Canadian Cyber Threat Exchange
Informing Canadian Business

Échange canadien de menaces cybernétiques
Informer les entreprises canadiennes

Weekly Summary Activity Report – April 24, 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 20, **Facebook takes Canada's privacy czar to court over personal data probe**

Canadian Security Magazine published an article about Facebook's court case against Canada's federal privacy watchdog, requesting a judge to dismiss a finding that its lax practices allowed personal data to be used for political purposes. An investigation report from the federal privacy agency cited major shortcomings in Facebook's procedures and called for stronger laws to protect Canadians. Facebook shared data retrieved from its app known as "This is Your Digital Life" which encouraged users to perform a personality quiz. Recipients of the information included Cambridge Analytica, the firm that was involved in U.S political campaigns. Over 600,000 Canadians downloaded the app. Read more at canadiansecuritymag.com

April 20, **Gorgon uses COVID-19 outbreak to launch cyber attacks on Canada and other regions**

Security researchers from 360 Total Security published a blog on recent attacks attributed to the Gorgon APT organization targeting Canadians using COVID-19 themed lures. The South Asian Gorgon APT cybercriminal group is spreading malicious email attachments masquerading as emails sent by the Canadian government. The title of the attachment in the phishing email was "CVOID19Relief.docx" and the text content is related to the Coronavirus relief response. Once the victim clicks on the attachment, it runs a malicious macro code which downloads a malware loader that executes PowerShell. Read more at 360totalsecurity.com

Global

April 22, **Zero-Day Warning: It's Possible to Hack iPhones Just by Sending Emails**

The hacker news published a report detailing vulnerabilities within iPhones and iPads which may allow a remote attacker to secretly take control over the Apple device by sending an email to a target victim with his account logged into the vulnerable app. According to the cybersecurity experts at ZecOps, the vulnerabilities are remote code execution flaws that are located within the MIME library of the Apple mail app. The flaws have existed for 8 (eight) years, since the release of iOS6 and it affects the current iOS release 13.4.1 with no patch available yet. Read more at thehackernews.com

April 21, **Phishing campaign aims to steal Zoom credentials using fake layoff notifications**

SC Magazine published a news report detailing a phishing campaign using fake layoff notifications to steal Zoom credentials. The phishing campaign targets Office 365 users masquerading as a reminder that the recipient has a meeting with HR for termination. The campaign attempts to trick email recipients into thinking they are getting laid off due to the Coronavirus pandemic. The link within the email leads to a malicious page hosted at zoom-emergency.myftp[.]org. Read more at scmagazine.com

April 20, **COVID-Themed Lures Target SCADA Sectors with Data Stealing Malware**

The Hacker News published a report about a new Coronavirus themed malware campaign discovered by Cisco Talos security experts. According to Cisco Talos security researchers, the malware campaign is targeting Azerbaijan government and energy sectors delivering a remote access trojan (RAT) that exfiltrate sensitive documents, keystrokes, passwords and even images from the webcam. The attack deploys a Python-based RAT dubbed "PoetRAT" which specifically targets supervisory control and data acquisition (SCADA) systems in the energy industry, such as wind turbine systems. Read more at thehackernews.com

April 20, **Hackers Raid Crypto Firms in $25m Attacks**

Infosecurity magazine published an article about cybercriminals making at least $25m from re-entry attack from two crypto currency firms. The raids affected Lendf.me and crypto exchange Uniswap platforms. The cybercriminals exploited a vulnerability within Uniswap in combination with the ERC777 token standard. A re-entry attack allows attackers to continuously withdraw digital funds without being challenged until the status of the initial transaction changes. Read more at infosecurity-magazine.com

April 17, **Clipboard Hijacking Malware Found in 725 Ruby Libraries**

ZDNet published a report about the discovery of over 700 malicious ruby libraries within the RubyGems repository used to hijack users' clipboards. According to the report, the malicious libraries were discovered by ReversingLabs security experts. All the ruby libraries were copies of legitimate libraries including additional malicious files. The libraries were uploaded to the repository between February 16 and 25, but they were removed two days later. According to ReversingLabs security officials, the libraries were downloaded by thousands of users, nevertheless the cybercriminals have not been able to hijack any payments. 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 events observed on CCTX sensors for the last week.

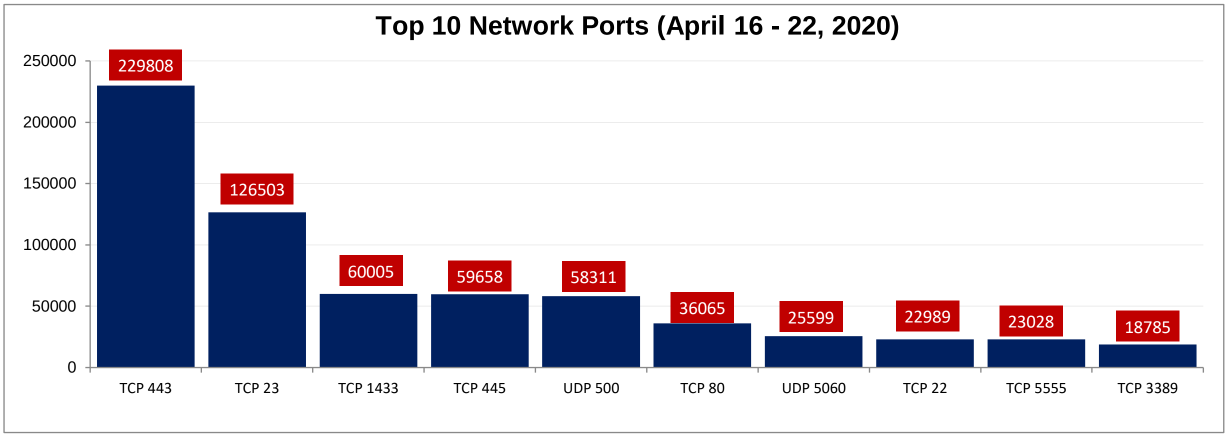

Figure 1: Top 10 Destination Ports (April 16 - 22, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	**Port Number**	**Previous Week Ranking**	**Ranking Change (+/-)**	**% Probe Volume Change (+/-)**
1	TCP 443	1	-	-1.0%
2	TCP 23	2	-	-24.7%
3	TCP 1433	4	+1	7.5%
4	TCP 445	5	+1	11.9%
5	TCP 80	3	-2	-49.5%
6	UDP 5060	6	-	-5.8%
7	TCP 5555	7	-	-14.9%
8	TCP 22	11	+3	31.8%
9	TCP 3389	9	-	-12.2%
10	TCP 8080	10	-	-2.0%
11	TCP 8291	119	+108	1,414.5%

This week's analysis of the top 10 network probe ports as displayed in Table 1 reveal several minor changes across the most commonly targeted ports. We observed decreases in traffic targeting TCP/443, TCP/23 and TCP/80, while TCP/22 increased by 31%. However, the week's most significant development was outside the top 10 as observed with the spike in network traffic scans targeting port TCP/8291. On our sensors, we observed a spike in traffic by over

1,414% which could indicate attacker interest in identifying exposed services running on TCP/8291. We provide an in-depth analysis of this spike in section below.

TCP 8291

Beginning April 20th, CCTX SOC observed a spike in network probes targeting TCP port 8291 on our IDS sensors. TCP port 8291 is a default port used on MikroTik RouterOS Winbox devices. Our network telemetry data show over 1,400% increase in scans to TCP port 8291 over metrics observed from the previous week. As shown in Figure 2, this spike was observed between 20th and 22nd April 2020. We were unable to determine which group is behind these scans but they may be related to a new or existing botnet trying to exploit MikroTik RouterOS vulnerabilities. On January 14th, Tenable released a security advisory addressing a man-in-the-middle vulnerability (CVE-2019-3981) that exploits the MikroTik RouterOS WinBox interface on TCP port 8291. An attacker can use this vulnerability to steal credentials. [1] On 17th April, Mikrotik released a new version of Winbox software (version 3.23) and based on comments from its user forum, some users are reporting several old issues were not addressed in the new update. Mikrotik is usually setup via Winbox (TCP/8291) and their proprietary closed source config utility, even though http/ssh config is also possible. [2] The default password is blank which could potentially expose devices with the default mode settings. The following source IP addresses were detected with the highest hits: 62.173.145.203 (Russia), 171.236.41.130 (Vietnam), 102.69.227.81 (Kenya), 161.142.229.218 (Malaysia), 80.82.77.33 (Netherlands), 94.102.49.193 (Netherlands), 71.6.199.23 (United States), 185.142.239.16 (Netherlands) and 71.6.135.131 (United States).

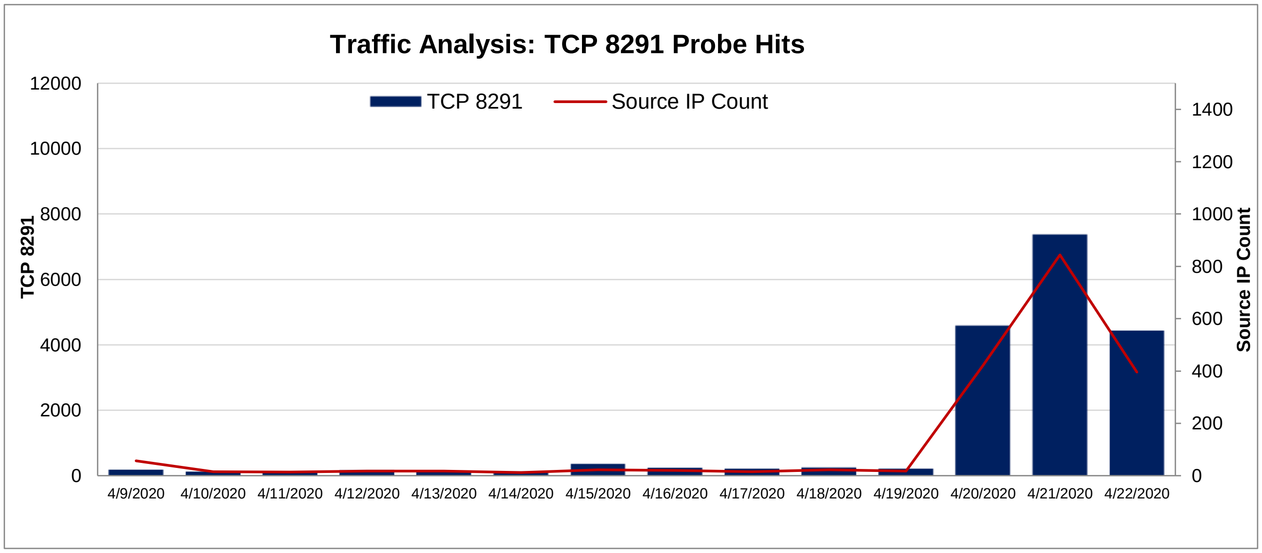

Figure 2: TCP Port 8291 Analysis (April 16 – 22, 2020)

References

[1] MikroTik WinBox Man-in-the-Middle Password Hash Disclosure - https://www.tenable.com/security/research/tra-2020-01

[2] MikroTik Forum Discussions - https://forum.mikrotik.com/viewtopic.php?f=21&t=160050&p=788210&hilit=Winbox#p788210