Weekly Summary Activity Report – May 1st, 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

April 28, **House of Commons meeting virtually on a platform described as a 'gold rush for cyber spies'**

CBC published an article about Canada's House of Commons reconvening for a virtual meeting on Zoom's videoconferencing platform, and how it could present opportunities for cyber spies. According to researchers from University of Toronto's Citizen Lab, Zoom did not implement true end to end encryption and theoretically could decrypt and monitor calls. To address some of the security concerns, the House of Commons will be using a reconfigured version of Zoom with security features different from free and standard paid consumer versions. Read more at cbc.ca

April 28, **Cyberattack behind Manitoba beer shortages**

Global News published a report suggesting that a cyber attack at Brewers Distributor Ltd. (BDL) is behind the shortage of beer products across popular brands in Western Canada. The cyber attack took place last month and forced the company to run its operations and process orders manually. These challenges have led to many local vendors running low on supplies and deliveries being behind schedule. Read more at globalnews.ca

April 26, **Kaspersky report: Nearly half of employees don't know how to respond to ransomware attacks**

IT World Canada published a report about a recent study by Kaspersky Labs, where they discovered that 45% of the employees within Canada and U.S. do not know how to respond to a ransomware attack. Thirty-seven percent of the respondents do not know what a ransomware attack is. According to the survey results, nearly 40 per cent of the respondents believe that companies should pay ransom to retrieve their personal data. And yet, 67 per cent of the respondents stated they would outright refuse to pay a ransom if they were a victim. Read more at itworldcanada.com

April 21, **Canadian accounting firm MNP gets hit by cyberattack**

Insurance Business Canada published a story about the ransomware attack which impacted MNP, a major accounting firm in Canada. According to the initial reports published by Bleeping Computer, the attack was discovered on 5 April 2020 and it forced the firm to shut down their systems to limit the spread of the malware. Read more at insurancebusinessmag.com

Global

April 29, **High-severity Cisco IOS XE flaw threatens SD-WAN routers**

Threat post published an article detailing a high severity vulnerability within Cisco IOS XE, which may allow an attacker to execute arbitrary commands with root privileges. Cisco IOS XE is a Linux-based version of Cisco Internetworking Operating System (IOS) which is used in Cisco software-defined wide area network (SD-WAN) routers. The flaw exists in the command line interface (CLI) utility of Cisco IOX XE, used to configure the network device. Read more at threatpost.com

April 29, **445 million attacks detected since the beginning of 2020, COVID-19 wreaks havoc**

HelpNet Security blog published a report related to the rapid increase in cases of transaction fraud and abuse attempts. According to Arkose Labs security analysts, in the first quarter of 2020, their network recorded a 20% increase in transaction frauds over the previous quarter. Over twenty-six percent of all transactions recorded on their network were fraudulent. The global pandemic crisis presented cybercriminals more opportunities to seek to financially exploit people. Read more at helpnetsecurity.com

April 27, **Attackers exploiting a zero-day in Sophos firewalls, have yours been hit?**

HelpNet Security blog published an article with details of the exploitation of the zero-day SQL injection vulnerability within Sophos XG Firewalls which allowed the attackers to perform remote code execution. Sophos' security experts identified the flaw on April 22nd, in which the attack targeted physical and virtual XG Firewall units. The attack utilized several Linux Shell scripts that downloaded ELF binary executable malware. The malware is designed to collect details of public IP address, its license key, firewall users along with firmware version, CPU type, and so much more. Read more at helpnetsecurity.com

April 27, **Single malicious GIF opened Microsoft teams to nasty attack**

Threat post published an article detailing a vulnerability within Microsoft Teams which may allow an inside attacker to leak data and steal Teams account information of a target organization by weaponizing a single GIF image. The attack involves malicious actors being able to abuse a JSON Web Token ("authtoken") and a second "skype token". The flaw is within the application programming interfaces (APIs) which are used to conduct communication among the servers and services. 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 events observed on CCTX sensors for the last week.

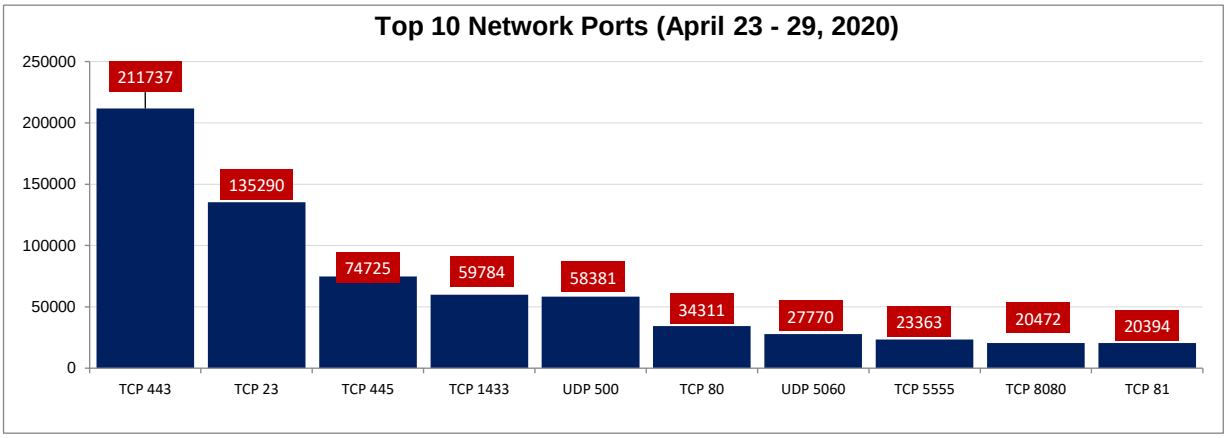

Figure 1: Top 10 Destination Ports (April 23 - 29, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 443	1	-	-7.9%
2	TCP 23	2	-	6.9%
3	TCP 445	4	+1	25.3%
4	TCP 1443	3	-1	-0.4%
5	UDP 500	5	-	0.1%
6	TCP 80	6	-	-4.9%
7	UDP 5060	7	-	8.5%
8	TCP 5555	9	+1	1.5%
9	TCP 8080	12	+3	9.2%
10	TCP 81	13	+3	32.1%

This week's analysis of the top 10 network probe ports is presented in Table 1 and it shows no significant changes among the top 10 most commonly targeted ports. We observed double-digit percentage increases in the volume of traffic targeting TCP/445 and TCP/81. We provide an in-depth analysis of traffic directed towards TCP/445.

TCP 445

On April 28th and 29th, CCTX SOC observed a moderate increase in network scans targeting TCP port 445 on our IDS sensors. Our analysis of the traffic as shown in Figure 2 reveal that this increase is likely as a result of malware-controlled bots scanning for internet-exposed Server Message Block (SMB) services. We assess that these scanning activities are likely related to the recent Microsoft vulnerability affecting SMB version 3. On March 12, 2020, Microsoft released a security advisory (CVE-2020-0796) for a critical remote code execution vulnerability [1] in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests. Threat researchers have since released proof of concept (PoC) code which could be used to identify vulnerable installations on the internet [2]. The following are source IP addresses observed as the top talkers targeting TCP/445 on our sensors: 45.148.10.141, 67.213.210.23, 178.236.136.33 and 80.82.77.240.

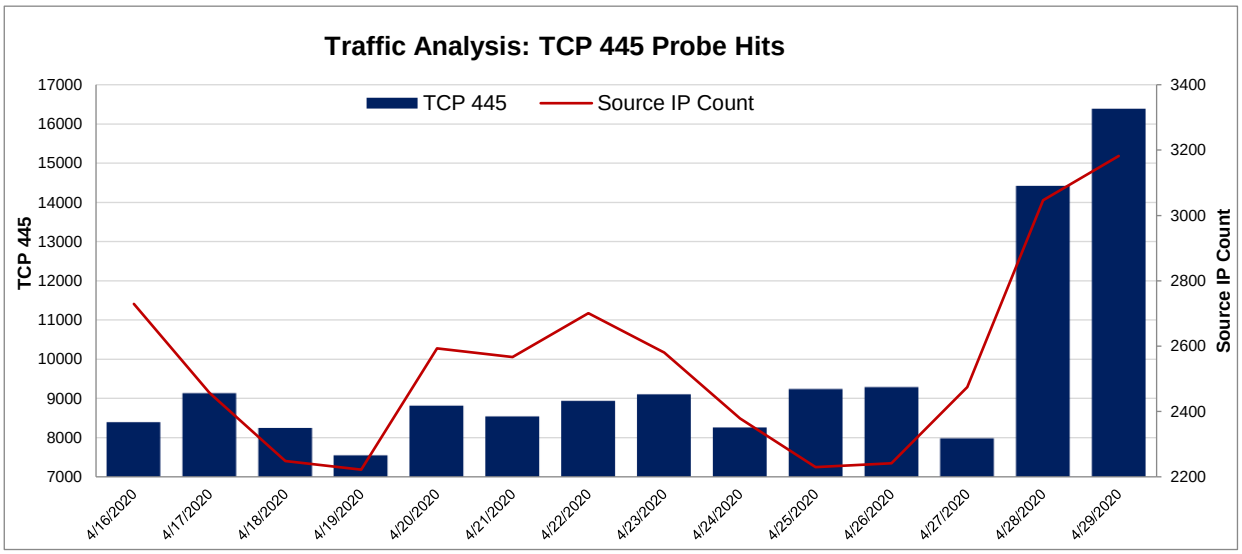

Figure 2: TCP Port 445 Analysis (April 23 – 29, 2020)

References

[1] Windows SMBv3 Client/Server Remote Code Execution Vulnerability (CVE-2020-0796) - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

[2] CVE-2020–0796 Windows SMBv3 LPE Exploit POC Analysis - https://medium.com/@knownsec404team/cve-2020-0796-windows-smbv3-lpe-exploit-poc-analysis-c77569124c87