NEWS

New 'AcidRain' malware may be connected to Viasat attack

SentinelOne did not directly attribute the malware to the Viasat attack. That said, researchers argued the "AcidRain" malware's functionality matches open source intelligence.

Alexander Culafi, News Writer

Published: **31 Mar 2022**

A post from SentinelOne describes a new wiper malware dubbed "AcidRain" that may be connected to last month's Viasat attack.

Viasat, a U.S.-based communications company, confirmed via press release Wednesday that it suffered a cyber attack last month. The attack targeted the company's KA-SAT satellite internet network and affected "several thousand" customers in Ukraine, as well as tens of thousands of fixed broadband customers across Europe.

The internet provider called the attack "multifaceted and deliberate," and gave some specific attack details in its press release. Viasat did not attribute the attack to a specific threat actor however, nor did it provide complete details regarding how the attack occurred.

A Thursday blog post by SentinelOne's SentinelLabs discussed the attack as well as a potential malware -- and threat actor -- behind it. The security vendor described AcidRain as a "malware designed to wipe modems and routers."

Wipers are a destructive class of malware intended to erase the storage contents of the devices it infects, as opposed to something like ransomware, which typically has an end goal of extortion. SentinelLabs researchers and post authors Juan Andres Guerrero-Saade and Max van Amerongen referred to AcidRain as the seventh wiper used in the ongoing Russian war with Ukraine.

The authors described the wiper's functionality as "relatively straightforward."

"AcidRain's functionality is relatively straightforward and takes a brute-force attempt that possibly signifies that the attackers were either unfamiliar with the particulars of the target firmware or wanted the tool to remain generic and reusable," the post read. "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 hypothesized that AcidRain was utilized alongside other potential binaries and scripts through a supply chain attack, mainly due to the functionality of the malware and how it matches with open source intelligence surrounding the attack.

Viasat told SearchSecurity in a statement that it does not view the incident as a supply chain attack or vulnerability, and the company expects to share more details when the investigation is complete.

"The facts provided in the Viasat incident report yesterday are accurate," the statement read. "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."

SentinelOne did not attempt to directly attribute AcidRain to any specific threat actor. However, the vendor assessed "with medium confidence" developmental and code overlaps between the malware and a VPNFilter plugin attributed to prominent Russian APT Sandworm. Sandworm is known for the 2017 NotPetya ransomware attacks and, more recently, a botnet known as "Cyclops Blink."

Guerrero-Saade told SearchSecurity that the destructive motivations of AcidRain "fit the bill perfectly" with the Sandworm seen in 2018 and prior, but added he and van Amerongen "wanted to present the development overlaps with the least possible hyperbole given the sensitive nature of the attack."

Asked to explain the code overlap further, Guerrero-Saade said that judging such similarities "takes a lot of expertise and care."

"This isn't source code compared to source code, but rather the output of a compiler (with all of its settings and optimizations) that creates an executable binary," he said via email. "That means there's a lot of boilerplate standard library code, there are compiler optimizations, and then there's custom written code. It appears that the compiler and its settings are the same, the same standard library (libc), and some code implementation similarities (and dissimilarities), hence putting it at medium confidence. It's worth noting that there's an approximate four-year gap between the development of that VPNFilter plugin and AcidRain, and changes are to be expected."

Alexander Culafi is a writer, journalist and podcaster based in Boston.

Related Resources

Desktop Admin for BYOD: Security Chapter
–SearchSecurity.com

E-Guide: Wireless LAN access control: Managing users and their devices
–SearchSecurity.com

Dig Deeper on Network security

Russian cyber attacks on Ukraine driven by government groups

By: Shaun Nichols

SentinelOne discusses the rise of data-wiping malware

By: Arielle Waldman

US, EU attribute Viasat hack to Russia

By: Arielle Waldman

NCSC pins Viasat cyber attack on Russia

By: Alex Scroxton

SearchNetworking

How AI and ML in Open RAN alleviates network complexity

Incorporating AI and ML into Open RAN networks could help MNOs simplify operations and deliver 5G enhanced capabilities of high ...

VMware goes deep into multi-cloud universe

With its rebranded Explore conference, VMware made it clear its focus is on supporting customers' multi-cloud and edge computing ...