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 (36)

This report contains selected cyber-security information from 22nd July to 4th August 2023.

Synopsis

1. Cl0p ransomware group continues to reveal more MOVEit! Victims. BlueBravo is a newly discovered Russian cybercampaign targeting European diplomats. NoName targets Italian companies. Russian cybersecurity executive imprisoned for 14 years. Russia claims U.S. is using Ukrainian allies to attack its critical infrastructure. Three Chinese cyber campaigns discovered.

2. 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: infrastructure, political, and media organizations as well as targets of opportunity. The number, scope and quality of Russian cyber attacks continues to increase.

MOVEit!

3. The MOVEit! hack continues to grow. A German cybersecurity firm estimated that by 3 August, at least 567 organizations have been victimized. In addition, an estimated 34.7 to 39.7 million individuals have had personal data compromised.[1] These estimates are based on Cl0p's ransomware data leak site and breach notifications by organizations. So far Cl0p appears to be content to go after organizations, ignoring individuals. The cybersecurity report notes that the percentage of victims that paid ransoms "*in the second quarter of 2023 fell to a record low of 34%. ... While the MOVEit campaign may end up impacting over 1,000 companies directly, and an order of magnitude more indirectly ... It is likely that the Cl0p group may earn $75-100 million dollars just from the MOVEit campaign, with that sum coming from just a small handful of victims that succumbed to very high ransom payments.*"[2]

4. The Cl0p ransomware group is trying new tactics to increase the percentage of victims that 'pay up'. This includes setting up dedicated web sites to expose major

1 Source: KonBriefing. MOVEit hack victim list
2 Source: Security Week. MOVEit Hack Could Earn Cybercriminals $100M as Number of Confirmed Victims Grows

targets, posting stolen data, and recruiting other hacker gangs to help process victims. According to IT World Canada: *"The first publicly posted alleged stolen data were from consulting firms PwC, EY, Aon and financial firm TDAmeritrade. Soon after they were publicly posted the websites were unavailable. It isn't clear why."*[3] Analysts Comment: It should be noted that the estimates provided are based on conservative data. We don't have a picture of how many victims have paid quickly in order not to be embarrassed. Since Cl0p has recruited other hackers to assist them, there is no way to tell if anyone has commenced demanding ransoms from individuals. *We assess* that this hack will continue to claim more victims for the foreseeable future.

Russia vs Ukraine CyberWarfare

5. A new Russian cyber campaign targeting European diplomatic entities has been identified. The cyber attacks are attributed to one of Russia's Foreign Intelligence Service's (SVR) hacking group known as BlueBravo. The campaign uses phishing attacks containing a file 'lure' to deliver a new backdoor called GraphicalProton.[4] Recorded Future reports: "*BlueBravo appears to prioritize cyber espionage efforts against European government sector entities, possibly due to the Russian government's interest in strategic data during and after the war in Ukraine. As the war in Ukraine continues, it is almost certain that BlueBravo will continue to consider government and diplomatic institutions high-value targets for the foreseeable future. ... It is likely that BlueBravo, and by extension the Russian intelligence consumers* [that are] *reliant on the data BlueBravo provides, views these organizations as providing strategic insight into the decision-making process of governments allied with Ukraine."*"[5]

6. The Russian hackivist group Noname057(16) claimed credit for Denial of Service (DoS) attacks against websites of Italian transportation companies on 1st of August. This was followed by attacks on at least five Italian banks on August 2nd. "*A source at one of the banks targeted in the attack said that their site crashed because of heavy traffic but only for a short period of time.*"[6] Noname057(16) said the attacks were "revenge" for the meeting of Prime Minister Meloni with US President Biden.[7]

7. **Expanding Russian Target List**: Canada's Communications Security Establishment (CSE) through its Canadian Centre for Cyber Security (Cyber Centre) is warning of attacks by ALPHV/BlackCat ransomware. "*ALPHV/BlackCat has presented a threat to Canadian organizations since at least January 2022 and will very likely continue to threaten Canadian and international organizations into the latter half of 2023.*"[8] The warning is based in part on the work of Blackberry who said: "*BlackCat has most often*

3 Source: ITWorldCanada. Cyber Security Today, July 24, 2023
4 Source: The Hacker News. BlueBravo Deploys GraphicalProton Backdoor Against European Diplomatic Entities
5 Source: Recorded Future. BlueBravo Adapts to Target Diplomatic Entities with GraphicalProton Malware
6 Source: Reuters. Russian hackers crash Italian bank websites, cyber agency says
7 Source: Breaking Latest News. Pro-Russian attacks on sites of Italian banks and transport companies. Limited outages
8 Source: Canadian Security Establishment (CSE). Alert - ALPHV/BlackCat Ransomware Targeting of Canadian Industries

targeted companies in the financial, manufacturing, legal, and professional services industries — but BlackCat's exploits span all industries."[9] ALPHV/BlackCat is known for their use of a triple-extortion tactic: making individual ransom demands for the decryption of infected files; for not publishing stolen data; and for not launching denial of service (DoS) attacks.

8. Anonymous Sudan, a Russian hacking group, claimed a one-hour distributed denial of service attack on 'OnlyFans'.[10] Only Fans describes itself as "*18 + subscription platform empowering creators to own their full potential, monetize their content, and develop authentic connections with their fans."*[11] Others describe the social media platform as a platform for sex workers and content creators. Analysts Comment: Attacking a porn site is a good way to lose credibility.

9. **Russian cybersecurity executive imprisoned for 14 years**. Ilya Sachkov founded 'Group-IB', a cybersecurity firm that specializes in the "*detection and prevention of cyberattacks and works with Interpol and several other global institutions."* Sachkov was considered a star in Russia's technology world, receiving an award from President Putin in 2019. The case is classified in Russia, however it is believed that he is accused of "*passing classified information to foreign spies."*[12] According to Bloomberg News he 'personally' passed information on the Russian 'Fancy Bear' influence operation against the 2016 United States Presidential election to the U.S. government. Ilya Sachkov has been sentenced to fourteen years in a high-security penal colony. Group-IB was not named in the charges, however it is noteworthy that the company exited the Russian marketplace in April 2023.

10. Analysts Comment: It is *assessed* as *highly likely* that the Russian government did not want evidence of its hackers activity in the American elections provided to the U.S. government. 'Fancy Bear' is a hacker group attributed to Russian Military Intelligence (GRU). Since Group-IB was moved to Singapore (from Russia) and is out of reach of the Russian government, Ilya Sachkov is being held accountable.

11. **Russia claims U.S. is attacking its critical Infrastructure**: On the 24th of July Nikolay Patrushev, Secretary of the Russian Security Council, said "*The United States is launching cyberattacks against Russia's critical information infrastructure. … The Pentagon's cybercommand, the National Security Agency and the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence are planning and steering information attacks under the Ukrainian flag … American special services enlist Ukrainian hacker groups for such attacks … It is a secret to no one that Washington and its allies are directly involved in the conflict in Ukraine,*" he noted. "*Along with the aggressive information and propaganda campaign and weapons supplies, the US Special Operations Command is supervising the activities of the Ukrainian Center for Information and Psychological Operations.*"[13] Analysts Comments: No proof of American involvement or NATO involvement in offensive operations against Russia has been

9 Source: Blackberry. BlackCat Malware (AKA ALPHV)
10 Source: CyberScoop. Pro-Russian hacktivists increase focus on Western targets. The latest is OnlyFans.
11 Source: Only Fans. Who We Are
12 Source: Reuters. Russian court jails cyber security executive for 14 years in treason case
13 Source: Tass. US mounts cyberattacks on critical Russian infrastructure 'under Ukrainian flag'

provided.

Chinese Campaigns Breach Sensitive American Infrastructure

12. A report in Ars Technica outlines three Chinese cyber campaigns "*intent on burrowing into the farthest reaches of sensitive infrastructure, ... establishing permanent presences there if possible. In the past two years, they have scored some wins that could seriously threaten national security.*" The threats are:

- Zirconium, also known as APT31 or Judgement Panda is a known Chinese government hacking group. They planted "a *detailed suite of advanced spying tools used over the past two years by one group to establish a "permanent channel for data exfiltration" inside industrial infrastructure. The attacks include targeting air-gapped systems. According to Kaspersky a worm component of the malware can infect removable drives that when plugged into an air-gapped device, locate sensitive data stored there and copy it. When plugged back into an Internet-connected machine, the infected disk device writes it there."*[14]
- A Chinese campaign known as Volt Typhoon (aka "Vanguard Panda,") compromised US military critical infrastructure, hiding malware that could cause disruptions inside in bases. First found in Guam, "*Biden administration officials have confirmed that Volt Typhoon's malware is much more endemic than previously thought; responders have found it planted inside numerous networks controlling the communications, power, and water feeding US military bases at home and abroad.*"[15] This attack is described as 'unresolved'. Investigation is ongoing
- Chinese APT Storm-0558 "*acquired an inactive signing key used to grant access to Microsoft consumer cloud accounts. ... The hack allowed Storm-0558 to track the email accounts of about 25 organizations, including the US Departments of State and Commerce and other sensitive organizations for roughly a month."*[16]

13. The U.S. Congress reacted strongly to the third attack, launching an investigation into 'Microsoft's neglience'. The House Committee on Oversight and Accountability requested briefings from the House Committee on Oversight and Accountability requested briefings, observing: "*China appears to be graduating from 'smash and grab heists' that used to be 'noisy' and 'rudimentary' to a level described by security experts as 'among the most technically sophisticated and stealthy ever discovered.*"[17]

---

14 IBID.
15 Source: DarkReading. China's Volt Typhoon APT Burrows Deeper Into US Critical Infrastructure
16 Source: Ars Technica. Multiple Chinese APTs establish major beachheads inside sensitive infrastructure
17 Source: NextGov.com. House panel probes China-linked email hacks