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: PRC Launches 'Salt Typhoon' 2.0

This report contains selected cyber-security information from 7th to 20th February 2025.

Synopsis

1. The PRC's 'Salt Typhoon' hackers compromise more telecoms. Google says cyber criminals have become a 'National Security Threat'. Russian ISP's are linked to ransomware groups. One Russian GRU hacking team is systematically compromising western critical infrastructure, while another is compromising 'Microsoft Teams'. Ukraine hacks Russia's gas provider, again. A PRC cyber-espionage team has a side gig: ransomware.

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'.

People's Republic of China: Salt Typhoon Attacks Continue

3. There are multiple reports that the PRC 'Salt Typhoon' hacking spree continues. Five more telecommunications companies, including two U.S. companies, have been compromised through unpatched Cisco 'Edge' devices. "*Recorded Future's Insikt Group ... researchers observed the threat group attempting to compromise more than 1,000 such devices across the globe in the two-month span. ... Researchers also observed Salt Typhoon targeting Cisco devices at* [12] *universities across the globe, including UCLA, Loyola Marymount University, Utah Tech University and California State University. ... more than half of the targeted Cisco devices were located in the U.S., South America and India.*" Recorded Future said that they could confirm successful exploitation in five telecommunication companies. They also warned that they could not rule out that other devices and organizations had been compromised.[2]

4. "*The intrusions happened between December 2024 and January 2025 with the Chinese government snoops attempting to exploit more than 1,000 internet-facing*

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: CyberSecurityDive. China-backed hackers continue cyberattacks on telecom companies

Cyber-Intelligence Report

Cisco-made boxes before successfully breaking into at least seven that were unpatched."[3] The reports say that two unpatched vulnerabilities were used to compromise the networks. 'Salt Typhoon' activity continues despite the sanctions imposed by the U.S. Treasury department last month. As we previously reported, sanctions targeted PRC "*firm Sichuan Juxinhe Network Technology Co., accusing the company of having "direct involvement" with China's Ministry of State Security in the Salt Typhoon infiltrations.*" A report in NextGov quoted 'a person familiar with China's cyber activities', granting them anonymity to be candid. "*China doesn't think of getting 'small stuff,' ... That's where I think they're ahead of the game from an intelligence perspective, because they have been collecting massive amounts of data, ... I think [the report] highlights that the PRC is focused not just on current capabilities, but on R&D for future capabilities."*[4] The attacks on universities appeared to target intellectual property in telecommunications.

5. Analysts Comments: The most common response to a detected and countered cyber espionage campaign is for the hackers to withdraw, shutting-down the operation. When a hacking team stays on-task, like 'Salt Typhoon' has, it can be an indication of the importance of the campaign and it also infers that the campaign was not fully countered. We *assess* that both are true: The PRC considers the campaign important AND it was *probably* not completely shut down.

Google says: Cyber Criminals Are A 'National Security Threat'

6. Google's Threat Intelligence Group (GTIG) is warning "*that financially motivated cybercriminal activity should be treated as a threat to national security requiring coordinated international cooperation.*" Criminal hacking is usually categorized as 'financially motivated' or state-backed (IE. Cyber-espionage). Google warns: *"Adversarial nations can and do co-opt criminals for state activity and can and do purchase criminal capabilities to further their political aims. ... Sandworm (APT44) is a good example of the intermingling of state actors and criminal tools. While linked to the GRU (a Russian military intelligence unit), APT44 has employed malware available from cybercrime communities to conduct espionage and disruptive operations in Ukraine."*[5]

7. GTIG warns that "*cybercrime isn't treated as seriously at the national level as state-backed operations. ... The vast cybercriminal ecosystem has acted as an accelerant for state-sponsored hacking, providing malware, vulnerabilities, and in some cases full-spectrum operations to states, ... governments must designate cybersecurity as a national security priority where it isn't already, and lawmakers should be properly incentivizing the implementation of best practices, especially in critical infrastructure.*" The report observed that "*the "Big Four" - Russia, China, Iran, and North Korea*"[6] are all deepening their ties with criminal organizations.

3 Source: The Register. More victims of China's Salt Typhoon crew emerge: Telecos just now hit via Cisco bugs.

4 Source: NextGov. Salt Typhoon hackers possibly targeted telecom research at US universities

5 Source: Security Week. Cybercrime Threatens National Security, Google Threat Intel Team Says

6 Source: The Register. Crimelords and spies for rogue states are working together, says Google

Cyber-Intelligence Report

Russian Hosting Service Seized for Supporting Cybercrime

8. On 11th February, the US, UK, and Australia sanctioned Zservers/Xhost, a Russian Internet Service Provider, for supporting Russian based cybercriminals. "*A few days later, Dutch police announced it took 127 servers,* [located in Amsterdam] *associated with the bulletproof hosting service Zservers/XHost offline*." The press release from the Dutch police read in part: "*During the raid on February 12, ... a server was found with hacking tools from Conti and Lockbit. They are known as the most productive and damaging ransomware groups in the world.*"[7] The companies advertise themselves as 'Bulletproof Hosting Providers' (BHP), ultra-secure alternatives [Internet Service Providers or ISP] that can't be touched by law enforcement. "*Bulletproof hosting services ... are used in other types of cybercrime, such as child exploitation, misinformation, and hate speech, as well as ransomware gangs.*"[8] The companies are headquartered in Barnaul, Russia, with operations in Russia and the Netherlands.

Russia vs Ukraine

9. **Russia's 'Sandworm' group hacking Critical Infrastructure**. Microsoft Threat Intelligence is warning that "*Sandworm, the offensive cyber operations group that works for the Russian Military Intelligence Unit 74455 (GRU), ... wriggled its way into networks within the US, UK, Canada and Australia, stealing credentials and data from "a limited number of organizations.*" The group "*has been carrying out a "near-global" initial access campaign dubbed "BadPilot" since at least 2021. ... while its initial focus was Ukraine, by 2023 the BadPilot campaign had achieved persistent access to "numerous" high-value sectors in the US, Europe, Central Asia and the Middle East. A year later, it "honed its focus" on US, UK, Canada and Australian victims. ... After nearly all of its successful exploits, the intruders established persistence on compromised systems. And in at least three of these cases, this long-term access preceded destructive attacks.*"[9]

10. Analysts Comment: It can not be overstated that Russia can and does conduct 'destructive cyber attacks'. This has included attacks on U.S. Water Treatment Plants by Russian affiliated groups.

11. **Russia Targeting 'Microsoft Teams'**. Microsoft's Threat Team is warning that an emerging Russian threat group it calls 'Storm-2372' has a new trick. "T*he attack involves sending phishing emails that masquerade as Microsoft Teams meeting invitations that, when clicked, urge the message recipients to authenticate using a threat actor-generated device code, thereby allowing the adversary to hijack the authenticated session using the valid access token.*" The attacks last as long as the stolen tokens are valid. Users are targeted via "*messaging apps like WhatsApp, Signal, and Microsoft Teams by falsely claiming to be a prominent person relevant to the target in an attempt to build trust. ... The attacks have targeted government, non-governmental organizations (NGOs), information technology (IT) services and*

7 Source: Security Affairs. Dutch Police shut down bulletproof hosting provider Zservers and seized 127 servers
8 Source: The Register. UK, US, Oz blast holes in LockBit's bulletproof hosting provider Zservers
9 Source: The Register. Russia's Sandworm caught snarfing credentials, data from American and Brit orgs

technology, defense, telecommunications, health, higher education, and energy/oil and gas sectors in Europe, North America, Africa, and the Middle East."[10]

12. **Russia's 'NoName' Hackers Hit Italy**. On 17th February, Russia's 'NoName057(16) launched a new wave of DDoS attacks against Italian targets. "*The group targeted the websites of Linate and Malpensa airports, the Transport Authority, the bank Intesa San Paolo, and the ports of Taranto and Trieste. ... The Pro-Russia hacktivists also targeted private organizations, including Vulcanair and Olidata.*"[11] The attack was retaliation for President Mattarella's statements drawing historical parallels between the Russian Federation and Nazi Germany. The attacks were described as having 'minor impact'.

13. **Ukraine Hacks Gazprom, Again**. On 7-8 February, Ukraine's Intelligence Agency (HUR) hacked Russia's Gazprom's "primary contractor" Gazstroyprom and its subsidiaries. Twenty-three companies involved in the construction and maintenance of Russia's oil and gas infrastructure were affected. According to 'Euromaidan' "*more than 120 servers hosting over 1,500 virtual machines were disabled, file storage containing over 2 million GB of documentation was destroyed, over 10,000 employee computers were disabled, and all systems and services were shut down.*"[12] Russian losses have been estimated as high as several billion rubles.

PRC's 'Earth Preta' hacks Using Ransomware as 'Side Gig'

14. In November 2024, an Asian software and services company was hacked using a tool exclusively used by PRC cyber espionage group 'Earth Preta', sometimes called 'Mustang Panda'. The group "*encrypted the software company's Windows computers with RA World ransomware and demanding a $2 million ransom.*" offering to reduce the ransom to $1 million if paid in three days. This is seen as evidence "*that Mustang Panda, or someone using Mustang Panda's backdoor somehow, is not only spying on governmental organizations, it's also extorting victims with ransomware.*"[13] Analysts Comment: PRC cyber espionage has been disciplined, not crossing over into criminal activity. It is unknown if an individual or a hacking group has gone rogue.

---

10 Source: The Hacker News. Microsoft: Russian-Linked Hackers Using 'Device Code Phishing' to Hijack Accounts

11 Source: Security Affairs. Pro-Russia collective NoName057(16) launched a new wave of DDoS attacks on Italian sites

12 Source: Euromaidan. HUR: Ukraine's cyberattack cripples 23 Russian energy firms with insider's help

13 Source: The Register. Chinese spies suspected of 'moonlighting' as tawdry ransomware crooks

14 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.