity. The IP address is listed on the CBL Abuse blacklist.
- 195.231.11.179 (Italy/ Aruba Cloud): No previous record associating IP with malicious activity. Not on any known public blacklist.

## References

[1] Two high-risk vulnerabilities in GoAhead web server: https://nsfocusglobal.com/advisory-two-high-risk-vulnerabilities-goahead-web-server/