Volume 5: Edition 5

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 2025. This report is **TLP:CLEAR**[1] and MAY be shared freely.

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

Cyber Intelligence: Deprioritizing Russia as a Cyber Threat?

This report contains selected cyber-security information from 21st February to 6th March 2025.

Synopsis

1. We deep dive into the Trump administration's deprioritizing of Russia as a cyber threat. Russia's Kaspersky Labs joins the Russian Cyber order of battle. Russia DDoSes Italy, for a week, but is less successful with Ukrainian Notaries and its GhostWriter Campaign. Ukraine hacks Russian IT support for Banking, Oil Production, and Telecommunications. The PRC has new attacks against: Belgian Intelligence, Microsoft 365, and Medical Imagery, as well as more 'Silk Typhoon'.

2. It is our *assessment* that the three major cyber conflicts, (Russia vs Ukraine, Iran vs Israel, and the People's Republic of China) are the most likely sources for the creation of next generation malware and/or a primary source of cyber attacks. This includes government funded hackers (military, intelligence and civilian employees), affiliated hackers (criminals and mercenaries), and volunteer 'supporters'.

U.S. Cyber Policy Reversed

3. On Friday, 28th February, there were two significant events.

- President Zelensky of Ukraine was asked to leave the White House after a spectacular showdown with the President and Vice-President.[2]
- This was followed by U.S. Secretary of Defense, Pete Hegseth ordering US Cyber Command, "*to pause offensive operations against Russia.*"

To quote 'The Register': "*The reported retreat by the Pentagon marks a major about-face in American operations against Russia, as America's military has not only conducted these in the past against President Putin's regime, but then even spoken publicly about them and how they were used to support Ukraine in its response to Russia's devastating invasion.*"[3] On Wednesday, 5th March, there were reports that the

[1] Definition **TLP:CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.

[2] Source: BBC. Zelensky told to leave White House after angry spat with Trump and Vance

[3] Source: The Register. So ... Russia no longer a cyber threat to America?

CIA has been ordered to cease sharing Intelligence with Ukraine.[4] Although the U.S. government's cybersecurity agency, CISA, claims there is 'No change in our posture'[5], quoting 'The Register' again: "*The message seems clear to us: Russia is all right and doesn't deserve to be treated as the bad guy quite as much anymore ... the Kremlin praised the sudden shift in US policy.*"[6]

4. **U.S. Cyber Organization.** The United States cyber operations can (in general) be described as follows:

> A. Special / Intelligence Operations: 'Secret' operations of all types are conducted by American Intelligence organizations, notably the National Security Agency (NSA).
>
> B. Military Cyber Operations: The Pentagon operates though 'Cyber Command' who "*conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations.*"[7]
>
> C. Defensive Operations: This includes: Cybersecurity and Infrastructure Security Agency (CISA), The Federal Bureau of Investigation (FBI) and the Department of Justice (DoJ). Collectively these agencies: detect (or are informed of) incoming cyber attacks, investigate the attacks, prosecute the attackers and sometimes remediate the attacks.
>
> NOTE: These are the agencies that feed data to industry and other cybersecurity organizations such as 'Intelligence Sharing and Analysis Center's' or (ISAC). These are collaborative organizations, combining industry groups and cybersecurity organizations.

5. Suspension of U.S. cyber operations against Russia has serious consequences. Operations such as 'Hunt Forward'[8] had two aspects: to strengthen countries cyber defences and to disrupt attackers. If attackers are not identified early, there is little or no warning of cyber attacks, and no indicators of compromise. This provides Russia with unfettered opportunities to deploy its cyber attacks, or stated a different way, Russian hackers have a higher probability of launching a successful attack.

6. Analysts Comment: A. Once a Russian cyber actor launches an attack, given the statements out of the White House and some Republican's, it is *assessed* that prosecution by the U.S. DoJ is *less likely*. It is *assessed* that both warning of attacks and notification of indicators of compromise (IOC) will *very probably* be degraded due to the downgraded Pentagon activity.

B. Given the alignment of Present Trump, his Secretary of Defence and Director of National Intelligence with Kremlin speaking points, it is *assessed* as *highly unlikely* any analysis of cyber attacks that are unfavourable to Russia will be published. If this

[4] Source: CBC News. U.S. is not currently sharing intelligence with Ukraine, American officials confirm

[5] Source: Security Week. CISA: No Change on Defending Against Russian Cyber Threats

[6] Source: The Register. So ... Russia no longer a cyber threat to America?

[7] Source: The Register. So ... Russia no longer a cyber threat to America?

[8] Source: Cybercom.mil. "Shared threats, shared understanding": U.S., Canada and Latvia conclude defensive Hunt Operations

assessment is accurate, there will *almost certainly* be a major degradation in the U.S. government analysis of Russian malware products and the identification of Russian-linked threat actors.

7. **Kaspersky Effectively In Russian Cyber Order of Battle.** American cybersecurity journalist, Brian Krebs, reports that: “*One of the most notorious providers of abuse-friendly “bulletproof” web hosting for cybercriminals (Prospero OOO) has started routing its operations through networks run by the Russian antivirus and security firm Kaspersky Lab.*” Kaspersky Lab is the company behind Kaspersky Anti-Virus, a once highly-regarded anti-virus solution. “*Bulletproof hosts are so named when they earn or cultivate a reputation for ignoring legal demands and abuse complaints.*” One ad for a bulletproof host reads in part: “*If you need a server for a botnet, for malware, brute, scan, phishing, fakes and any other tasks, please contact us*” … *Russia-based service provider Prospero OOO (the triple O is the Russian version of “LLC”) has long been a persistent source of malicious software, botnet controllers, and a torrent of phishing websites.”*

8. Analysts Comment: The links between Russian based cyber criminals and the Russian government are well established. Russian based cyber criminals rely on ‘bulletproof hosts’ for many things including command and control and anonymous access to the Internet outside Russia. Prospero OOO’s use of Kaspersky Labs networks, makes Kaspersky Labs an integral part of Russian cyber operations.

Russia vs Ukraine

9. **Italy DDoSed For A Week.** On 23rd February, Italian media reported DDoS attacks by Russian hacking group NoName057(16) were ongoing for the seventh day. The attacks focused on “*the websites of the Ministries of Foreign Affairs, Business and Defence were involved, as well as the Air Force and the personal website of the Prime Minister, Giorgia Meloni.*”[9] Analysts Comment: NoName057(16) has launched DDoS attacks multiple times since late December 2024. This attack was unusual in that it was sustained for a week. We see this sustained cyber attack as one element in an uptick in Russian hacking operations.

10. **Russian IT Services Supporting Banking Sector Hacked**. On 24th February, Russia's National Coordination Center for Computer Incidents (NKTsKI) warned that ‘LANIT’, a major Russian IT service and software provider, was ‘breached’. The company is considered Russia’s largest system integrator, specializing in support to banking technology and services including ATMs.[10] Reports did not identify the attackers. Analysts Comment: Pro-Ukrainian hackers have DDoSed Russian banking systems, blocking access. This report is significant because it is reporting a system breach (the attackers penetrated the network).

11. **Russian Cyber Campaign Targets Ukrainian Notaries**. On the 26th February, The Computer Emergency Response Team of Ukraine (CERT-UA) warned of an ongoing ‘phishing’ campaign targeting Ukrainian Notaries. Since mid-January, emails claiming to be from the Ukrainian Ministry of Justice were sent to ‘supplier companies’. If the

[9] Source: Nova.news. Seventh day of hacker attacks on Italian sites

[10] Source: Bleeping Computer. Russia warns financial sector of major IT service provider hack

attached file was executed (clicked on), a series of malware programs were installed to provide Russian Intelligence with: remote access, network scanning tools and the ability to steal sensitive data. The victims computer would also be used to send additional 'phishing lures'.[11] Analysts Comment: The nature of the reporting suggest there is not mush victim impact.

12. **Russia Launches New Version of 'GhostWriter' Campaign**. Cyber Security company 'SentinelLABS' is reporting Russia has a new cyber campaign that targets 'opposition activists' in Belarus as well as Ukrainian military and government organizations. The ongoing campaign, nicknamed 'GhostWriter', uses weaponized Microsoft Excel documents as lures. The attacks are attributed to two Russian government hacking groups, UNC1151, and UAC-0057.[12] Analysts Comment: There are no indications that this is a successful campaign.

13. **Ukraine Continues Cyber Attacks On Russian Oil Industry**. On 28th February, "*Ukrainian hacker group BO Team claims to have destroyed data and server infrastructure of Moscow-based internet provider CWN (PJSC Pronet), which serviced Russia's oil industry.*" This is the same group that attacked Vladimir-based provider Megaseti, reportedly stopping its operations. Estimated time to restore operations was two weeks. This "*attack allegedly wiped out CWN's servers and data, impacting companies such as oil equipment manufacturer Ochersky Machine-Building Plant and the oil and gas research center VNIIONG.*"[13] Analysts Comment: If this report is accurate, this *is probably* causing a major reduction in Russian oil production.

14. **Russian Telecom 'Beeline' Went Offline During DDoS Attack**. On 3rd March, 44 million subscribers of Russia's 'Beeline' Internet service were forced offline due to DDoS attacks from pro-Ukrainian hackers in a one day event. "*Earlier in February, a similar attack caused widespread disruptions to Beeline, bringing down the company's website and mobile application while also affecting home and mobile internet services. The attack on Beeline follows a similar disruption at Russian telecom giant MegaFon in January, which was also attributed to a large-scale DDoS attack. ... The attack on Beeline comes amid a broader wave of cyber incidents in Russia's telecommunications sector.*"[14]

People's Republic of China

15. **PRC Growing It's Cyber Espionage Threat**. CSO Magazine is warning that Chinese (PRC) cyber espionage is growing across all industries. During 2024, "*researchers from security firm CrowdStrike observed a 150% average increase in intrusions by Chinese threat actors worldwide ... also identified seven new Chinese-origin cyberespionage groups. ... CrowdStrike attributes China's increasingly dominant*

[11] Source: The Hacker News. CERT-UA Warns of UAC-0173 Attacks Deploying DCRat to Compromise Ukrainian Notaries

[12] Source: Security Affairs. New Ghostwriter campaign targets Ukrainian Government and opposition activists in Belarus

[13] Source: Euromaidan. Ukrainian hackers destroy oil industry provider's servers in second major Russian infrastructure attack this month

[14] Source: The Record. Russian telecom Beeline facing outages after cyberattack

position in global cyberespionage to a decade of strategic investments … include investments in university programs to cultivate a highly skilled cyber workforce; private sector contracts to provide People’s Liberation Army (PLA), Ministry of Public Security (MPS), and Ministry of State Security (MSS) cyber units with skilled operators and infrastructure; running domestic bug hunting and capture-the-flag competitions to fuel exploit development programs; and industry networking events where PLA and MSS cyber operators obtain unique tools and tradecraft.”[15]

16. **PRC Hackers breach Belgian Intelligence Email**. Between 2021 and May 2023, “… *hackers working for Chinese espionage exploited a breach in an American cyber company to siphon off 10% of the Belgian intelligence service’s incoming and outgoing emails. Classified information is not affected, but personal data of nearly half of the members of the Sûreté is potentially compromised.”* The hackers exploited a vulnerability in the Barracuda Barracuda Email Security Gateway Appliance (ESG). *“Mandiant identified a suspected China-nexus actor, currently tracked as UNC4841, targeting a subset of Barracuda ESG appliances to utilize as a vector for espionage, spanning a multitude of regions and sectors. … Mandiant assesses with high confidence that UNC4841 is an espionage actor behind this wide-ranging campaign in support of the People’s Republic of China.”*[16]

17. **‘Likely’ PRC Threat Targeting Microsoft 365 Accounts**. Cyber Security company ‘SecurityScorecard’ has identified a ‘botnet’ powered by more than 130,000 compromised devices aimed at hacking Microsoft 365 accounts. The attacks are described as “*an immediate threat. … The attack is stealthy because the password spraying attempts are recorded in non-interactive sign-in logs, which are often not monitored by security teams.*”[17] Work on attribution of the attacks is ongoing.

18. **U.S. Charges 12 PRC Nationals in Silk Typhoon Attacks**. The CSO Magazine warning (previous paragraph) follows the charges against 12 Chinese nationals *“acting as freelancers or as employees of i-Soon, conducted computer intrusions at the direction of the PRC's MPS and Ministry of State Security (MSS) and on their own initiative,’ the DoJ said. ‘The MPS and MSS paid handsomely for stolen data.’ … The eight i-Soon employees, alongside two MPS officers, have been accused of breaking into email accounts, cell phones, servers, and websites from at least in or around 2016 through in or around 2023. … The [FBI] further pointed out that the Chinese government is using formal and informal connections with freelance hackers and information security companies to compromise computer networks worldwide.”*[18]

19. **Silk Typhoon Linked to U.S. Treasury Break-in**. According to ‘The Register’, PRC hackers known as ‘Silk Typhoon’ are reponsible for “*the break-in at the US Treasury Department, during which Beijing's cyberspies stole data from workstations belonging to the Office of Foreign Assets Control (OFAC), which administers economic and trade sanctions, as well as the Office of the Treasury Secretary. … the Chinese*

[15] Source: CSO Magazine. Chinese cyber espionage growing across all industry sectors

[16] Source: Security Affairs. China-linked threat actors stole 10% of Belgian State Security Service (VSSE)’s staff emails

[17] Source: Security Week. Chinese Botnet Powered by 130,000 Devices Targets Microsoft 365 Accounts

[18] Source: The Hacker News. U.S. Charges 12 Chinese Nationals in State-Backed Hacking Operations

snoops are believed to have gained access after stealing a BeyondTrust digital key used for remote technical support.”[19]

20. **‘Silk Typhoon’ Changes Tactics and Targets**. Microsoft is reporting that “*it caught the threat actor using stolen API keys and compromised credentials to breach a range of companies in the IT supply chain to extend their reach to downstream customer environments. ... the Chinese government-backed hacking team uses these IT supply chain entry points to conduct extensive reconnaissance, collect sensitive data, and move laterally within victim networks. ... “This threat actor holds one of the largest targeting footprints among Chinese threat actors,” Microsoft declared, warning that Silk Typhoon is well-resourced and capable of quickly pouncing on zero-day discoveries in a wide range of software products.”*[20]

21. **‘Silver Fox’ Spoofs Medical Imaging Applications**. *“Forescout's Vedere Labs researchers on Monday sounded the alarm after identifying dozens of malware samples masquerading as Philips DICOM medical image viewers and other legitimate software. ... instead of running the expected medical imaging application on the victim's machine, these samples deploy ValleyRAT, a backdoor remote access tool (RAT) used by Beijing-backed crew Silver Fox.”* Silver Fox is a known PRC hacking group that typically targets Chinese-speaking victims. "*the new malware cluster we identified, which includes filenames mimicking healthcare applications, English-language executables, and file submissions from the United States and Canada, suggests that the group may be expanding its targeting to new regions and sectors.*"[21]

22. **PRC-Linked ‘Lotus Blossom APT Has New Tools and a Renewed Campaign.** Talos security has released a report that a long-established PRC threat actor has some new malware in its attacks against “*the Philippines, Vietnam, Hong Kong and Taiwan. ... The APT group is using two new Sagerunex backdoor variants in attacks against telecom, media, government, and manufacturing sectors. These variants use cloud services like Dropbox, Twitter, and Zimbra for C2, replacing the original VPS method. ... The variants are designed to gather, encrypt, and exfiltrate target host information to a remote server controlled by the attacker. ... The variants are designed to gather, encrypt, and exfiltrate target host information to a remote server controlled by the attacker.*”[22]

This cyber-intelligence product is produced by David Swan. It is copyright ©David Swan 2025. This report is **TLP:CLEAR**[23] and MAY be shared freely.

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

[19] Source: The Register. China's Silk Typhoon, tied to US Treasury break-in, now hammers IT and govt targets

[20] Source: Security Week. China Hackers Behind US Treasury Breach Caught Targeting IT Supply Chain

[21] Source: The Register. China's Silver Fox spoofs medical imaging apps to hijack patients' computers

[22] Source: Security Affairs. Chinese Lotus Blossom APT targets multiple sectors with Sagerunex backdoor

[23] Definition **TLP: CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.