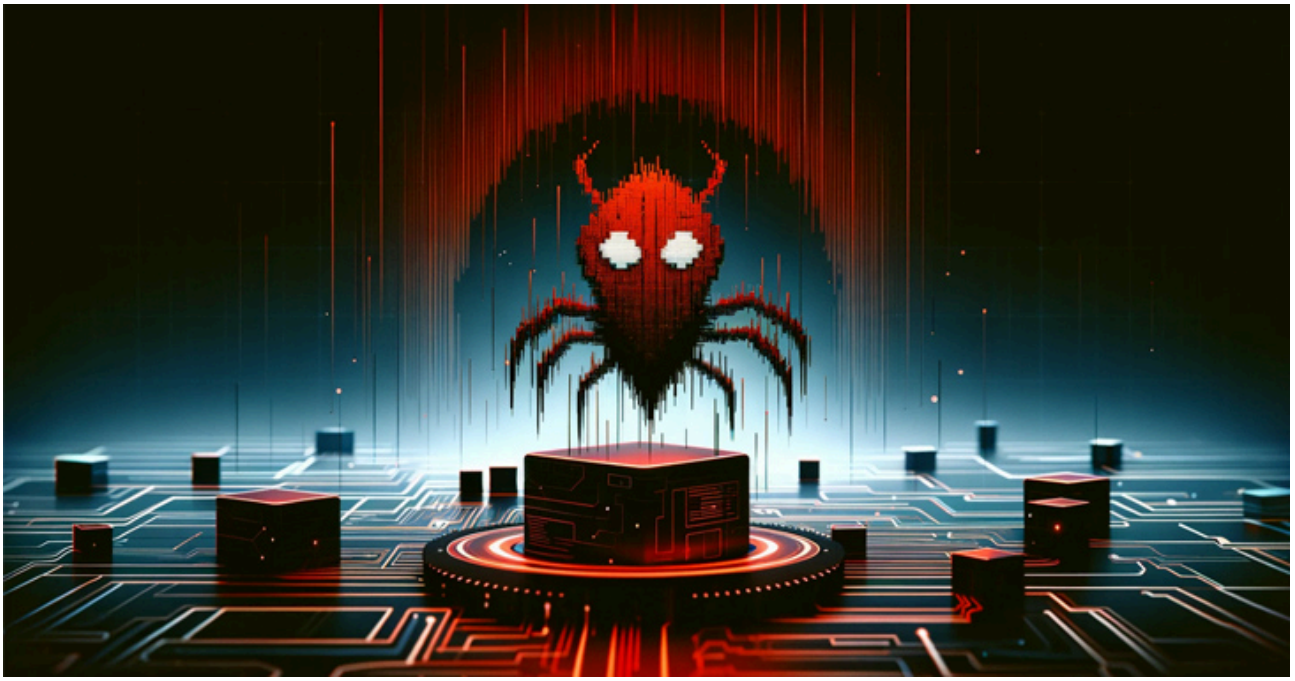
New BiBi-Windows Wiper Targets Windows Systems in Pro-Hamas Attacks

By The Hacker News

Published: 2023-11-13 · Archived: 2026-04-02 11:26:56 UTC



Cybersecurity researchers have warned about a Windows version of a wiper malware that was previously observed targeting Linux systems in cyber attacks aimed at Israel.

Dubbed **BiBi-Windows Wiper** by BlackBerry, the wiper is the Windows counterpart of BiBi-Linux Wiper, which has been put to use by a pro-Hamas hacktivist group in the wake of the Israel-Hamas war last month.

"The Windows variant [...] confirms that the threat actors who created the wiper are continuing to build out the malware, and indicates an expansion of the attack to target end user machines and application servers," the Canadian company said Friday.

Slovak cybersecurity firm ESET is tracking the actor behind the wiper under the name BiBiGun, noting that the Windows variant (bibi.exe) is designed to overwrite data in the C:\Users directory recursively with junk data and append ".BiBi" to the filename.

The BiBi-Windows Wiper artifact is said to have been compiled on October 21, 2023, two weeks after the onset of the war. The exact method by which it is distributed is currently unknown.

Besides corrupting all files with the exception of those with .exe, .dll, and .sys extensions, the wiper deletes shadow copies from the system, effectively preventing the victims from recovering their files.

Another notable similarity with its Linux variant is its multithreading capability.

"For the fastest possible destruction action, the malware runs 12 threads with eight processor cores," Dmitry Bestuzhev, senior director of cyber threat intelligence at BlackBerry, said.

It's not immediately clear if the wiper has been deployed in real-world attacks, and if so, who the targets are.

The development comes as Security Joes, which first documented BiBi-Linux Wiper, said the malware is part of a "larger campaign targeting Israeli companies with the deliberate intent to disrupt their day-to-day operations using data destruction."

The cybersecurity firm said it identified tactical overlaps between the hacktivist group, who call themselves Karma, and another geopolitically motivated actor codenamed Moses Staff (aka Cobalt Sapling), which is suspected to be of Iranian origin.

"Although the campaign has primarily centered around Israeli IT and government sectors up to this point, some of the participating groups, such as Moses Staff, have a history of simultaneously targeting organizations across various business sectors and geographical locations," Security Joes said.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2023/11/new-bibi-windows-wiper-targets-windows.html