Espionage group using USB devices to hack targets in Southeast Asia

By Alexander Martin

Published: 2023-01-09 · Archived: 2026-04-02 12:45:25 UTC

USB devices are being used to hack targets in Southeast Asia, according to a new report by cybersecurity firm Mandiant.

The use of USB devices as an initial access vector is unusual as they require some form of physical access — even if it is provided by an unwitting employee — to the target device.

Earlier this year the FBI warned that cybercriminals were sending malicious USB devices to American companies via the U.S. Postal Service with the aim of getting victims to plug them in and unwittingly compromise their networks.

The new campaign in Southeast Asia potentially began as far back as September 2021, according to a post on the Mandiant Managed Defence blog, published on Monday. Mandiant is now a part of Google Cloud.

The hackers behind it are concentrating on targets in the Philippines. The researchers assess the group has a China nexus, although it did not formally attribute the cyber espionage operation to a specific state-sponsored group.

Operations conducted by the threat actor, followed as UNC4191, “have affected a range of public and private sector entities primarily in Southeast Asia and extending to the U.S., Europe, and APJ [Asia Pacific Japan],” the researchers said.

“However, even when targeted organizations were based in other locations, the specific systems targeted by UNC4191 were also found to be physically located in the Philippines,” it added.

After the initial infection via the USB devices, the hackers use legitimately signed binaries to side-load malware onto the target computers.

Mandiant has identified three new families of malware, which it calls MISTCLOAK, DARKDEW, and BLUEHAZE.

These provide a reverse shell on the victim system, giving the UNC4191 hackers backdoor access. The malware then self-replicated by infecting any new removable drives that are plugged into the compromised computers, allowing the malware to spread to even air-gapped systems.

“Given the worming nature of the malware involved, we may have detected the later stages of this malware’s proliferation,” the researchers stated.

They believe the campaign “showcases Chinese operations to gain and maintain access to public and private entities for the purposes of intelligence collection related to China’s political and commercial interests.”

The main targets of the operation appeared to be in the Philippines “based on the number of affected systems located in this country that were identified by Mandiant.”

Alexander Martin

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79
