Canadian Cyber Threat Exchange
Informing Canadian Business

Échange canadien de menaces cybernétiques
Informer les entreprises canadiennes

Weekly Summary Activity Report – June 19th, 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 17, **Companies still struggle with SOC staff shortages, security skills gap**

Companies still struggle with staff shortages in their security operations centers (SOC), according to organizations surveyed in the U.S., the U.K., Canada, Germany and Australia. The survey was conducted by Exabeam for their “2020 State of the SOC Report”. One of the key takeaways from the survey, which had 295 respondents, is that 39% of organizations acknowledged being understaffed in their SOC environments. Finding qualified people was identified as the main issue within these organizations. Understaffing leads to incidents and breaches going unnoticed for a longer period of time. ...Read more at helpnetsecurity.com

June 16, **Toronto accounting firm hit by ransomware**

Several confidential documents have been confirmed to be stolen from an unnamed Toronto accounting firm, following a ransomware attack. Expense forms, bank credentials and answers to security questions are believed to be part of the data that was accessed and stolen. The data is for sale on a dark website run by the REvil/Sodinokibi threat group. Threat actors that specialize in ransomware attacks now auction off small pieces of data to prove to victims that they have their data, increasing the pressure for ransoms to be paid. ...Read more at itworldcanada.com

June 15, **Expert says Huawei’s cyber risks can’t be mitigated in a 5G network**

There is no way to mitigate the risk that network equipment from Huawei could be used by Chinese intelligence agencies to spy on Canada’s 5G networks, according to cyber expert, Melissa Hathaway, a distinguished fellow at the Centre for International Governance Innovation based in Waterloo, Ontario. In her assessment, 5G networks are primarily about software-defined networks and software code implemented on Huawei equipment lacks secure coding practices which could easily be exploited by state actors. ...Read more at itworldcanada.com

June 15, **PEI government deliberately withheld information on missing emails**

Missing emails are at the centre of a report released by PEI’s privacy commissioner. In March 2015, an employee with Innovation PEI, a provincial Crown corporation noticed that archived emails between June 2010 and April 2012 had been deleted. The deleted emails included five access-to-information requests from two different sources. An investigation was launched after one of the applicants sued the province, alleging breach of contract. Some of the missing emails pertained to a failed online gambling application.... Read more at cbc.ca

June 11, **Qbot banking trojan still up to its old tricks**

Active since 2008, the Qbot malware has been targeting banking institutions around the globe, including some Canadian institutions. The main goal of this malware family is to steal bank account credentials, browsing activity and any other financial information. Financial institutions around the world have been targeted including Scotiabank, TD, Citibank and Capital One. A recently reviewed Qbot campaign showed that the trojan primarily uses browser hijack and web traffic redirection as its main attack techniques. ...Read more at f5.com

Global

June 17, **Petitions demand Zoom changes end-to-end encryption stance**

In early June, Zoom announced that only users that have paid accounts will have end-to-end encryption enabled for their conversations. Zoom CEO, Eric Yuan, claimed the company wanted to work together with law enforcement whenever Zoom was being used for malicious purposes. In response to the announcement, a petition was raised to have encryption enabled on all Zoom products. The petition was signed by over 19,000 users and it argued that encryption is more important now than ever and that they don’t want political activists and protestors to be the target of government surveillance. …Read more at infosecurity-magazine.com

June 17, **Avoid scoring a cyber own goal when Premier League returns**

Excitement is growing as the Premier League is set to return within the week, with millions of fans around the world ready to stream games. The National Cyber Security Centre (NCSC) released an article warning fans to be careful where they watch their streams and how they store their credentials. A previous report shows that approximately 700,000 accounts have been compromised in the past due to easy passwords such as ‘arsenal’, ‘chelsea’ and ‘liverpool’. Additionally the NCSC warns of fake streaming services aimed at stealing financial information… Read more at ncsc.gov.uk

June 16, **Chipmaker MaxLinear hit by Maze ransomware attack**

MaxLinear, a radio-frequency chip maker announced they were hit with a cyberattack. The attackers posted some proprietary information online to prove they had stolen the data, a common tactic to increase ransom payments. The ransomware believed to have hit the MaxLinear operational systems is known as Maze, a common malware whose distributors usually threaten to release all of the victim’s information online if payment is not made. A third party has been called in to help them address the attack… Read more at reuters.com

June 15, **New mobile internet protocol vulnerabilities let hackers target 4G/5G users**

Vulnerabilities in the GPRS Tunnelling Protocol (GTP) used by mobile network operators could allow an attacker to carry out man-in-the-middle attacks, perform fraud or cause a denial-of-service concludes a research paper from cybersecurity firm, Positive Technologies. The research revealed many flaws including the fact that the protocol does not check the geographic location of the traffic, making it difficult to verify the legitimacy. The second notable flaw is with how subscriber credentials are verified, which could allow a threat actor to spoof credentials and read network traffic. …Read more at thehackernews.com

June 15, **Intel adds CPU-level malware protection to Tiger Lake processors**

Intel has announced a new security product that would provide hardware-level protection against malware threats. The product known as Control-Flow Enforcement Technology (Intel CET) will offer protection against malicious control-flow and hijacking attacks on devices installed with Intel's Tiger Lake mobile processors. Intel CET is built into the microarchitecture and will be available on future desktop and server platforms. Intel has worked closely with Microsoft to include support for Intel CET on the Windows 10 OS products…Read more at bleepingcomputer.com

June 12, **Snake ransomware slithering across connected networks**

The same threat group linked to the ransomware attack at Honda has been linked to another attack targeting Enel Argentina, a South American energy company. The Snake ransomware variant used against both companies is significantly more advanced than previous versions. The ransomware is known to target industrial control systems, mostly the systems manufactured by General Electric. The malware was also linked to attacks on Fresenius, Europe's largest private hospital provider in May 2020. …Read more at scmagazineuk.com

June 11, **U.S. intelligence bill takes aim at commercial spyware makers**

Commercial spyware developers, like the NSO Group and the Hacking Team, are the main targets of a new U.S. Senate Intelligence bill. The bill's main intention is to stop spyware tools developed within the U.S. from falling into the hands of unfriendly foreign governments. Government agencies will be required to submit reports to the U.S. Congress on the threats posed by the use cyber intrusion and other surveillance technology against U.S. citizens and residents. The report should also highlight what export controls can be applied to prevent such technologies from getting into the wrong hands. … Read more at techcrunch.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.

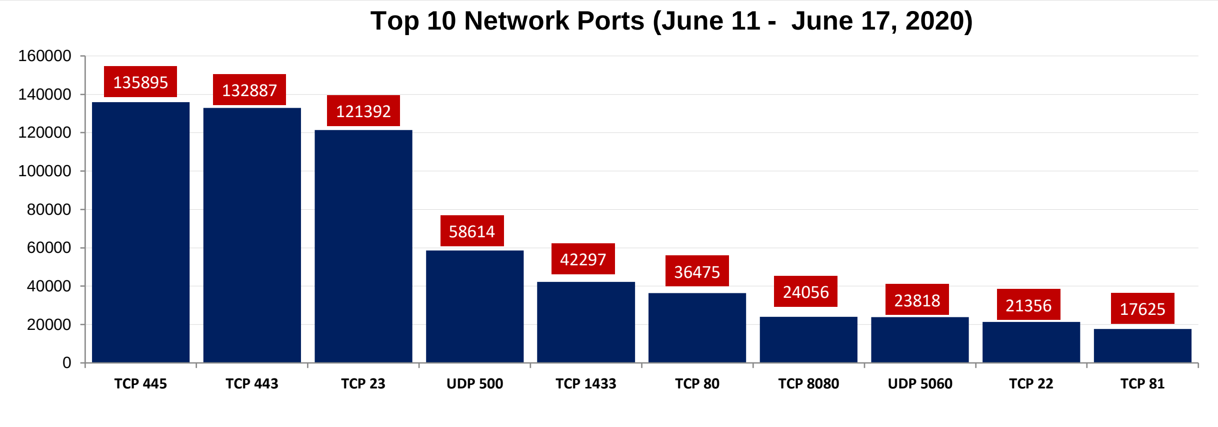

Figure 1: Top 10 Destination Ports (June 11 – June 17, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 445	2	+1 ⬆	2.8% ⬆
2	TCP 443	1	-1 ⬇	-22.7% ⬇
3	TCP 23	3	-	4.0% ⬆
4	UDP 500	4	-	0.6% ⬆
5	TCP 1433	5	-	-5.6% ⬇
6	TCP 80	6	-	0.5% ⬆
7	TCP 8080	7	-	4.0% ⬆
8	UDP 5060	9	+1 ⬆	14.9% ⬆
9	TCP 22	8	-1 ⬇	-1.4% ⬇
10	TCP 81	11	+1 ⬆	-14.5% ⬇

This week's data from our top ten most targeted ports shows an overall decrease in traffic. We observed a large decrease in probe scans to TCP port 443, which is usually the top port targeted. The new #1 is TCP port 445, the port used for the SMB protocol. Many other ports saw minor increases in scans, including TCP port 23, UDP port 500 and TCP port 80. As part of our deeper dive this week, we investigate probe scans targeting UDP port 5060 (a port associated with the SIP protocol). Over the last week, scan probes targeting this port (UDP/5060) recorded an increase of almost 15%.

UDP 5060

Session Initiation Protocol (SIP) is a protocol used by many VoIP providers. Cisco, Siemens, Vonage, Motorola and Polycom have all used SIP and UDP port 5060 in their VoIP phones [1].

On 3 June 2020, Cisco released a security advisory which detailed a new vulnerability (CVE-2020-3226) that affected some of their devices using the SIP protocol [2]. As shown in Figure 2, a few days after the advisory was released the traffic targeting UDP port 5060 increased and has sustained that growth over the two-week period. Vulnerability scanners are still targeting vulnerable Cisco devices. This high risk vulnerability is due to insufficient checks on incoming SIP messages, and this could allow an unauthenticated, remote attacker to create a denial-of-service (DoS) condition [2].

In addition to the June 3 vulnerability, Cisco released an advisory that detailed a vulnerability that could allow and attacker to view sensitive information on affected Cisco IP Phones [3]. The advisory was published on June 17, 2020. Coincidentally June 17 was the day that UDP port 5060 saw the most traffic, within the time period analyzed. Below are the top source hits from our data:

- 192.3.181[.]138 (Colocrossing, U.S.),
- 193.203.14[.]130 (Dedipath, U.S.),
- 51.91.75[.]22 (OVH, France),
- 109.236.60[.]42 (Dedipath, U.S.).

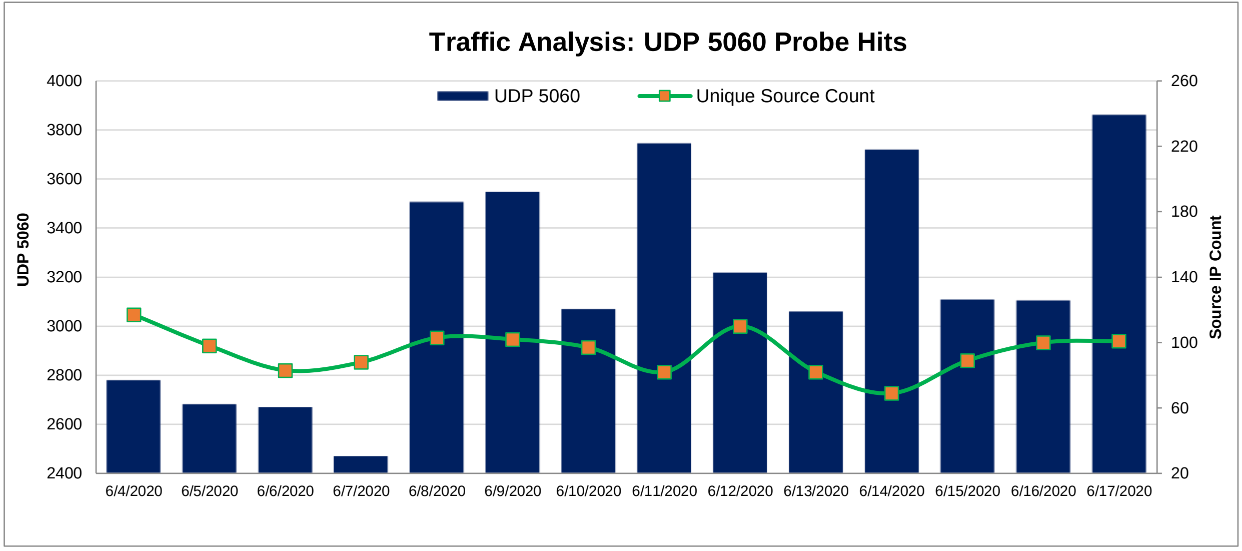

Figure 2: UDP Port 5060 Analysis (June 4 – June 17, 2020)

References

[1] Port 5060 Details - https://www.speedguide.net/port.php?port=5060

[2] Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sip-Cv28sQw2

[3] Cisco IP Phones Call Log Information Disclosure Vulnerability - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-logs-2O7f7ExM