Weekly Summary Activity Report – July 3rd, 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

June 30, **Check your CRA account for any CERB scams**

Cybercriminals are targeting Canadians to steal their CRA online access information and then use the details to redirect Canada Emergency Benefit (CERB) payments to newly opened bank accounts. The Canada Revenue Agency (CRA) and the police are now advising Canadians to check and validate their direct deposit instructions on their online CRA account. …Read more at fool.ca

June 30, **Promethium APT attacks surge, new Trojanized installers uncovered**

Advanced persistent threat (APT) group, Promethium has launched a new wave of espionage attacks against new targets including some in Canada. The Promethium campaign, dubbed as StrongPity typically focuses on targets in Turkey and Syria. However, Cisco Talos researchers recently found new victims in Colombia, India, Canada and Vietnam. In order to infect more victims, the APT group deployed newer toolkits designed to install the StrongPity version 3 spyware. ... Read more at zdnet.com

June 29, **Canadian privacy commissioners to investigate Tim Hortons data collection practices**

Canada's privacy commissioner and three provincial counterparts have launched an investigation into Tim Hortons' mobile app. According to the details, the Tim Hortons' mobile app beeped its location data every three to five minutes back to its servers. Using that information, Tim Hortons may be able to track the latitude and longitude of a user's precise location including their workplace or their presence at a competitor's location. ....Read more at itworldcanada.com

June 25, **This training tool could be the answer to stop mass cyberattacks**

Cyber operators from the US Cyber Command and three other member nations of the Five Eyes alliance –Britain, Canada and New Zealand, participated in a cyber training exercise between June 15-26. The purpose of this exercise was to build their defensive cyber operations and improve their overall capability to defend against mass cyberattacks in real-time. ...Read more at c4isrnet.com

Global

June 30, **Fake "DNS Update" emails targeting site owners and Admins**

Researchers at Sophos recently identified a fake "DNS Update" phishing campaign which was targeting WordPress users. The attackers sent fake update notification emails with malicious links and asked victims to enter their admin account login credentials. The email included text related to an update in the DNS Security Extension (DNSSEC) to convince the victims to click. …Read more at helpnetsecurity.com

June 29, **India bans 59 Chinese apps, including TikTok, UC Browser, Weibo, and WeChat**

The Indian government has banned 59 Chinese mobile applications which they believe are being used to collect data on Indian users. This ban comes after the Indian military clashed with Chinese forces on June 15th, 2020. The Indian Ministry of Information Technology said they had received complaints from users regarding data privacy and security issues on some of the banned apps. It is unknown how the Indian government plans to enforce this ban. …Read more at zdnet.com

June 29, **Half of internet users fall victim to cyber attacks**

A survey report has revealed that half of computer users have fallen victim to a form of cyber attack. The result was based on a survey of 1,400 internet users in the US and UK. According to the survey details, over 55% of British and 67% of American respondents admitted that they had encountered malicious cyber activities such as computer virus, phishing scams and stolen passwords… Read more at securityboulevard.com

June 28, **Australian ACSC report confirms the use of Chinese malware in recent attacks**

Australia's Cyber Security Centre (ACSC) confirmed that a Chinese APT group was involved in recent malware attacks against the nation. In a threat report released, ACSC provided details of how the hackers targeted unpatched versions of the Telerik user interface application by exploiting several vulnerabilities. The APT group also targeted Microsoft SharePoint users by exploiting remote code execution vulnerabilities on SharePoint systems. …Read more at securityaffairs.co

June 26, **Russian hacker group Evil Corp targets US workers at home**

Symantec released a threat report warning that Russian-based hacking group, Evil Corp is launching ransomware attacks against US companies. The group has tried to target at least 31 US organisations whose employees are working remotely due to the COVID-19 pandemic. The hackers are using VPNs to identify their targets, then infect the user's computer when they visit a public or commercial site. …Read more at bbc.com

June 25, **New Zealand Police seize alleged bitcoin raider's $90m in assets**

Police in New Zealand have seized about $90m worth of assets belonging to a 38-years-old alleged cyber criminal, Alexander Vinnik. He was arrested in Greece in 2017 on money laundering charges and extradited to France. … Read more at infosecurity-magazine.com

June 25, **Critical bugs and backdoor found in GeoVision's fingerprint and card scanners**

A Taiwanese manufacturer of video surveillance systems and IP cameras, GeoVision recently patched multiple critical flaws impacting its card and fingerprint scanners. The flaws affected at least 6 device families with over 2,500 vulnerable devices discovered online across Brazil, US, Germany, Taiwan and Japan. The vulnerabilities could allow an attacker to gain backdoor access, collect passwords, or run unauthorized code on the devices…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 alarms observed on CCTX sensors for the last week.

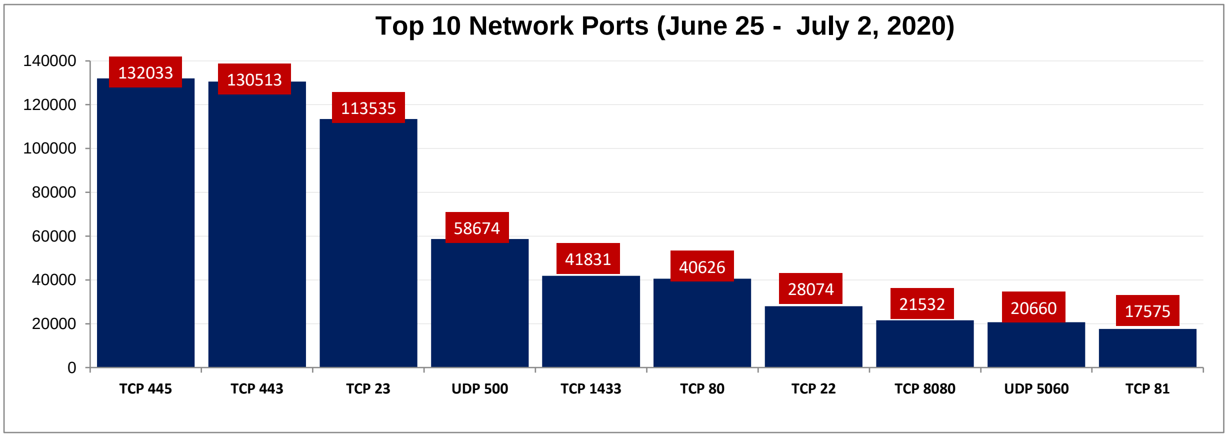

Figure 1: Top 10 Destination Ports (June 25 – July 2, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	**Port Number**	**Previous Week Ranking**	**Ranking Change (+/-)**	**% Probe Volume Change (+/-)**
1	TCP 445	1	-	-0.5% ⬇
2	TCP 443	2	-	-0.8% ⬇
3	TCP 23	3	-	-6.0% ⬇
4	UDP 500	4	-	0.6% ⬆
5	TCP 1433	5	-	0.1% ⬆
6	TCP 80	6	-	23.5% ⬆
7	TCP 22	7	-	26.8% ⬆
8	TCP 8080	9	+1 ⬆	4.9% ⬆
9	UDP 5060	8	-1 ⬇	-6.6% ⬇
10	TCP 81	12	+2 ⬆	19.9% ⬆

This week's data from our top ten most targeted ports shows an increase in scan volumes. We observed the largest increase in probe scans in the traffic targeting TCP port 22. Over the period under review, scan probes targeting TCP port 22 increased by almost 27%. A couple other network ports recorded double-digit percentage increases. They are TCP port 80 and TCP port 81. Our sensors recorded a drop of over 6% in probe scans to UDP port 5060 and TCP port 23, both historically associated with Mirai bots. As part of our deeper dive for this week, we investigate the increase in probe scans targeting TCP port 22 (a port associated with the SSH protocol).

TCP 22

TCP port 22 is a Session Shell Protocol (SSH) used for secure logins, file transfer (scp, sftp) and port forwarding. It's most common used for command line access, secure replacement of Telnet, or used as an encrypted tunnel for secure communication of virtually any service [1].

On 27 June 2020, PuTTY released a security advisory which detailed a use-after-free vulnerability in some versions of the software [2]. As shown in Figure 2, a few days after the advisory was released probe scans targeting TCP port 22 increased. In addition, a security researcher discovered information leak vulnerabilities in two widely used SSH clients (CVE-2020-14002 and CVE-2020-14145). A vulnerability exists in PuTTY Dynamic host key which could lead to information about host keys being leaked. Secondly, information leak in OpenSSH 5.7-8.3 and PuTTY 0.68-0.73 can allow an attacker to carry out targeted man-in-the-middle attacks. Users can protect themselves by always verifying the fingerprint of the server during an initial connection attempt [4] [3] [5].

Below are the top source hits from our data:

- 85.209.0[.]100 (Moscow, Russia),
- 218.92.0[.]178 (Jiangsu, China),

- 222.186.42[.]13 (Shanghai, China),
- 87.251.74[.]48 (Novosibirsk Oblast, Netherlands).

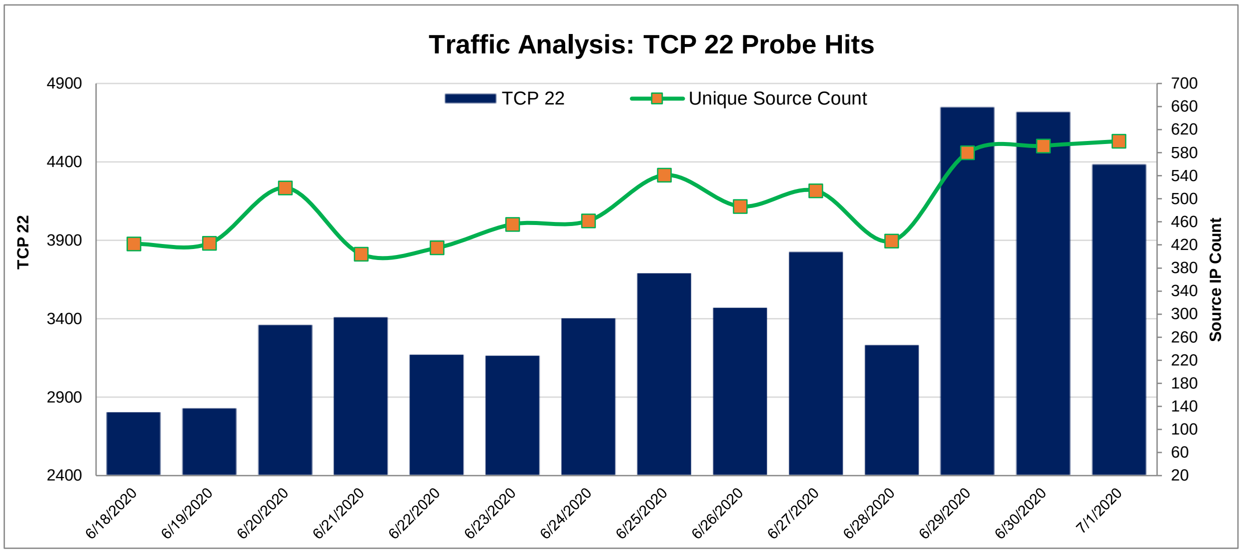

Figure 2: TCP Port 22 Analysis (June 18 – July 01, 2020)

References

[1] Port 22 Details - https://www.speedguide.net/port.php?port=22

[2] PuTTy Vulnerability - https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-agent-keylist-used-after-free.html

[3] CVE-2020-14002- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14002

[4] PuTTY vulnerability vuln-dynamic-hostkey-info-leak - https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-dynamic-hostkey-info-leak.html

[5] FSA-2020-2 Targeted MitM Attacks Using Information Leakage in SSH Clients - https://www.fzi.de/en/news/news/detail-en/artikel/fsa-2020-2-ausnutzung-eines-informationslecks-fuer-gezielte-mitm-angriffe-auf-ssh-clients/