Satellite modems nexus of worst cyberattack of Ukraine war

March 30 2022, by Frank Bajak

In this photo released by Ukrainian Foreign Ministry Press Service, the building of Ukrainian Foreign Ministry is seen during snowfall in Kyiv, Ukraine. Prior to the invasion and war by Russia, hackers knocked offline or defaced Ukrainian government websites. Credit: Ukrainian Foreign Ministry Press Service via AP

A malicious software command that immediately crippled tens of

thousands of modems across Europe anchored the cyberattack on a satellite network used by Ukraine's government and military just as Russia invaded, the satellite owner disclosed Wednesday.

The owner, U.S.-based Viasat, issued a statement providing details for the first time of how the most serious known cyberattack of the Russia-Ukraine war unfolded. The wide-ranging attack affected users from Poland to France, getting quick notice by knocking off remote access to thousands of wind turbines in central Europe.

Viasat would not say who it believed was responsible for the attack when asked separately by The Associated Press. Ukrainian officials blame Russian hackers.

The Viasat attack, coming just as Russia was launching its invasion, was considered at the time by many a harbinger of serious cyberattacks that could extend beyond Ukraine. Such attacks haven't yet materialized, though security researchers say the most impactful war-related cyber operations are likely occurring in the shadows, focused on intelligence-gathering.

A free-for-all of lesser attacks, many apparently carried out by volunteers, have been launched against both Russia and Ukraine. A persistent drumbeat of malicious hacking that Ukrainian officials and cybersecurity researchers blame on Russia-affiliated attackers has plagued Ukraine throughout the more than month-long conflict. One of the most serious hacks largely knocked offline the internet and cellular service of a major telecommunications company that serves the military, Ukrtelecom, for most of Monday.

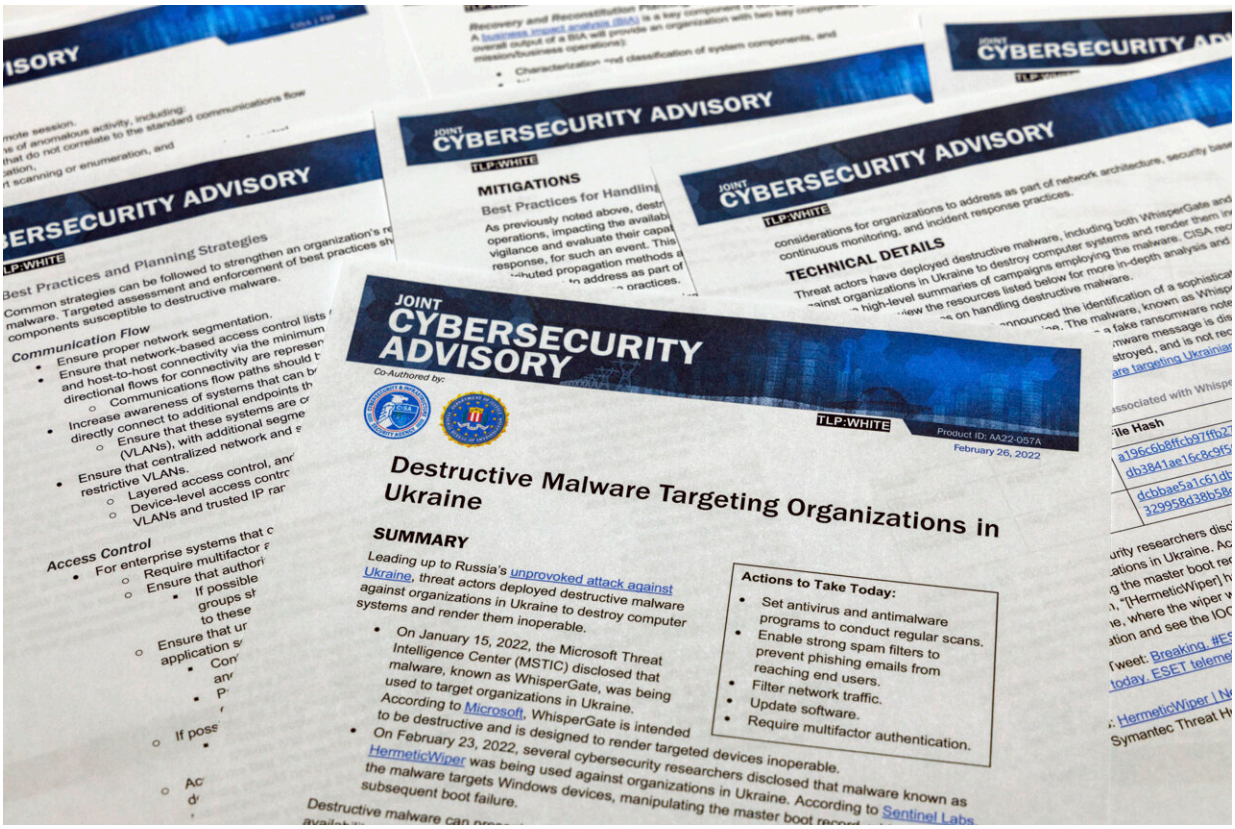
On Wednesday, Google said it had identified a state-backed Russian hacking group engaged in a credential-phishing campaign targeting the militaries of multiple Eastern European countries and a NATO think

tank. It said it did not know if any of the targets were successfully compromised.

The attack on the KA-SAT satellite network highlighted how vulnerable commercial satellite networks that serve both military and non-military clients can be, with the impact felt by individuals and businesses far from the battlefield.

It began in the early hours of Feb. 24 with a distributed denial-of-service onslaught that knocked a large number of modems offline. A destructive attack followed in which a malicious software command sent across the network rendered tens of thousands of modems across Europe inoperable by overwriting key data in their internal memory, Viasat said. "We believe the purpose of the attack was to interrupt service," it said.

It said it has shipped 30,000 replacement modems to affected customers across Europe, most of whom use the service for residential broadband internet access.



A Joint Cybersecurity Advisory published by the Cybersecurity & Infrastructure Security Agency about destructive malware that is targeting organizations in Ukraine is photographed Monday, Feb. 28, 2022. Credit: AP Photo/Jon Elswick

The attack caused a major loss in communications in Ukraine in the early hours of Russia's invasion, top Ukrainian cybersecurity official Victor Zhora told reporters earlier this month. Asked by the AP last week who was responsible, Zhora said, "We don't need to attribute it since we have obvious evidence that it was organized by Russian hackers to disrupt connection between customers that use this satellite system."

He said he did not have information on whether the service had been restored and could not say which Ukrainian agencies beyond the military were affected. Contracts show, however, that Zhora's own agency, the

State Service for Special Communications, is among customers that also include police agencies and municipalities. Viasat said "several thousand customers" located in Ukraine were impacted.

Viasat, based in Carlsbad, California, said the initial denial of service attack had emanated from modems inside Ukraine. It did not specify how the destructive malware entered the network other than to say a "misconfiguration" in a virtual private network appliance was compromised, allowing the attackers to gain remote access from the internet to a "trusted" management console used to administer the satellite network.

From there, the attackers were able to simultaneously send the disabling command to modems across Europe, rendering them useless but not permanently unusable, Viasat said.

It was not known how the attackers breached the VPN appliance. Satellite cybersecurity researcher Ruben Santamarta said it was important to know whether they had obtained credentials or exploited a known vulnerability. Viasat declined to provide specifics Wednesday, citing an ongoing investigation.

Gregory Falco, a Johns Hopkins University professor specializing in satellite system security, said the impact on affected systems was minor compared to what the attackers were capable of doing.

Falco said it's likely they've maintained a foothold. "The attackers don't want to show their whole hand or any of their positioning for how they plan to persist in the network," he said.

The hacked ground-based network is run by Skylogic, an Italy-based subsidiary of Eutelsat, from which Viasat purchased the KA-SAT satellite in April of last year.

Viasat's investigation of the attack was done by the U.S. cybersecurity firm Mandiant.