
APT-41
AXIAL

A SURVEY ON DOUBLE DRAGON: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

APT 41 also known as Double Dragon is a threat actor out of China with the motivation of Financial gain. They are also known as Wicked Panda where they are motivated to carrying out intrusions and attacks against the public as well as the private sector. They have been operational since 2014. Initially, they targeted video gaming companies, stealing their code-signing certificates. Then they moved onto common interests of the government of the People's Republic of China. APT41 is highly sophisticated and innovative in its methods.

II. TARGET SECTORS

APT 41 has a broad set of political, military, and economic targets in East Asia, Europe, and the US.

V. LINKS TO OTHER ACTORS

APT 41 partially overlaps with groups such as BARIUM and WINNITI.

III. ENGAGEMENTS

- On January 2020, APT 41 attempted exploits of Citrix Application Delivery Controller and Citrix Gateway devices with CVE-2019-19781
- In February 2020, APT 41 successfully exploited Cisco RV320 routers and downloaded a 32-bit ELF binary payload compiled for a 64-bit MIPS processor.
- In March 2020, APT 41 attempted and successfully exploited Zoho ManageEngine vulnerability (CVE-2020-10189).

IV. METHODS USED

APT 41 applies multitudes of techniques to perform initial compromise, including spearphishing, leveraging stolen credentials, moving laterally from trusted third parties, accessing victim organizations using RDP software such as TeamViewer.

AX1AL

VI. IOC

C&C

1. sexyjapan.ddns.info
2. bugcheck.xigncodeservice.com
3. exchange.dumb1.com
4. 66.42.98[.]220

MD5

1. eddfbf35ac07fa9ab25cc4c421e205fe
2. 04fb0ccf3ef309b1cd587f609ab0e81e
3. 36711896cfeb67f599305b590f195aec
4. 37e100dd8b2ad8b301b130c2bca3f1ea
5. 557ff68798c71652db8a85596a4bab72
6. 77c60e5d2d99c3f63f2aea1773ed4653
7. 7d51ea0230d4692eeedc2d5a4cd66d2d
8. 830a09ff05eac9a5f42897ba5176a36a
9. 849ab91e93116ae420d2fe2136d24a87
10. 97363d50a279492fda14cbab53429e75
11. a0a96138b57ee24eed31b652ddf60d4e

VII. Attributions

- Two identified personas using the handles "Zhang Xuguang" and "Wolfzhi" linked to APT41's operations have also been identified in Chinese forums. Multiple domains leveraged by early APT41 activity were registered by emails and names associated with both Zhang Xuguang and Wolfzhi.
- Additional indicators include the reliance on malware used exclusively by Chinese espionage operators, the use of Chinese-language strings, time zone, and operational time analysis, and targeting consistent with Beijing's interests.

VIII. References

- https://content.fireeye.com/apt-41/rpt-apt41/https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf
- https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
- https://www.darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/
- https://kc.mcafee.com/corporate/index?page=content&id=KB92410&locale=en_US