Canadian Cyber Threat Exchange
Informing Canadian Business

Échange canadien de menaces cybernétiques
Informer les entreprises canadiennes

Weekly Summary Activity Report – April 9, 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 7, **Zoom's video conferencing security issues**
CBC published an article about Taiwanese government officials announcing a ban on the use of Zoom due to reported issues linked to the platform's security and privacy policies. Canadian officials had previously issued a similar warning to all government agencies and staff stating "the security aspects of Zoom have not been assessed by the Canadian Centre for Cyber Security (Cyber Centre), and it has not been approved for any government discussions that require secure communications". Zoom's video conferencing platform is facing security issues as many users are worried about the lack of end to end encryption and the rise in zoom-bombing attacks. Read more at cbc.ca

April 7, **Cyber attack on a Canadian University**
London Free Press published an article about an Israeli threat intelligence firm's report stating that a Canadian University's network could be at risk from a cyber attack. According to the Israeli firm, a threat actor on the Russian dark web advertised for sale administrative access credentials to the network domain of the unnamed Canadian university. According to the post on the dark web, the hacker has access to two domain users and can connect and maintain access from an external machine through a non-standard port. The threat intelligence company stated the post was very detailed and considers it a valid threat. Read more at lfpress.com

April 6, **Facial recognition and data privacy**
Reuters published a news report that plans by a Canadian real estate firm to use facial scans to access buildings have sparked criticism from data privacy groups. According to the real estate firm, facial scans will help keep tenants safe by not allowing unauthorized access to their buildings. However, privacy activists consider the plan an invasion of privacy and underscores the need to modernize Canada's laws on the collection and use of personal information. Read more at reuters.com

Global

April 8, **(CVE-2020-0688) 315,000+ vulnerable on-premise Exchange servers**
HelpNet published a news article on the analysis of an internet-wide scan performed by Rapid7 security researchers which identified at least 315,000 vulnerable on-premise Exchange servers. According to Rapid7, cybercriminals are looking to exploit the Microsoft Exchange vulnerability (CVE-2020-0688) which was rated as critical. The security researchers discovered over 31,000 Microsoft Exchange 2010 server installations that have not been updated since 2012 as well as

10,731 Microsoft Exchange 2007 servers that are no longer supported. One notable reason that would make the exploitation of (CVE-2020-0688) vulnerability tough to exploit is that attackers are required to have compromised valid email credentials to access the server. Read more at helpnetsecurity.com

April 7, **INTERPOL warns of increased COVID-19 ransomware attacks on hospitals**
Infosecurity published a story about the international criminal police organization (INTERPOL) issuing an alert about the high risk of ransomware attacks on hospitals and other healthcare facilities as they battle the Coronavirus pandemic. As the Coronavirus pandemic continues, cybercriminals are taking advantage of the crisis to attack healthcare organizations. The law enforcement organization has issued a notice to 194 member countries highlighting the scale of the threat. Spoofed phishing emails as if sent from a trusted government source are the main threat vector. Read more at infosecurity.ca

April 7, **BlackBerry analysts discover APT on Linux servers**
Techrepublic published a report about a Chinese hacker targeting Linux servers with weak security measures. According to the analsysis conducted by BlackBerry, Chinese cybercriminal groups (APT) have been using remote access trojans to exploit a network component on Linux servers. Five APT groups working with the Chinese government are targeting Ubuntu Linux environments as well as Red Hat Enterprise and CentOS servers for espionage and intellectual property theft purposes. The hackers appear to be using WINNTI-style tooling to secretly control the Linux servers and to remain undetected. Read more at techrepublic.com

April 6, **200 VPN servers and 174 servers connected to Chinese government networks hacked**
ZDNet published an article related to DarkHotel hackers utilizing a VPN zero-day vulnerability to breach Chinese government agencies. According to Qihoo 360 security researchers, during the last month a state-sponsored cybercriminal group have established a hacking operation targeting Chinese government agencies along with their employees. The intrusion exploited a zero-day vulnerability within Sangfor SSL VPN servers that are used to provide access to enterprise and government networks. According to Qihoo, the threat actor hacked over 200 VPN servers and 174 servers connected to Chinese government networks. 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 as observed on our sensors 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.

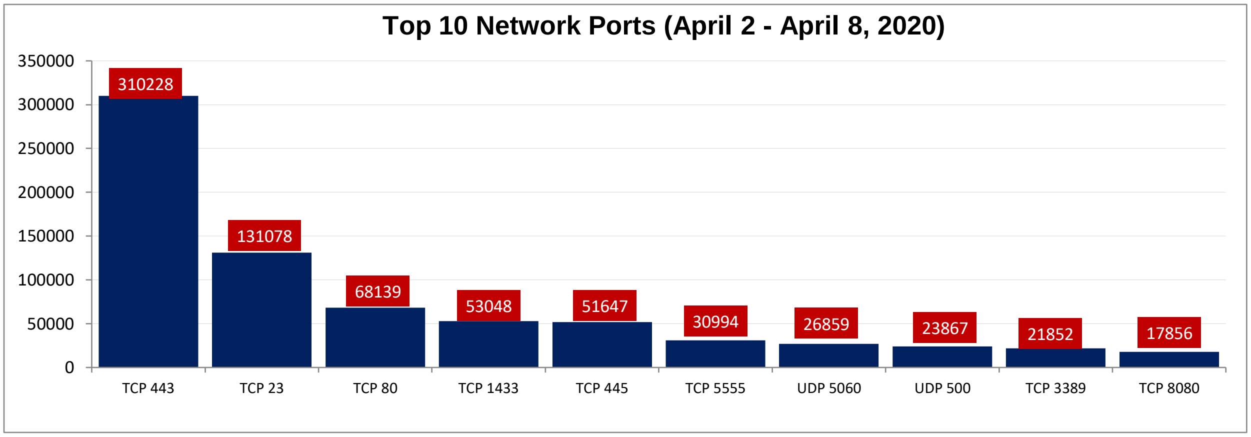

Figure 1: Top 10 Destination Ports (April 2 - April 8, 2020)

Table 1: Top 10 Network Probe Activity Report

Rank	Port Number	Previous Week Ranking	Ranking Change (+/-)	% Probe Volume Change (+/-)
1	TCP 443	1	-	74.5%
2	TCP 23	2	-	-11.8%
3	TCP 80	3	-	11.2%
4	TCP 1433	6	+2	10.6%
5	TCP 445	5	-	5.1%
6	TCP 5555	7	+1	6.7%
7	UDP 5060	8	-1	2.1%
8	UDP 500	4	-4	-59.4%
9	TCP 3389	9	-	6.4%
10	TCP 8080	11	+1	3.6%

Reviewing the summary data as shown in Table 1, we observed an increase in scanning traffic targeting many ports which may indicate threat actors showing more interest in identifying open ports associated with web application services. Ports TCP/443, TCP/80 and TCP/1433 recorded scanning increases by about 75%, 11% and 11% respectively. This increased interest may indicate a shift in attacker focus away from targeting remote working services observed in the previous weeks, to vulnerabilities present in exposed web server applications.

TCP 443

Our sensors detected a significant increase in attack traffic targeting TCP Port 443 as shown in both Table 1 and Figure 2. We recorded a 74.5% increase in scanning traffic targeting TCP/443 over the previous week. Similar increases were also observed across many other web service ports which may suggest threat actor activity pivoting to target vulnerable web applications. Considering the infrastructure challenges many organizations are facing with respect to the COVID-19 lockdowns, many IT teams are stretched and are experiencing difficulties to adequately secure their web service applications. As shown in Figure 2, beginning March 29, we observed a spike in unique source IP addresses targeting port TCP/443. This is typically associated with botnet activity potentially launching a Distributed Denial of Service (DDoS) attack. We observed over 7,600 unique IP addresses scan our networks for open access to TCP port 443. Since then, we have seen a steady increase in activity but for fewer sources. We recorded our highest number of traffic hits on April 7. According to additional OSINT analysis, these activities is part of a TCP SYN/ACK reflective DDoS attack which were launched from a couple servers. The attacked also targeted several other TCP ports including TCP/23, TCP/22 and TCP/80 [1]. The top source IPs we observed were 54.93.50.35 (AmazonAWS / Germany), 178.62.212.134 (Digital Ocean / Netherlands), 88.99.240.164 (your-server.de / Germany), 84.16.228.183 (LeaseWeb / Germany) and 84.16.228.9 (LeaseWeb / Germany).

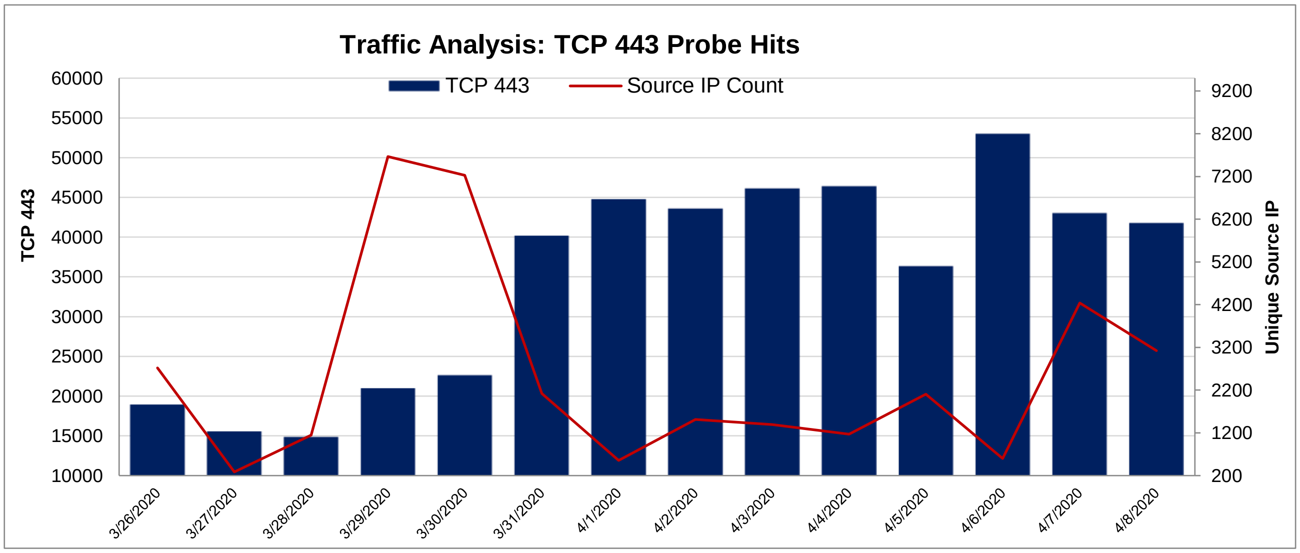

Figure 2: TCP Port 443 Analysis (April 2 – April 8, 2020)

References

[1] Bad Packets Report - https://twitter.com/bad_packets/status/1246902528953835520