Weekly Summary Activity Report – April 17, 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

April 14, **Ransomware attacks lock two Manitoba law firms out of computer systems**

CBC published a story about a ransomware attack which affected two Manitoba law firms, preventing access to their computer systems, data and backups. The affected law firms were not named, but it is believed the attacks may have started from employees clicking on a link within a malicious email. According to the Law Society of Manitoba, the Maze ransomware variant was deployed in both attacks. The Maze cybercriminal group is known for huge ransoms and has been linked to several similar ransomware attacks within the last six months. Read more at cbc.ca

April 14, **Federal government breached privacy of Canadians on virus-stricken cruise ship**

CTV news published an article about a privacy breach that affected over 240 Canadian citizens aboard the MZ Zaandam cruise ship. The Canadian federal government had inadvertently shared the passenger manifest with every Canadian aboard the ship, including their names, dates of birth, home addresses, phone numbers and passport numbers in a notification email sent. Affected individuals have been informed about the privacy breach. Read more at ctvnews.ca

April 14, **Malicious hackers target government and medical organizations with COVID-19 phishing campaigns**

Palo Alto networks published a report detailing various COVID-19 phishing campaigns that targeted some Canadian institutions involved in the coronavirus pandemic response. According to Palo Alto's analysis, they observed a ransomware campaign targeting various individuals within Canadian health institutions and an info stealer infection campaign (AgentTesla) which targeted Canadian universities conducting research related to the Coronavirus outbreak. Read more at paloaltonetworks.com

Global

April 15, **Microsoft fixes three zero-day vulnerabilities in April**

Info Security published an article on Microsoft's security updates for April 2020 with details of 113 vulnerabilities disclosed affecting Microsoft products including three zero-day flaws already exploited in the wild. Two of the zero-day vulnerabilities, CVE-2020-1020 and CVE-2020-0938,

are remote code execution vulnerabilities within Microsoft Windows Adobe Type Manager Library. The third zero-day vulnerability, CVE-2020-1027, is a memory corruption flaw within internet explorer as a result of improper handling of objects within scripting engine. Read more at infosecurity-magazine.com

April 15, **COVID-19 medical supplies targeted by BEC scams**

ThreatPost published an article about the recent increase in email scams targeting government agencies responsible for COVID-19 supplies. The shortage of personal protective equipment (PPEs) and other medical supplies have led to several government agencies buying ventilators from threat actors masquerading as suppliers. The FBI issued a warning that threat actors are taking advantage of the Coronavirus crisis to spread new business email compromise (BEC) scams targeting the organizations. The FBI mentioned that they were aware of multiple incidents in which the state government agencies were tricked to sending advance funds to fraudulent brokers for things like N95 masks. Read more at threatpost.com

April 15, **US issues North Korean cyber-threat warning**

Info Security published an article about an alert regarding possible North Korean cyber threat activities targeting the international financial system. The warning, issued by the United States Department of Homeland and Security, warned American citizens to be vigilant about crypto-jacking extortion attacks, cyber-enabled financial theft as well as money laundering scams. The warning was not restricted to possible attacks against US assets alone but also international institutions. Read more at infosecurity-magazine.com

April 14, **Thousands of Zoom accounts passwords and email addresses are for sale on the dark web**

NBC news published an article about over 530,000 Zoom accounts, passwords and email addresses offered for sale on the dark web. Zoom refused to share any specific details about how the information could have been leaked. According to a Zoom spokesperson, the organization is investigating and locking down accounts found to be compromised. They are asking users to change their passwords. Read more at nbcnews.com

April 14, **Boeing, Lockheed Martin, SpaceX docs leaked by a ransomware gang**

Secure World published an article about the DoppelPaymer ransomware attack that targeted Visser, a manufacturing and design contractor for many aerospace and defence companies which include Boeing, Lockheed Martin and SpaceX. Visser refused to pay the ransom demanded and the cybercriminals publicly released sensitive documents belonging to Visser's clients. The documents released included design details of Lockheed-Martin's military equipment such as an anti-mortar defence system. Read more at secureworldexpo.com

April 12, **New Wiper Malware impersonates a security researcher as prank**

Bleeping computer published a report about a ransomware variant impersonating security researchers and falsely blaming them for infections. Once a device is infected, the system will display a message stating that the victim was infected by Vitali Kremez and MalwareHunterTeam who are both known security researchers. The ransomware notice includes their email and phone numbers, asking the victim to contact them. It looks like the malware developer is trying to tarnish the image of the researchers in a destructive campaign. Read more at bleepingcomputer.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 as observed on our sensors 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.

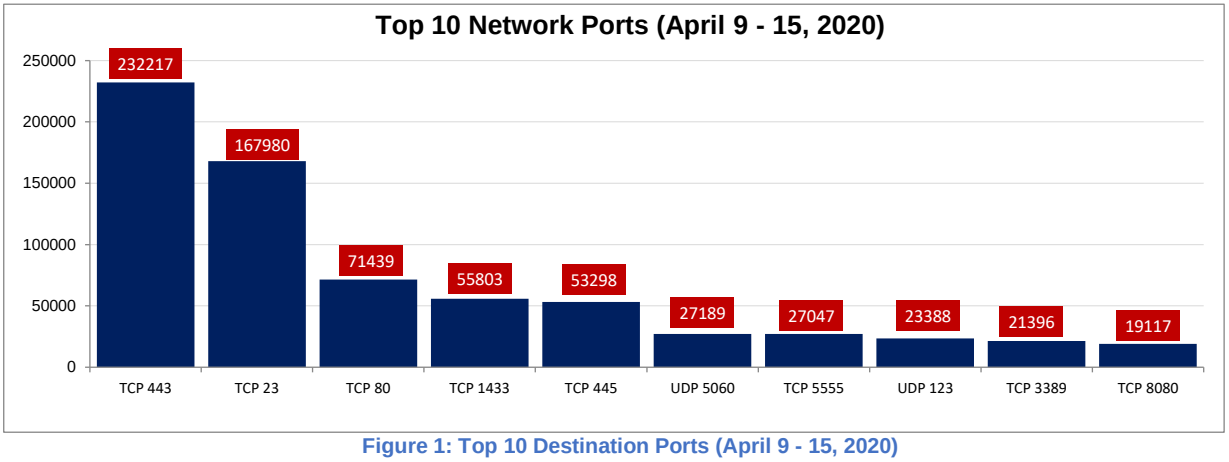

Figure 1: Top 10 Destination Ports (April 9 - 15, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 443	1	-	-25.1%
2	TCP 23	2	-	28.2%
3	TCP 80	3	-	4.8%
4	TCP 1433	4	-	5.2%
5	TCP 445	5	-	3.2%
6	UDP 5060	7	+1	1.2%
7	TCP 5555	6	-1	-12.7%
8	UDP 123	12	4	41.7%
9	TCP 3389	9	-	-2.1%
10	TCP 8080	10	-	7.1%

This week, analysis of the network probe data as shown in Table 1 reveal slight increases in probe activity across several ports. We observed significant increases in traffic targeting UDP port 123 and TCP port 23, as well as a decline in traffic targeting TCP/443. Network probe traffic targeting port UDP/123 increased by 41.7% and traffic targeting TCP/23 increased by 28.2%. Our assessment of these activities suggest they may be part of larger set of attacks targeting vulnerable IoT devices to harness them form larger botnets. Attackers may be targeting recently disclosed vulnerabilities affecting the NTP protocol and launching brute force attacks via Telnet to identify vulnerable IoT devices.

UDP 123

UDP Port 123 is used widely as the default port for the Network Time Protocol (NTP) service on UNIX systems. In the past, attackers have targeted vulnerabilities present in the NTP service to launch Distributed Denial of Service (DDoS) amplification attacks, using spoofed “get monlist” requests to an NTP server to amplify responses to a client. Beginning April, we started observing increases in daily scans targeting UDP port 123. As shown in Figure 2, these daily increases continued and peaked on April 9th. Our assessment of these scans is they are likely related to recent reports of increases in DDoS attacks targeting several web services. On April 10th, Dutch authorities announced the arrest of a 19-year-old man and took down 15 DDoS-for-hire services as part of crackdown on DDoS booter services. [1] In March 2020, NTP foundation released an update to address three security issues in ntpd. One of the vulnerabilities addressed could lead to a Denial of Service (DoS) attack on an unauthenticated client. A system running affected versions of ntp that only has one unauthenticated time source could be attacked in a way that causes the victim’s next poll to be delayed [2]. An attacker can send specially crafted packets every second that would prevent the ntpd service on a client from sending any requests to a spoofed address. When the attack is sustained over a period may lead to system time out of sync or denying service to the NTP client. We assess these scans may be related with identifying vulnerable versions exposed on the internet. Most of the traffic we observed were from 185.216.140.87 (Netherlands), 46.88.240.4 (Germany), 80.82.64.110 (Netherlands) and 62.210.129.208 (France).

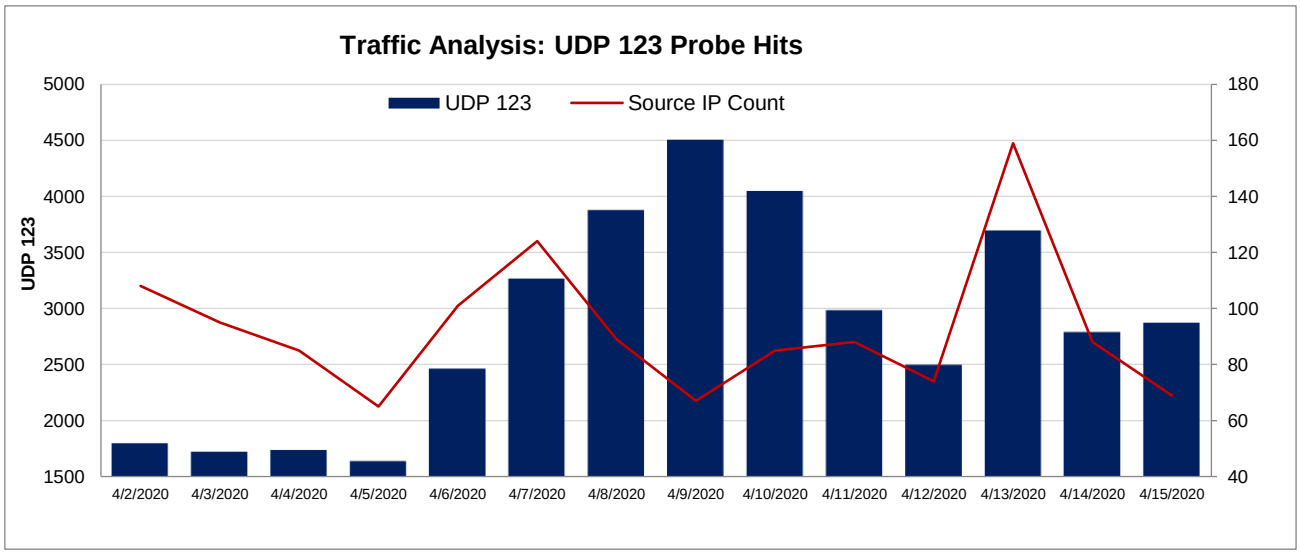

Figure 2: UDP Port 123 Analysis (April 9 – 15, 2020)

References

[1] Dutch Police Take Down 15 DDoS Services in a week - https://www.zdnet.com/article/dutch-police-take-down-15-ddos-services-in-a-week/

[2] NTP Security Advisory, March 2020 - http://support.ntp.org/bin/view/Main/SecurityNotice#March_2020_ntp_4_2_8p14_NTP_Rele