Whitepaper

Operation Wocao: Shining a light on one of China’s hidden hacking groups

December 19, 2019

Operation Wocao (我操, “Wǒ cāo”, used as “shit” or “damn”) is the name that Fox-IT uses to describe the hacking activities of a Chinese based hacking group.

This report details the profile of a publicly underreported threat actor that Fox-IT has dealt with over the past two years. Fox-IT assesses with high confidence that the actor is a Chinese group and that they are likely working to support the interests of the Chinese government and are tasked with obtaining information for espionage purposes. With medium confidence, Fox-IT assesses that the tools, techniques and procedures are those of the actor referred to as APT20. We have identified victims of this actor in 10 countries, in government entities, managed service providers and across a wide variety of industries, including Energy, Health Care and High-Tech.

Beyond the technical details, this report should serve to remind us all how focused and result-oriented high-end threat actors work to achieve their goals. This actor profile reveals that:

- They carry out most of their activities on the basis of access through “legitimate” channels. VPN access is an example of such a channel, and we have even seen APT20 directly targeted and retrieved.

- As much as is possible, they remove file system based forensic traces of their activities, making it much harder for investigators to determine what happened after the fact.
- On the basis of the above, an attacker can efficiently achieve their goal of exfiltrating data, sabotaging systems, maintaining access and jumping to additional targets.
- Overall the actor has been able to stay under the radar even though the tools and techniques they use for their hacking operations are relatively simple and to the point.

Knowing how high end threat actors work should also remind us that we, the defenders, have to continually revisit our defensive strategies:

- Zero Trust or Robust segmentation must be one of the guiding principles of any infrastructure, both for systems and identities. As part of that, leveraging Microsoft's Enhanced Security Administrative Environment (ESAE) where applicable will greatly increase your resilience and can prevent many attacks from succeeding.
- Timely detection of and adequate response to any serious incident depends on a combination of high-level and low-level telemetry from network and endpoints.

Indicators of compromise related to this actor can be found on our GitHub page.

For inquiries or more information on Fox-IT's Managed Detection & Response (MDR) offering please contact fox@fox-it.com.

Download report
Report 'Operation Wocao'
Download

Register for future Fox-IT updates
Fox-IT news updates
Register

For a more secure society
Experts Services Technology