CENTRE FOR AIR POWER STUDIES

In Focus

New Delhi

CAPS InFocus: 55/2022

04 August 2022

Decoding Chinese Hacking Syndicate – APT 41

Ms Khyati Singh

Research Associate, Centre for Air Power Studies

Keywords: Cyber Security, Chinese Hackers, APT 41, Cyber Attack, Double Dragon, Wicked Panda

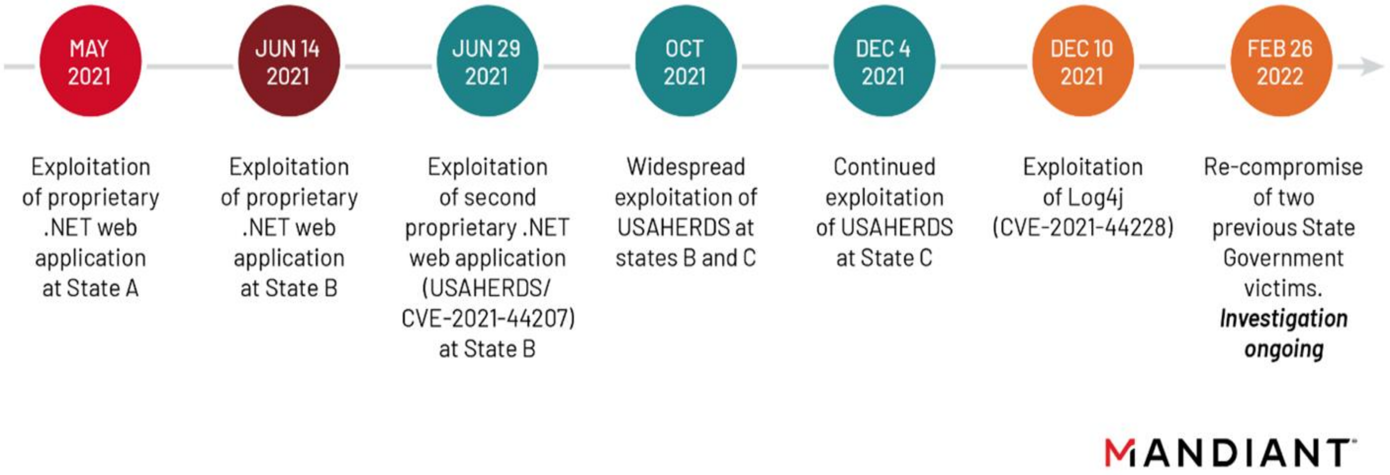
Image Source: APT 41 - Bing images

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS]

It has become nearly impossible to talk about any international venture without the mention of China. One such domain has been cyber-security and cyber-attacks. The cyber-attacks perpetuated by China have become the new normal and have been a cause of concern for several institutions in the United States. Furthermore, these attacks are not only being conducted by the Chinese state, but the People's Liberation Army (PLA) and the Ministry of State Security are backing various hacker groups to follow a similar trail.[1]

Recently, nearly six states have come under cyber-attacks, most of which were conducted through an application which is used to track disease in livestock, known as USAHEARDS. This attack is suspected to have been carried out by the infamous APT41 criminal hacking group located in Chengdu. APT stands for Advanced Persistent Threat, and has many names like Wicked Panda, Winnti, Double Dragon, Barium, and Wicked Spider.[2] APT 41, the official name that the US security agencies have given it, also targets organizations to collect ransoms. It has been active in the public domain since 2012 and has been targeting all possible spheres of public conduct, from health care and telecom to video games and other everyday use applications. These targets are aligned with China's economic plans and try to gain strategic access to various organizations.

Earlier it was involved in exploiting the vulnerabilities, and mass scanning but it is expanding its target audience and range. The US government has uncovered that it is actively involved in activities that directly affect and harm state governments. APT 41 tried to exploit a vulnerability through a SQL(Structured Query Learning) injection and was countered by Mandiant Managed Defense. In a series of attacks that followed between the two, it was identified that they had been exploiting various kinds of vulnerabilities, especially in commercial applications. Furthermore, it has been quick on the part of its operations as it picks on the publicly available vulnerabilities and adapts to its needs in no time. They have been increasingly trying to penetrate the state government structure. Mediant released the following chart to map out the series of attacks. [3]


MAY 2021
Exploitation of proprietary .NET web application at State A
JUN 14 2021
Exploitation of proprietary .NET web application at State B
JUN 29 2021
Exploitation of second proprietary .NET web application (USAHERDS/ CVE-2021-44207) at State B
OCT 2021
Widespread exploitation of USAHERDS at states B and C
DEC 4 2021
Continued exploitation of USAHERDS at State C
DEC 10 2021
Exploitation of Log4j (CVE-2021-44228)
FEB 26 2022
Re-compromise of two previous State Government victims. *Investigation ongoing*
MANDIANT

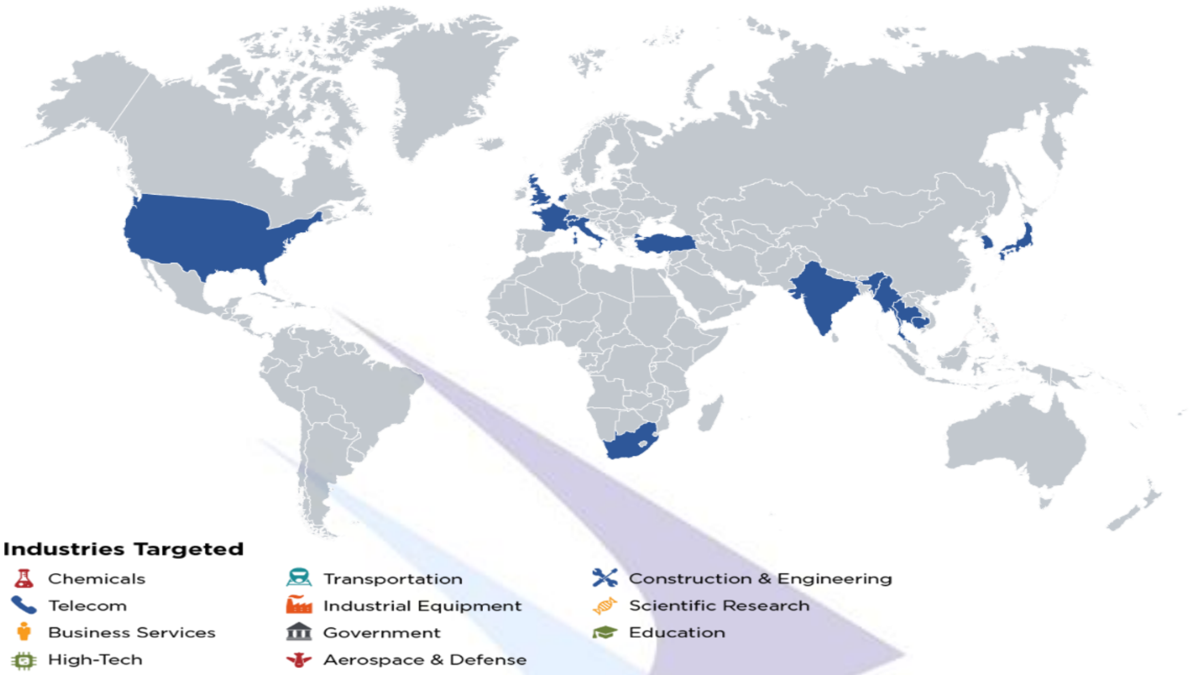
APT 41 has been able to perform instant reconnaissance after penetrating an internet server. In addition, it continues to deploy advanced malware in its operations. DEADEYE launcher and Lowkey being one of them. These anti-analysis technologies allow them to keep away from any investigation and operate undetected. APT 41 has been working to advance its capabilities and has successfully upgraded the guardrail capabilities of DEADEYE. 'Guardrailing' is a tactic deployed by malware to ensure that the binary only unleashes on the system that is chosen by the threat actor. Hence, narrowing down the margin of error. To remain undetected APT 41 keeps leveraging advanced tradecraft, it kept blocking identification servers to persist. [4]

The group, being financially motivated, is expanding its base and is increasingly targeting the video game industry, where it tries to deploy ransomware and dictate virtual currency. Moreover, due to its flexible and adaptive nature, it has been able to move laterally within the networks and has affected the biggest system providers like Linux and Windows. By hacking these systems, they steal source code, which comes in handy to sign malware. They further compromise supply chains by injecting malicious codes into legitimate files that are distributed to the organizations. Therefore, creating a series of discrepancies.

What makes APT 41 different from its contemporaries is the vast range of malware it has at its disposal. It has 46 different malware systems to leverage and accomplish the task. It also masquerades with the commonly available systems, and hence its detection becomes difficult. For instance, for a majority of its operations, it relies on spear-phishing emails that have attachments like HTML (.chm), which are not easily identified. In a single hacking attack, APT 41 uses up to 150 unique sets of malwares, including rootkits, keyloggers, backdoors, and credential stealers.[5]

Following the trail of other Chinese espionages, APT 41 is also moving to conduct more strategic operations and is working on intelligence collection. However, that is not keeping it away from extracting gains by exploiting private players or exploiting the video game industry. The state's support, in fact, is enhancing its capabilities and allowing it to evade any scrutiny from that end.

The US alone is not on the radar of such attacks. India too has come under cyber-attacks from APT 41 in the past. In 2021, BlackBerry Research and Intelligence researchers identified a series of phishing attacks that targeted victims in India. These contained data about new tax legislation and COVID-19 records and statistics. They masqueraded as the Indian government to maintain its credibility.[6] They have targeted many pro-democracy activists and countries like Hong Kong, France, Japan, Myanmar, Italy, Thailand, Turkey, Singapore, South Korea, the UK, Switzerland, South Africa, and Vietnam. A report by FireEye also found them responsible for some of the most exploitative supply chain attacks, where they exploited profiles available in the public domain to appear as legitimate network traffic, like the ones that come from Gmail, Amazon, and OneDrive. [7] The following map was shared by FireEye in its report that points out countries where the attacks have been rampant, along with the list of industries that they target.



To mitigate these attacks, it is important to keep updating network-based security measures and parameters, along with the focus on the protection of sensitive content. The US Information Assurance Directorate issued some strategies that can be used to counter the APT 41 threat. These included damage containment, device integrity, secure and available transport, and account protection.[8]

It is crucial to tap into the cyber domain now more than ever. Aggressive states are using the cyber front as a proxy front to penetrate into the system and affect critical infrastructure. APT 41 is one such group, while there are way too many in operation. The fact that they have state cover allows them to exploit their capabilities to the fullest. Cyberspace is growing every day, and so are threat actors. Any delay on the part of the states ends up proving a strategic loss which is felt both in terms of money and matters.

NOTES:

[1] Garrett O'Brien, "A deep dive into APT41, one of the most aggressive and effective Chinese cyber hacking groups.", *The Wire China*, July 31, 2022, https://www.thewirechina.com/2022/07/31/who-is-apt41/. Accessed on August 02, 2022

[2] Ibid.

[3] Rufus Brown et al, "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments", *Mandiant* 2022. Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments | Mandiant. Accessed on August 02, 2022.

[4] Ibid.

[5] "FireEye Identifies Prolific Chinese Cyber Threat Group", *FIREEYE*, APT41: FireEye Identifies Prolific Chinese Cyber Threat Group. Accessed on August 02, 2022.

[6] Shubhobrota Dev Roy, "Chinese hacker group APT41 targeting Indian citizens with phishing attacks, credential stealers", *TechCircle,* Chinese hacker group APT41 targeting Indian citizens with phishing attacks, credential stealers (techcircle.in). Accessed on August 02, 2022

[7]FireEye Identifies Prolific Chinese Cyber Threat Group", *FIREEYE*, APT41: FireEye Identifies Prolific Chinese Cyber Threat Group. Accessed on August 02, 2022

[8] "Strategies for Mitigating Advanced Persistent Threats (APTs)", *Encyclopaedia Kaspersky*, Strategies for Mitigating Advanced Persistent Threats (APTs) P.1 | Kaspersky IT Encyclopaedia. Accessed on August 03,2022.