Red Apollo

By Contributors to Wikimedia projects

Published: 2019-06-30 · Archived: 2026-04-05 17:41:39 UTC

From Wikipedia, the free encyclopedia

This article is about the threat actor. For the butterfly, see Parnassius epaphus. For the element, see Potassium.

Red Apollo

Formation	c. 2003–2005[1]
Type	Advanced persistent threat
Purpose	Cyberespionage, cyberwarfare
Region	China
Methods	Zero-days, Phishing, backdoor (computing), RAT, Keylogging
Official language	Chinese
Parent organization	Tianjin State Security Bureau of the Ministry of State Security
Formerly called	APT10 Stone Panda MenuPass RedLeaves CVNX POTASSIUM

Red Apollo (also known as **APT 10** by Mandiant, **MenuPass** by FireEye, **Stone Panda** by Crowdstrike, and **POTASSIUM** by Microsoft)[1][2] is a Chinese state-sponsored cyberespionage group which has operated since 2006. In a 2018 indictment, the United States Department of Justice attributed the group to the Tianjin State Security Bureau of the Ministry of State Security.[3]

The team was designated an advanced persistent threat by FireEye, who reported that they target aerospace, engineering, and telecom firms and any government that they believe is a rival of China.

FireEye stated that they could be targeting intellectual property from educational institutions such as a Japanese university and is likely to expand operations into the education sector in the jurisdictions of nations that are allied with the United States.[4] FireEye claimed that they were tracked since 2009, however because of the low-threat nature they had posed, they were not a priority. FireEye now describes the group as "a threat to organizations worldwide."[4]

The group directly targets managed information technology service providers (MSPs) using RAT. The general role of an MSP is to help manage a company's computer network. MSPs were often compromised by Poison Ivy, FakeMicrosoft, PlugX, ArtIEF, Graftor, and ChChes, through the use of spear-phishing emails.[5]

2014 to 2017: Operation Cloud Hopper

[edit]

Operation Cloud Hopper was an extensive attack and theft of information in 2017 directed at MSPs in the United Kingdom (U.K.), United States (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa, India, Thailand, South Korea and Australia. The group used MSP's as intermediaries to acquire assets and trade secrets from MSP-client engineering, industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies.

Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to persist in Microsoft Windows systems even if the computer system was rebooted. It installed malware and hacking tools to access systems and steal data.[5]

2016 US Navy personnel data

[edit]

Hackers accessed records relating to 130,000 US Navy personnel (out of 330,000).[6] Under these actions the Navy decided to coordinate with Hewlett Packard Enterprise Services, despite warnings being given prior to the breach.[7] All affected sailors were required to be notified.

A 2018 indictment showed evidence that CVNX was not the name of the group, but was the alias of one of two hackers. Both used four aliases each to make it appear as if more than five hackers had attacked.

Post-indictment activities

[edit]

In April 2019 APT10 targeted government and private organizations in the Philippines.[8]

In 2020 Symantec implicated Red Apollo in a series of attacks on targets in Japan.[9]

In March 2021, they targeted Bharat Biotech and the Serum Institute of India (SII), the world's largest vaccine maker's intellectual property for exfiltration.[10]

- China–United States relations
- Cyberwarfare and China

1. ^ *"APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat"*. *FireEye*. *Archived from the original on 2021-04-28. Retrieved 2021-03-07.*
2. ^ *Kozy, Adam (2018-08-30). "Two Birds, One STONE PANDA". Archived from the original on 2021-01-15. Retrieved 2021-03-07.*
3. ^ *"Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information". United States Department of Justice. 2018-12-20. Archived from the original on 2021-05-01. Retrieved 2021-03-07.*
4. ^ Jump up to: ***a*** ***b*** *"APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat « APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat". FireEye. April 6, 2017. Archived from the original on April 28, 2021. Retrieved June 30, 2019.*
5. ^ Jump up to: ***a*** ***b*** *"Operation Cloud Hopper: What You Need to Know - Security News - Trend Micro USA". trendmicro.com. April 10, 2017. Archived from the original on June 30, 2019. Retrieved June 30, 2019.*
6. ^ *"Chinese hackers allegedly stole data of more than 100,000 US Navy personnel". MIT Technology Review. Archived from the original on 2019-06-18. Retrieved 2019-06-30.*
7. ^ *"US Navy Sailor Data 'Accessed by Unknown Individuals'". bankinfosecurity.com. Archived from the original on 2019-06-30. Retrieved 2019-07-12.*
8. ^ *Manantan, Mark (September 2019). "The Cyber Dimension of the South China Sea Clashes". No. 58. The Diplomat. The Diplomat. Archived from the original on 17 February 2016. Retrieved 5 September 2019.*
9. ^ *Lyngaas, Sean (17 November 2020). "Symantec implicates APT10 in sweeping hacking campaign against Japanese firms". www.cyberscoop.com. Cyberscoop. Archived from the original on 18 November 2020. Retrieved 19 November 2020.*
10. ^ *N. Das, Krishna (1 March 2021). "Chinese hacking group Red Apollo (APT10) had identified gaps and vulnerabilities in the IT infrastructure and supply chain software of Bharat Biotech and the Serum Institute of India (SII), the world's largest vaccine maker". Reuters. Archived from the original on 3 May 2021. Retrieved 1 March 2021.*
