Weekly Summary Activity Report – June 12th, 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 9, **Canada's Fitness Depot suffers Magecart style attack**

Security Boulevard published a report that one of Canada's largest fitness equipment suppliers, Fitness Depot, suffered a Magecart style attack. Information released shows that a malicious web form was embedded on the company's website on February 18, 2020 and was active until May 22, 2020 when Fitness Depot was informed of the issue. As soon as the injected form was discovered the e-commerce section of the website was shut down and investigation commenced. According to early statements from the company, they do not believe any customer data was stolen, but they do encourage customers to come forward if they believe their information was compromised... Read more at securityboulevard.com

June 8, **Study shows Canadian organizations are behind on risk analysis**

A report conducted by Ernst and Young (EY) cybersecurity found that 34% of Canadian organizations have yet to fully evaluate the cybersecurity risks they face, compared to 16% of organizations globally. With the sudden shift to more remote work, organizations have fallen behind on understanding and mitigating the risks of their workforce working from home. The report stresses the need for cybersecurity professionals to communicate in a manner that their organization's board understands.... Read more at canadiansecuritymag.com

June 5, **How COVID-19 is accelerating digital transformation for three Canadian CISOs**

At a webinar organized by Palo Alto Networks, which included representatives from RBC, Finning International and Toronto's Hospital for Sick Kids, the talk focused on technical changes and challenges due to the current pandemic. The panel agreed that the pandemic has forced digital transformation and that some of the changes will likely continue to be regular practice. Toronto Hospital for Sick Kids said that. being a specialized hospital, many patients would travel for up to two hours for a visit. Video conferencing methods for shorter appointments has proved to be an effective and efficient solution.... Read more at itworldcanada.com

June 3, **Notice of cyber incident involving the CPA Canada website**

The Chartered Professional Accountants (CPA) of Canada released a notice on their website detailing an unauthorised access to account information that stemmed from a possible targeted email phishing attempt. Immediate steps were taken to secure data that was accessed, and the incident was reported to the Canadian Anti-Fraud Centre, as well as other appropriate privacy

authorities. The incident took place April 24, 2020. All CPA Canada members were notified of the incident... Read more at cpacanada.ca

Global

June 10, **Slovak police seize wiretapping devices connected to government network**

Authorities in Slovakia have arrested four suspects after launching an investigation into a series of suspicious devices found connected to the government's network. The devices were connected to GOVNET, a network that connects Slovakian government agencies. The devices were removed from the networks of law enforcement agencies and the judiciary. Two of the suspects arrested were high-ranking officials within the National Network and Electronic Services Agency, one worked in the office of the Deputy Prime Minister and the fourth worked in the private sector… Read more at zdnet.com

June 10, **U.S. officials ask Juniper Networks about investigation into 2015 backdoor**

Security Week reported that more than a dozen U.S. officials have sent a letter to Juniper Networks asking for an update on the unauthorized code investigation that began in late 2015. In some versions of Juniper's ScreenOS unauthorized code was discovered, which led to two vulnerabilities being present within the company's firewalls. The Senators and Congressmen are asking the company to reveal what their investigation results, giving the company one month to reply before further actions are taken. … Read more at securityweek.com

June 8, **How to protect your vote**

Researchers from Massachusetts Institute of Technology (MIT) and University of Michigan have released a report on their analysis of a voting system set to be used in the upcoming US Presidential elections. The electronic voting system called OmniBallot, has been deployed in Delaware, West Virginia and other jurisdictions. The system was determined to be vulnerable, allowing an individual's vote to be exposed or manipulated while in transmission. As a result, the researchers recommend that ballots not be submitted by an electronic means and suggest that voting by mail was the safest option, after voting in person. … Read more at mit.edu

June 4, **Trump, Biden campaign staffers targeted by APT phishing emails**

Threat Post reported on tweets from Google's Threat Analysis group regarding two separate phishing campaigns that have targeted staffers working on the presidential campaigns of Donald Trump and Joe Biden. The campaign targeting the Biden campaign was credited to a China-linked APT group, while the campaign sent to Trump staffers was credited to an Iranian-linked APT group. The timeline and scale of the campaigns are unknown, but these types of attacks are expected to grow as the November 3, 2020 election draws closer... 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.

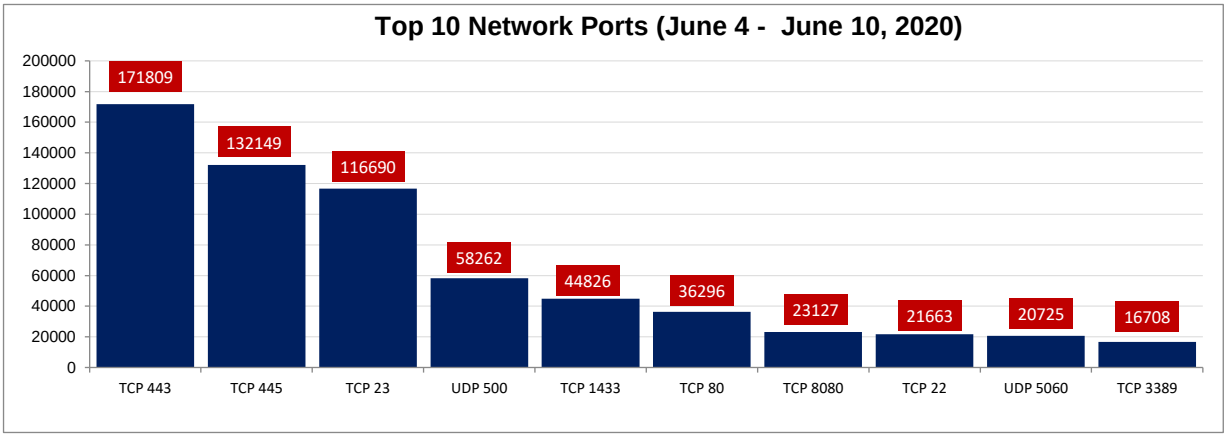

Figure 1: Top 10 Destination Ports (June 4 – June 10, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 443	1	-	16.9% ↑
2	TCP 445	2	1 ↑	9.7% ↑
3	TCP 23	3	1 ↓	-4.3% ↓
4	UDP 500	4	-	-0.1% ↓
5	TCP 1433	5	-	21.7% ↑
6	TCP 80	6	-	-1.5% ↓
7	TCP 8080	7	2 ↑	34.8% ↑
8	TCP 22	8	1 ↓	2.3% ↑
9	UDP 5060	9	1 ↓	0.6% ↑
10	TCP 3389	10	-	6.7% ↑

This week's data from our top ten most targeted ports shows an upward trend in all ports except for three. We observed an increase in scan volumes across all the major ports except traffic to TCP port 23, UDP port 500 and TCP port 80, which decreased by 4.3%, 0.1% and 1.5% respectively. As part of our deeper dive this week, we investigate probe scans targeting TCP port 1433 (a port associated with MSSQL servers). Recently, scan probes targeting this port (TCP/1433) have shown an increase of over 20%.

TLP-GREEN

TCP 1433

TCP port 1433 is the default port associated with Microsoft SQL server communications. Microsoft SQL servers could be installed with other Microsoft applications and therefore could be installed on a system without a user's knowledge. This would mean that the default credentials for access could still be in use. Making the SQL server a huge target for threat actors.

An active botnet campaign has been targeting this port for two years, trying to spread a cryptomining malware. A report on KingMiner, the botnet in question, was published earlier this week, on June 9, 2020 [1]. As shown in Figure 2, the day of the report, was the day that TCP port 1433 was probed the most in the last two weeks.

The commonality of MS SQL servers has always made them a target, but the recent campaigns have shown how vulnerable they can be. Not just to gain access to a system, but also to carry out the attacks. Due to how the servers communicate they can also be used to spread the malware, not just be the infection site. Below are the top hits from our data:

- 61.163.192.28 (Unicom, China),
- 83.97.20.31 (OvO Systems, Romania),
- 87.251.74.18 (xWeb Ltd, Netherlands),
- 202.79.173.146 (RackIP, Hong Kong).

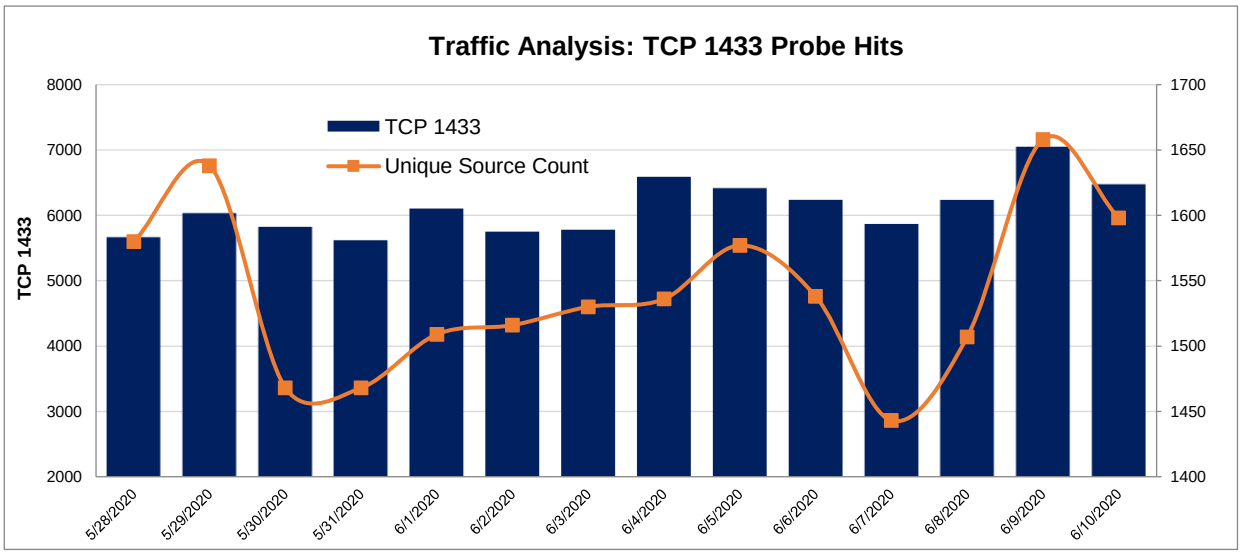

Figure 2: TCP Port 1433 Analysis (May 28 – June 10, 2020)

References

[1] KingMiner Botnet Brute-Froces MSSQL Databases to Install Cryptocurrency Miner - https://www.zdnet.com/article/kingminer-botnet-brute-forces-mssql-databases-to-install-cryptocurrency-miner/

TLP-GREEN

TLP-GREEN