German government warns of APT27 activity targeting local companies

By Catalin Cimpanu

Published: 2023-01-17 · Archived: 2026-04-05 15:24:07 UTC

The German government said on Tuesday that a Chinese cyberespionage group known as APT27 has repeatedly attacked German companies over the past few months using vulnerabilities in software like Microsoft Exchange and Zoho SelfService.

The attacks, which have been taking place since at least March 2021, have aimed to install a version of the HyperBro malware inside corporate networks for the purpose of intelligence collection from infected hosts, the Federal Office for the Protection of the Constitution (BfV) said in a press release.

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

APT27 leveraged Microsoft Exchange and Zoho bugs

According to the agency, APT27, also known as Emissary Panda, has used the following exploits as a way to get a foothold inside companies that failed to patch their internet-exposed servers:

- **CVE-2021-40539** - Zoho Manage Engine ADSelfService Plus
- **CVE-2021-26855** - Microsoft Exchange
- **CVE-2021-26857** - Microsoft Exchange
- **CVE-2021-26858** - Microsoft Exchange
- **CVE-2021-27065** - Microsoft Exchange

All of the above are well-known vulnerabilities previously exploited by other Chinese hacking groups. For example, the four Exchange bugs, also known as ProxyLogon, were also used by a group known as Hafnium, according to Microsoft.

The Zoho vulnerability is also the exact same one that was used to breach the Port of Houston authority last year and which was also heavily abused through the fall and winter, according to CISA.

In the case of the attacks against German companies, the BfV said that the final payload was HyperBro, a malware strain seen in attacks as far back as 2018, typically used by APT27, and which can grant the group full control over infected systems.

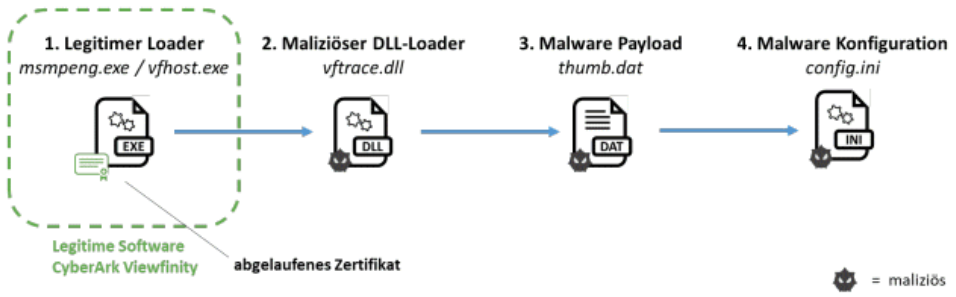

Abbildung 1: Komponenten von HYPERBRO

The BfV reports [PDF, TXT] contains indicators of compromise that both German and non-German organizations and their security teams could use to set up protective measures.

The recent report fits in a general trend that has been shaping up in recent years, where Chinese hackers have often targeted large German companies, from where they are believed to have stolen intellectual property and other business information.

Past victims include software company TeamViewer, steel producer ThyssenKrupp, pharmaceutical giant Bayer, and many others.

German authorities have warned the local business sector about Chinese cyber-espionage since at least 2018.

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
