Canadian Cyber Threat Exchange
Informing Canadian Business

Échange canadien de menaces cybernétiques
Informer les entreprises canadiennes

Weekly Summary Activity Report – April 3, 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 network probe activity as observed from the CCTX SOC sensors over the reporting period, (Wednesday to Wednesday).

Noteworthy Security News

Canadian

April 1, Cyberscoop published a story about the NERC (North American Electric Reliability Corporation) releasing its results from a cyber drill conducted by North American energy utilities in November 2019. The exercise involved electric utilities across North America. It mimicked the disruptive malware incident that affected Ukraine in 2016. The report recommended utility corporations setup a strategic supply of critical electric equipment and that organizations should take concrete actions toward improving the resiliency of their electrical grid. Read more on this cyberscoop.com

30 March, CBC reported that cybercriminals were exploiting the Coronavirus crisis to target Canadians. Hackers are doubling their efforts with several phishing campaigns exploiting the situation around the COVID-19 global pandemic. Fraudsters purporting to be processing Employment Assistance (EI) claims are targeting Canadians that may have lost their jobs due to the pandemic and asking them to provide their personal information. Other phishing themes being used are fake email messages appearing to be from the Public Health Agency of Canada, Shoppers Drug Mart or the World Health Organization. Read more at cbc.ca

27 March, CTV News published a story on Hydro-Quebec's warning to residents asking them to watch out for COVID-19 related scam messages. Cybercriminals are using bogus reimbursement messages to target potential victims. The actors were using SMS messages with hyperlinks which redirect to websites asking for credit card numbers or confidential personal information. Read more at ctvnews.ca

27 March, IT World Canada published a report on how the coronavirus pandemic is forcing several hospitals and healthcare facilities in Ontario to establish new virtual healthcare solutions, forcing many to implement new technologies and infrastructure with wider cybersecurity implications. According to security experts, the strict deadlines on some of these projects, pace of deployments and lack of in-depth security review may expose these services to attackers. Read more at ITWorldcanada.com

25 March, McGill University published a report regarding a CRA phishing campaign that is rapidly spreading among employees and students within the university. The phishing email targets Canadian taxpayers with text informing recipients that their CRA (Canada Revenue Self Assessment) notification is now available. The email contains a hyperlink which redirects to a malicious website to collect visitor's personal information. Read more at mcgill.ca

Global

April 1, Microsoft issued a warning that advanced threat actors behind the REvil ransomware are likely behind recent VPN attacks targeting the healthcare sector. According to Microsoft's threat intelligence, these threat actors are targeting vulnerable network devices like gateways and virtual private network (VPN) appliances. Microsoft identified several hospitals with exposed vulnerable network devices and strongly recommends that enterprises implement available patches on their VPN infrastructure. Read more at microsoft.com

31 March, SCMagazine published an article on Marriott's recent data breach which was discovered in late February 2020 and estimated to have impacted 5.2 million guests. The breach's source was an application used by customers to order various services. The data compromised includes guest names, mailing addresses, phone numbers, email addresses, employers and date of birth information. Marriott has established a self-service portal for customers to check if they were affected. Read more at scmagazine.com

30 March, The United States Federal Bureau of Investigation (FBI) issued a warning regarding hijack attacks targeting zoom video conference users. Bleepingcomputer published more details about the hijacking attacks called zoom-bombing. Some users are joining ongoing video conferences for the sole purpose of causing disruptions and sharing hate messages. The FBI received several of such reports and recommended zoom conference hosts implement specific measures to safeguard their meetings. Read more at bleepingcomputer.com

30 March, ZDNet published an article regarding a recent fraudulent email phishing campaign that is spreading the Zeus sphinx malware, exploiting the confusion around the coronavirus crisis. Zeus sphinx is a banking Trojan and was first seen in August 2015. The malware uses a self-signed certificate to evade anti-virus detection. Once a system is infected, the malware dynamically writes itself to files and folders and creates registry keys. According to IBM X-Force, the malware was observed being delivered through phishing campaigns using COVID-19 themed relief payments. Read more at zdnet.com

27 March, InfoSecurity published a story regarding a recent analysis by Trustwave security analysts related to a highly targeted attack on a US company. According to Trustwave, one of its customers received a mail containing an unsolicited letter which was disguised as a Best Buy thank you message which included a $50 gift card and a USB device. The letter claimed that the USB contains a list of items the gift card could be spent on. The USB was determined as malicious as the firmware had been rewritten to automatically execute malicious code once connected to a device. Read more at infosecurity-magazine.com

25 March, Infosecurity published an article regarding the increase in threat campaigns by the Chinese APT group exploiting Citrix and Zoho endpoints. According to FireEye security officials, APT41 cybercriminal gang targeted 75 customers between January 20 and March 11 attacking their Citrix NetScaler/ADC, Cisco routers, and Zoho ManageEngine Desktop Central products. The attacked victims were across the globe, and across various industries, including manufacturing, healthcare, telecommunication and finance. The criminal group exploited Cisco

RV320 router vulnerabilities CVE-2019-1653 and CVE-2019-1652 as well as Zoho vulnerability (CVE-2020-10189). Read more at infosecurity-magazine.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 these events as observed on our sensors is provided below. Figure 1 shows the destination ports with the highest number of network events observed on CCTX sensors for the last week.

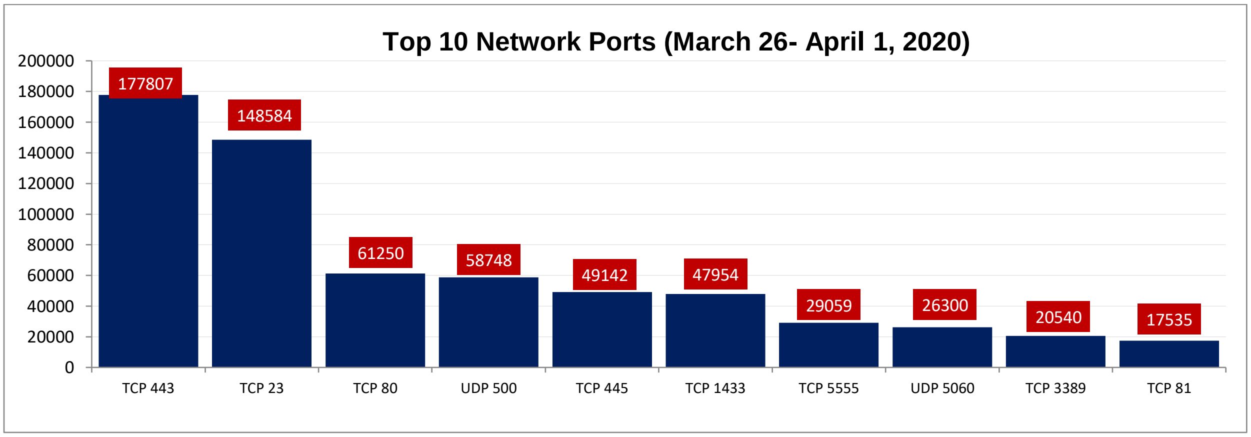

Figure 1: Top 10 Destination Ports (March 26 - April 1, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 443	1	-	6.3%
2	TCP 23	2	-	5.5%
3	TCP 80	3	-	-10.9%
4	UDP 500	4	-	0.4%
5	TCP 445	5	-	-5.2%
6	TCP 1433	6	-	-2.5%
7	TCP 5555	8	+1	29.7%
8	UDP 5060	7	-1	15.9%
9	TCP 3389	9	-	-1.2%
10	TCP 81	11	+1	-10.6%

Reviewing the details as shown in Table 1, we observed significant increases in probe scanning traffic targeting ports TCP/5555 and UDP/5060 which recorded a traffic increase of 29.7% and

15.9% respectively. This may indicate an increased activity by the Mirai botnet or its variant in the past week. We will continue to monitor this associated activity.

TCP 5555

We continue to observe high levels of attack traffic targeting TCP Port 5555 as shown in Table 1 and Figure 1. TCP Port 5555 is used by the ADB daemon (the Android Debug Bridge, for administrating local Android devices). The Android OS is used on numerous IoT devices including TVs and Internet enabled home devices. This port is not enabled by default on Android OS but it was reported that some device manufacturers may have inadvertently exposed this port and shipped devices with the ADB bridge enabled and unauthenticated. [1] On our sensors we observed an increase in scanning traffic probing for internet-accessible services running on TCP Port 5555. IoT botnet operators are known to target and exploit vulnerable Android devices. In August 2019, Ares IoT botnet was reported targeting Android set-top boxes manufactured by HiSilicon, Cubetek, and QezyMedia.[2]. Based on data telemetry available from our sensors the following were source IPs linked to this scanning activity: 183.230.196.157 (China Mobile Guangdong / CHINA), 71.41.35.108 (RoadRunner Email Service / US), 50.196.140.189 (Comcast / US), 195.133.223.12 (Horizon Scope Mobile Telecom / IRAQ), 99.231.24.19 (Rogers Cable / CANADA) and 172.96.170.46 (Fuse Telecom LLC / Puerto Rico)

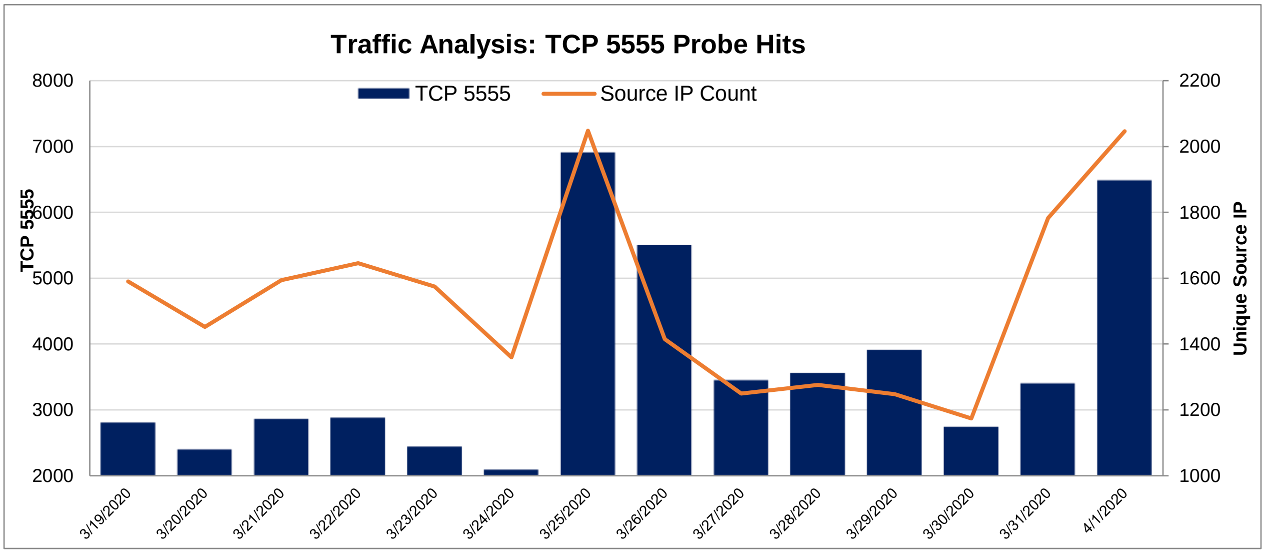

Figure 1: TCP Port 5555 Analysis (March 19 – April 1, 2020)

References

[1] Root Bridge: How Thousands of Internet Connected Android Devices Now have No security – https://doublepulsar.com/root-bridge-how-thousands-of-internet-connected-android-devices-now-have-no-security-and-are-b46a68cb0f20
[2] A new IOT Botnet is Infecting Android-based Set-top Boxes - https://www.zdnet.com/article/a-new-iot-botnet-is-infecting-android-based-set-top-boxes/