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 (30) Russian Cyber Ops Falter

This report contains selected cyber-security information from 29th April to 12th May 2023.

Synopsis

1. Russia targets Ukraine's government organizations in three malware campaigns. Sweden's parliament and France's Senate were hit by Russian DDoS attacks. Russia's 'patriotic' hacker group, KillNet, reorganizes again. A 20 year Russian cyber campaign is shutdown.

2. Russia appears to be committed to the following 'Course of Action' for its cyber forces:

> **Ongoing**: Russian cyber forces, including allied forces, have launched a series of cyber campaigns against both Ukrainian targets and their allies. Targeting Includes strategic and general targets as well as vulnerable governments. **Russian cyber attacks are increasing against Ukrainian Allies.**

Russia

3. **Russian cyber operations vs Ukraine**: Ukraine's Computer Emergency Response Team (CERT-UA) reports that Russian hackers have been targeting government organizations with fake Windows Update emails. The emails actually contain a command that "*downloads a PowerShell script on the computer, simulating a Windows updating process while downloading a second PowerShell payload in the background. The second-stage payload is a basic information harvesting tool that abuses the* '*tasklist*' *and* '*systeminfo*' *commands to gather data and send them to a Mocky service API via an HTTP request."* The 'Mocky' application is "*abused in this case for data exfiltration."*[1]

4. The attacking unit is reported to be APT38, also known as 'Fancy Bear', linked by some security companies such as 'Mandiant' to Russia's GRU [military] intelligence agency.[2] The objective appears to be information collection, as opposed to ransomware or destructive 'wipers'. The campaign is highly targeted. Meaning it is focused on specific organizations and individuals. Email addresses were *very probably* (70-89%) collected by a combination of: NTC Vulcan (Russian cyber consulting company) and

[1] Source: Bleeping Computer. Hackers use fake 'Windows Update' guides to target Ukrainian govt

[2] Source: Register. Russia's APT28 targets Ukraine government with bogus Windows updates

Russian criminal hacker specialists.

5. Another campaign by a different GRU hacker group, ‘Sandworm’ aka ‘Voodoo Bear’ uses WinRAR in destructive attacks on Ukraine’s public sector. The attacks start with stolen VPN (Virtual Private Network) credentials. A script-based wiper malware called RoarBAT performs a recursive search for files with a specific list of extensions and irrevocably deletes them using the legitimate WinRAR utility.[3]

6. An ongoing campaign is using ‘invoice-themed lures’ targeting Ukrainian Public Sector organizations. Again, targeted emails are sent “*using compromised accounts and come with a ZIP archive that, in reality, is a polyglot file containing a decoy document and a JavaScript file. The JavaScript code is then used to launch an executable that paves for the execution of the SmokeLoader malware. SmokeLoader, first detected in 2011, is a loader whose main objective is to download or load a stealthier or more effective malware onto infected systems. This operation is assessed as a financially motivated operation carried out with the goal of stealing credentials and making unauthorized fund transfers. CERT-UA attributed the activity to a threat actor it calls UAC-0006”*[4] Analysts Comment: UAC-0006 is assessed with high probability (70-89%) as a Russian based criminal hacker group. The impact of all three campaigns is *assessed* as low.

7. **Russian cyber operations vs West:** The hacker group 'Anonymous Sudan' claimed responsibility for a series of cyber attacks against Israel. The attacks commenced on April 25th with *the distributed denial-of-service (DDoS) attacks that took down the personal website of Israeli Prime Minister Benjamin Netanyahu and the hijacking of his Facebook account.... it is believed that the group is responsible for the attacks on the websites of Haifa Port and Israel Ports Development company. ... They also claimed responsibility for bringing down the National Insurance Institute's website as well as that of Mossad, Israel's spy agency. ...* this was followed by *the sprawling power outages in Israel, including major cities such as Tel Aviv and Beersheba”*.[5] *“The websites of Israel Aerospace Industries (IAI), Israel Weapon Industries (IWI) – an Israeli firearms manufacturer, Rafael Advanced Defense Systems Ltd. and Evigilo Ltd., which develops and delivers emergency mass-notification and alert multi-channel solutions, were hacked.* On the next Sunday more attacks *“targeted the Hebrew-language Radio 103FM and the website of Check Point Software Technologies Ltd., an American-Israeli multinational provider of software and combined hardware and software products for cyber security.”*[6]

8. Analysts Comments: 'Anonymous Sudan' has previously been identified by some cyber security companies as a ‘cover’ for a Russian hacking group. As Iran routinely rediscovers, Israel does **not** like being hacked. Retaliation cyber attacks are common and will probably originate from Israel’s cyber force known as 8200.

9. A Russian hacker group identified as ‘Nomadic Octopus’ “*has been observed spying*

[3] Source: Security Affairs. Russia-linked Sandworm APT uses WinRAR in destructive attacks on Ukraine’s public sector

[4] Source: The Hacker News. CERT-UA Warns of SmokeLoader and RoarBAT Malware Attacks Against Ukraine

[5] Source: Dark Reading. 'Anonymous Sudan' Claims Responsibility for DDoS Attacks Against Israel

[6] Source: PressTV IR. Israeli radio station, software company targeted by cyber attack

on Tajikistan’s high ranking government officials, public service infrastructures, and telecoms services”. This campaign “*has been ongoing since 2020, resulting in the compromise of government networks, individual computers, and operational technology (OT) devices, such as gas station systems. ... However, the group was seen removing access to victims that were not deemed valuable and which were unrelated to government infrastructure or public services.*” Computer security company ‘Prodaft’ believes access was gained through Tajikistan’s telecommunications company, probably since 2000.[7] Analysts Comment: We *assess* this campaign as part of Russia’s ‘normal’ activities and not part of the Ukrainian conflict.

10. On the same day that Swedish politicians met Ukraine's president, Volodymyr Zelenskiy, Sweden’s parliament was hit by a Distributed Denial of Service (DDoS) attack. “*The website of the Swedish parliament, known as the Riksdag, is used by Swedish citizens to access an array of public services, as well as to find information about the workings of the government.*”[8] The parliamentary web site was partially down on May 3rd and reported as slow May 4th.[9]

11. On May 5th the web site of the French Senate was forced offline by a DDoS attack. The pro-Russian hacker group ‘NoName’ claimed responsibility on it’s ‘Telegram’ channel saying: “*it had acted because “France is working with Ukraine on a new ‘aid’ package which may include weapons.*[10] ... *According to NoName’s Telegram posts, the collective targeted several other French organizations, such as France’s National Centre for Space Studies and Naval Group, a French industrial group specializing in naval defense manufacturing.”*[11]

12. **KillNet:** The American cybersecurity company ‘Flashpoint’ has released an analysis of the Russia patriotic group ‘KillNet’. Flashpoint reports: *KillNet announced on April 27 on Telegram that it is ending its hacktivist activities and rebranding as Black Skills, which the group dubbed a “private military hacking company.” According to the group, it will continue attacking Western entities - but instead of doing so “altruistically” it will instead take orders from private and public entities for money*.[12] The announcement was made a couple of days after information about the alleged real-life identities of Killnet’s core group members had started circulating online. Part of the announcement is a reorganization, the third since last fall when it turned itself into a “collective,” aiming to absorb smaller hacktivist groups under its umbrella.

13. Flashpoint reports that KillNet has been unsuccessful in making money. The group has tried:[13]

- Applying for sponsorship from the Russian state and from Russian business people several times over the past months,
- Selling access to various documents exfiltrated from NATO countries,

[7] Source: Security Week. Russian APT Hacked Tajikistani Carrier to Spy on Government, Public Services

[8] Source: Tech Monitor. Swedish government website hit by DDoS cyberattack

[9] Source: Reuters. Swedish parliament website hit by DDoS attack

[10] Source: Security Week. Pro-Russian Hackers Claim Downing of French Senate Website

[11] Source: Cybernews. Pro-Russian group knocks out French Senate’s website

[12] Source: Flashpoint. For Money and Attention: Killnet Apparently Reorganizes Again

[13] Source: Flashpoint. For Money and Attention: Killnet Apparently Reorganizes Again

- Selling the “Infinity” forum, which the group created in December 2022,
- Promoting its paid “hacking school” ($249 for a course) which is apparently yet to launch,
- Advertising its paid DDoS services, and
- Soliciting money from its followers.

14. Flashpoint says: Killnet remains widely ridiculed on top-tier Russian-speaking forums. Flashpoint has also pointed that Killnet has remained a primarily financially-motivated group using the media exposure provided by an eager Russian pro-Kremlin media ecosystem to promote its DDoS-for-hire services. Some hackers groups who started with KillNet, such as Phoenix, AKUR and Legion, have moved towards cybercrime, operating within Russia’s cyber targeting preferences.

15. **20 year Russian Cyber Campaign ‘Snake Malware’ ‘disrupted’:** For 20 years Russian hacker group “Turla”, *“a unit within Center 16 of the Federal Security Service of the Russian Federation (FSB),”* has been operating ‘Snake Malware’. Snake malware compromised target computers in NATO (and other) countries, “*to steal sensitive documents of governments, journalists, and other targets of interest to the Russian Federation.”*[14] *“Russian government actors have used this tool for years for intelligence collection,” said Rob Joyce, NSA Director of Cybersecurity. “Snake infrastructure has spread around the world.* [over 50 countries] *The technical details will help many organizations find and shut down the malware globally.”*[15]

16. “*The Snake implant is considered the most sophisticated cyber espionage tool designed and used by Center 16 of Russia’s Federal Security Service (FSB) for long-term intelligence collection on sensitive targets. To conduct operations using this tool, the FSB created a covert peer-to-peer (P2P) network of numerous Snake-infected computers worldwide. Many systems in this P2P network serve as relay nodes which route disguised operational traffic to and from Snake implants on the FSB’s ultimate targets. Snake’s custom communications protocols employ encryption and fragmentation for confidentiality and are designed to hamper detection and collection efforts. ... Although Snake uses infrastructure across all industries, its targeting is purposeful and tactical in nature.”*[16]

17. The effort to disassemble the malware is remarkable. The snake malware was rewritten causing it to circulate and neutralize its own code. Technical specifications were circulated internationally and publicly. The investigation is ongoing.

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

[14] Source: U.S. Justice Department. Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service

[15] Source: U.S. NSA. U.S. Agencies and Allies Partner to Identify Russian Snake Malware Infrastructure Worldwide

[16] Source: U.S. Defence Department. Hunting Russian Intelligence “Snake” Malware