Cyber-Intelligence Report

This Cyber-Intelligence Report is reduced in scope to allow our team time for Remembrance Day. It focuses on recent attacks on Canadian businesses. The next Cyber-Intelligence Report on CyberWarfare between Russia and Ukraine will be released 17th November.

This cyber-intelligence product is produced by David Swan. Collection of information is in accordance with guidelines provided by clients. It contains 'observations', meaning headlines and links to information published online. It *MAY* contain comments and analysis. It is copyright ©David Swan 2022. It MAY be circulated.

If this report does not meet your requirements, is in error or if you need additional information and/or analysis, please contact David Swan at DSC.Ops.Vulcan@gmail.com

Canadian Companies Get Hacked

This report contains selected cyber-security information from 29th October to 10th November 2022.

Synopsis

1. WFCU Credit Union, Empire Company and Maple Leaf Foods were hacked, suggesting serious problems with the Canadian approach to cyber-security. Microsoft is reporting that some governments have increased the amount of hacking they are doing – especially on critical infrastructure. China has been stockpiling vulnerabilities. Lastly, Canadian Prime Minister is now aware of Chinese interference in Canadian elections.

Canadian Hacks

2. **WFCU Credit Union**: On Friday [28th October], WFCU posted an alert to members stating “we have detected a number of weak Personal Access Codes (PAC), indicating some online banking accounts could be easily compromised.”Over the Halloween weekend WFCU Credit Union serving Wessex and Essex Counties in Ontario, “discovered unauthorized activity on some of its members’ accounts.”[1] “Further investigation led us to believe that this unauthorized activity was being caused by bad actors preying on weak passwords and getting access, unauthorized access, into some of our members’ accounts,” WFCU president and CEO Eddie Francis said. WFCU took steps to close all access to “weak password protected accounts” by locking those accounts from online access.

3. According to the WFCU website, members who had their accounts locked must: “Adhere to industry standard complex password rules” ... and “monitor their accounts for signs of unusual activity and ensure they sign up for security alerts on their online banking account.”[2] Analysts Comment: The instructions leave me wondering why “industry standard complex password rules” were not being enforced and why members have to sign up for security alerts. I recognize that Credit Unions are not the same as charter banks however this makes me wonder how good Canadian banking

1 Source: CTV News Windsor: WFCU locks access to online banking for some members after security breach
2 Source: WFCU Credit Union web site: Online Banking Update – November 1, 2022

security is.

4. **Empire Company**: On 7th November The Empire Company said: “an "information technology systems issue" was causing some of its pharmacies to experience difficulty fulfilling prescriptions. Signs posted at some stores also said the gift card and Scene points systems were down.”[3] The company has not released any further information about the issues, and did not respond to questions posed by media. Empire Company owns 1,500 stores across Canada, including Sobeys, Lawtons, IGA, Safeway, Foodland, Needs and other grocery outlets.

5. Comments from cyber security specialists were blunt: "This is totally embarrassing for a company, saying I was held hostage and I had to pay a fine," Robert Hudema with the Ted Rogers School of Management at Toronto Metropolitan University said. "A lot of companies are reluctant to spend money on things that are equivalent to fire extinguishers or alarms or things like that to prevent bad things from happening, and as a consequence, bad things happen." Carmi Levy, an independent technology analyst said: "If you admit that you were hit by a ransomware attack, then you admit that you didn't invest enough in cybersecurity and you didn't take your clients' and stakeholders' data seriously enough. And nobody wants to admit that — it's like the modern day equivalent of the Scarlet Letter."[4]

6. **Maple Leaf Foods**: On Sunday 6th November Maple Leaf Foods reported it was “experiencing a system outage linked to a cybersecurity incident.”[5] One source reported that the hack was reported on Friday 4th November, “just hours after that happened.”[6] When the company’s statement and the IT World Canada reporting is combined the incident becomes much clearer:

> A. “Upon learning of the incident, Maple Leaf Foods took immediate action and ***engaged cybersecurity and recovery experts***,” the company said in a statement. Analysis Comment: I translate that ‘corporate speak’ as confirmation that Maple Leaf Foods was 'hacked' and suffered data loss.[7]
>
> B. “***The company is executing its business continuity plans*** as it works to restore the impacted systems; however, it expects that full resolution of the outage will take time and result in some operational and service disruptions.” Analysis Comment: This infers that Maple Leaf Foods was hit by a ransomware attack. The logic is that ransomware attacks lock companies out of their own files, hence executing business continuity plans is a big indicator.[8]
>
> C. "a Maple Leaf spokesperson said in an email Monday morning that the outage is creating some operational and ***service disruptions that vary by business***

3 Source: CBC: Sobeys, Safeway grappling with IT issues as Maple Leaf Foods announces cybersecurity incident
4 Ibid.
5 Source: Canada.com from IT World Canada: Maple Leaf Foods suffers IT outage after cybersecurity incident
6 Source: SaltWire (Atlantic Canada Business): Four days in, Sobeys still mum on ‘IT issue’ affecting stores
7 Source: Canada.com from IT World Canada: Maple Leaf Foods suffers IT outage after cybersecurity incident
8 Ibid.

unit, plant, and site." Analysis Comment: This infers the hack was discovered before the hackers could access and encrypt all systems. This happens to hackers when they break into complex corporate networks. Another possibility is that the attackers are not top tier hackers, and made some mistakes.[9]

7. Security Week made the following observation: "Maple Leaf is not the first large meat company to have its operations be impacted by a cyberattack. In mid 2021, JBS, the largest meat processing company in the word, was disrupted by a ransomware attack that forced an operational shutdown, just weeks after a similar incident shut down the Colonial Pipeline."[10]

8. Analysts Comment: Hacks of this scale [Empire Company and Maple Leaf Foods] are not easily resolved. In most cases the organization pays the ransom. Paying the ransom does NOT guarantee that all files will be recovered. Restoring IT systems to full operation is normally a matter of weeks – NOT days. Further, it is common for a network that has been hacked to be hit a second time, especially if the organization has not rapidly patched and upgraded their security systems.

State-Based Hacking Has Increased

9. According to Microsoft's third annual Microsoft Digital Defense Report[11] state-based cyber attacks are increasing. Microsoft says cyberattacks targeting critical infrastructure have grown from 20 percent to 40 percent of all government attacks. The majority of those attacks are attributed to Russia however, Iran, North Korea and China have all increased their attacks on critical infrastructure.[12]

A. Iran has launched: destructive attacks, ransomware attacks, hack and leak operations and 'nuisance' attacks [like the one that turned on Israeli air-raid sirens]. The most frequent target is Israel. The US and the EU are also on the target list.

B. North Korea is most notable for its attempts to hack cryptocurrency companies and cryptocurrency holdings. North Korea's most successful hackers, the Lazarus Group have been upgraded from 'criminal hackers' to an 'Advanced Persistent Threat' and labelled a "state-sponsored hacking organization" by the F.B.I.[13]

C. The Chinese Communist Party has approved its 14th Five Year Plan, declaring: "informatization is entering a new phase of accelerated digitized development and building a digital China."[14] Historically when China listed technical development in its Five Year Plan, one of the ways that manifested itself was in increased cyber espionage, theft of intellectual property. China's increased

9 Source: Canada.com from IT World Canada: Maple Leaf Foods suffers IT outage after cybersecurity incident
10 Source: Security Week: Canadian Meat Giant Maple Leaf Foods Disrupted by Cyberattack
11 Reference: Microsoft Digital Defense Report 2022
12 Source: TechBuzz: State cyberattacks grow more brazen as authoritarian leaders ramp up aggression | ICT Business | 11 November
13 Source: "PARK JIN HYOK". Federal Bureau of Investigation.
14 Source: Stanford University: 14th Five-Year Plan for National Informatization

hacking activity suggests that hacking efforts to collect the best technology available are already underway.

China

10. **China Stockpiling Zero-Days**: Microsoft Digital Defense Report 2022 suggests that China is probably 'stockpiling and deploying vulnerabilities'.[15] This is based on observed activity and Chinese Internet regulation. In 2021 China implemented a law requiring Chinese makers of network software and hardware to "alert Beijing within two days of learning of a security vulnerability in their products." China's National Internet Information Office, Ministry of Industry and Information Technology, and Ministry of Public Security is in charge of coordinating and managing network security vulnerabilities. Article nine of the regulations says details of security flaws must be "kept under wraps until patches are available or special permission is granted by the government to go public." Articles twelve to fifteen make it clear that "anyone who breaks these rules and related legislation will feel the full force of the Chinese government."[16]

11. Microsoft Security has made a direct link between China's vulnerability reporting regulation that went into effect September 2021 and a surge in zero-day attacks. Microsoft says "China's government hacking groups have become "particularly proficient at discovering and developing zero-day exploits" after strict mandates around early vulnerability disclosure went into effect."[17] Microsoft urges defenders to 'prioritize patching' as soon as patches are available.

12. **China Interfering in Canadian Elections**: Global News reported that Canadian intelligence had concluded Beijing worked to undermine the democratic process "targeting Canada with a vast campaign of foreign interference, which includes funding a clandestine network of at least 11 federal candidates running in the 2019 election."[18] Analysts Comment: None of this *should* be news. The People's Republic has a history of hacking and other 'interference' in Canada, including indictments for stealing: "shipbuilding secrets (2013), satellite technology (2016), and espionage by a Toronto Permanent Resident (2017). Cyber forensic investigators, ranging from university computer security teams to cyber security firms, have provided overwhelming evidence of PRC cyber attacks."[19] The question is: will this election interference drive a change in Canadian Government policy? Will that policy include any cyber protection?

---

15 Source: The Register: China is likely stockpiling and deploying vulnerabilities, says Microsoft
16 Source: The Register: So nice of China to put all of its network zero-day vulns in one giant database no one will think to break into
17 Source: Security Week: Microsoft: China Flaw Disclosure Law Part of Zero-Day Exploit Surge
18 Source: Global News: China allegedly interfered in 2019 Canadian election
19 Source: MacDonald Laurier Institute: Swan: The Canada-China Cyber Agreement remains questionable