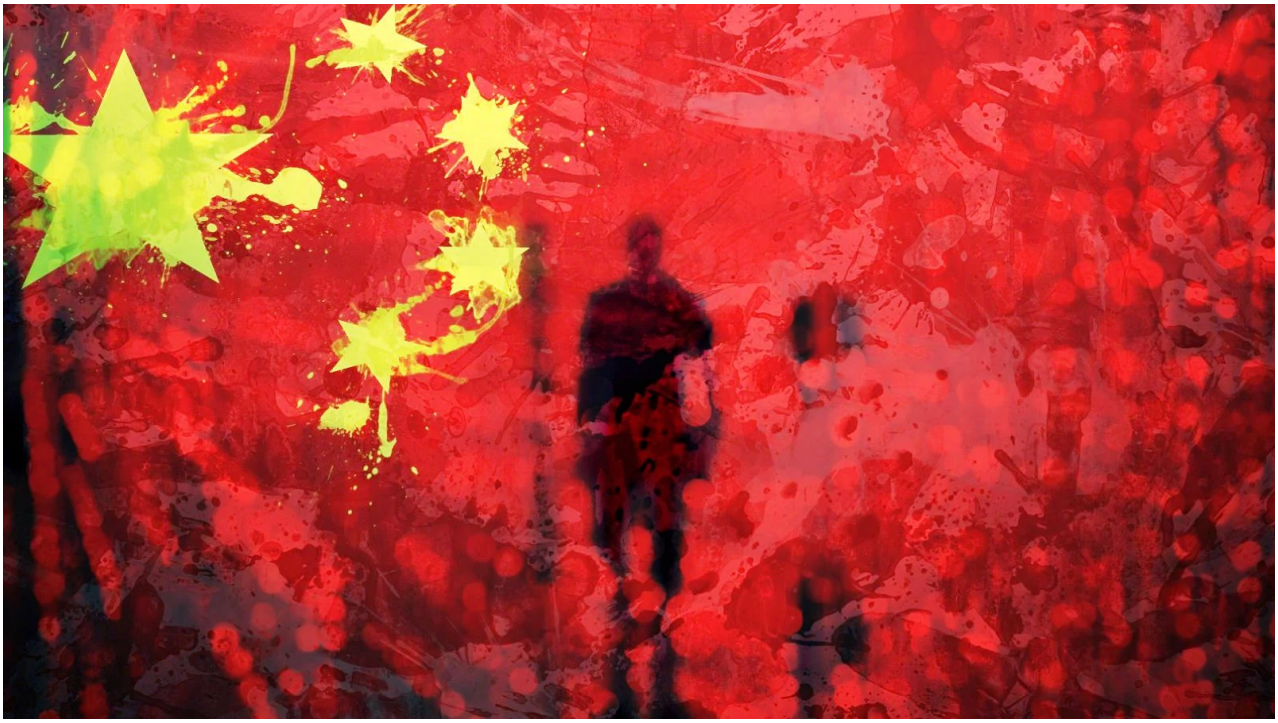
German govt warns of APT27 hackers backdooring business networks

bleepingcomputer.com/news/security/german-govt-warns-of-apt27-hackers-backdooring-business-networks



The BfV German domestic intelligence services (short for Bundesamt für Verfassungs-schutz) warn of ongoing attacks coordinated by the APT27 Chinese-backed hacking group.

This active campaign is targeting German commercial organizations, with the attackers using the HyperBro remote access trojans (RAT) to backdoor their networks.

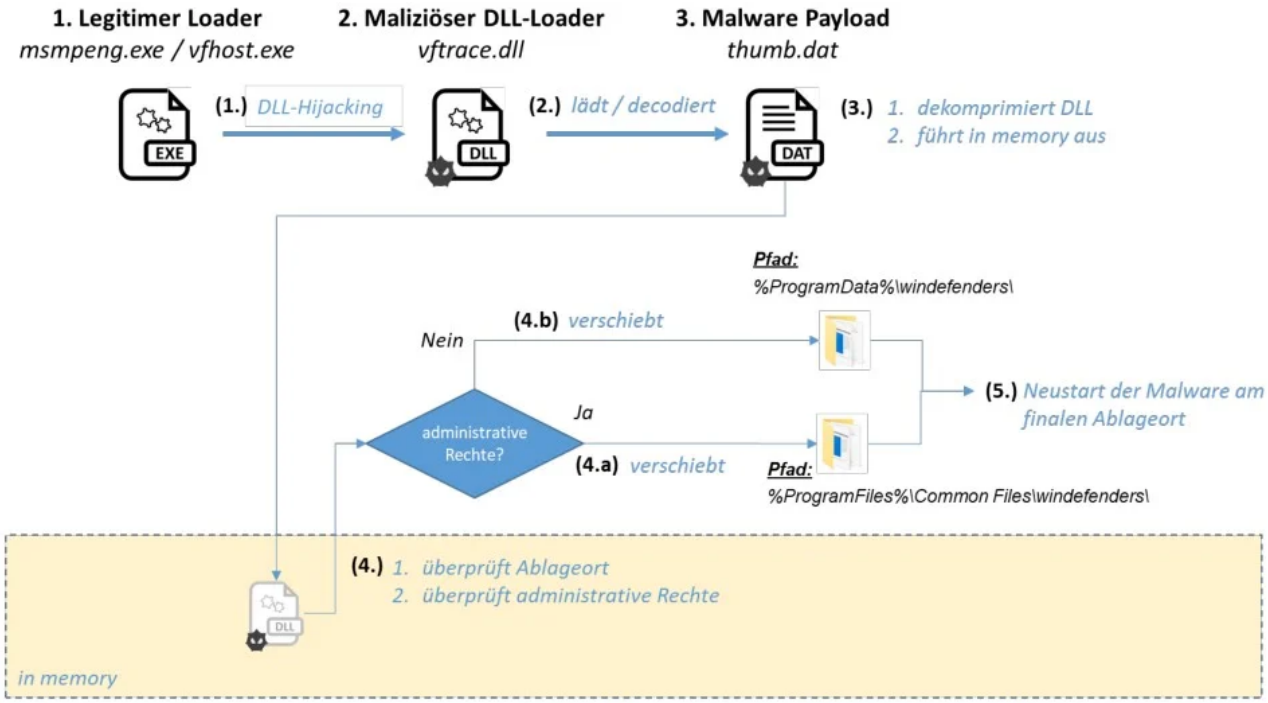
HyperBro helps the threat actors maintain persistence on the victims' networks by acting as an in-memory backdoor with remote administration capabilities.

The agency said the threat group's goal is to steal sensitive information and may also attempt to target their victims' customers in supply chain attacks.

"The Federal Office for the Protection of the Constitution (BfV (Federal Office for the Protection of the Constitution)) has information about an ongoing cyber espionage campaign by the cyber attack group APT27 using the malware variant HYPERBRO against German commercial companies," the BfV said.

"It cannot be ruled out that the actors, in addition to stealing business secrets and intellectual property, also try to infiltrate the networks of (corporate) customers or service providers (supply chain attack)."

The BfV also published indicators of compromise (IOCs) and YARA rules to help targeted German organizations to check for HyperBro infections and connections to APT27 command-and-control (C2) servers.



HyperBro infection chain (BfV)

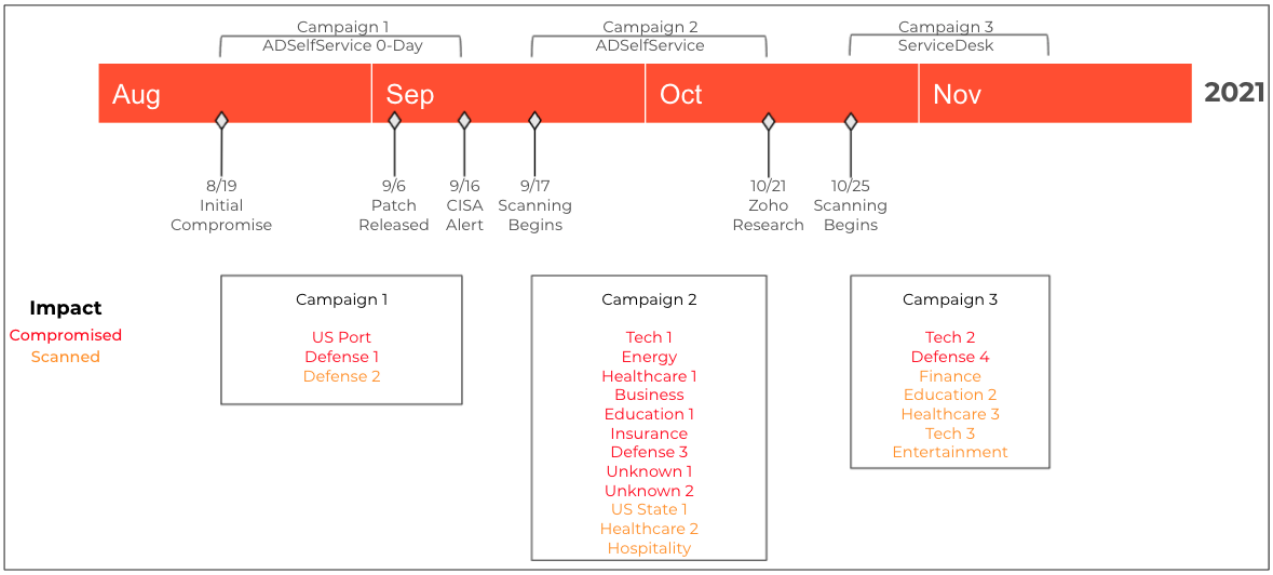
Breaching networks via Zoho and Exchange servers

APT27 (also tracked as TG-3390, Emissary Panda, BRONZE UNION, Iron Tiger, and LuckyMouse) is a Chinese-sponsored threat group active since at least 2010 and known for its focus on information theft and cyberespionage campaigns.

The German intelligence agency says APT27 has been exploiting flaws in Zoho AdSelf Service Plus software, an enterprise password management solution for Active Directory and cloud apps, since March 2021.

This aligns with previous reports of Zoho ManageEngine installations being the target of multiple campaigns in 2021, coordinated by nation-state hackers using tactics and tooling similar to those employed by APT27.

They first used an ADSelfService zero-day exploit until mid-September, then switched to an n-day AdSelfService exploit, and started exploiting a ServiceDesk bug beginning with October 25.



Zoho ManageEngine campaigns (Unit 42)

In these attacks, they successfully compromised at least nine organizations from critical sectors worldwide, including defense, healthcare, energy, technology, and education, according to Palo Alto Networks researchers.

In light of these campaigns, the FBI and CISA issued joint advisories (1, 2) warning of APT actors exploiting ManageEngine flaws to drop web shells on the networks of breached critical infrastructure orgs.

APT27 and other Chinese-backed hacking groups were also linked to attacks exploiting critical ProxyLogon bugs in early March 2021 that allowed them to take over and steal data from unpatched Microsoft Exchange servers worldwide.

US and allies (the European Union, the United Kingdom, and NATO) officially blamed China in June for last year's widespread Microsoft Exchange hacking campaign.