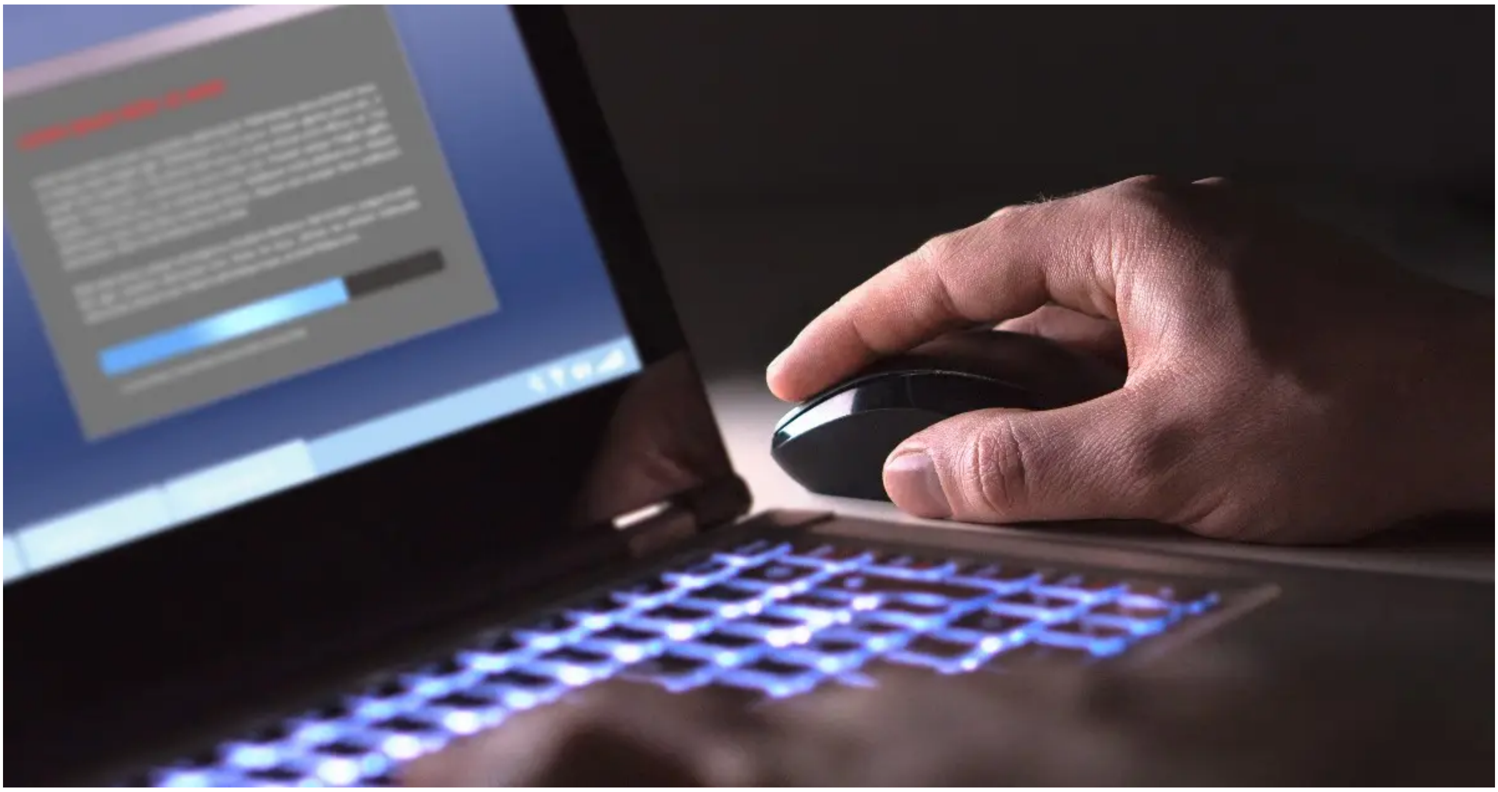
AcidRain Malware Shuts Down Thousands of Modems in Ukraine



NEWS | May 18, 2022

Share

By **Jonathan Reed** | 2 min read

On Thursday, February 24, a cyber attack rendered Viasat KA-SAT modems inoperable in Ukraine, according to a recent Viasat report. Collateral damage from this attack also deactivated the remote monitoring or control of 5,800 Enercon wind turbines in Germany.

The cause of the attack was allegedly a newly discovered data wiper malware that wipes routers and modems. Dubbed AcidRain, the malware was deployed to target the KA-SAT satellite broadband service to wipe SATCOM modems. This incident affected thousands of modems in Ukraine and tens of thousands more across Europe.

What Is Wiper Malware?

When threat actors launch wiper malware attacks, they often aren't asking for ransom. Instead, wiper malware leads to the destruction or wiping of data. For example, the

struck Saudi Aramco and other Middle Eastern oil companies between

The Shamoon wiper spreads itself through shared network disks. It jumps between devic and makes it impossible to recover destroyed data. The RawDisk driver overwrites disks and then wipes the master boot record, which also prevents the system from booting up.

Meanwhile, Meteor wiper malware can change passwords, disable recovery mode and issue malicious commands. Other well-known wiper malware types include NotPetya and ZeroCleare.

AcidRain Wiper Malware Incident Details

AcidRain can brute-force device file names and wipe every file it can find. A Viasat company blog post said the incident began when “high volumes of focused, malicious traffic were detected emanating from several SurfBeam2 and SurfBeam 2+ modems and/or associated customer premise equipment physically located within Ukraine and serviced by one of the KA-SAT consumer-oriented network partitions. This targeted denial of service attack made it difficult for many modems to remain online.”

According to the Viasat post, tens of thousands of modems dropped off the network. The modems did not attempt to re-enter the network, either. The attack impacted a large number of modems within Ukraine and a substantial number of other devices throughout Europe.

Wide

CONTINUE READING

Since the start of 2022, six strains of wiper malware have been connected with the conflict in Ukraine: WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper and

MORE FROM NEWS

NEWS | September 7, 2022

Congress Wants to Study the Cybersecurity of Satellites

NEWS | August 31, 2022

40% of Zero Day Exploits From the Last Decade Happened in 2021

NEWS | August 24, 2022

Congress Considers New Healthcare Cybersecurity Bill

NEWS | August 17, 2022

64% of Security Leaders Can’t Stop a Supply Chain-Related Attack