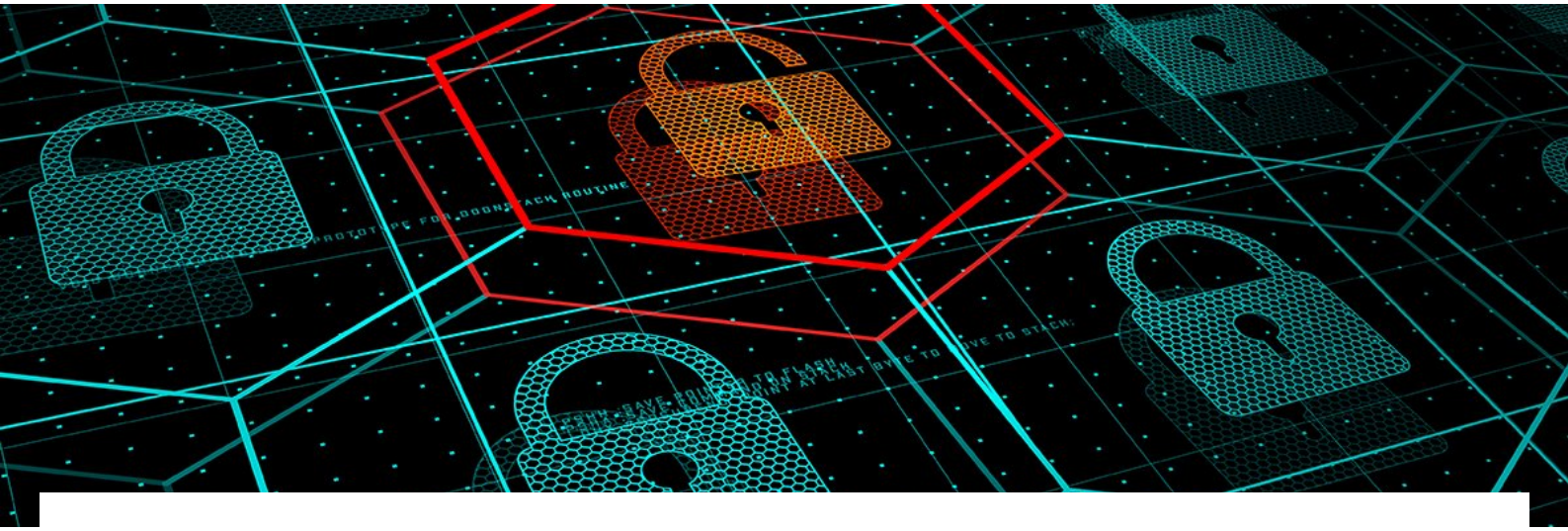
ASKHAT - STOCK.ADOBE.COM



NEWS

Viasat confirms cyber attack on Ukraine customers

The U.S.-based satellite internet provider said a 'multifaceted and deliberate cyber attack' struck Viasat's KA-SAT network on the first day of Russia's invasion of Ukraine.

Arielle Waldman, News Writer

Published: **30 Mar 2022**

Viasat suffered a cyber attack last month that targeted the company's satellite internet network and affected residential modems in Ukraine.

In a blog post Wednesday, the U.S.-based communications company said the attack was limited to European customers, including several thousand located in Ukraine. It referred to the attack, which occurred on Feb. 24 against its KA-SAT network, as "multifaceted and deliberate."

While Viasat owns the KA-SAT network, it is operated by a Eutelsat subsidiary Skylogic. Viasat last year acquired Eutelsat's share of Euro Broadband Infrastructure and the KA-SAT network, but Viasat said it has not taken full control of the all the assets following the acquisition.

The attack, which was limited to a consumer-focused partition of the KA-SAT network, affected "several SurfBeam2 and SurfBeam 2+ modems and/or associated customer premise equipment (CPE) physically located within Ukraine." Viasat said it has shipped nearly 30,000 replacement modems to distributors to restore service for customers.

Subsequently, Viasat enlisted the services of incident response vendor Mandiant, as it continues an investigation into the attack alongside law enforcement and U.S. and international government agencies. The network remained offline for several days, according to the blog. Precautionary measures were taken to "ensure other essential back-office applications and reporting/analytics services were not impacted."

While the ongoing investigation found no evidence that user data, personal equipment or the KA-SAT satellite were compromised, it appears they attributed a motive.

"We believe the purpose of the attack was to interrupt service," the blog post said.

While Viasat did not mention Russia's invasion of Ukraine in its statement, the attack coincided with the start of the invasion, and several other cyber attacks and malware campaigns against the country have been observed by both government agencies and security vendors.

Viasat also revealed the initial attack vector was a misconfigured VPN appliance, which the attacker exploited to gain remote access to the KA-SAT network. Vulnerabilities in VPNs have become a popular target for threat actors, and past government advisories have warned enterprises of the threat.

"Specifically, these destructive commands overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable," the blog said.

Viasat said it is still working to bring customers back online.

The company said it cannot publicly offer specific technical details on mitigation steps at this time, but that it is "leveraging lessons learned from the incident to enhance the security features of its products."

A Viasat spokesperson told SearchSecurity countries outside of Ukraine were affected by the cyber attack but could not share additional information. "Modems were impacted in Ukraine and in other countries within Europe. We cannot provide specific details at this time," the spokesperson said.

While the potential for spillover attacks to other regions is unclear at this point, several analysts and vendors have warned that attacks targeting Ukraine could affect the U.S. and other non-Russian allies.

One day prior to the attack, the Cybersecurity and Infrastructure Security Agency announced that Viasat joined CISA's Enhanced Cybersecurity Services program as a new service provider. One goal of the partnership was the ability to "provide its customers with early warning against sophisticated cyber attacks," according to the announcement.

Dig Deeper on Threat detection and response

Russian cyber attacks on Ukraine driven by government groups

By: Shaun Nichols

Prepare for long-term cyber threat from Ukraine war, says NCSC

By: Alex Scroxton

How Russian sanctions may be helping US cybersecurity

By: Peyton Doyle

Nature of cyber war evolving in real time, says Microsoft president

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 ...