Volume 4: Edition 4

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: Law Enforcement Strikes Back

This report contains selected cyber-security information from 9th to 22nd Feb 2024.

Synopsis

1. The FBI gets busy, tackling Russia's GRU Hackers, the ALPHV/BlackCat ransomware group and China's 'Volt Typhoon' hackers. The UK's crime agency shuts down the LockBit ransomware group. Apparently China has developed sub-contractors who conduct hacking operations for the PRC. Israel attacks Iran's pipelines, but was it a cyber attack?

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.

Russia's Cyber Attacks Get Compromised

3. **FBI vs Russia's GRU**. "*Cybercriminals installed Moobot malware on Ubiquiti Edge OS routers using publicly known default administrator passwords. ...* "*Well over a thousand*" *home and small business routers were infected turning them into a 'botnet'.*"[1] "*Botnets are groups of hijacked hardware or systems that are chained together across other compromised equipment, forming a clustered data transfer network.*"[2] "Then the GRU hackers (tracked as APT 28, Forest Blizzard, and Fancy Bear among other names) used Moobot to install scripts and files changing the botnet, "*into a global cyber espionage platform.*"[3]

4. The U.S. Department of Justice got court authorization to take over the Moobot botnet. The new release said they "*leveraged the Moobot malware to copy and delete stolen and malicious data and files from compromised routers.*"[4] U.S. Attorney General Merrick Garland said "*Russian intelligence services turned to criminal groups to help them target home and office routers, but the Justice Department disabled their scheme.*"[5]

[1] Source: The Register. Feds dismantle Russian GRU botnet built on 1,000-plus home, small biz routers

[2] Source: Next Gov. FBI disrupts botnet controlled by Russian security services

[3] Source: The Register. Feds dismantle Russian GRU botnet built on 1,000-plus home, small biz routers

[4] Source: Security Week. FBI Dismantles Ubiquiti Router Botnet Controlled by Russian Cyberspies

5. **Another GRU Hacking Campaign Exposed:** A Russian government hacking team known as ‘Winter Vivern’ (other aliases include ‘TA473’ and ‘UAC0114’) is exploiting a Roundcube email server flaw to “*collect military and political intelligence, particularly associated with the conflict in Ukraine.*”[6] “*Over 80 organizations ... primarily located in Georgia, Poland, and Ukraine*”, have been victimized. “*Recorded Future said it also found evidence of TAG-70 targeting the Iranian embassies in Russia and the Netherlands, as well as the Georgian Embassy in Sweden. ... The targeting of Iranian embassies in Russia and the Netherlands suggests a broader geopolitical interest in assessing Iran's diplomatic activities, especially regarding its support for Russia in Ukraine.*"[7]

6. **Russian ‘Turla’ malware campaign Exposed**: Cisco Talos security researchers discovered new malware they call TinyTurla-NG and TurlaPower-NG. Talos was collaborating with a Polish NGO when it discovered the new malware “*used by the Russian hacker group Turla to maintain access to a target’s network and to steal sensitive data. The threat actor used multiple websites running vulnerable versions of WordPress for command and control (C2) purposes and to host malicious PowerShell scripts. Turla is a cyber espionage threat group active since at least 2004 and linked to a Russian intelligence service, the Federal Security Service (FSB).”*[8]

7. **FBI vs ALPHV/BlackCat:** The FBI has also been dealing with the Russia based ALPHV/BlackCat ransomware gang. On 19th December, 2023, the FBI replaced the groups website with an announcement that it had been seized. A decryption tool for the gangs ransomware was published by law enforcement. The hackers regained “*control over its dark website on multiple occasions. This triggered an intense back-and-forth struggle on the dark web, pitting the criminal syndicate against the formidable U.S. government agency. ... a confidential source played a pivotal role in helping the FBI access more than 900 public/private key pairs controlling ALPHV ‘s darknet infrastructure. ... This operation allowed the FBI to monitor the gang’s activities for months, culminating in the successful seizure of its websites in December. The ALPHV /BlackCat ransomware gang has been a prolific threat, earning $300 million in ransom proceeds from over 1,000 victims worldwide.”*[9] ALPHV/BlackCat has not surrendered. Instead, they have changed their business processes, their communications with subordinate groups, and their ransomware, all while increasing their collaboration with the LockBit ransomware group.

8. ALPHV/BlackCat is continuing to operate, compromising Canadian oil and gas pipeline operator Trans-Northern Pipelines. On 14th February, the group claimed that 190GB of data was exfiltrated. “*Trans-Northern later confirmed that some of its internal computer systems had been targeted by a cyber incident in November*. ... *In addition to admitting an attack against Trans-Northern, ALPHV/BlackCat has also*

[5] Source: The Register. Feds dismantle Russian GRU botnet built on 1,000-plus home, small biz routers

[6] Source: Spice Works. Roundcube Vulnerabilities Exploited by Russian Hackers to Attack More Than 80 Organizations

[7] Source: The Hacker News. Russian-Linked Hackers Target 80+ Organizations via Roundcube Flaws

[8] Source: Bleeping Computer. Turla hackers backdoor NGOs with new TinyTurla-NG malware

[9] Source. The Cyber Express. The Cat-and-Mouse Game: ALPHV Ransomware vs. FBI – A Cybersecurity Saga Unfolds

taken credit for infiltrating the systems of U.S. electric utility cooperative Lower Valley Energy, Canadian crude oil treatment and water management firm Rush Energy Services, and Spanish electricity provider SerCide."[10]

9. **UK's NCA vs LockBit:** On 20th February a group of Law Enforcement Agencies lead by the UK's National Crime Agency seized "*the entire "command and control" apparatus for the ransomware group LockBit.*" ... "*Europol said that two LockBit actors had been arrested in Poland and Ukraine, and that a further two defendants, thought to be affiliates, had been arrested and charged in the US. Two more individuals have been named, and are Russian nationals still at large. Authorities have also frozen more than 200 cryptocurrency accounts linked to the criminal organisation.*"[11]

China

10. **FBI vs Volt Typhoon:** Excerpts from SC Magazine's article: Going from defense to offense against China's Volt Typhoon APT group dated: 20 Feb 2024.[12] For far too long, cybersecurity has been considered "preventive" or "reactive." ... We are now witnessing the rise of offensive cyber operations by a (U.S.) domestic law enforcement agency that has demonstrated a significant ability to identify, penetrate, and dismantle criminal and nation-state networks. ... A logical move was to target the infrastructure that underpinned the cyber capability to deny our adversaries the cyberspace assets needed to conduct their campaigns.

11. According to a recent joint CISA/FBI/NSA advisory issued February 7: "Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions." It's clear what Volt Typhoon intends. They are preparing for a future war. ... this was Intelligence Preparation of the Battlefield. In the book Emerging Cyber Threats and Cognitive Vulnerabilities, the authors estimated in 2017 that China had more people actively involved in cyber than the United States, United Kingdom, Russia, Germany, and North Korea combined.

12. Analysts Comment: I have previously noted that China has a track record of hacking critical infrastructure and maintaining access.[13] This does NOT negate the assessment that Volt Typhoon was engaged in "Intelligence Preparation of the Battlefield". I do not *assess* the threat from Volt Typhoon's hacks as immediate. However, the hacked systems are a strategic vulnerability to Western Nations.

13. **i-Soon data leak:** Apparently a disgruntled staff member who works for I-Soon (aka Anxun), a Chinese private contractor, leaked a range of the company's hacking tools and services. The company operates as an Advanced Persistent Threat (APT)-for-hire for China's Ministry of Public Security (MPS). Cyber Security company 'SentinelOne' described I-Soon as "*a company who competes for low-value hacking*

[10] Source: SC Magazine. Canada's Trans-Northern Pipelines claimed to be attacked by ALPHV/BlackCat
[11] Source: The Guardian. Seized ransomware network LockBit rewired to expose hackers to world
[12] Source. SC Magazine. Going from defense to offense against China's Volt Typhoon APT group
[13] Source: Cyber Intelligence Report. CyberWarfare Update plus Cybercrime in Canada

contracts from many government agencies. ... Chinese government agencies supply a list of targets they're interested in ... and something of a competitive industry has sprung up to gain the access requested. ... SentinelOne and Malwarebytes found I-Soon claims to have developed tools capable of compromising devices running Linux, Windows, macOS, iOS, and Android. The Android attack code can apparently retrieve and send a user's entire messaging history from Chinese chat apps, plus Telegram."[14] Other capabilities include:

- Portable devices for attacking networks from the inside.
- Special equipment for operatives working abroad to establish safe communication.
- User lookup database which lists user data including phone number, name, and email, and can be correlated with social media accounts.
- Automated penetration testing framework.[15]

14. Analysts Comment: Having private contractors hacking for the Chinese government *infers* that the private contractors can hire hackers. The Chinese government gets to maintain separation (and deniability) from criminal hackers.

Israel vs Iran

15. **Israel Strikes Iran's Pipelines**: Iran's Oil Minister Javad Owji has accused Israel of a series of attacks targeting Tehran's nuclear program. On 14th February, "*blasts hit a natural gas pipeline running from Iran's western Chaharmahal and Bakhtiari province up north to cities on the Caspian Sea."* The "*explosion of the gas pipeline was an Israeli plot,*" Owji said. "*The enemy intended to disturb gas service in the provinces and put people's gas distribution at risk.*"[16] "*Local governors and officials from Iran's national gas company spoke of widespread outages in five provinces. ... Energy experts estimated that the attacks on the pipelines, which run 800 miles and carry 2 billion cubic feet of natural gas per day to major cities like Tehran and Isfahan, cut 15 per cent of Iran's daily natural gas production.*"[17]

16. Analysts Comment: None of the sources said *how* the pipelines were attacked. The attacks could have been physical or cyber. Although Israel has not commented, this is the type of strategic attack we have been forecasting.

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

[14] Source: The Register. Giant leak reveals Chinese infosec vendor I-Soon is one of Beijing's cyber-attackers for hire

[15] Source: Malwarebytes Lab. A first analysis of the i-Soon data leak

[16] Source: CTV News. Iran accuses Israel of sabotage attack that saw explosions strike a natural gas pipeline

[17] Source: The Jewish Chronicle. Israel reportedly behind gas pipeline attacks in Iran