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 (24) Updates and Sanctions

This report contains selected cyber-security information from 3rd to 17th February 2023.

Synopsis

1. Russia got very close to hacking a dozen U.S. energy providers as it launched it's war with Ukraine. Russia launched two new cyber attacks against Ukraine. The UK and U.S. have begun 'sanctioning' Russia's criminal hackers. Russia's parliament is considering recognizing cyber-criminals contributions to *the defense of its interests,* potentially formalizing immunity from foreign prosecution. Anonymous claims they hacked a Russian ISP providing surveillance information on Russian citizens. Vmware servers get hacked and rehacked. Canada's bookseller, Indigo, remains partially closed.

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 strategic targets and general targets** as well as vulnerable governments.
>
> **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. Hackers linked to Russia got very close to being able to take a dozen U.S. electric and gas facilities offline in the first weeks of the war in Ukraine, ... "*It [PIPEDREAM] wasn't employed on one of its targets, they weren't ready to pull the trigger, they were getting very close.*" The U.S. government disclosed last year that the new malware — called PIPEDREAM — was capable of infiltrating U.S. industrial control systems across multiple key sectors, Robert M. Lee, the founder and CEO of Dragos, which helps companies respond to cyberattacks, comments suggested that the danger was more acute than officials had disclosed. Lee described the malware as a "*state-level, wartime capability.*" PIPEDREAM malware is the "*first ever*" type that can be used across a variety of industrial control systems, and that was not designed to disrupt one specific

system — making it particularly dangerous. The malware also does not get into systems through vulnerabilities that could be patched, making it very hard to defend against. Deployment was halted by a coalition of U.S. government and cyber industry groups. Lee said that Dragos worked with partners including the Cybersecurity and Infrastructure Security Agency, the Department of Energy, the FBI and the National Security Agency.[1]

4. Analyst Comments: The PIPEDREAM attack on a dozen U.S. energy providers could have caused long term destruction of oil and gas pipelines and energy distribution systems. Hacking or in this case 'cyberwarfare', would have manifested in the physical world with no oil and gas for millions of people. Russia has used similar tactics before.[2] Given that Russia is not 'winning' against Ukraine, we can extrapolate that Russia/Putin will '*Almost Certainly'* use these tactics again to achieve his objectives. This raises two questions: 1. When will the next cyber attack on infrastructure happen? And 2. When does a cyber attack become a declaration of war?

5. **Update ION Group Hack:** In February 2nd the Russian Lockbit hacker group hacked the ION Group, part of the commodities group of the London Stock Exchange. Trading in commodities was ceased. On February 6th the hackers said a 'ransom has been paid' although they declined to say how much it was or offer any evidence. ION declined to comment.[3]

6. **New Cyber Attacks on Ukraine:** The Ukrainian Computer Emergency Response team (CERT-UA) issued a warning on February 8th that Russian hackers had launched attacks using a legitimate remote access software named Remcos. Bogus emails from Ukrainian telecom company Ukrtelecom contain an executable for Remcos remote access software. This would give the attacker full access to the victims system. CERT-UA identified a Russian state-sponsored threat actor known as Gamaredon or (UAC-0050) as the originator.[4] Another group, Nodaria or (UAC-0056) launched 'Graphiro' which is an information harvester. The Symantec security team assessed that: "*While Nodaria was relatively unknown prior to the Russian invasion of Ukraine, the group's high-level activity over the past year suggests that it is now one of the key players in Russia's ongoing cyber campaigns against Ukraine.*"[5]

7. Russian based criminal hacking gangs have extorted hundreds of millions of dollars from victims while causing massive disruption. In a new joint effort, UK and US governments are unmasking some gang members. Seven alleged members of the Conti and Trickbot ransomware gangs are being sanctioned with the publishing of their real-world names, dates of birth, email addresses, and photos. Other sanctions include: freezing of financial assets, travel restrictions and having indictments unsealed.[6]

1 Source: Politico. Russian-linked malware was close to putting U.S. electric, gas facilities 'offline' last year
2 Russia is responsible for more than 25 known major cyber attacks since 2007. Source: Privacy Sharks. Russian CyberAttacks – Detailed Statistics and History
3 Source: Business Insurance. Hackers who breached ION say ransom paid
4 Source: The Hacker News. CERT-UA Alerts Ukrainian State Authorities of Remcos Software-Fueled Cyber Attacks
5 Source: The Hacker News. Russian Hackers Using Graphiron Malware to Steal Data from Ukraine
6 Source: Wired Magazine. Russia's Ransomware Gangs Are Being Named and Shamed

8. The sanctioned hackers are accused of working in various capacities for TrickBot and Conti, ranging from developing ransomware to money laundering and managing communication and command-control servers. The most senior member, Vitaly Kovalev, is accused of hacking US bank accounts dating back to at least 2010. TrickBot has been one of the more prolific cyber crime outfits since it first appeared in 2016. Trickbot and Conti's longevity may be owed in part to connections to Russian intelligence. The U.S. Treasury Department, the U.S. Office of Foreign Assets Control, U.K.'s Foreign, Commonwealth, and Development Office are collectively enforcing the sanctions.[7]

9. Analysts Comment: Sanctions are thought to be responsible for a recent reduction in ransom payments.

10. Alexander Khinshtein, head of the [Russian] Duma committee on information policy, said "*The Russian government recognizes the importance of cybercriminal gangs and hacktivists' contribution to the defense of its interests. ... The question of their exemption from liability needs to be worked out. ... We are talking about, in general, working out the exemption from liability of those persons who act in the interests of the Russian Federation in the field of computer information both on the territory of our country and abroad.*" The Russian Parliament announced that this proposal will be discussed more in detail in the next months with the intent to better formulate this initiative.[8]

11. Analyst Comments: Russian Law Enforcement has co-operated with external police agencies such as InterPol and EU Security to arrest the most outrageous hackers, even during the Ukrainian invasion. If the Russian Duma pass 'exemption from liability' legislation, all Russian based hackers will be out of the reach of western authorities. Recovery of ransoms or any other extorted fees would be impossible. 'Sanctions' as discussed in paragraph five would be much less effective. Russia would almost certainly acquire additional support from protected hackers.

Ukraine

12. The hacker group 'Anonymous' has breached Russian Internet provider Convex. Sources disagree on how much data was exfiltrated, either 128 Gigabytes OR 128 Terabytes of data.[9] What sources agree on is that Anonymous has documentation of the Kremlin's unauthorized monitoring of Russian citizens. This includes illegal wiretapping, espionage, and unwarranted monitoring of citizens, all of which are against Russian law. The EU protested that Russia's laws for 'Operative Investigative Activities' surveillance system did not provide sufficient and adequate protection guarantees. Russia responded to the EU by passing a law enabling police to demand ISP records and data without a court order.

7 Source: CPO Magazine. More Russian Hackers Hit With Sanctions as TrickBot Ransomware Gang Members Make the List

8 Source: Security Affairs. Russian Government evaluates the immunity to hackers acting in the interests of Russia

9 Assessment: Given the wide ranging material that the Russian government is receiving, 128 Terabytes is an entirely plausible quantity of data. Anonymous has leaked 128 Gigabytes of the stolen data. Source: Information Security Buzz: 128GB Of Russian ISP Convex Data Leaked By Anonymous Hacker

13. A hacker who is part of Anonymous affiliate group called Caxxii has released 128 Gigabytes of the Convex data. They claim that Russia's Federal Security Service (FSB) runs the 'Green Atom monitoring program' which monitors citizens' phone and internet activities. *"'Green Atom' (TS ORM fsb) refers to the installation and maintenance of wide-ranging surveillance equipment that is used to monitor the online activity of all traffic in and out of Convex." ... "They are actively transmitting data to Moscow. It's not just preemptive tapping."* Anonymous/Caxxii claims they hold additional, unpublished details about the FSB's intelligence-gathering operations.[10]

14. **VMWare:** The FBI and CISA are aware of more than 3,800 servers that were compromised around the world in ESXiArgs ransomware attacks. Victims include Florida's Supreme Court and universities in the United States and Europe. An analysis of the file-encrypting malware deployed in the ESXiArgs attacks showed that it has targeted files associated with virtual machines (VMs). However, experts noticed that the ransomware mainly targeted VM configuration files, but did not encrypt the flat files that store data, allowing some users to recover their data.[11] The US Cybersecurity and Infrastructure Security Agency (CISA) created an open source tool designed to recover their files without paying a ransom. Days later a new malware variant was published and is reinfecting servers rapidly. In 24 hours 900 hosts were "upgraded to the latest ransomware variant".[12] The issue was vmware servers were not being kept patched and up to date. That allowed the attacker to use old exploits.

Canada

15. On Friday 10th February Canada's Indigo (Chapters) bookstores were hacked. Within hours, the company posted a message on its website, saying it "experienced a cybersecurity incident. Indigo said that customer debit and credit card information were not compromised. The company has changed its in-store payment technology as part of its incident response. Their website remains offline as of Thursday 16th leaving customers unable to place on-line orders, accept exchanges and returns. Multiple cybersecurity companies say the incident has all the hallmarks of a ransomware attack.[13] It is notable that no Indigo data has been posted and no hacker groups are boasting about the hack.

---

10 Source: Security Affairs. Anonymous leaked 128GB of data stolen from Russian ISP Convex revealing FSB's warrantless surveillance

11 Source: Security Week. ESXiArgs Ransomware Hits Over 3,800 Servers as Hackers Continue Improving Malware

12 Source: Tech Target. New ESXi ransomware strain spreads, foils decryption tools

13 Source: CBC. Indigo website still offline nearly 1 week after cybersecurity incident