CHINA'S EVOLVING CYBER OPERATIONS: A LOOK INTO APT19'S SHIFT IN TACTICS

Published: 2017-04-26 · Archived: 2026-04-05 13:14:46 UTC

There has been a significant change in China-based operations over the past few years. China-based threat groups appear to be less active and they continue to evolve. APT19, a group also known publicly as Codoso, is one such group. In 2016, we observed several shifts in their operations to include changes in targeting, techniques, and malware. Historically, we observed APT19 using continually updated custom tools, suspected to be developed in-house or on-demand, and at least one 0-day. Because of this, we consider them one of the more sophisticated China-based groups. TTPs of the group appeared to be consistent until as recently as 2016, when APT19 conducted a spear-phishing campaign using attachments with malicious macros to target victims. The threat actors then used a publicly available tool from Metasploit to download next stage malware, also available publicly. We believe this represents a marked TTP shift, especially for a China-based group. Despite the threat group's evolving TTPs, we demonstrate how analysts are able to continue to attribute and find newer activity conducted by thisgroup. Using pivoting techniques by looking at the macros used, download URLs, and C2 infrastructure, analysts can find additional activity and conduct attribution.
