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: China's Cyber Espionage and Russia's Cyber Attacks

This report contains selected cyber-security information from 9th to 21th March 2024.

Synopsis

1. Is a 'Digital Pearl Harbour' a possibility? People's Republic of China identified as the attacker in two massive cyber campaigns, Volt Typhoon and Earth Krahang. Russia cyber attacked Microsoft and lastly, Russia's other cyber attacks.

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's Cyber Espionage

3. **Digital Pearl Harbour?** President Biden's National Security Advisor, Jake Sullivan, has issued a warning to water companies across the US. The warning is based on the *HIGH PROBABILITY* that state-sponsored groups linked with Iran and China have carried out cyber-attacks on water and waste water infrastructure. The warning letter, released by the White House, says "*Drinking water and wastewater systems are an attractive target for cyber attacks because they are a lifeline critical infrastructure sector, but often lack the resources and technical capacity to adopt rigorous cybersecurity practices, ... cyber actors targeted and disabled a common type of operational technology used at water facilities where the facility had neglected to change a default manufacturer password.*"[1] The letter warns of the potential for a '*digital Pearl Harbor*'.

4. Analysts Comments: Historically the nations who have hacked into critical infrastructure (IE. China), such as water systems and electrical systems, who have not utilized their access. Russia has accessed other nations critical infrastructure, crippling it during an invasion (IE. Russian invasion of Georgia in 2008). Russia has attempted to cripple Ukraine's critical infrastructure during the current war. Iran has also attacked critical infrastructure. Iran's 'Islamic Revolutionary Guard Corps'(IRGC) continues to cyber attack Israel's critical infrastructure, while continuing to break into

1 Source: Computing Co.UK. US National Security Advisor Jake Sullivan warns of 'digital Pearl Harbor' targeting infrastructure

Cyber-Intelligence Report

American water systems.

5. Analysis: The phrase ‘digital Pearl Harbour’ can feel ‘over the top’, especially for anyone who has not lived under threat of war. Unfortunately, Russia and Iran have ‘normalized’ attacks on critical infrastructure, because they have cyber attacked critical infrastructure – to no significant international response. Worse, criminal hackers have also attacked critical infrastructure (IE. Ransomware attack on the ‘Colonial Pipeline’ in the U.S.). They have not suffered significant consequences.

- The possibility of a cyber attack designed to cripple a western / NATO nation’s critical infrastructure (IE. water, wastewater and/or energy) is **at least** *PROBABLE* (60 to 79%).
- Given the war between Russia and Ukraine, and the Israel vs Gaza/Iran conflict, the possibility of a ‘Digital Pearl Harbour’ against the United States is between *PROBABLE* (60 to 69%) and *VERY PROBABLE* (70 to 89%).
- The possibility of a cyber attack on Canadian critical infrastructure approaches *CERTAINTY* (90 to 100%) due to: Canada’s lack of defences, inability to retaliate, and based on the fact some critical infrastructure has already been attacked (oil pipelines have been cyber attacked).

6. The ‘Five Eyes’ Intelligence Community[2] has issued a warning about the ‘urgent risk’ posed by People’s Republic of China (PRC) state-sponsored hackers known as “Volt Typhoon.” The bulletin is titled: “PRC STATE-SPONSORED CYBER ACTIVITY: ACTIONS FOR CRITICAL INFRASTRUCTURE LEADERS”[3]. Previous editions of ‘Cyber Intelligence Reports’ have reported on the discovery of Volt Typhoon’s penetration of U.S. telecommunications on the U.S. base on Guam, followed by the discovery the attackers had penetrated U.S. strategic communications, as well as over a thousand sites, spread across many nations. The penetration of strategic infrastructure was so deep that ‘Five Eyes’ Intelligence organizations assessed the effort as “preparations for a future war”.[4] The bulletin contains ‘instructions for leaders’ as well as a general set of best practices for securing and maintaining the security of cyber infrastructure.

7. Analysts Comment: As the People’s Republic of China continues to build its capability to project military force, the Five Eyes concern is that a conventional conflict such as the invasion of Taiwan, could trigger a cyber attack that would cripple strategic telecommunications and other critical infrastructure. We stand by our *assessment* that there is no immediate threat. That said, given the current activities of

2 The ‘Five Eyes’ countries are: Australia, Canada, New Zealand, UK and U.S. The Five Eyes Intelligence community is: Australian Signals Directorate, Communications Security Establishment (Canada) including Canadian Centre for Cyber Security, National Cyber Security Directorate (NZ), National Cyber Security Directorate (UK), and from the U.S.; National Security Agency (NSA), Federal Bureau of Investigation (FBI), Departments of Energy and Treasury, Transportation Security Agency (TSA), CyberSecurity & Infrastructure Security Agency (CISA), and Environmental Protection Agency (EPA).

3 Source: U.S. CyberSecurity & Infrastructure Security Agency (CISA). PRC STATE-SPONSORED CYBER ACTIVITY: ACTIONS FOR CRITICAL INFRASTRUCTURE LEADERS

4 Source: Cyber Intelligence Report Volume 4 Edition 2 dated 240221.

the PRC, Russia and Iran, we see the Five Eyes Bulletin as an important warning, in addition to the 'digital Pearl Harbour' warning.

8. In yet another PRC government sponsored hacking campaign, "*Chinese cyberspies have compromised at least 70 organizations, mostly government entities, and targeted more than 116 victims across the globe.*"[5] The campaign has been named "Earth Krahang". Government organizations seem to be the gang's primary focus, with education, telecommunications and other sectors also being targeted. Earth Krahang exploits Apache and Oracle web application vulnerabilities to gain unauthorized access and deploy malware.[6] "*Earth Krahang also uses brute-force attacks to obtain credentials and steal victims' emails.*" Once they have access to networks, their primary target appears to be "*public-facing servers and using phishing emails to deploy two custom backdoors.*" When the attackers have network access "*favorite tactics involve using its malicious access to government infrastructure to attack other government entities, abusing the infrastructure to host malicious payloads, proxy attack traffic, and send spear-phishing emails to government-related targets using compromised government email accounts.*" Computer security company 'Trend Micro' notes the gang has a "*preference for high-value targets, and their use of compromised government infrastructure for espionage purposes.*"[7]

9. Trend Micro theorizes that 'Earth Krahang' and another Chinese hacking group, Earth Lusca, could be two penetration teams working for I-Soon. I-Soon is the "*Chinese security contractor that recently had a trove of documents leaked on GitHub. The files contained extensive details about Beijing's extensive hacking campaigns against foreign governments.*" Analysts Comment: The 'Earth Krahang' campaign[8] is **in addition to** the cyber attacks that caused the 'digital Pearl Harbour' warning and the 'Volt Typhoon' campaign. It is worth repeating that the size of the PRC's cyber espionage/hacker infrastructure dwarfs the combined cyber infrastructure of all other nations.

10. **Microsoft Compromised, Again**: on 12th January, 2024, the Microsoft Security Team detected an attack on Microsoft's corporate email systems. The Russian government hackers known as Midnight Blizzard, part of the NOBELIUM hacking group was inside Microsoft's corporate network. What has just been discovered was that in addition to stealing corporate information and reading the email of senior executives, Midnight Blizzard stole source code[9], and is already exploiting vulnerabilities they discovered in that source code to further attack Microsoft. "*It is apparent that Midnight Blizzard is attempting to use secrets of different types it has found. ... Midnight Blizzard's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus. It may be using*

5 Source: The Register. Beijing-backed cyberspies attacked 70+ orgs across 23 countries
6 Source: CyberSecurityNews. Chinese APT Hackers Exploits Government Web & Exchange Servers
7 Source: The Register. Beijing-backed cyberspies attacked 70+ orgs across 23 countries
8 The 'Earth Krahang' information was released *after* a number of critical infrastructure compromises and the 'Volt Typhoon' cyber campaign was discovered.
9 'Source Code' is the term used to describe the computer code used to make operating systems such as 'Windows' work. In the case of Microsoft it also refers to th code used to operate major applications such as Microsoft exchange (email) etc.

the information it has obtained to accumulate a picture of areas to attack and enhance its ability to do so. This reflects what has become more broadly an unprecedented global threat landscape, especially in terms of sophisticated nation-state attacks."[10] Analysts Comments: I have been working in computers long enough to remember when Microsoft sold its Microsoft Windows 'source code' to Russia. That provided Russia with the ability to analyze the source code, bootstrapping Russian computer capabilities. It seems obvious that the buyer/the student has now 'mastered' the code.

Russia's Cyber Attacks

11. Estonia: "*Over the weekend (9-10 March), the websites of numerous Estonian government institutions were targeted by the largest wave of DDoS (Distributed Denial of Service) attacks in the country's history. ... Among the targeted sites were those of the Estonian Police and Border Guard Board (PPA), the tax and customs board, and the Ministry of Justice. ... The attacks, [were] claimed by pro-Kremlin hackers."*[11] The Postimees newspaper reported that the impact was minimal.

12. Also on 11th March, French media reported that "*several government departments have been the targets of multiple cyber attacks ... of "unprecedented intensity"*[12] Anonymous Sudan claimed credit on its Telegram page. French unemployment agency France Travail and its subsidiary Cap Emploi were compromised exposing the data of 43 million users.[13]

13. Belgium: On 12th March Belgium's telecommunications operator 'Edpnet' warned its customers it was under cyber attack. Apparently hackers were able to penetrate its administrative systems. Impact appears to have been limited. "*Edpnet is the third major Belgian victim hackers made in a week. A ransomware attack first hit the Duvel Moortgat breweries. A few days later, that was followed up by a cyber attack on the computer systems of Koffie Beyers."*[14] (A coffee roasting company)

14. The state of Alabama confirmed that a cyber attack on 'state-sytems' began on 12th March. The attacks targeted both cities and state government. "*We understand that the disruptions were initially widespread across state services, and those effects have diminished throughout the day"*[15] Anonymous Sudan claimed responsibility.

---

10 Source: Microsoft. Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard
11 Source: TVPWorld. Estonian gov't institutions targeted in largest cyber attack in country's history
12 Source: CyberNews. French gov hit with cyberattacks of 'unprecedented intensity'
13 Source: TechReport. Massive Cyberattack On France Government Departments Leaves The Data of 43 Million Users Exposed
14 Source: Techzine. Belgian telecom operator Edpnet reports cyber attack on systems
15 Source: Dark reading: Alabama Under DDoS Cyberattack by Russian-Backed Hacktivists