Breach Notification , Business Continuity Management / Disaster Recovery , Cybercrime

Viasat Confirms 'AcidRain' Malware Could Have Wiped Modems

No Smoking Gun, But Code Overlaps With Russian VPNFilter Malware, SentinelOne Finds

Mathew J. Schwartz (euroinfosec) • April 1, 2022

Security researcher Ruben Santamarta analyzes one of the attacked Viasat modems.

The disruption of tens of thousands of Viasat consumer broadband modems on the day Russia invaded Ukraine may have involved wiper malware.

See Also: Live Webinar Tomorrow | Prevent, Detect & Restore: Data Security Backup Systems Made Easy

So report SentinelOne security researchers Juan Andrés Guerrero-Saade and Max van Amerongen, based on a sample of the malware they spotted, which they've dubbed "AcidRain."

The binary was uploaded on March 15 to VirusTotal from Italy and had the filename "ukrop," which they say may refer to "Ukraine operation."

At least circumstantially, there's an Italy connection to the Feb. 24 outage, which affected 30,000 or more consumer broadband modems across central Europe, including Ukraine. These Tooway-branded modems were distributed by Italy-based Skylogic - a subsidiary of French satellite operator Eutelsat, which is one of Viasat's business partners (see: *Viasat Traces Outage to Exploit of VPN Misconfiguration*).

The outage of the modems, which connect to Viasat's KA-SAT satellite communications network, began Feb. 24, around the time that Russian forces began their most recent invasion of Ukraine. The attack has yet to be attributed to any nation-state or attack group, although Russia or a close ally remain obvious suspects.

Teardown: AcidRain

The AcidRain malware is a Linux MIPS ELF executable that "performs an in-depth wipe of the filesystem and various known storage device files," the SentinelOne researchers say. "If the code is running as root, AcidRain performs an initial recursive overwrite and delete of non-standard files

in the filesystem."

While there's no direct evidence tying AcidRain to the Viasat outage, the researchers suggest that after attackers gained access to the satellite communications network provider's management console, they might have executed "a supply-chain attack to push a wiper designed for modems and routers."

They say that "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."

Viasat, in its latest update issued Wednesday, says the attack rendered affected modems unable to connect to the internet. It has said specific commands were sent to the modems to make them do this, but had not suggested that malware might have been involved. It adds that "there is no evidence that any end-user data was accessed or compromised."

Now, Viasat has confirmed many of the findings published by SentinelOne, as TechCrunch first reported.

"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 spokeswoman tells Information Security Media Group.

While SentinelLabs has suggested this may have been a supply chain attack, Viasat disagrees. "We don't view this as a supply chain attack or vulnerability," the spokeswoman says, referring to the report Viasat issued Wednesday. It says: "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."

How Viasat Got Attacked

Viasat has said that in the wake of the disruption, it hired incident response firm Mandiant to investigate and that it has also been working with multiple governments' cybersecurity agencies and law enforcement authorities as part of an ongoing investigation.

"We expect we can provide additional forensic details when this investigation is complete," the Viasat spokeswoman says.

Thus far, the company has continued to issue updates, including about service restoration.

Viasat's Wednesday update for the first time detailed stages of the Feb. 24 attack against it:

1. An attacker exploited "a misconfiguration in a VPN appliance to gain remote access to the trusted management segment of the KA-SAT network," Viasat says.
2. "The attacker moved laterally through this trusted management network to a specific network segment used to manage and operate the network," and then issued a number of commands via "several SurfBeam2 and SurfBeam2+ modems."
3. At first, this appeared to involve telling the modems to issue tons of garbage traffic, effectively denying service to other modems on the consumer-focused network segment. This made it difficult for the tens of thousands of modems connecting to the network segment to get online.
4. Attackers issued a number of direct commands to the modems, instructing them to disconnect from the network.

Viasat says that affected modems were not left unrecoverable or bricked.

But recovery has not necessarily been easy. Service for some modems was restored using over-the-air updating functionality to instruct them to reconnect. In many cases, however, Viasat says the quickest way to get consumers back online has been for its distributors to provide customers with replacement modems.

So far, Viasat says it has provided its distributors with 30,000 replacement modems and that more are available if required.

Flurry of Wiper Malware

If AcidRain was used to attack the modems, that would make it the seventh known piece of wiper malware tied to the Russia-Ukraine war - and events preceding it - following WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper and DoubleZero.

"Despite what the Ukraine invasion has taught us, wiper malware is relatively rare," the SentinelOne researchers say. "More so wiper malware aimed at routers, modems or IoT devices."

Even so, the software stacks that run such devices very often aren't secure by design. Numerous routers, modems and IoT devices also feature publicly known vulnerabilities but oftentimes do not get updated by manufacturers or do not get updated in a timely manner. Even when updates or security fixes do get released, many times users never install them.

Code Crossover With VPNFilter

The SentinelOne researchers say one interesting takeaway from AcidRain is that it shares some code with VPNFilter, which is modular malware discovered by Cisco Talos that targets SOHO routers and QNAP storage devices.

In 2018, the FBI attributed that malware campaign to the Russian government, and specifically to the nation-state hacking group Fancy Bear, aka APT28, Pawn Storm, Sandworm, Sednit, Sofacy, Tsar Team and X-Agent. Security experts say they believe the group has been operating since at least 2007 and is run by the GRU, which is Russia's military intelligence agency.

Pictured: FBI affidavit, vulnerable router

Evidence of code overlap proves nothing, except that someone may have reused code previously seen in another attack.

Potential Vulnerabilities Persist

Viasat says that whoever attacked it continues trying to do so but that it has been successfully blocking these attacks.

Nevertheless, the modems it is shipping might be in need of security improvements.

European security researcher Ruben Santamarta, who physically obtained both a targeted Viasat SurfBeam2 modem as well as a working one, found several shortcomings. Notably, both modems' auto-configuration server is set to "install (upload and run) arbitrary binaries on the modem, without requiring either a signature verification or a complete firmware upgrade," he says in a post to his ReverseMode blog.

"This functionality seems to match both the Viasat statement as well as the approach to deploy the 'AcidRain' wiper described by SentinelOne," he says, although he adds that without more information, it's impossible to say to say if this is how the attackers proceeded.

In spite of that, "the security posture of the SurfBeam2 firmware does not look good," he says. "Hopefully these vulnerabilities are no longer present, otherwise that would be a problem."

About the Author

Mathew J. Schwartz

Executive Editor, DataBreachToday & Europe, ISMG

Schwartz is an award-winning journalist with two decades of experience in magazines, newspapers and electronic media. He has covered the information security and privacy sector throughout his career. Before joining Information Security Media Group in 2014, where he now serves as the executive editor, DataBreachToday and for European news coverage, Schwartz was the information security beat reporter for InformationWeek and a frequent contributor to DarkReading, among other publications. He lives in Scotland.