Weekly Summary Activity Report – May 22nd, 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 20, **Cybersecurity Survey By Canadian Law Firm Offers Surprising Results**

IT World Canada published an article on a survey conducted by Blake, Cassels & Graydon, a Canadian Law firm, which revealed that just over half of Canadian organizations affected by ransomware in 2019 paid the hackers to get the decryption keys for restoring their data. The law firm's representative believes that the numbers most likely have gone up since the COVID-19 pandemic. In addition, the survey identified that 33% of organizations surveyed had a business disruption, 25% of the organizations suffered a financial loss, 21% saw an impact on their relationship between partners and around 50% needed two weeks to recover. Read more at itworldcanada.com

May 19, **Facebook Fined $9 Million Over Canadian Privacy Concerns**

CBC published an article about a fine imposed on Facebook for misleading Canadian users about its data privacy practices. According to Canada's Competition Bureau, Facebook must pay $9 million in penalties for misinforming Canadian users on how their personal information is used. The Bureau discovered that users were falsely informed that they could control who could see and access their personal information. According to the findings, third-party developers were able to access data belonging to Canadian Facebook users. Additionally, Facebook must pay $500,000 to the Bureau for the cost of investigating and testing Facebook's policies. Read more at cbc.ca

May 15, **COVID-19: Canadian Security Agencies Warn Of Cyber Threats To Research**

Radio Canada released an article on a warning issued by Canada's security agencies that COVID-19 research has become a target for nation-state actors. The Canadian Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS), released a joint statement indicating that COVID-19 research facilities are targets for "state actors". The statement also indicated an elevated level of risk to the cyber security safety of Canadian health care organizations. State actors are targeting medical research, manufacturing, distribution and policy-making organizations. The statement did not identify which states are behind the attacks, however, China and Russia could be amongst the countries interested in Canadian Health care and research data. Read more at rcinet.ca

Global

May 20, **Verizon DBIR 2020: Cloud Apps, Stolen Credentials, and Errors**

Tripwire released an analysis of Verizon's 13th edition of the annual "Verizon Data Breach Investigations Report". This year, Verizon analyzed about 32,000 incidents, from which almost four thousand incidents were confirmed to be a data breach. According to the report, 86% of breaches are financially motivated, 70% of breaches were caused by outside entities, 27% were ransomware incidents, and 81% reported that the breaches were contained within a day. Read more at tripwire.com

May 19, **TrickBot BazarLoader In-Depth**

AT&T security researchers published a blog on an in-depth analysis of a new variant of the TrickBot malware. This new variant was updated with new modules named "BazarLoader" and "BazarBackdoor" which provide Command and Control (C2) communications with the Emercoin DNS (EmerDNS) ".bazar" domains. AT&T Alien Labs researchers discovered that the malware developers included new features which have increased the obfuscation techniques exhibited by the malware. This new variant is being distributed via a phishing campaign with COVID-19 lures through Sendgrid's email marketing platform. Read more at att.com

May 19, **REvil to Auction Stolen Madonna Data**

Infosecurity Magazine published a news article on REvil's plan to auction stolen data. The threat group, REvil, stole over 700GB of data from New York lawyers Grubman Shire Meiselas & Sack using a ransomware attack. The Law firm works with celebrities such as Madonna, LeBron James and Mariah Carey. The Law firm released a statement in which they confirmed that it suffered a ransomware attack earlier in May. In addition, the firm stated that it has been cooperating with security experts and the FBI, and it has concluded that negotiating or paying the ransom would be against the federal criminal law. However, paying for the encrypted files has not been ruled out. REvil indicated that it will make money by first auctioning data that belong to singer Madonna on May 25, and the bidding will start at $1 million. Read more at infosecurity-magazine.com

May 18, **Netwalker Fileless Ransomware Injected via Reflective Loading**

Trend Micro released an in-depth analysis of the ransomware called Netwalker. The malware is written in PowerShell and ran in memory, which creates a challenge for detection tool. The developers created a fileless malware running directly in memory and it does not require a DLL loader or any windows loader for it to be loaded. Additionally, the malware script is hidden behind encryption, obfuscation, and encoding techniques. Lately, attackers added the Reflective DLL injection to Netwalker's arsenal, making it more difficult to trace and investigate. Read more at trendmicro.com

May 18, **Mercedes-Benz Onboard Logic Unit (OLU) Source Code Leaks Online**

ZDNet published a news article regarding the source code leak at Mercedes-Benz. Till Kottmann, a Swiss-based software engineer, discovered that he could register an account on

Git web portal belonging to Daimler AG and download the source code from onboard logic units (OLUs) that are installed in Mercedes-Benz vans. OLU is a component that is located between the car's hardware and software and provides connection to the cloud. ZDNet investigated the leak and discovered a user could also get access to server images, internal Daimler components for managing remote OLUs, internal documentation, and more. Read more at zdnet.com

May 14, **Australia's BlueScope Steel says Cyber 'Incident' Causing Disruptions**

Reuters published a news article on the cyber incident at Australia's BlueScope. Melbourne-based steelmaker, BlueScope Steel Ltd, said its manufacturing and sales operations in Australia were impacted by a cyber incident. The steel manufacturer operates in Australia, Asia, New Zealand and the US; all locations had at least a minor service disruption. The manufacturer has decided not to release if the incident was due to cyberattack or an internal systems failure for now and are just referring to it as an "incident". Read more at reuters.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.

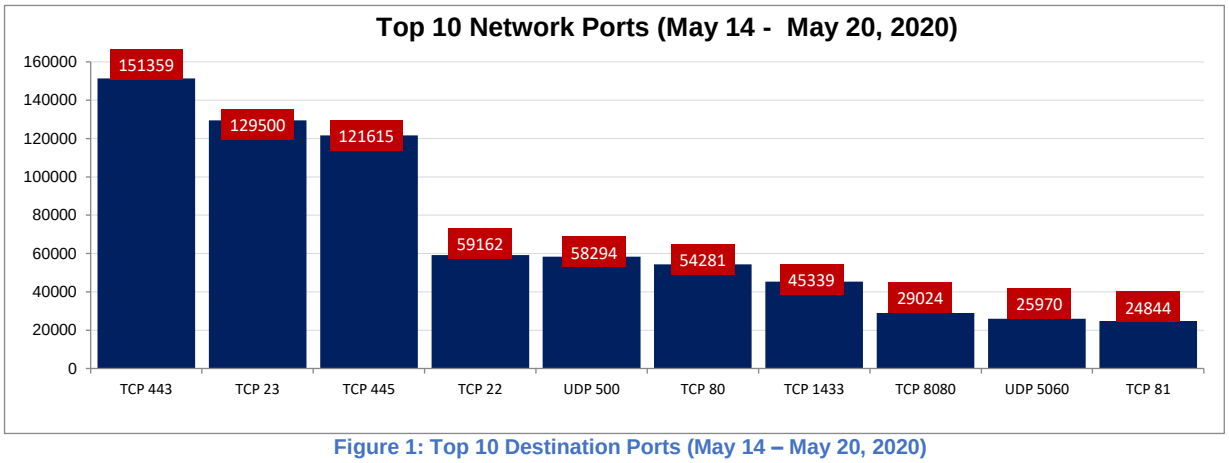

Figure 1: Top 10 Destination Ports (May 14 – May 20, 2020)

Table 1: Top 10 Network Probe Activity Report				
Rank	**Port Number**	**Previous Week Ranking**	**Ranking Change (+/-)**	**% Probe Volume Change (+/-)**
1	TCP 443	1	-	-8.1%
2	TCP 23	3	*+1*	11.7%
3	TCP 445	2	*-1*	1.6%
4	TCP 22	8	*+4*	132.4%
5	UDP 500	4	*-1*	0.1%
6	TCP 80	6	-	18.9%
7	TCP 1433	5	*-2*	-6.1%
8	TCP 8080	9	*+1*	26.9%
9	UDP 5060	7	*-2*	-13.7%
10	TCP 81	10	-	8.6%

This week, we observed increases across most of our top ten targeted network ports as shown in Table 1. The major highlight for the week was the significant increase in network scans targeting TCP port 22. We recorded over 130% increase in the volume of probe scans targeting TCP port 22 over the previous week. We investigate the probable causes in an in-depth analysis in the section below. Other highlights for the week include an increase in scans targeting TCP port 8080 with more than 26% increase over last week, TCP port 80 with about 19% increase and TCP port 23, with about 12% increase.

TCP 22

TCP port 22 is the default port associated with the Secure Shell (SSH) protocol and is also used to host secure file transfers such as SCP and SFTP. Over the last two weeks, we have observed an uptick in actors scanning for accessible TCP port 22 on our edge network. As shown in Figure 2, packet data collected from our sensors show slight increases in traffic starting 7th May. Equally, as shown in Figure 2, there was a correlated increase in the number of IP addresses suggesting these scans maybe linked to a botnet activity. After further analysis, we identified the following IP addresses as top-talkers: 85.209.0.100 (Russian Federation), 85.209.0.101 (Russian Federation), 85.209.0.102 (Russian Federation), 85.209.0.103 (Russian Federation), 87.251.74.56 (Russian Federation) and 222.186.42.13 (China). We assess that these SSH scans are likely as a result of a script-based brute force attack. In addition, this may be linked to a new strain of an Internet of Things (IoT) malware reported earlier in May, 2020. The IoT malware was named Kaiji and was reported to target SSH ports with brute force attacks. The Kaiji botnet spreads using brute-force attacks against IoT devices, targeting the root account with dictionary password attacks. [1]

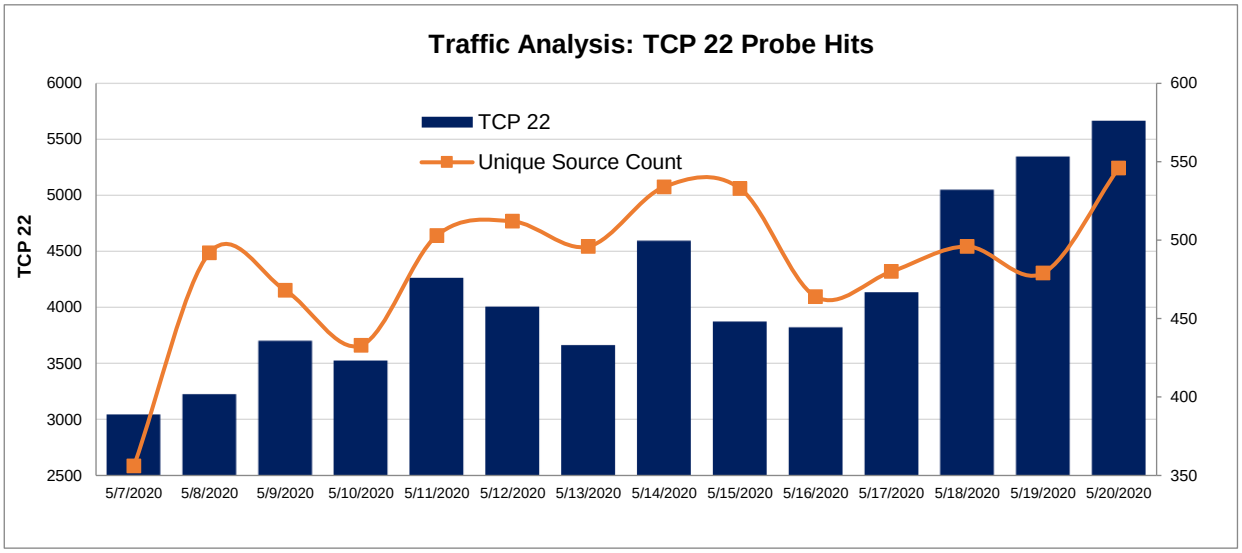

Figure 2: TCP Port 22 Analysis (May 7 – May 20, 2020)

References

[1] New Kaiji Malware Targets IoT Devices via SSH Brute Force Attacks: https://www.zdnet.com/article/new-kaiji-malware-targets-iot-devices-via-ssh-brute-force-attacks/