Volume 4: Edition 3

Cyber-Intelligence Report

This cyber-intelligence product is a snapshot of selected cyber events. Collection of information is in accordance with clients' guidelines. It contains 'observations', meaning headlines and links to online information. It *MAY* contain comments and analysis. It is copyright ©David Swan 2024. This report MAY be circulated.

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

CyberWarfare Update plus Cybercrime in Canada

This report contains selected cyber-security information from 27th January to 8th February 2024.

Synopsis

1. Chinese hackers Volt Typhoon get even the Canadian government issuing 'advisories'. Russia vs Ukraine update. Russian cyber attacks. Ukrainian cyber attacks. How is Iran organizing it's cyber forces? How bad is cyber crime in Canada? Pretty bad. Atlantic Canada Telephone Scam, Funeral Home Scam, cyber attacks on RUSI(NS) continue.

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.

China

3. **Five Eyes 'Advisory' on China:** The US government's cybersecurity agency CISA, has issued an 'advisory' on Chinese hacking group 'Volt Typhoon'. "*[We] have confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations in the continental and non-continental United States and its territories, including Guam.*"[1] Mandiant, a U.S. cybersecurity company had previously warned that Volt Typhoon had "*burrowed deep into thousands of organizations around the world.*"[2] The advisory warns "*the hacking team's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations. … the US government believes the Chinese hackers are "pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions, … "[We] are concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts,*"[3]

[1] Source: Security Week. US Says China's Volt Typhoon Hackers 'Pre-Positioning' for Cyberattacks Against Critical Infrastructure

[2] Source: Security Week. Mandiant Intelligence Chief Raises Alarm Over China's 'Volt Typhoon' Hackers in US Critical Infrastructure

4. The advisory follows an operation by the U.S. Justice Department to shutdown a botnet (a network) of compromised small office and home Internet routers being used by the Chinese as a command and control network. The attackers were also the Chinese ‘Volt Typhoon’ hacker group but their ultimate targets were assessed as “*included water treatment plants, the electrical grid and transportation systems across the United States.*”[4]

5. Analysts Comments: While it is true that ‘Volt Typhoon’ has penetrated deeply into critical infrastructure, this is NOT a new behaviour. A far back as 2010 there was evidence indicating that Chinese hackers had penetrated North American telecommunications and power transmission. What has changed since then is that Russian cyber attacks on Georgia and Ukraine have provided nasty evidence of what can happen if a foreign power has access to critical infrastructure. This lesson was driven home to American security officials when the colonial Pipeline was attacked by ransomware in May 2021. Their fear is that China learned the same lesson.[5]

6. What is different is that ‘Volt Typhoon’ was discovered having access to the American base at Guam including ‘secure’ American military telecommunications. As the investigation progressed long-term Chinese penetration into many, perhaps thousands of systems has been discovered. This does NOT mean China’s strategies have changed or that a cyber attack from China is imminent. It does means that Five-Eyes Intelligence leaders have had a massive ‘wake-up’ call. Is critical infrastructure as compromised as the advisory suggests? Yes. Volt Typhoon won’t be the only Chinese attacker or China the only country attacking.

Russia vs Ukraine

7. **Russia’s Attacks**: Late in January Russia began staging a number of attacks on Ukraine.

A. On January 25th “Several major Ukrainian state organisations on Thursday reported cyber attacks on their systems, in the latest wave that a source close to the government blamed on Russian intelligence.

I. State-run energy company Naftogaz said one of the data centres had been hit by a "large-scale cyberattack."

II. Ukrainian national postal service Ukrposhta reported a "significant technical failure" in its IT systems.

III. Ukrtransbezpeka, a state transport safety agency, which maintains the border crossing system for Ukrainian drivers, also reported problems with its data centre.

IV. A convention centre and the ticket sales system for Ukrainian state

[3] Source: Security Week. US Says China’s Volt Typhoon Hackers ‘Pre-Positioning’ for Cyberattacks Against Critical Infrastructure

[4] Source: Security Week. US Says It Disrupted a China Cyber Threat, but Warns Hackers Could Still Wreak Havoc for Americans

[5] Source: Defense One. Chinese hacking operations have entered a far more dangerous phase, US warns

railways also reported suspected cyber attacks.[6]

B. On 28th January Ukraine's Coordination Headquarters for the Treatment of Prisoners of War reported they were attacked by a Distributed Denial of Service Attack (DDoS). The attack was only partially successful as there was limited access "*to some functions and resources*".[7]

C. On 30th January Ukraine's National Cyber Security Coordination Center (NCSCC) warned that Russia's "*APT28 is specifically targeting military personnel and units of the Ukrainian Defense Forces using phishing emails in an attempt to gain access to military email accounts.*" The NCSCC believes the objective is "*access to Ukraine's military situational awareness and command and control systems by stealing military personnel's credentials*"[8]

D. On 2nd February the Computer Emergency Response Team of Ukraine (CERT-UA) "*warned that more than 2,000 computers in the country have been infected by a strain of malware called DirtyMoe.*"[9] The attacker is UAC-0027, who is associated with the Russian FSB. How the malware is injected is unknown.

E. Killnet 2.0 has announced its emergence as the coordinating body for 'patriotic hackers'. Analysts Comment: It remains to be seen if Killnet 2.0 is more substantial than the original.

F. A Russian cyber attack on Finnish cybersecurity company 'Tietoevry Oyj' spilled over into Sweden. "*A ransomware group known as Akira targeted a Tietoevry data center in Sweden. ... A large number government agencies and private companies in Sweden have been hit, including the country's parliament and its biggest cinema chain. ... Sweden's central bank has filed a police report after some of its IT systems were rendered inaccessible by a ransomware attack.*"[10] Sweden's Civil Defense Minister warned that some systems might be down for weeks.[11]

8. **Ukraine Attacks**: Ukraine has continued to mount cyber attacks against strategic targets in Russia. All of the attacks reported were reported by Ukraine's ''Main Intelligence Directorate'. Analysts Comment: This infers *at least* coordination if not inter-operability or even integration into Ukraine's official cyber forces.

A. On January 27th the "*pro-Ukraine hackers group "BO Team" wiped the database of the Far Eastern Scientific Research Center of Space Hydrometeorology "Planet." The Russian center processes data received from*

[6] Source: Reuters. Several Ukrainian state-run bodies report cyber attacks

[7] Source: Ukrinform. Coordination HQ hit by cyberattack

[8] Source: Cybernews. Russian APT28 phishing Ukraine's military to steal login info

[9] Source: The Hacker News. DirtyMoe Malware Infects 2,000+ Ukrainian Computers for DDoS and Cryptojacking

[10] Source: Data Center Knowledge. Sweden's Riksbank Turns to Police Following Cyber-Attack On Tietoevry Data Center

[11] Source: Bloomburg. Damage From Cyber Attack on Sweden May Take Weeks to Recover

satellites and also provides relevant products to more than 50 state entities, including the Ministry of War, the General Staff and the services of the Ministry of Defense of the Russian Federation. ... The hackers wiped 2 petabytes of data from 280 servers.”[12]

B. Also on 27th of January Ukraine’s Main Intelligence Directorate (GUR) announced a successful cyberattacks against *IPL Consulting, a Russian company specializing in implementing information systems for Russian industry. IPL Consulting billed itself as one of Russia’s most high-tech companies, assisting institutions involved in automotive, aviation, heavy machinery, equipment, and instrument manufacturing, including for the Russian defense-industrial complex. The GUR said its experts “infiltrated IPL Consulting’s internal network and destroyed the company’s entire 60+ terabyte IT infrastructure, dozens of servers and databases.”*[13]

C. On 30th January the Main Intelligence Directorate of Ukraine (GUR) announced a successful cyberattack on a special communications server of the Russian Ministry of Defense. There were reports that there were widespread outages in Russian domain websites. “*The internet disruptions were not confined to a single region. Significant interruptions were reported in several major Russian cities, including St. Petersburg, Moscow, Yekaterinburg, Tyumen, and Rostov-on-Don, in the Far East, as well as in Kaliningrad, Samara, Omsk, and Kazan. Major Russian websites like Yandex and VK and various media outlets also faced operational issues.”*[14]

9. The American cyber security journalist Brian Krebs may have answered the question of ‘how close the ties are between cyber criminals and the Russian government’. Data from the exclusive Russian cybercrime forum Mazafaka reveals that “*a former officer in the special forces of the GRU, the foreign military intelligence agency of the Russian Federation*,” ... was an “*attorney who advised Russia’s top hackers on the legal risks of their work, and what to do if they got caught.”* The article follows Krebs efforts to identify the officer. The final comment went to a Mark Rash a former cybercrime prosecutor for the U.S. Department of Justice: “*The guy is heavily hooked into the Russian cyber community, and that’s useful for intelligence services,” Rasch said. “He could have been infiltrating the community to monitor it for the GRU. Or he could just be a guy wearing a military uniform.”*[15] In any case the answer is that the ties between the Russian government and cyber criminals in that country are tight, very tight.

Iran

10. Iran’s Cyber Operations Getting Organized: As reported “*Many of Iran’s immediate operations after October 7 were hasty and chaotic*”. These attacks were largely ineffective. Microsoft is reporting that they are tracking fourteen (14) pro-Iranian cyber

[12] Source: Security Affairs. Pro-Ukraine Hackers Wiped 2 Petabytes of Data From Russian Research Center

[13] Source: Euromaidan. Ukrainian cyberattacks cripple Russian defense contractor, weather center

[14] Source: Euromaidan. Ukrainian cyberattack disrupts Russian MoD server

[15] Source: Krebs On Security. From Cybercrime Saul Goodman to the Russian GRU

groups. The other big increase is in AI (Artificial Intelligence) influence operations. In December 2023 “*Iran interrupted streaming television services and replaced them with a fake news video featuring an apparently AI-generated news anchor. ... The disruption reached audiences in the UAE, UK, and Canada.*”[16]

11. A separate report by cybersecurity company ‘Recorded Future’ suggests how Iran may have gotten its cyber troops organized. The company has identified “*long-standing relationship between intelligence and military organizations and Iran-based contractors. Public records point to an ever-growing web of front companies connected via individuals known to serve various branches of the IRGC ... This has included affiliations with organizations like the IRGC Electronic Warfare and Cyber Defense Organization (IRGC-EWCD), the IRGC Intelligence Organization (IRGC-IO), and even the IRGC’s foreign operations branch, the Quds Force (IRGC-QF).*” Companies include: ”*contractors like “Ayandeh Sazan Sepehr Aria Company”, “Sabrin Kish”, “Soroush Saman Company”, and other sanctioned entities like “Najee Technology Hooshmand Fater LLC (Najee Technology)” and “Emen Net Pasargad”, which are reported to have been involved in international attack operations at the behest of the IRGC.*”[17]

Current Hacks and Scams

12. **Atlantic Canada Telephone Scam:** Please advise: family, friends and organizations you belong to. There is a new and surprisingly detailed scam underway in Atlantic Canada. The person answered his phone because it displayed a local telephone number. The scammers:

- Had their full name;
- Knew they had a landline telephone – AND what company it was with;
- Knew they had two cellphones with a different company;
- **Offered** a new phone package with:
    - two new cell phones; and
    - lower monthly fee.

13. The good news to this story is their bank flagged and stopped a purchase being made on the victim’s credit card, from Bangladesh. They recovered their cell phone accounts (which had been hacked), dumped their credit card, resolved their account with their land-line provider before the scammer called back.

14. Analysts Comment: This is almost certainly a result of data breaches such as the MOVEit! Breach by the Cl0p Ransomware Group. According to the Konbriefing one hundred fifty-two (152) Canadian organizations have lost data through the MOVEit! Breach.[18] There is enough personal information for sale on the dark web, that criminals can purchase the data, do some correlation between different data sets and they have ample information to attempt a detailed scam. UPDATE DURING WRITING: We have confirmed reports of this scam being used on people in both Nova Scotia and New Brunswick. We *assess* that there are *almost certainly* victims of this scam in

[16] Source: Microsoft blogs/on-the-issues. Iran accelerates cyber ops against Israel from chaotic start

[17] Source: Recorded Future. Leaks and Revelations: A Web of IRGC Networks and Cyber Companies

[18] Source: Konbriefing. MOVEit hack Victim List

Prince Edward Island. It is *highly likely* that similar scams are running in Newfoundland and Labrador.

15. **Scams on Funeral Homes:** DSC was asked to verify an order sent to a funeral home for: a memorial service, a specific band to play at the service, and a catered post-service luncheon for approximately thirty people. The total order was for more than $8,000.00 (Canadian Dollars) in goods and services. The ‘references’ for the order were all online and seemed plausible. Under detailed investigation the references (Facebook pages, web sites and phone numbers) did not hold up to scrutiny and the initial email was found on Reddit under r/Scams. Investigation by the RCMP immediately determined that many Funeral Homes had been approached.

16. **Attacks on RUSI(NS):** Attempts to hack into the Royal United Service Institute(Nova Scotia) or RUSI(NS) web site, are ongoing. Initially between eight and twenty-four attacks were attempted daily, *apparently* from different locations[19], and run against various site logins. The logins were *probably* harvested from either the web site (before security was increased) or one or more executive members of RUSI(NS). The current attacks *appear* to be manual attacks, run from once to four times daily. UPDATE DURING WRITING: We have been advised that there are phishing attacks against RUSI(NS)’s ‘X’ (Twitter) account.

17. **Analysts Warning:** The incidents above were reported to us within a 72 hour time period. The pace of cyber attacks and computer assisted fraud operating in Canada is staggering. None of the ‘targets’ are wealthy or significant. All of the targets can be described as ‘ordinary Canadians’. The range of attackers is from an individual, to a scam centre and *very probably* a nation[20]. In addition to these attacks there are the cyber espionage / theft of intellectual property attacks from China. Often these attacks are discounted because they have no immediate ‘visible’ cost. Although no cash was lost, in every case there was loss in time and resources – at least 1/2 a day – in order to interdict or recover from an attack.

18. Cyber attacks and scams occur in Canada because we are functionally ‘undefended’. There is minimal legislation addressing cyber crime. Few police departments are funded well enough to establish expertise to investigate and prosecute cyber criminals. Federal efforts to protect Canadian organizations are under-funded and under manned. Government resources protecting individual Canadians are minimal. As long as Canadians remain undefended we can expect to see an increasing number of cyber attacks and cyber crime intruding on daily life.

To unsubscribe from this service send an email to DSC.Ops.Vulcan@gmail.com

[19] It is unlikely that the attacks came from South-East Asia. It is *more likely* that either a VPN (Virtual Private Network) or some kind of obfuscation script was used to hide the location of the attacks.

[20] The attack on the funeral home is *probably* from an individual. The telephone scam is *very likely* a scam call center based in Bangladesh. The attack on RUSI(NS) is *very likely* a Russian government attack.