Researchers spot updated version of malware that hit Viasat

By AJ Vicens

Published: 2024-03-18 · Archived: 2026-04-05 20:06:16 UTC

A new variant of the wiper malware used to disrupt Ukrainian military communications at the onset of the Russian invasion emerged over the weekend, demonstrating what researchers describe as the continuing development of a tool used to carry out one of the most notable cyberattacks of the war.

On Feb. 24, 2022, the night before the Russian government launched its full-scale invasion, Russian-backed hackers targeted thousands of modems linked to Viasat, the U.S.-based satellite and internet communications company, and relied on by the Ukrainian military. The attack — attributed to the Russian government by the United States and its allies — relied on a piece of malware that researchers with SentinelLabs dubbed "AcidRain."

On Saturday, a new variant of that malware was uploaded to VirusTotal, a malware information-sharing platform, and spotted by Tom Hegel, principal threat researcher at SentinelOne.

Dubbed "AcidPour" by Hegel and his colleagues, the new variant is concerning because it has new features and could be used as part of a "larger service disruption by Russia" and wipe the contents of not just modems but a range of other devices, Hegel told CyberScoop in an email Monday.

A representative of the State Service of Special Communications and Information Protection of Ukraine told CyberScoop in an email early Tuesday that they're aware of AcidPour and "other related malicious capabilities and its repetitive usage against targets within Ukraine."

The agency's Computer Emergency Response Team (CERT-UA) has been in contact with "some of the victims," the representative said, and the agency has attributed the activity to a unit within Russian military intelligence (GRU) tracked as UAC-0165, which itself is a sub cluster within a larger group tracked widely as Sandworm, one of the Russian military's most potent and enduring hacking units.

Wiper attacks have been a go-to for Russian attacks on Ukrainian government and private-sector targets in the past two years, and the latest version of the software used to target Viasat shows how Russian hacking groups are evolving their tools.

While the original version was designed to wipe modems and routers, the updated software is far more capable. "Now AcidPour is markedly different on a technical level — it has different architecture, and new features," Hegel said. "This time the attacker can wipe RAID arrays and UBI – which could be used for a different level of impact, and potentially even more difficult to prevent and recover from."

RAID and UBI generally refer to a system's memory functions, and it appears the updated malware could be used to target memory in embedded devices — components within larger systems — including IoT, networking devices and "maybe some [industrial control systems]," Juan Andres Guerrero-Saade, the associate vice president of the SentinelLabs research unit at SentinelOne, wrote on X.

“The identification of impacting RAID, and Unsorted Block Image File Systems (UBIFS) used by embedded devices — which of course can span many types of real-world devices — is noteworthy,” Hegel explained. “Embedded devices are particularly concerning as they often serve critical needs yet lack simple detection and recovery options if they were to be wiped.”

Hegel said he would expect the malware to be deployed to “many devices,” including those in data centers, network-attached storage devices or others. “It should work on them all,” he said. “Big open door for what it could be used on.”

It’s not clear where this malware has been deployed, Guerrero-Saade said, and authorities in Ukraine have been notified.

Updated March 19, 2024: *This story has been updated to include comments from the State Service of Special Communications and Information Protection of Ukraine*.
