Operation Diplomatic Specter - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:59:20 UTC

APT group: Operation Diplomatic Specter

Names	Operation Diplomatic Specter *(Palo Alto)* CL-STA-0043 *(Palo Alto)* TGR-STA-0043 *(Palo Alto)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2022
Description	(Palo Alto) A Chinese advanced persistent threat (APT) group has been conducting an ongoing campaign, which we call Operation Diplomatic Specter. This campaign has been targeting political entities in the Middle East, Africa and Asia since at least late 2022. An analysis of this threat actor's activity reveals long-term espionage operations against at least seven governmental entities. The threat actor performed intelligence collection efforts at a large scale, leveraging rare email exfiltration techniques against compromised servers.
Observed	Sectors: Defense, Education, Embassies, Government, Retail, Telecommunications. Countries: USA and Middle East, Africa and Asia.
Tools used	Agent Racoon, China Chopper, Gh0st RAT, HTran, JuicyPotatoNG, LadonGo, Mimikatz, Mimilite, nbtscan, Ntospy, PlugX, SharpEfsPotato, SweetSpecter, TunnelSpecter, Yasso.
Information	<https://unit42.paloaltonetworks.com/operation-diplomatic-specter/> <https://www.paloaltonetworks.com/blog/security-operations/through-the-cortex-xdr-lens-uncovering-a-new-activity-group-targeting-governments-in-the-middle-east-and-africa/> <https://unit42.paloaltonetworks.com/new-toolset-targets-middle-east-africa-usa/>

Last change to this card: 19 June 2024

Download this actor card in PDF or JSON format