Viasat confirms satellite modems were wiped with AcidRain malware

bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/

Sergiu Gatlan

By
Sergiu Gatlan

- March 31, 2022
- 01:25 PM
- 0

A newly discovered data wiper malware that wipes routers and modems has been deployed in the cyberattack that targeted the KA-SAT satellite broadband service to wipe SATCOM modems on February 24, affecting thousands in Ukraine and tens of thousands more across Europe.

The malware, dubbed AcidRain by researchers at SentinelOne, is designed to brute-force device file names and wipe every file it can find, making it easy to redeploy in future attacks.

SentinelOne says this might hint at the attackers' lack of familiarity with the targeted devices' filesystem and firmware or their intent to develop a reusable tool.

AcidRain was first spotted on March 15 after its upload onto the VirusTotal malware analysis platform from an IP address in Italy as a 32-bit MIPS ELF binary using the "ukrop" filename.

Once deployed, it goes through the compromised router or modem's entire filesystem. It also wipes flash memory, SD/MMC cards, and any virtual block devices it can find, using all possible device identifiers.

"The binary performs an in-depth wipe of the filesystem and various known storage device files. If the code is running as root, AcidRain performs an initial recursive overwrite and delete of non-standard files in the filesystem," SentinelOne threat researchers Juan Andres Guerrero-Saade and Max van Amerongen explained.

To destroy data on compromised devices, the wiper overwrites file contents with up to 0x40000 bytes of data or uses MEMGETINFO, MEMUNLOCK, MEMERASE, and MEMWRITEOOB input/output control (IOCTL) system calls.

After AcidRain's data wiping processes are completed, the malware reboots the device, rendering it unusable.

Used to wipe satellite communication modems in Ukraine

Based on the name of the AcidRain binary uploaded to VirusTotal, which could be an abbreviation of "Ukraine Operation," SentinelOne said the malware might have been developed explicitly for an operation against Ukraine and likely used to wipe modems in the KA-SAT cyberattack.

"The threat actor used the KA-SAT management mechanism in a supply-chain attack to push a wiper designed for modems and routers," SentinelOne hypothesized.

"A wiper for this kind of device would overwrite key data in the modem's flash memory, rendering it inoperable and in need of reflashing or replacing."

This directly contradicts a Viasat incident report on the KA-SAT incident saying it found "no evidence of any compromise or tampering with Viasat modem software or firmware images and no evidence of any supply-chain interference."

However, Viasat confirmed SentinelOne's hypothesis, saying the data destroying malware was deployed on modems using "legitimate management" commands.

"The analysis in the SentinelLabs report regarding the ukrop binary is consistent with the facts in our report - specifically, SentinelLabs identifies the destructive executable that was run on the modems using a legitimate management command as Viasat previously described," a Viasat spokesperson told BleepingComputer.

"We expect we can provide additional forensic details when this investigation is complete."

The use of AcidRain to wipe modems was also confirmed by security researcher Ruben Santamarta who dumped the flash memory of a SATCOM modem corrupted in the attack against KA-SAT.

As SentinelOne says, the destructive pattern observed by Santamarta matches the output of AcidRain's overwriting wiper method.

> If you're wondering what that might look like...https://t.co/vbCNsgcwtz
>
> — J. A. Guerrero-Saade (@juanandres_gs) March 31, 2022

The fact that Viasat shipped almost 30,000 modems since the February 2022 attack to bring customers back online and continues to even more to expedite service restoration also hints that SentinelOne's supply-chain attack theory holds water.

As a side note, the IOCTLs used by this malware also match the ones used by the VPNFilter malware 'dstr' wiper plugin, a malicious tool attributed to Russian GRU hackers (Fancy Bear or Sandworm).

Seventh data wiper deployed against Ukraine this year

AcidRain is the seventh data wiper malware deployed in attacks against Ukraine, with six others having been used to target the country since the start of the year.

The Computer Emergency Response Team of Ukraine recently reported that a data wiper it tracks as DoubleZero has been deployed in attacks targeting Ukrainian enterprises.

One day before the Russian invasion of Ukraine started, ESET spotted a data-wiping malware now known as HermeticWiper, that was used against organizations in Ukraine together with ransomware decoys.

The day Russia invaded Ukraine, they also discovered a data wiper dubbed IsaacWiper and a new worm named HermeticWizard used to drop HermeticWiper payloads.

ESET also spotted a fourth data-destroying malware strain they dubbed CaddyWiper, a wiper that deletes user data and partition information from attached drivers and also wipes data across Windows domains it's deployed on.

A fifth wiper malware, tracked as WhisperKill, was spotted by Ukraine's State Service for Communications and Information Protection (CIP), who said it reused 80% of the Encrpt3d Ransomware's code (also known as WhiteBlackCrypt Ransomware).

In mid-January, Microsoft found a sixth wiper now tracked as WhisperGate, used in data-wiping attacks against Ukraine, disguised as ransomware.

Update: A Viasat spokesperson sent the following statement after the story was published:

> The facts provided in the Viasat Incident Report yesterday are accurate. The analysis in the SentinelLabs report regarding the ukrop binary is consistent with the facts in our report - specifically, SentinelLabs identifies the destructive executable that was run on the modems using a legitimate management command as Viasat previously described.
>
> As noted in our report: "the attacker moved laterally through this trusted management network to a specific network segment used to manage and operate the network, and then used this network access to execute legitimate, targeted management commands on a large number of residential modems simultaneously."
>
> Additionally, we don't view this as a supply chain attack or vulnerability. As we noted, "Viasat has no evidence that standard modem software or firmware distribution or update processes involved in normal network operations were used or compromised in the attack." Further, "there is no evidence that any end-user data was accessed or compromised."
>
> Due to the ongoing investigation and to ensure the security of our systems from ongoing attack, we cannot publicly share all forensic details of the event. Through this process, we have been, and continue to cooperate with various law enforcement and government agencies around the world, who've had access to details of the event.
>
> We expect we can provide additional forensic details when this investigation is complete.

Related Articles:

US, EU blame Russia for cyberattack on satellite modems in Ukraine

Ukraine warns of "chemical attack" phishing pushing stealer malware

Phishing attacks target countries aiding Ukrainian refugees

Sandworm hackers fail to take down Ukrainian energy provider

Google: Russian phishing attacks target NATO, European military

- AcidRain
- Data-wiper
- KA-SAT
- Malware
- Ukraine
- Viasat

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: