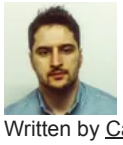
# FBI warns about ongoing attacks against software supply chain companies

zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/


Home Innovation Security

Exclusive: FBI alerts US private sectors about attacks aimed at their supply chain software providers.

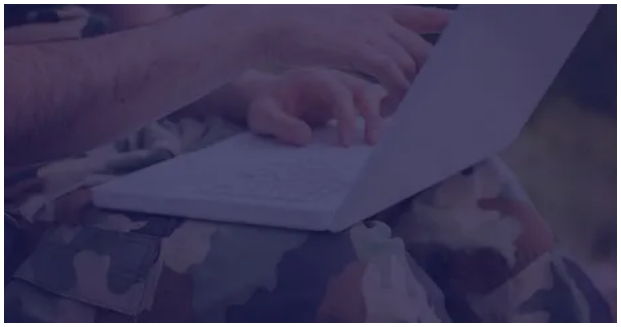


Written by Catalin Cimpanu, Contributor on Feb. 10, 2020

- 
- 
- 
- 
- 


Image: FBI, ZDNet, Florian Krumm

## Special feature



The FBI has sent a security alert to the US private sector about an ongoing hacking campaign that's targeting supply chain software providers, ZDNet has learned.

The FBI says hackers are attempting to infect companies with the Kwampirs malware, a remote access trojan (RAT).

"Software supply chain companies are believed to be targeted in order to gain access to the victim's strategic partners and/or customers, including entities supporting Industrial Control Systems (ICS) for global energy generation, transmission, and distribution," the FBI said in a private industry notification sent out last week.

Besides attacks against supply chain software providers, the FBI said the same malware was also deployed in attacks against companies in the healthcare, energy, and financial sectors.

The alert did not identify the targeted software providers, nor any other victims.

Instead, the FBI shared IOCs (indicators of compromise) and YARA rules so organizations can scan internal networks for signs of the Kwampirs RAT used in the recent attacks.

## Kwampirs malware

The Kwampirs malware was first described in a report published by US cyber-security firm Symantec in April 2018.

At the time, Symantec said a group codenamed Orangeworm had used the Kwampirs malware to similarly target supply chain companies that provided software for the healthcare sector.

Symantec said Orangeworm had been in operation since 2015 and was focused on the healthcare industry primarily.

"Orangeworm's secondary targets include Manufacturing, Information Technology, Agriculture, and Logistics," Symantec said at the time. "While these industries may appear to be unrelated, we found them to have multiple links to healthcare, such as large manufacturers that produce medical imaging devices sold directly into healthcare firms, IT organizations that provide support services to medical clinics, and logistical organizations that deliver healthcare products."

A Lab52 report released a year later, in April 2019, confirmed the Symantec findings and the group's focus on the healthcare industry.

## New attacks appear to be targeting the ICS energy sector

However, the FBI alert sent out last week specifically warns that attacks employing Kwampirs have now evolved to targeting companies in the ICS (Industrial Control Systems) sector, and especially the energy sector.

In 2018 and 2019, neither Symantec nor Lab52 made any attribution on the group's country of origin.

The FBI, however, claims that new evidence from code analysis suggests that Kwampirs contains "numerous similarities" with Shamoon, an infamous data-wiping malware developed by APT33, an Iranian-linked hacking group.

"While the Kwampirs RAT has not been observed incorporating a wiper component, comparative forensic analysis has revealed the Kwampirs RAT as having numerous similarities with the data destruction malware Disttrack (commonly known as Shamoon)," the FBI said.

The Shamoon malware has been used in multiple data-wiping attacks against companies in the energy sector, and more specifically, in the oil & gas fields [1, 2, 3].

The FBI urged companies to scan networks for any signs of Kwampirs and report any infections.