Operation Crimson Palace - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:34:03 UTC

APT group: Operation Crimson Palace

Names	Operation Crimson Palace *(Sophos)*
Country	China
Motivation	Information theft and espionage
First seen	2022
Description	(Sophos) In May 2023, in a threat hunt across Sophos Managed Detection and Response telemetry, Sophos MDR's Mark Parsons uncovered a complex, long-running Chinese state-sponsored cyberespionage operation we have dubbed "Crimson Palace" targeting a high-profile government organization in Southeast Asia. MDR launched the hunt after the discovery of a DLL sideloading technique that exploited VMNat.exe, a VMware component. In the investigation that followed, we tracked at least three clusters of intrusion activity from March 2023 to December 2023. The hunt also uncovered previously unreported malware associated with the threat clusters, as well as a new, improved variant of the previously-reported EAGERBEE malware. In line with our standard internal nomenclature, Sophos tracks these clusters as Cluster Alpha (STAC1248), Cluster Bravo (STAC1807), and Cluster Charlie (STAC1305).
Observed	Countries: Southeast Asia.
Tools used	
Information	<https://news.sophos.com/en-us/2024/06/05/operation-crimson-palace-sophos-threat-hunting-unveils-multiple-clusters-of-chinese-state-sponsored-activity-targeting-southeast-asia/> <https://news.sophos.com/en-us/2024/09/10/crimson-palace-new-tools-tactics-targets/>

Last change to this card: 23 October 2024

Download this actor card in PDF or JSON format
