Weekly Summary Activity Report – July 10th, 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

July 7, **Royal Military College weighs damage after cybersecurity attack**

Canadian military colleges suffered a cyberattack which led them to shut down their e-mail systems. The government agencies did not reveal or comment on anything related to the cyberattack. It's undetermined what type of data breach is under investigation by the RMC and if it involves loss of personal data, research or intellectual property. Read more at headtopics.com

July 5, **Stay alert for common COVID-19 scams, says RCMP**

The RCMP issued a warning for the public to stay vigilant about COVID-19 related scams as the country is starting to reopen. COVID-19 is presenting cybercriminals an opportunity to lure people through CERB applications, door to door sales, and return to work strategies. People who have any information related to scams are asked to report them to the Canadian Anti-Fraud Centre at info@antifraudcentre.ca. Read more at nsnews.com

July 2, **Nanaimo RCMP issues warning about scam phone calls**

The Nanaimo RCMP and other Vancouver Island jurisdictions are warning the public about a spike in fraudulent calls. Over the past month, the Nanaimo RCMP detachment has received over 50 complaints per day related to phone scams. Multiple people have been victimized by phone scams causing them to lose several thousand dollars. Most of these scammers were impersonating government agencies, such as Canada Revenue Agency and Service Canada. Read more at vancouverislandfreedaily.com

July 2, **Data breach at Canadian insurance firm exposes personal information**

The Heartland Farm Mutual insurance firm suffered a data breach that resulted in some of their client's personal information being leaked. Heartland Farm Mutual is a Canadian firm that provides insurance for agriculture businesses within Canada. The firm did not reveal when the data breach took place, however they stated that the incident did not affect a high number of clients. The company reacted to the incident immediately by blocking the unauthorized access and employing an external cybersecurity team to investigate. Read more at portswigger.net

Global

July 8, **Criminals auction off stolen domain admin credentials for up to £95k.**

Cybercriminals are selling about 15 billion stolen domain admin login credentials over the dark web for up to £95,000. According to Digital Shadows security experts, the stolen credentials equate to approximately two login details for every human on the planet. Five billion out of the 15 billion stolen login credentials are said to be unique. Read more at theregister.com

July 8, **Fxmsp hacker indicted by feds for selling backdoor access to hundreds of companies**

Fxmsp, a 37 year old hacker fromKazakhstan, is believed to be behind a criminal enterprise selling backdoor access to hundreds of companies across the globe. The hacker was indicted by the US Department of Justice (DoJ) and charged for running a hacking enterprise victimizing hundreds of people on six continents. Read more at zdnet.com

July 7, **Russian BEC gang targets hundreds of multinational companies**

Agari security analysts recently discovered a Russia-based business email compromise group that has been targeting hundreds of multinational corporations in over 40 different countries since 2019. The cybercriminal group is called Cosmic Lynx which uses highly sophisticated methodologies targeting companies that lack security protections and authentication checks. Read more at databreachtoday.com

July 5, **Purple Fox EK adds exploits for CVE-2020-0674 and CVE-2019-1458 to its arsenal**

According to Proofpoint security researchers, the Purple Fox exploit kit appears to have been built to replace the RIG exploit kit for the distribution of the Purple Fox malware. The Purple Fox fileless downloader component was recently modernized to include attack vectors which are targeting two new vulnerabilities to access networks. Read more at proofpoint.com

July 2, **Sixteen Facebook apps caught secretly sharing data with third-parties**

According to an academic study conducted by the University of Iowa, sixteen Facebook apps were identified to be secretly sharing user data with third-parties. The researchers used honeytokens, which are unique email addresses, to register Facebook accounts and then monitor the honeytoken email inbox for new traffic. If the inbox received new email messages from unknown sources, it was clear that the app shared the user's data with third-parties. Read more at zdnet.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.

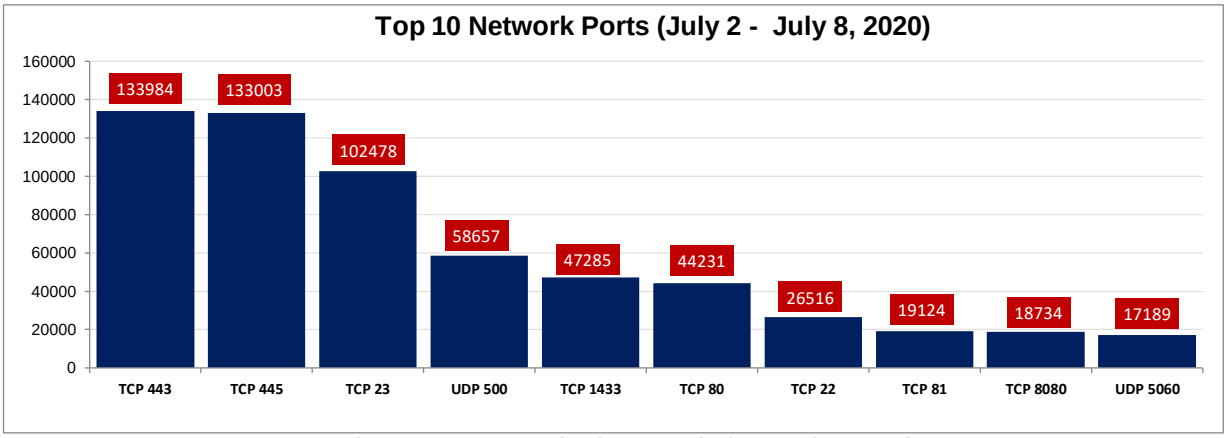

Figure 1: Top 10 Destination Ports (July 2 – July 8, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 443	2	+1	3.0%
2	TCP 445	1	-1	1.0%
3	TCP 23	3	-	-10.0%
4	UDP 500	4	-	-0.03%
5	TCP 1433	5	-	13.0%
6	TCP 80	6	-	9.0%
7	TCP 22	7	-	-6.0%
8	TCP 81	10	+2	9.0%
9	TCP 8080	8	-1	-13.0%
10	UDP 5060	9	-1	-17.0%

This week's data from our top ten most targeted ports show a decrease in scan volume. We observed the largest increase in probe scans in the traffic targeting TCP port 1433 (MSSQL), TCP port 80 (HTTP) and TCP port 81 as well as large decreases in traffic targeting TCP port 23 (Telnet), TCP port 8080 and UDP port 5060 (SIP). Our sensors recorded a drop of approximately 1% in overall traffic. As part of our deeper dive for this week, we investigate the increase in probe scans targeting TCP port 443, a port associated with the HTTPS protocol.

TCP 443

TCP port 443 is associated with HTTPS and is intended for secure web browsing traffic. This port sees a lot of traffic weekly, however this week TCP port 443 is centre stage due to a vulnerability that was discovered and exploited over the past week.

On 30 June 2020, F5 released a vulnerability notice detailing a vulnerability that was discovered in multiple F5 products [1]. The user interface of the devices run on TCP port 443. At the time of the release, a scan revealed 8,000 F5 devices that were vulnerable to the flaw identified as CVE-2020-5902. This remote code execution vulnerability can give an attacker full control of the F5 product. Some products had a patch available on June 30, while others were able to patch on July 9. Shortly following the notice, a proof of concept exploit was posted on GitHub that could have been used to allow any attacker to start exploiting this vulnerability [2].

Below are the top source hits from our data:

- 66.46.77[.]194 (Allstream, Canada),
- 184.150.224[.]4 (Bell, Canada)
- 159.18.26[.]96 (Allstream, Canada)
- 35.173.107[.]231 (Amazon, USA)

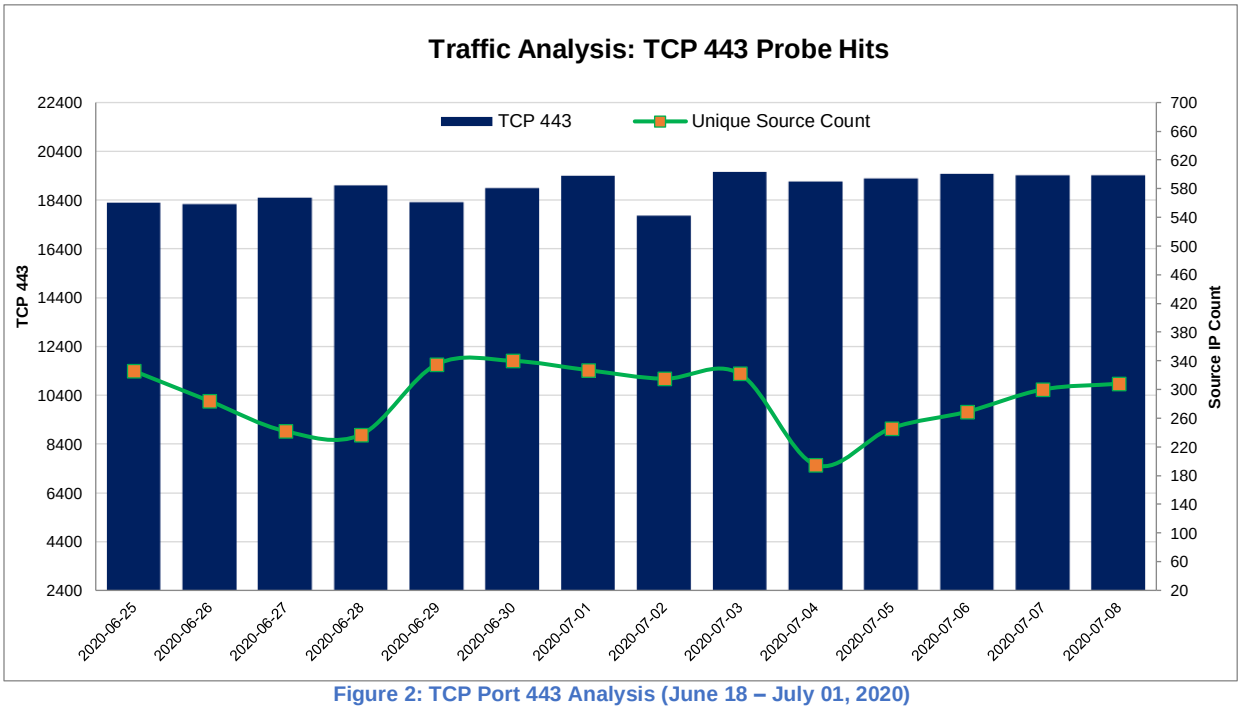

Figure 2: TCP Port 443 Analysis (June 18 – July 01, 2020)

References

[1] K52145254: TMUI RCE Vulnerability CVE-2020-5902 - https://support.f5.com/csp/article/K52145254

[2] Hackers Start Exploiting Recently Patched BIG-IP Vulnerability - https://www.securityweek.com/hackers-start-exploiting-recently-patched-big-ip-vulnerability