FBI re-sends alert about supply chain attacks for the third time in three months

By Catalin Cimpanu

Published: 2020-03-31 · Archived: 2026-04-05 22:05:56 UTC

The FBI has issued an alert on Monday about state-sponsored hackers using the Kwampirs malware to attack supply chain companies and other industry sectors as part of a global hacking campaign.

This marks the third alert about this particular group sent this year, in as many months, after the FBI sent alerts on January 6 and February 5.

This time around, the FBI highlighted that some of the group's targets are organizations in the healthcare industry, currently grappling with the coronavirus (COVID-19) outbreak.

Besides sending out a PIN (Private Industry Notification), the FBI has also published two Flash alerts, one containing YARA rules to identify the group's Kwampirs malware on infected networks, and the second containing a technical report, complete with IOCs (indicators of compromise).

Both Flash alerts are re-releases of the February and January reports, with additional information.

FBI warns of Kwampirs attacks on healthcare

The FBI named the group behind these attacks as Kwampirs, after the malware they used in their intrusions. They described the group as an Advanced Persistent Threat (APT), a term normally used to describe government-backed hacking groups.

FBI investigators said the group has been active since 2016 when the first attacks with the Kwampirs remote access trojan (RAT) have been observed in the wild.

"Through victimology and forensic analysis, the FBI found heavily targeted industries include healthcare, software supply chain, energy, and engineering across the United States, Europe, Asia, and the Middle East," the FBI said. "Secondary targeted industries include financial institutions and prominent law firms."

But above all, the FBI wanted to point out in its report that the group has heavily targeted the healthcare sector in the past.

According to the FBI, "Kwampirs operations against global healthcare entities have been effective."

The FBI said the group gained "broad and sustained access" to targeted healthcare entities. According to the bureau, hacked targets range from major transnational healthcare companies to local hospital organizations.

Kwampirs gained access to hospitals through the supply chain

"The FBI assesses Kwampirs actors gained access to a large number of global hospitals through vendor software supply chain and hardware products," the agency said.

"Infected software supply chain vendors included products used to manage industrial control system (ICS) assets in hospitals," the FBI said.

In some attacks, the hackers accessed a few machines, in others, they compromised entire enterprise networks.

The FBI credited this to the Kwampirs malware's ability to propagate laterally across networks via the Server Message Block (SMB) protocol or via hidden admin shares.

The FBI points organizations to its two Flash technical alerts for details on detecting the group's malware.

While FBI officials did not attempt to attribute the group to a specific country, they did point out that the Kwampirs malware contained code similarities with Disttrack, a piece of malware commonly known as Shamoon, and known to have been developed and deployed by hackers associated with the Iranian regime.

However, it is unclear if the FBI sent out yesterday's alerts because the Kwampirs group has begun increasingly targeting healthcare organizations in recent weeks, or because the group is known to have historically targeted healthcare organizations and the bureau is attempting to put the healthcare sector on alert against future cyber-attacks.

Attacks on the healthcare industry to be expected right now

At the moment, due to the ongoing COVID-19 pandemic and the frantic search for a vaccine, healthcare and medical research organizations are now one of the most sought-after targets of cyber-attacks and cyber-espionage operations.

Last week, Reuters reported that a state-sponsored hacking group attempted to breach the World Health Organization earlier this month.

In the Risky Business Live webcast yesterday, show producer and presenter Patrick Gray said attacks on healthcare and medical research organizations are to be expected due to the current circumstances.

On the same webcast, Crowdstrike co-founder Dmitri Alperovitch described intelligence services who did not engage in intelligence gathering about the current COVID-19 pandemic as "derelict of duty."

"Right now, you have a disaster on an unimaginable scale affecting nearly every country in the world, and [it] presents an existential threat to the economy," Alperovitch said. "The one thing that intelligence agencies are supposed to do is to help policymakers figure out how to get up crises like these."

While the FBI shied away from saying if the Kwampirs group was engaged in intelligence gathering on the coronavirus outbreak, it did recommend that healthcare organizations take precautions to protect themselves.

ReversingLabs published a technical breakdown of the Kwampirs malware last week.
