Canadian Cyber
Threat Exchange
Informing Canadian Business

Échange canadien
de menaces cybernétiques
Informer les entreprises canadiennes

Weekly Summary Activity Report – June 26th, 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 24, **Fake Canadian COVID-19 tracing app with ransomware discovered**

Security vendor ESET discovered two fake COVID-19 tracing mobile apps designed to target Canadian Android users. The mobile apps were masquerading as Health Canada’s official COVID-19 tracing app. When installed on an Android device, the app delivers a new ransomware variant named CryCyptor that will encrypt files on a victim’s smartphone. These websites have been reported to Canadian Centre for Cyber Security. Both websites were hosted in the Netherlands. ...Read more at itworldcanada.com

June 22, **Canadians at greater risk of banking app fraud due to COVID-19 trends**

Canadians are using more banking apps and cashless solutions due to the COVID-19 pandemic. As a result, the Canadian Anti-Fraud Centre (CAFC) is warning that fraudsters could take advantage of this trend to defraud users. The CAFC is tracking an increase in mobile banking fraud attempts being recorded in the United States and~~,~~ expects Canada may likely see similar attacks in the coming weeks. .... Read more at finance.yahoo.com

June 18, **Hackers hijack Samsung Canada servers to evade Microsoft 365 security**

Check Point security researchers recently released a threat report~~,~~ revealing details of how hackers hijacked cyber assets belonging to Samsung Canada and the University of Oxford to send phishing emails to several Microsoft Office 365 users. The emails, which were targeting network access credentials, included URL links hosted on a Samsung Canada domain. Once the link is clicked, it redirects to a fake webpage requesting a user’s Office 365 credentials. ...Read more at forbes.com

June 18, **Shopify, BlackBerry and Ontario to help Canada launch contact tracing app**

Canadian Prime Minister Justin Trudeau announced that Shopify, BlackBerry and the Province of Ontario will launch a contact tracing app in early July 2020. This application is meant to supplement contact tracing efforts already in place by public health authorities. The new app is built using the COVID Shield, an exposure notification solution built by volunteers, many from Shopify. The new app will use Google/Apple's contact-tracing and exposure-notification APIs. Downloading the app will be completely voluntary, and no personal information will be collected or share...Read more at itworldcanada.com

Global

June 23, **Oregon city pays $48,000 cyber ransom**

The City of Keizer in Oregon State, U.S. paid about $48,000 in ransom to regain access to its computer systems following a recent ransomware attack. On June 10, the threat actors successfully infiltrated the city’s network, preventing access to files and email accounts. After a week of unsuccessfully trying to recover the encrypted files, city officials agreed to make the ransom payment. … Read more at infosecurity-magazine.com

June 22, **Apple’s new iOS privacy updates will show how apps are tracking you**

Apple has announced new privacy features for its devices that would limit the sharing of location data and use of microphone and camera features. Apple introduced labels for app permissions which will show what data is linked to each user and what data is used to track the user. …Read more at cnet.com

June 19, **Google loses appeal against 50m-Euro French fine**

Google has lost its appeal against a 50 million euro (about $56 million) fine imposed by France’s data watchdog, the CNIL. The fine was imposed in 2019 after Google failed to provide adequate information on its data consent policies. The Council of State, France's highest administrative authority, dismissed Google’s appeal and upheld the initial ruling that information provided to users "does not meet the requirements of clarity and accessibility required by the GDPR law". … Read more at securityweek.com.

June 19, **Hackers use fake Windows error logs to hide malicious payload**

Huntress Labs released details of an attack technique which can allow hackers to use fake error logs to store ASCII characters disguised as hexadecimal values. Once the ASCII characters are decoded, they can be used as inputs for a malicious script that would contact a command and control server for the next stage of the attack. Typically, the attacker already has access to the target system before the technique can be used. …Read more at bleepingcomputer.com

June 18, **Trump’s 2020 re-election app exposed secrets, keys**

Security researchers at Website Planet released a report that the “Official Trump 2020” mobile apps for both Android and iOS devices exposed their confidential secret keys in various parts of the app. The researchers discovered that the apps exposed their Twitter application keys and secrets which could allow hackers to access any user’s account information. … Read more at securityweek.com

June 18, **Over 32 million Chrome users targeted by stealthy malware campaign**

A sophisticated spyware operation led to over 32 million chrome browser users installing malicious chrome extensions. According to security researchers at Awake Security, about seventy (70) malicious extensions were identified as part of this sophisticated spyware operation. Google Chrome has up to 2 billion active users, this attack targeted users of the Chrome browser on home networks. …Read more at forbes.com

June 17, **LinkedIn ‘job offers’ targets aerospace, military firms with malware**

European and Middle East aerospace and defense firms were recently a target of a malicious spear-phishing campaign delivered via LinkedIn. The threat actors impersonated HR teams from Collins Aerospace and General Dynamic to send out fake job offers that included documents embedded with malware. According to ESET researchers, the spear-phishing campaign was of a target operation dubbed “Operation In(ter)ception”. The primary goal of the campaign was cyber espionage. … Read more at threatpost.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.

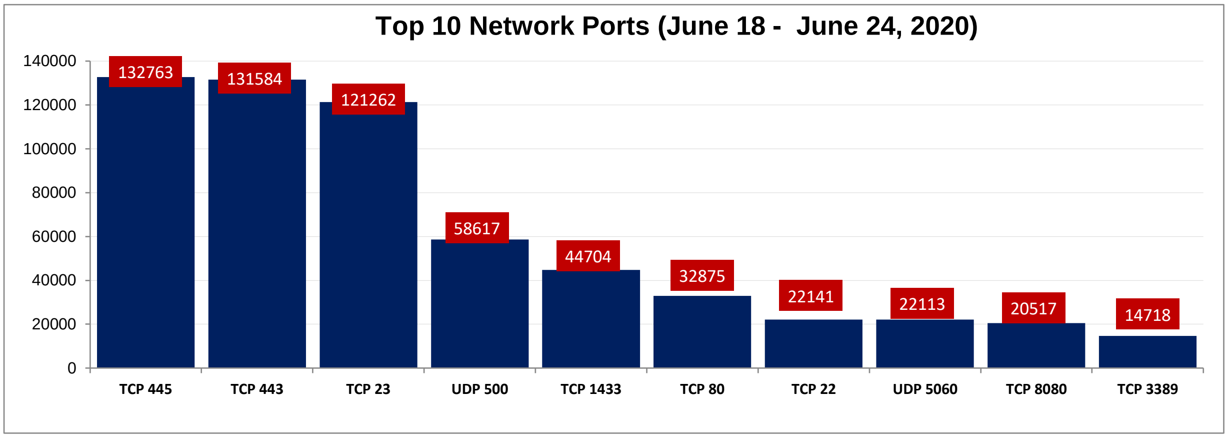

Figure 1: Top 10 Destination Ports (June 18 – June 24, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 445	1	-	-2.3% ↓
2	TCP 443	2	-	-0.9% ↓
3	TCP 23	3	-	-0.1% ↓
4	UDP 500	4	-	-0.7% ↓
5	TCP 1433	5	-	5.6% ↑
6	TCP 80	6	-	-9.8% ↓
7	TCP 22	9	+2 ↑	3.6% ↑
8	UDP 5060	8	-	-7.2% ↓
9	TCP 8080	7	-2 ↓	-14.7% ↓
10	TCP 3389	11	+1 ↑	3.0% ↑

This week's data from our top ten most targeted ports shows an overall decrease in traffic. We observed a significant decrease in probe scans to TCP port 8080, which declined by about 15%. Many other ports saw minor increases in scans, including TCP port 1433, TCP port 22 and TCP port 3389. For our deeper dive this week, we investigate probe scans targeting TCP port 23 (a port associated with the Telnet protocol). Over the last week, scan probes targeting port TCP/23 decreased marginally by about 0.1%.

TCP 23

TCP 23 (Telnet) is one of the oldest internet protocols and one of the most popular software for remote access to Unix machines. Historically, the Telnet protocol has been linked with several critical security vulnerabilities [1].

On 24 June 2020, Cisco released a security advisory with details of devices affected by a vulnerability (CVE-2020-10188) in the telnet service [2] [3]. CVE-2020-10188 is a vulnerability in Telnet servers (telnetd) which was initially published on 28 February 2020. Cisco investigated its product line and determined that all products running the Cisco IOS XE Software with persistent Telnet configured are vulnerable.

As shown in Figure 2, our data shows an increase in scans targeting TCP port 23, a couple of days before the public release of this Cisco advisory. Threat actors actively scan for internet exposed TCP/23 ports as they target weak credentials on IoT devices. We are likely to see an increase in probe scans specifically targeting Cisco devices affected by this vulnerability.

The Cisco IOS XE software is typically used on Cisco gateway products (gateway switches, VPN appliances and routers), that are likely to be internet exposed as a result of their functions. Organizations with affected devices in deployment should patch immediately or disable the persistent Telnet feature and consider using the Secure Shell (SSH) protocol instead. Below are the top source hits from our data:

- 185.23.214[.]140 (Amsterdam, Netherlands),
- 178.128.200[.]104 (New York, U.S.),
- 218.63.72[.]113 (Beijing, China),
- 185.177.57[.]56 (Sofia, Bulgaria.).

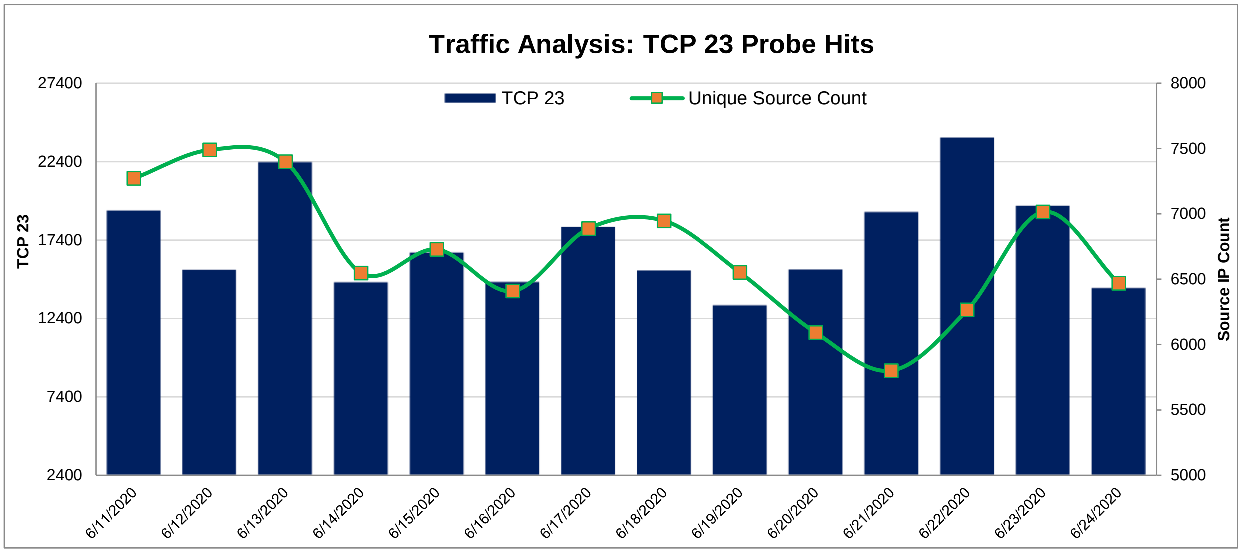

Figure 2: TCP Port 23 Analysis (June 11 – June 24, 2020)

References

[1] Port 23 Details - https://www.speedguide.net/port.php?port=23

[2] CVE-2020-10188 -

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10188

[3] Telnet Vulnerability Affecting Cisco Products: June 2020 - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-telnetd-EFJrEzPx

[4] BraveStarr – A Fedora 31 netkit telnetd remote exploit – https://appgateresearch.blogspot.com/2020/02/bravestarr-fedora-31-netkit-telnetd_28.html