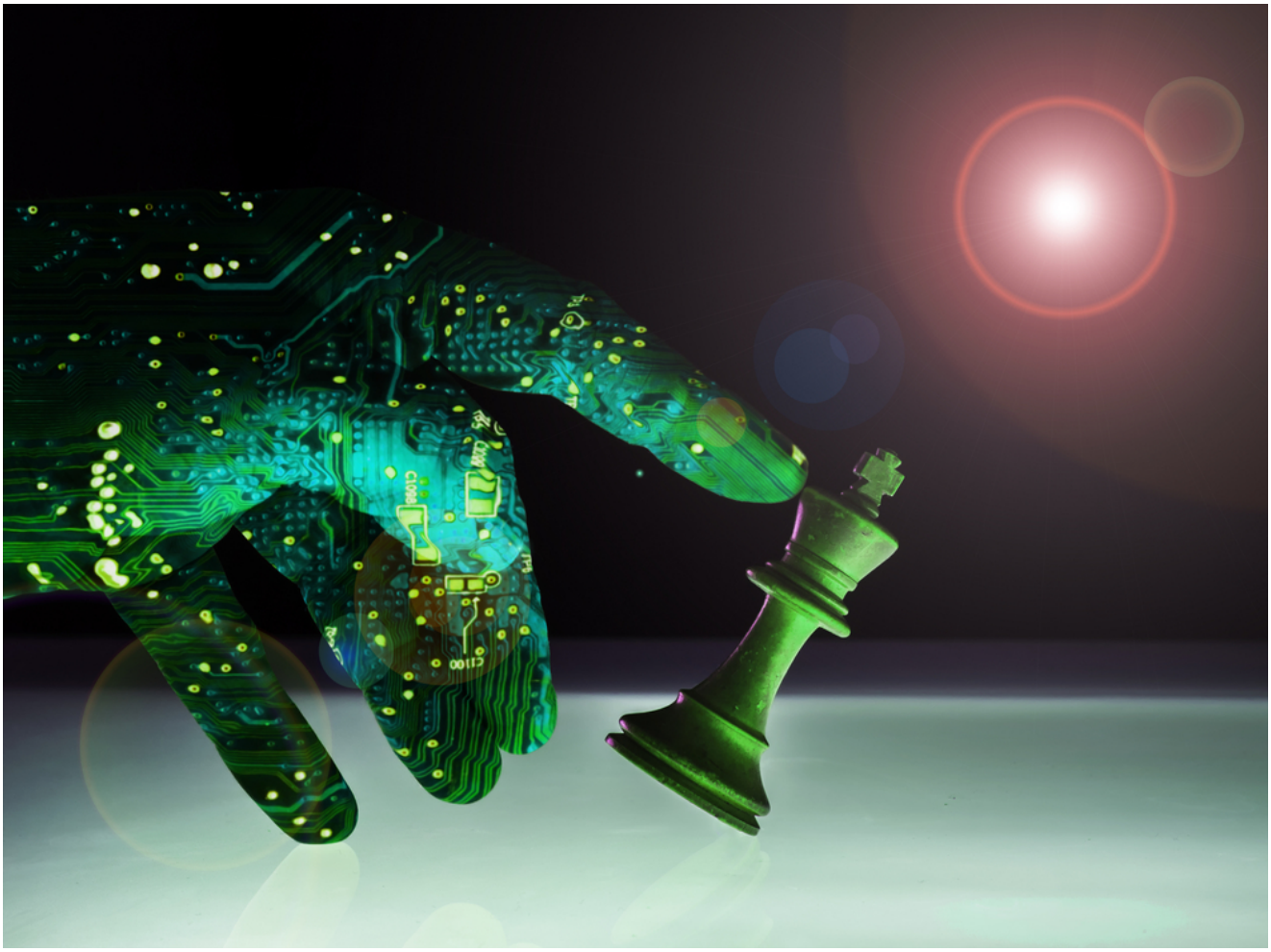
APT27 Group Targets German Organizations with HyperBro

cyware.com/news/apt27-group-targets-german-organizations-with-hyperbro-2c43b7cf/



A German intelligence service is warning against ongoing attacks by a China-backed hacking group. The group, identified as APT27, has been targeting commercial organizations in Germany.

HyperBro is the tool

According to German intelligence agency BfV, the attackers are using HyperBro RAT to backdoor targeted networks.

- The RAT acts as an in-memory backdoor with remote administration capabilities.
- The goal of the campaign seems to be stealing sensitive information and targeting victims' customers in supply chain attacks.
- Further, they may attempt to infiltrate the networks of corporate customers.

Moreover, the intelligence agency has published IOCs and YARA rules to help targeted German organizations check for infections.

Understanding APT27 campaigns

Experts revealed that APT27 has been exploiting flaws in Zoho AdSelf Service Plus software since March 2021.

- From March until mid-September, the APT group used an ADSelfService zero-day exploit (CVE-2021-40539), and then switched to exploited an n-day AdSelfService exploit before finally jumping to ServiceDesk flaw (CVE-2021-44077) 25 October onward.
- As per Palo Alto, the APT group had exploited ManageEngine flaws to deliver web shells on critical infrastructure organizations and associated with attacks abusing critical ProxyLogon bugs in March 2021.
- The Palo Alto Networks also noted that APT27 compromised nine organizations from critical sectors around the world, such as healthcare, energy, defense, education, and technology.

While no connection was formed between the RAT and the previous campaigns as of now, more information is awaited.

Closing thoughts

The recent warning should be considered serious and targeted organizations are suggested to be prepared with countermeasures. Targeted entities should protect their intellectual information with robust encryption and access systems. Further, make use of provided IOCs and YARA rules for better detection.

APT27 | German Organizations | HyperBro RAT | Zoho ManageEngine

Publisher

Cyware