Cyber-Intelligence Report

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 2023. This report 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

Cyberwarfare: Russia vs Ukraine (39) Canada Targeted

This report contains selected cyber-security information from 15th to 28th Sept 2023.

Synopsis

1. We start with Russia's three new cyber campaigns against Ukraine. Indian hackers deface Canadian websites. The forecast for hacking in Canada is grim.

2. Russia vs Ukraine cyberwar. Russia appears to be committed to the following ongoing 'Course of Action' for its cyber forces:

> Russian cyber forces, including allied and supporting hackers, continue to launch campaigns against Ukrainian targets, including perceived Ukrainian allies. Targeting Includes: critical infrastructure, industrial infrastructure, political, and media organizations as well as targets of opportunity.

Russian Cyber-Attacks

3. **Russia vs Ukraine**. There are multiple reports suggesting that Russia has launched new cyber campaigns against Ukraine.

> A. Ukraine's security agency reports that Russian hackers are "*infiltrating software supply chains*" in order to gain military intelligence.[1] Russia has done this before, most notably in the SolarWinds hack which provided Russia covert access to many companies. No other details were provided.
>
> B. Another new campaign was identified by the Ukrainian State Service of Special Communications and Information Protection (SSSCIP). It claims Russian cyberspies[2] are targeting its servers looking for data about alleged Kremlin-backed war crimes. The International Criminal Court (ICC) has reported being hacked saying its systems were 'breached' and the 'cybersecurity incident' is ongoing.[3] The ICC has not released any updates.
>
> C. A third Russian cyber campaign uses drone manuals as phishing lures. If someone clicks on a lure a Go-based open-source post-exploitation toolkit

1 Source: Computing (UK). Ukraine: Russian hackers infiltrating software supply chains

2 Source: The Register. Ukraine accuses Russian spies of hunting for war-crime info on its servers. The Ukrainian State Service of Special Communications and Information Protection (SSSCIP) identified intruders linked to Russia's Federal Security Service (FSB), Main Intelligence Directorate (GRU), and Foreign Intelligence Service (SVR).

3 Source: The Register. International Criminal Court hit in cyber-attack amid Russia war crimes probe

called Merlin is installed. "*Since drones or Unmanned Aerial Vehicles (UAVs) have been an integral tool used by the Ukrainian military, malware-laced lure files themed as UAVs service manuals have begun to surface,*" Securonix researcher said.[4] The cybersecurity company is tracking the campaign under the name STARK#VORTEX.

4. **Russia hacks Canada**. Russia used its 'patriotic hacker group' NoName057(16) to let Canada know it was not happy with President Zelenskyy of Ukraine speaking to Canadian parliament. Distributed Denial of Service (DDoS) attacks were launched against a number of Canadian government sites on Wednesday 13th Sept with the bulk of the attacks starting on the 14th:

I. Federal Government. Senate, Canada Border Services Agency (CBSA), the Canadian Air Transport Security Authority, and several airports were all targeted by NoName according to their website.[5]

II. P.E.I. Provincial government sites. Department of Education, Public Schools Branch, Health P.E.I. and other government departments were downed for approximately 11 hours.[6] Access to WiFi at the Shaw building was also disrupted.

III. Quebec. On Wednesday 'some' government-linked websites went down temporarily as a result of "a denial-of-service-style cyberattack'. "*Eric Caire, the province's cybersecurity minister, attributed the attack to NoName*."[7]

IV. Manitoba. Government websites went off-line "*at some point Thursday morning and were inaccessible for most of the day."* There was no comment on damage, details of the attack or who the attacker was.[8]

V. Yukon. In addition to the main government website being downed, "*access to Yukon government Wi-Fi, Microsoft Teams, SharePoint and other cloud-based software were affected, according to the memo, and a number of employees were unable to access their government emails or internet-based phone services.*" Most services were restored by end of day Friday.[9]

VI. Northwest Territory. The territorial government acknowledged the cyber attack but refused to speculate on who was behind it or comment on impact other than stating "*GNWT websites are up and running again. ... Users may experience temporary outages again as the disruption runs its course, but GNWT staff are addressing the situation."*[10]

5. The Canadian Centre for Cyber Security released an Alert "intended for IT

4 Source: The Hacker News. Ukrainian Military Targeted in Phishing Campaign Leveraging Drone Manuals
5 Source: Security Affairs. Pro-Russia hacker group NoName is suspected to have launched a cyberattack that caused border checkpoint outages at several Canadian airports.
6 Source: Saltwire. P.E.I. cyberattack appears part of co-ordinated cross-Canada attacks
7 Source: TorontoSun. Government websites down in four provinces, two territories; cyberattacks blamed
8 Source: CBC News Manitoba. Manitoba government websites crash was due to cyberattack: spokesperson
9 Source: CBC News. Yukon gov't website back after cyberattack, Nunavut gov't site still down
10 Source: Cabin Radio. NWT government acknowledges denial-of-service attack

professionals and managers" on 15th Sept. "Since 13 September 2023, the Cyber Centre has been aware and responding to reports of several distributed denial of service (DDoS) campaigns targeting multiple levels within the Government of Canada, as well as the financial and transportation sectors." The Centre's recommendations were limited recommending system and procedural reviews.[11]

Indian Hackers Attack Canada

6. On Monday the 18th of September, Prime Minister Trudeau claimed "agents of the Indian government" carried out the killing of a Sikh leader, Canadian citizen Hardeep Singh Nijjar, in Surrey B.C. .[12] India denounced the claim and expelled a Canadian diplomat. Over the next few days senior members of the Indian government criticized Canada, Prime Minister Trudeau and the 'unfounded accusation'. Subsequently a hacking group named 'Indian Cyber Force' began defacing Canadian websites[13].

7. On 25th Sept ITWorldCanada reported "*A group calling itself the Indian Cyber Force posted a threatening message last week on the X messaging platform. It says, "Get ready to feel the power of Indian Cyber Force attacks will be launching on Canada cyber space in the coming 3 days. It's for the mess your started." A website that appears to belong to a Canadian dental clinic has been defaced with a message, "Hacked by Indian Cyber Force." However, the real website, whose address begins with 'www,' isn't affected."*[14] On 28th Sept Canadian Armed Forces said that its website became unavailable (due to Indian hackers) to mobile users midday Wednesday, but was fixed within a few hours.[15]

8. The Canadian federal government responded to a query by ITWorldCanada by saying: *"CSE [the Canadian Security Establishment] and its Canadian Centre for Cyber Security (Cyber Centre) have observed that geopolitical events often result in an increase in disruptive cyber campaigns. We continue to monitor for any developing cyber threats and share threat information with our partners and stakeholders to help prevent incidents," says the statement.* ***However, the Cyber Centre's primary focus is on defending Government of Canada networks from cyber threats.*** *We focus on the type of threat, not where the threat originates. For that reason, we generally do not provide statistics, or information on reporting trends. We encourage Canadians and Canadian organizations to be aware of cyber threats and to remain vigilant."*[16]

---

11 Source: Government of Canada – Canadian Centre for Cyber Security. Alert - Distributed Denial of Service campaign targeting multiple Canadian sectors

12 Source: CBC News. Trudeau accuses India's government of involvement in killing of Canadian Sikh leader

13 Website defacing is similar to graffiti on buildings. A website may be completely overwritten or merely have a message from the hackers overlaid on the existing site. Sometimes website functions are disabled as well.

14 Source: ITWorldCanada. Cyber Security Today, Sept. 25, 2023 – Hackers from India say they are targeting Canadian web sites

15 Source: CTV News. Cyberattacks hit military, Parliament websites as India hacker group targets Canada

16 Source: ITWorldCanada. Canada cyber centre issues caution after group from India issues threat

Hacking Forecast for Canada

9. Currently there are two nation driven campaigns targeting Canada as well as an increasing perception among criminal hackers that Canada is an 'easy target'.

A. **Russian Cyber Attacks**: Russian 'patriotic hackers' such as 'NoName057(16)' will continue cyber attacks at irregular intervals, surging whenever: a Canadian politician supports Ukraine, or criticizes Russia. Even relatively benign announcements such as the announcement of support to re-build Ukraine are *likely* enough to re-energize attacks.

I. Most attacks *will probably* be Distributed Denial of Service (DDoS) attacks however other attacks, such as ransomware attacks and more destructive attacks should be expected.

II. DDoS attacks *will probably* last longer as Canada has demonstrated we have no defences.

III. Attacks will continue to target government web sites at any level of government and other web sites such as airlines, they perceive to have significant impact.

The only mitigating factor is probably that Canada is perceived to be a bit player in the Russia – Ukraine conflict, contributing minimally to Ukraine.

B. **Indian Hackers**: There *may be* additional attacks, however, as political rhetoric between the countries cools, attacks from Indian hackers will *almost certainly* decrease. Most attacks are likely to be web site 'defacement' (where the attacker puts their message on the web site) and DDoS attacks. If the Trudeau government releases additional information and/or if the Indian government under Prime Minister Modi decide they need to denounce Canada, attacks will *almost certainly* resume and increase.

C. **Criminal Hackers**: Functionally the Canadian government has announced that it will not take steps to pursue criminal hackers or protect Canadians on-line. To criminal hacking groups the lack of cyber laws, the lack of cyber capability across multiple levels of government, the lack of hack reporting requirements, the lack of co-ordinated law enforcement response, the declaration by the head of Canadian Security Establishment (CSE) that paying ransomware is a business decision, all add up to the perception that Canada is a easy and low-risk place to hack. This will *almost certainly* drive increases in:

I. Personal attacks: These will probably be mostly scam/fraud attacks focused on stealing money. Examples include: the new Social Insurance Number (SIN) scam, personal romance scams, Canada Revenue scams

and many, many more. Expect the number of scams to continue to increase.

II. Ransomware attacks: These attacks are based on identifying and exploiting vulnerabilities all types of organizations, including municipal governments. Since Canadians remain largely unaware of the threat, they are not improving their protections. The number of ransomware attacks has been increasing, a trend I expect to continue.

III. Targeted Attacks: (Multi-extortion ransomware based attacks). Large organizations such as: Maple Leaf Foods, Empire Group (Sobeys), Cargil, Air Canada[17] etc will come under increasing targeting. If the organizations have no perceived support, hackers will expect that large corporations will pay ransoms and extortion.

IV. Nation-State Attacks: Canada has not addressed cyber attacks from Russia, China, Iran or most recently India. Since there has been no push-back, Canadians should expect more attacks, more complex attacks and more targeted attacks across government, institutions and commercial environments.

10. The net impact of Canada's lack of cyber security will be that Canada will become an increasingly corrupted cyber environment. Some Canadian's are already losing faith in using the Internet and in particular Internet based systems. I can not predict what it will take to cause Canadian politicians to react, to get them to write legislation or empower police and security forces. As long as they (politicians) don't think cyber gets them votes I am confident they will NOT respond. That infers that the pain of being scammed / extorted / hacked being felt by many Canadians will continue and increase in at least the short and medium term.

Final Comment

11. Analysts Comment: It is embarrassing to write this about one's own country. What Canada's politician's have managed to do is write a definitive textbook on 'How NOT to Manage Cyber Security'. I can only hope that other people, from countries to cyber security personnel, learn from our high quality 'bad example'.

---

17 All of those organizations have been successfully hacked in the last year.