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 (27) The Expanding CyberWar

This report contains selected cyber-security information from 17th to 31 March 2023.

Synopsis

1. Largely ineffective against Ukraine, Russia targets Ukrainian allies doubling the number of attacks. The potential for cyber weapons to get released outside Ukraine is increasing with Russia trading cyber ware to Iran for drones and 'wiper ware' going into wider circulation. Some final thoughts on China and TiKTok.

2. Russian 'Courses of Action' for cyber forces, including allies such as 'patriotic', mercenary, and domestic criminal hackers are *assessed* as:

> **Ongoing**: Russian cyber forces, including allied forces, have launched a series of cyber campaigns against both Ukrainian targets and Ukrainian allies. Targeting Includes strategic and general targets as well as vulnerable governments. **Analysis suggests Russian cyber attacks are increasing against Ukrainian Allies.**
>
> **Worst Case Scenario**: President Putin decides to focus Russia's cyber attacks on one country (such as Canada) or a small group of vulnerable countries. *Assessed as UNLIKELY.*
>
> **Best Case Scenario:** Russia agrees to cease or is forced to cease offensive cyber operations. *Assessed as VERY UNLIKELY.*

Russia

3. French defence firm Thales said Russia's cyberwar on Ukraine largely failed and Moscow is increasingly targeting Kyiv's European allies. *Microsoft said in a threat assessment earlier this month that Russian actors had launched attacks in at least 17 European countries in the first six weeks of this year. Thales observed that Russia was hitting Poland, the Nordic and Baltic countries with an arsenal of cyber weapons aiming to sow divisions and promote anti-war messages.* This trend probably started late in 2022. The attacks are mostly carried out by "hacktivist" groups aligned with the Kremlin. *Thales says that Poland, Latvia and Sweden were among the most affected countries.*[1]

4. During the past few weeks, we found few reports of Russian cyber attacks in Ukraine. There are ongoing cyber attacks, however as previously reported[2], the attacks

1 Source: Barron's Magazine. Russia Ramps Up Cyberattacks On Ukraine Allies: Analysts

are increasingly espionage (data collection) oriented, as opposed to highly destructive 'wiper' attacks. These cyber attacks are not usually reported as they are not considered 'significant'. In order to verify the Thales report, and validate the change in targeting, we checked on Russian cyber attacks outside Ukraine, reported during the past two weeks.

- India. Cyber-security researchers from CloudSEK reported that a Russian hacker group called 'Phoenix' compromised the Indian Health Ministry website and accessed the data of its Health Management Information System. The hackers accessed the personal information and licensing data of all employees and Chief Physicians of all hospitals in the country.[3]
- Netherlands. The 'Play' ransomware group hit the Dutch maritime logistics company 'Royal Dirkzwager', announcing the theft of stolen private and personal confidential data, employee IDs, passports, contracts, etc. on its Tor data leak site.[4] Analyst Comment: Although most security analysts do not affiliate the 'Play' ransomware group with any nation, there are indications that some of its personnel and malware code originated with the 'Conti' ransomware group – one of the first to declare its support for Russia. Also, the groups target list contains a lot of Russian 'preferred targets'.
- India, Lithuania, Poland, Slovakia, and Vatican. Cyber-security firm SentinelOne has identified a Russia-linked advanced persistent threat (APT) actor, tracked as Winter Vivern active in a number of countries. "*Recent campaigns demonstrate the group's use of lures to initiate the infection process, utilizing batch scripts disguised as virus scanners to prompt downloads of malware from attacker-controlled servers,*" the cybersecurity firm notes.[5] Targets include government organizations, high profile individuals within governments and telecommunications companies.[6] Another tactic is to get targets to download fake anti-virus software.
- EU. Blackberrys security team reported 'NOBELIUM', also known as Cozy Bear, The Dukes and APT29, attributed to the Russian Foreign Intelligence Service of the Russian Federation (SVR), had created 'lures' using the Ministry of Foreign Affairs of Poland's recent visit to the U.S. The targets are EU diplomats interested in the diplomatic visit. The campaign attempts to leverage the electronic system for official document exchange in the EU called LegisWrite.[7]
- France. The French National Assembly web site was targeted and briefly shutdown by the Russian hacker group 'NoName' using a Distributed Denial

2 Source: David Swan Consulting. Cyber Intelligence Report 230317.
3 Source: Indiawest.com. Russian Hackers Hit Indian Health Ministry's Website
4 Source: Security Affairs. Play ransomware gang hit Dutch shipping firm Royal Dirkzwager
5 Source: Security Week. Winter Vivern APT Group Targeting Indian, Lithuanian, Slovakian, and Vatican Officials
6 Source: Bleeping Computer. Winter Vivern APT hackers use fake antivirus scans to install malware
7 Source: Blackberry Security Blog. NOBELIUM Uses Poland's Ambassador's Visit to the U.S. to Target EU Governments Assisting Ukraine

of Service (DDoS) attack. Typically, no data is stolen, and web site users are inconvenienced for a few hours. NoName claim they attack entities with pro-Ukraine stances.[8]

- Slovakia. Following Slovakia sending the first of its Mig-29 fighters to Ukraine, hackers from Anonymous RU sent a warning that Slovakia should not support Ukraine. This was followed by DDoS attacks on the websites of the National Council, the National Bank and the Ministry of Defence. The web sites were disabled for a number of hours.[9]

- U.S. ProofPoint Software is tracking a Russian group, TA473, that is targeting elected US officials supporting Ukraine. The group is exploiting unpatched Zimbra servers to hack email accounts. The campaign, which also targets officials of European nations, uses malicious JavaScript that's customized for individual webmail portals belonging to various NATO-aligned organizations. The intention is to steal targets' usernames, passwords, and other sensitive login credentials.[10]

5. Analyst Comments: These are the reports that I have collected using in-house sources, we may have missed some reporting. That noted, based on what we have collected, the number of attacks on Ukrainian allies has more than doubled. The bulk of the attacks are by 'patriotic hackers', not by government groups. Several reports did note increased 'shared code' and tactics that would increase groups capabilities.

6. The 'Wall Street Journal' has reported that Russia is supplying Iran with cyber weapons in exchange for drones. Iran's focus to date has been on internet censorship tools. Citizen Lab, a University of Toronto-based research center says Russia's PROTEI Ltd tools are part of a developing mobile-phone system that would "*enable state authorities to directly monitor, intercept, redirect, degrade or deny all Iranians' mobile communications, including those who are presently challenging the regime.*"[11] Analyst Comments: Iran is generally considered a 'second tier' player in its cyber capability. As the Russian Ukraine war continues and the Russian debt to Iran increases, there is the potential for Iran to demand top tier hacking tools and techniques. Iran has the ability to 'tool up' very quickly if they recognize the opportunity.

7. A critical battlefield capability for Ukrainian forces is the portable Starlink internet. Defense One is reporting that using the Starlink service has become a double-edged sword. Ukrainian soldiers are reporting a *variety of ways in which the Russians can locate, jam, and degrade the devices, which were never intended for battlefield use.* The Russians "will find you," the soldier said. "*You need to do it fast, then get out of there.*" *Jamming began two to three months ago, and that its intensity varied from place to place. "In one place everything's fine, and in another—it doesn't work." The end result is a MacGyver-esque arms race, as Ukraine rushes to innovate and Russia moves to overcome these innovations.*[12]

8 Source: Privacy Affairs. Russian Cybercriminals Target French National Assembly Website with DDoS Strike
9 Source: Slovakia Pravda. Russian hackers attack Slovak governmental websites after country supplies Mig-29s to Ukraine
10 Source: arsTechnica. Pro-Russian hackers target elected US officials supporting Ukraine
11 Source: Wall Street Journal. Russia Supplies Iran With Cyber Weapons as Military Cooperation Grows

8. Fortinet Security is warning that wiperware ... *will become increasingly commoditized and more easily accessible to cybercriminals. Between the first and second half of 2022, wiper malware saw a substantial increase in volume, and the year ended with a clearly higher uptick. In the first half of 2022 numerous organizations publicly linked most of the detected wipers—CaddyWiper, WhisperGate, HermeticWiper, etc.—to Russian state-sponsored actors. The expansion of wiper malware into other nations later in the year caused a 53% rise in wiper activity from Q3 to Q4 alone. ... Identified wipers were either attributed to pro-Russian hacktivist organizations like Somnia or to people who ... developed their own wipers. That's a very important shift to note, as it opens the door to more families, actors, and cybercrime in general. Wiper ware is now being adopted by cybercriminal organizations and is moving outside of Europe.*[13]

China

9. Is TikTok *really* a problem? Yes. 'TiKTok' and its Chinese version 'Douyin' are owned by a Chinese company 'ByteDance, headquartered in Beijing China. The company also has an office in Santa Monica, California.[14] Chinese Internet regulations *require any company in China to provide, on demand, full access to the company's networks*. It is that access to personal data that caused *Rob Joyce, the head of the US National Security Agency's cybersecurity arm, [to say] popular video-sharing app TikTok is China's "Trojan horse" and poses a long-term, strategic cybersecurity concern.*[15]

10. Unlike Russia, much of China's hacking is covert, or at least manages to stay largely unnoticed and/or unreported. The Hacker News reports: "*a recent campaign undertaken by Earth Preta demonstrates that nation-state groups aligned with China are getting increasingly proficient at bypassing security solutions. Attack chains mounted by the group commence with a spear-phishing email to deploy a wide range of tools for backdoor access, command-and-control (C2), and data exfiltration. The findings once again highlight the increased operational tempo of Chinese cyber espionage actors and their consistent investment in advancing their cyber weaponry to evade detection.*"[16] A report in Security Weekly observes that ONE Chinese Cyberespionage group 'Mustang Panda' is currently targeting over 200 organizations including *maritime, shipping, border control, and immigration organizations.*[17]

---

12 Source: Defense One. Using Starlink Paints a Target on Ukrainian Troops
13 Source: Fortinet. The Latest Intel on Wipers
14 Source: Entrepreneur Magazine. Who Owns TikTok (Updated 2023)
15 Source: Bloomberglaw. US Spy Agency Cyber Chief Warns TikTok Is China's 'Trojan Horse'
16 Source: The Hacker News. Researchers Uncover Chinese Nation State Hackers' Deceptive Attack Strategies
17 Source: Security Week. Over 200 Organizations Targeted in Chinese Cyberespionage Campaign