Weekly Summary Activity Report – May 15th, 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

May 12, **Investigation into "significant privacy breach" at Ontario care home**

Infosecurity Magazine published an article with details of an investigation being conducted by Ontario's privacy commissioner into a significant privacy breach at a long-term care home. According to Canada's long-term care minister, Merilee Fullerton, an investigation is being conducted into the unauthorized release of the confidential patient health information belonging to residents of the Orchard Villa retirement community in Pickering, Ontario. Read more infosecurity-magazine.com

May 11, **$37,000 transfer prompts scam warning from police**

CTV news published an article regarding an online fraud warning issued by the Norfolk County Ontario Provincial Police, as a result of an individual who was defrauded of $37,000. The victim transferred $37,000 to an unknown recipient believing he had been contacted by a friend via social media about a humanitarian grant from Texas. The police warning is asking Canadians to be vigilant and up to date with new techniques being used by online scammers. Read more at ctvnews.ca

May 8, **Coronavirus: Police in Okanagan issue CERB text scam warning**

Global news published a story about a recent SMS messaging scam campaign targeting the Canada Emergency Response Benefit (CERB). According to the RCMP, the text message is sent to a phone indicating that the recipient has received a CERB deposit. The message includes with a malicious link or an attachment. Once the recipient clicks on the link or attachment, a malware is either installed on the device, or they are redirected to a fake website which will harvest their credentials. Read more at globalnews.ca

May 8, **Canada hit by COVID-19 cheque fraud**

IT World Canada published an article about counterfeit COVID-19 CERB cheques being offered for sale on criminal forums. The cybercriminals are targeting the Canadian government's pandemic payment program by selling editable digital copies of cheques on dark web forums. According to an Israeli security firm, this cheque scam is simply an extension of other cheque fraud schemes available on the dark web. The Canadian Bankers Association confirmed that financial institutions regularly scan for these threats to identify these fraudulent cheques. Read more at itworldcanada.com

Global

May 13, **Ransomware attackers exfiltrate data from Magellan Health**

Healthcare Infosecurity published an article about how Magellan Health, a U.S. based healthcare company, became a victim of a ransomware attack which led to confidential patient data and employee information being stolen. The hackers gained access to corporate servers after a spear phishing email impersonating a client was accessed on the network. No information was provided on the ransomware variant behind the attack. However, a third-party forensics investigation confirmed that the threat actors exfiltrated data from the corporate network just a few days after the initial compromise. Read more at healthcareinfosecurity.com

May 13, **The U.S. government reveal Hidden Cobra APT's trove of espionage tools**

Threatpost published an article on a threat analysis report issued by the U.S. Department of Homeland Security and Federal Bureau of Investigation (FBI), exposing hacking tools used by a North Korean APT group, Hidden Cobra. According to US-CERT, the agencies published malware analysis reports for three malware families: COPPERHEDGE, TAINTEDSCRIBE and PEBBLEDASH which belong to a toolbox of Hidden Cobra. COPPERHEDGE is a remote access tool while TAINTEDSCRIBE and PEBBLEDASH are beaconing implants which use FakeTLS for session authentication. Read more at threatpost.com

May 12, **Astaroth malware hides command servers in YouTube channel descriptions**

ZDNet published a report about the Astaroth infostealer trojan and how it has evolved to one of the stealthiest malware strains today. The Ashtaroth infostealer trojan is capable of evading anti-analysis and anti-sandbox checks to prevent security experts from detecting and analyzing its operations. The malware has only targeted users in Brazil since it was discovered. The malware runs checks for anti-analysis and anti-sandbox before it operates to make sure it runs on a real computer. Read more at zdnet.com

May 11, **Sodinokibi ransomware uses MS API to encrypt open and locked files**

Security researchers with Intel471 Cyberintelligence announced the discovery of a new variant of the Sodinokibi ransomware (REvil) which can encrypt open or locked files. System processes lock files to prevent two or more processes modifying file content and this prevented ransomware from encrypting databases or mail servers. The threat actors now use Windows Restart Manager API to close processes or shut down Windows services that placed a lock on a file. Read more at securityaffairs.co

May 11, **Attackers pose as Zoom to steal Microsoft credentials**

Infosecurity magazine published an article about a recent phishing campaign where cybercriminals are impersonating the videoconferencing platform Zoom to lure victims and harvest Microsoft credentials. According security researchers, Zoom users are being targeted with bogus notification emails that contain malicious links. When a user clicks on the fake Zoom link, they are directed to a fake Microsoft login page with the name of the user's organization and Zoom on top of the sign in button. Read more at infosecurity-magazine.com

May 7, **Jump in vulnerable RDP ports is leaving networks open to hacking and cyberattacks**

ZDNet published a report detailing the rapid rise in insecure internet facing RDP ports that cybercriminals are attempting to exploit. As the coronavirus global pandemic forced employees to work from home to promote social distancing and limit the spread of the virus. Cyberattacks have rapidly increased targeting Microsoft Remote Desktop Protocol (RDP), where RDP is an essential component that enables remote work. Nevertheless, RDP ports are often left exposed to the internet, making them a valuable target for hackers. If successfully exploited, an attacker could utilize RDP ports to monitor and collect confidential information as well as distributing malware. 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 events observed on CCTX sensors for the last week.

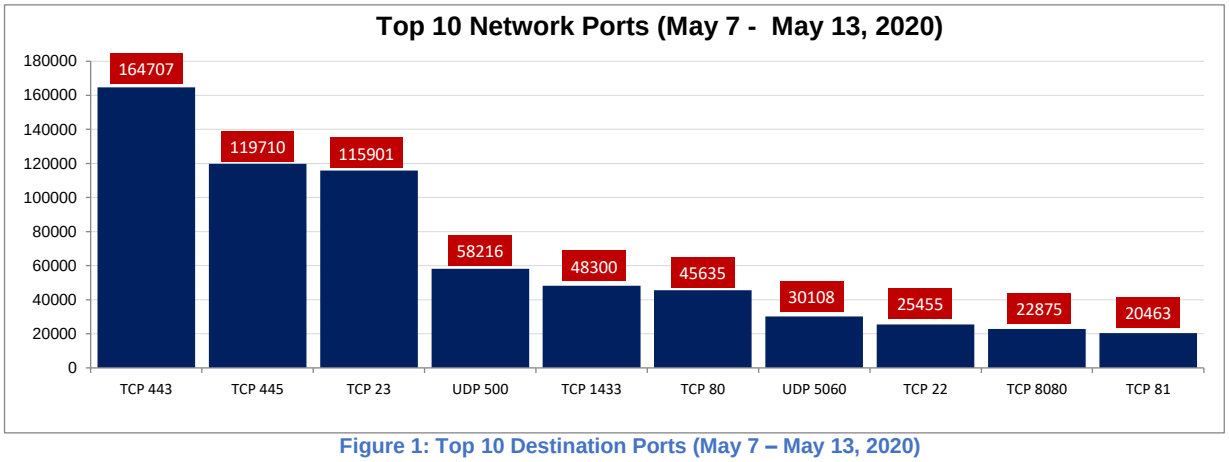

Figure 1: Top 10 Destination Ports (May 7 – May 13, 2020)

This week's analysis of the top 10 network probe ports is shown in Table 1. This week we observed an increase in network scans targeting port TCP/22 and TCP/80. TCP/80 has been attracting attention in recent weeks. From data we collected this week, we observed a 36.9% increase in scans targeting port TCP/22 and TCP/80. Our analysis could not identify if any correlation exists between both ports (TCP/22 and TCP/80) seeing similar weights in increased traffic. Additionally, we equally saw increases in traffic targeting ports TCP/8080 and UDP/5060. We assess these increases may be related to activities of malicious IoT botnets scanning for vulnerable and exposed IoT devices. For deeper insights this week, we investigate scans targeting port TCP/80.

Table 1: Top 10 Network Probe Activity Report				
Rank	**Port Number**	**Previous Week Ranking**	**Ranking Change (+/-)**	**% Probe Volume Change (+/-)**
1	TCP 443	1	-	-52.3%
2	TCP 445	3	+1	9.8%
3	TCP 23	2	-1	-8.6%
4	UDP 500	4	-	-0.4%
5	TCP 1433	5	-	8.5%
6	TCP 80	6	-	36.4%
7	UDP 5060	7	-	15.1%
8	TCP 22	13	+5	36.9%
9	TCP 8080	10	+1	22.1%
10	TCP 81	8	-2	-6.3%

TCP 80

TCP port 80 is the default port associated with the HTTP protocol and is widely known for plaintext HTTP services. Over the past couple weeks, we have observed an uptick in scans (Figure 3) targeting TCP port 80 on our edge network. Our analysis of these scans and telemetry data identified clusters in web applications targeted. Using a word cloud generator, Figure 2 presents an analysis of key words associated with web applications and attack techniques observed from these scanning hits on our sensors. Many of the scanning attempts detected were related to WordPress, SQL Injection, RDP exploits and Microsoft OWA vulnerabilities as shown.

Figure 2: Targeted Web Applications and Attack Word Cloud

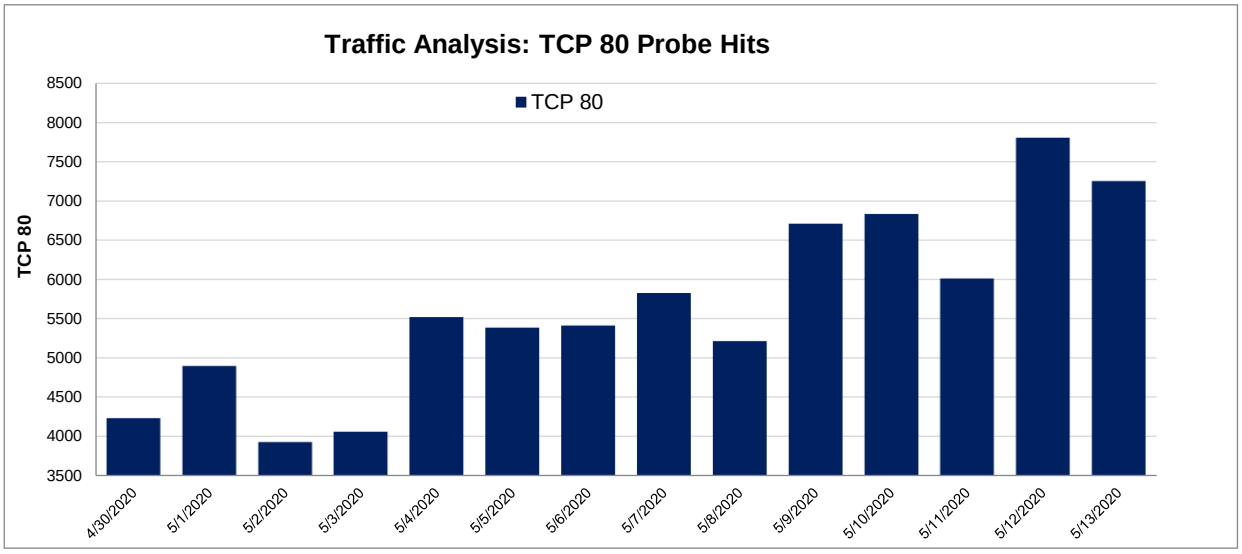

Figure 3: TCP Port 80 Analysis (April 30 – May 6, 2020)

Top talker analysis of data collected revealed some Russian IPs attempting to open an RDP connection on TCP port 80 by sending inbound connection PDU requests [1] with a cookie "*Cookie: mstshash=Administr".* Our assessment is threat actors may be using these scans to identify RDP services running on non-standard RDP port. Windows RDP default is TCP port 3389 but administrators may configure the service on other ports. These scans may also help the attacker fingerprint the underlying operating system behind the firewall. Similarly, attackers can get access to several devices using a compromised Windows computer that may be located behind a Firewall that allows RDP access. FireEye's research documented this technique where threat actors tunnel RDP traffic through connections through a compromised device on the network. [3] Below are some of the source IPs we identified:

- 185.202.2.147 (Russia)
- 185.153.197.11 (Russia)
- 45.143.200.15 (Russia)
- 45.141.87.4 (Russia)
- 45.136.108.20 (Russia)
- 41.216.186.89 (Saint Kitts and Nevis)

References

[1] Client X.224 Connection Request PDU - https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr/18a27ef9-6f9a-4501-b000-94b1fe3c2c10

[2] Mstshash=administr explained - https://github.com/olipo186/Git-Auto-Deploy/issues/221

[3] Bypassing Network Restrictions Through RDP Tunneling - https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html