Weekly Summary Activity Report – May 29th, 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 27, **Cyber defence agency found over 1,500 'malicious' fake Canadian Government COVID-19 websites**

The National Post published an article about the Canadian Centre for Cyber Security's (CCCS) report indicating that they identified over 1,500 websites pretending to be COVID-19 pages from the Government of Canada. These websites were targeting Canadians who are working from home and in sectors of strategic importance including financial services, healthcare and medical research. Read more at nationalpost.com

May 26, **Canada Post silent on possible financial cyber attacks**

New Westminster Record published an article about threat research conducted by Proofpoint on a new phishing campaign targeting Canadians that mimics Canada Post. This new campaign is distributing the ZLoader banking malware, which is targeting users of the Canadian postal service, government and educational institutions. The fake Canada Post emails include fake delivery attempt emails designed to trick recipients into clicking or opening the malicious attachment. Read more at newwestrecord.ca

May 25, **Canada still lacks cybersecurity 'Street Smarts' says CIRA director**

IT Business published an article about the CEO of CIRA's presentation to the Canadian government's committee on industry, science and technology (INDU) setup to review Canada's cyber response to COVID-19. The Canadian Internet Registration Authority (CIRA) believes that the Government of Canada needs to provide more support and funding for cybersecurity research, solutions and platforms, in order to protect Canadians and the digital economy. In another presentation, the Director of the Canadian Cyber Security Centre stated that threat actors are largely sticking to traditional cyber attack techniques to launch attacks against Canadians. Read more at itbusiness.ca

May 22, **Ontario health unit website leaves COVID-19 test results accessible**

IT World Canada published a news article indicating that The North Bay Parry Sound District Health Unit unintentionally exposed about 3,000 COVID-19 virus test results through their COVID-19 dashboard page on its website. Read more at itworldcanada.com

Global

May 27, **[F]Unicorn ransomware masquerading as COVID-19 contact tracing app**

Tripwire published an article about a new ransomware variant called [F]Unicorn. The malware disguises itself as a COVID-19 application containing information collected by the Center for Systems Science and Engineering at Johns Hopkins University. According to security researchers, the malware sends the password used to encrypt user data as plaintext. This may allow victims to retrieve the password from their network data and use it to recover the encrypted files. Read more at tripwire.com

May 22, **Researchers found North Dakota's contact-tracing app covertly sending location and advertising data to third parties**

Business Insider published an article about North Dakota's contact-tracing application released in late April called Care-19, which was designed to help track the spread of the coronavirus in their state. It appears that the app has been collecting location data and sending it to Foursquare, an organization known for selling data to advertising companies. North Dakota has released an announcement indicating that it will release a second app, which is promised to be more secure. Read more at businessinsider.com

May 21, **Beware of phishing emails urging for a LogMeIn security update**

Help Net security published an article indicating that hackers launched phishing campaigns mimicking LogMeIn, a remote connectivity service provider for collaboration, IT management and customer engagement. The hackers' emails containing fake security update requests were sent to several users. This is not the only remote connectivity platform that has been targeted by hackers lately. As more people are working from home, remote platforms have been releasing frequent updates to keep up with newly discovered issues, and cybercriminals are exploiting these to stage phishing attacks. Read more at helpnetsecurity.com

May 21, **Home Chef breach may affect millions of customers**

Info Security published an article about the data breach at Home Chef. A notice on their website announced that the personal information of their customers, including email addresses, encrypted passwords, last four digits of credit card numbers, addresses and other account information, had been compromised as a result of a data breach. In the notice, Home Chef indicated that only a few customers were affected. However, a hacker's post on the dark web claimed he had approximately eight million personal records available for sale. 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 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.

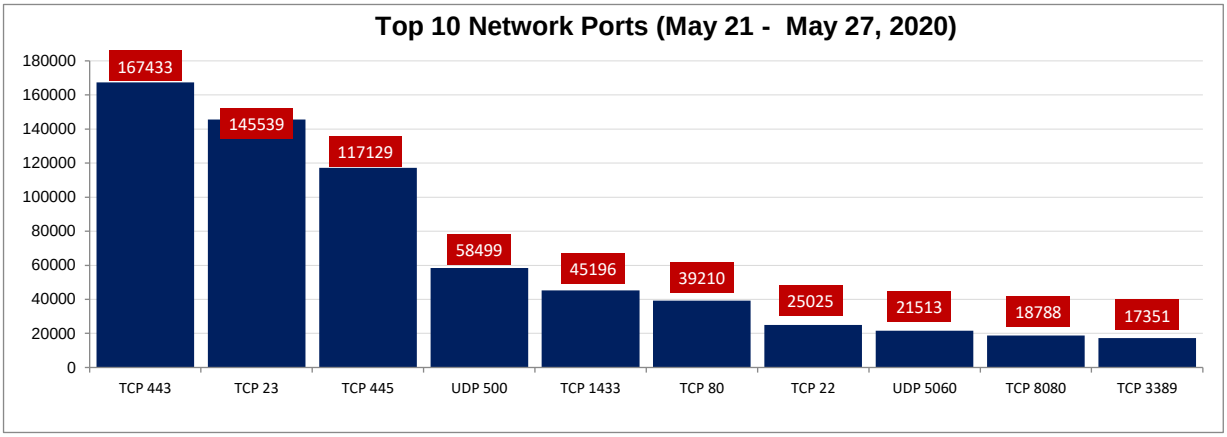

Figure 1: Top 10 Destination Ports (May 21 – May 27, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 443	1	-	10.6% ↑
2	TCP 23	2	-	12.4% ↑
3	TCP 445	3	-	-3.7% ↓
4	UDP 500	5	*+1*	0.4% ↑
5	TCP 1433	7	*+2*	-0.3% ↓
6	TCP 80	6	-	-27.8% ↓
7	TCP 22	4	*-3*	-57.7% ↓
8	UDP 5060	9	*+1*	-17.2% ↓
9	TCP 8080	8	*-1*	-35.3% ↓
10	TCP 3389	12	*+2*	5.9% ↑

This week, we observed significant declines in traffic volumes across most network ports on the top ten network probe list. We observed a significant drop in network scans targeting TCP port 22, TCP port 8080 and TCP port 80. These declines may indicate a change in attackers' approach, changing from continuous large-scale network scanning to targeted scanning schedules. Furthermore, we observed moderate increases in traffic scans targeting TCP port 23 and TCP port 443.

TLP-GREEN

TCP 23

TCP port 23 is the default port associated with the Telnet protocol. Telnet is a client-server network protocol used for text-based communication between the two hosts. Due to ease of its use and wider support, many Internet of Thing (IoT) devices implement the Telnet protocol by default, thus making these devices targets of threat actors for building malicious botnets. In a recent threat report, security researchers announced the discovery of a new version of the Mirai botnet named "Mukashi". This new malware is believed to be targeting a critical vulnerability in Zyxel network-attached storage (NAS) devices. [1] Figure 2 shows our sensor telemetry over the period under review which indicate fewer sources launching more scan probes for exposed TCP port 23 services.

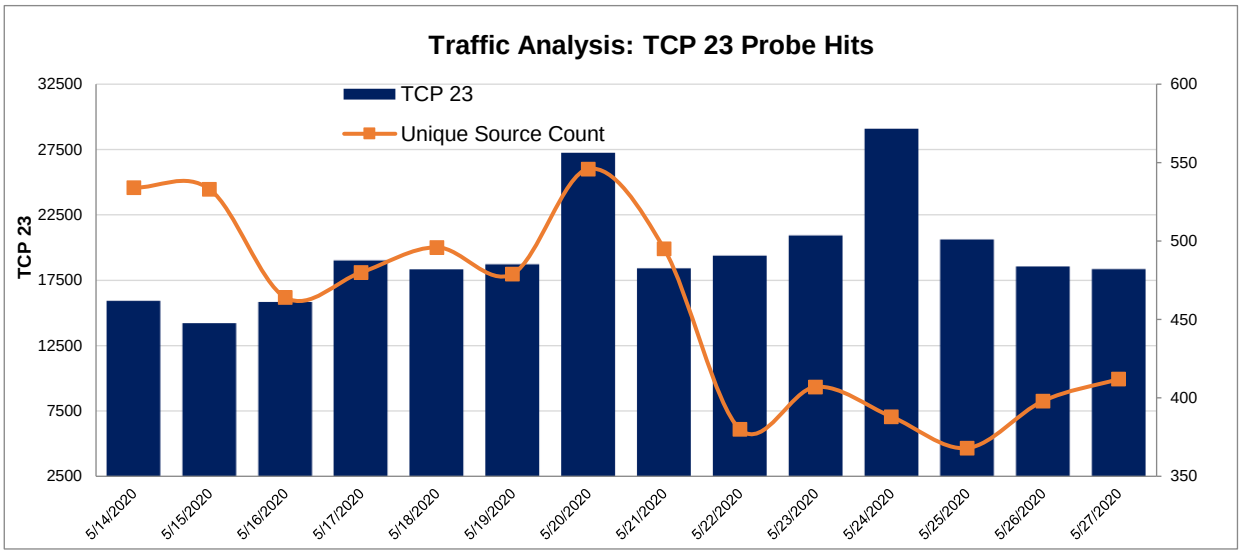

Figure 2: TCP Port 23 Analysis (May 14 – May 27, 2020)

References

[1] Mukashi: A New Mirai IoT Botnet Variant Targeting Zyxel NAS Devices: https://thehackernews.com/2020/03/zyxel-mukashi-mirai-iot-botnet.html

TLP-GREEN