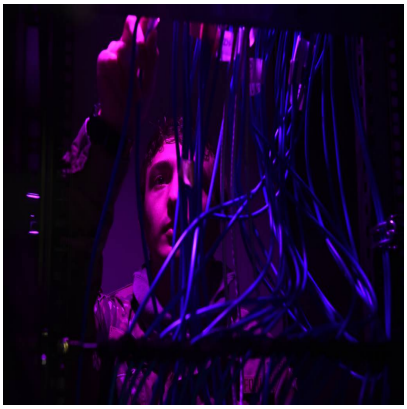

Following cyberattack, communication satellite operators want more guidance on reporting

Description

USA: Satellite communications companies said this week that new guidance from the FBI and the Cybersecurity and Infrastructure Security Agency asking industry to lower its threshold for reporting signs of possible cyber intrusions is a good step toward raising awareness of malicious activity and holding bad actors accountable.

On March 17, the two agencies issued an alert of a possible threat to U.S. and international SATCOM networks and recommended a number of mitigations for network providers and customers, including the use of secure authentication methods and additional monitoring for “anomalous traffic.” President Joe Biden further emphasized the threat this week, telling a group of business leaders on Monday: “Russia may be planning a cyberattack against us.”

The warnings follow reports of thousands of distributed denial-of-service attacks on Ukrainian systems as well as a cyberattack against communications provider Viasat’s KA-SAT system that occurred in late February, just as Russian forces were beginning their invasion of Ukraine. The satellite system provides high-speed internet coverage for users in Europe and the Mediterranean.

U.S. intelligence agencies continue to investigate the incident, and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger said this week during a White House press briefing the government has not yet attributed the attack.

Craig Miller, Viasat’s president of government systems, told C4ISRNET this week the company has identified a root cause, put mitigations in place and is “bringing users back online by the thousands per day.” The attack, the company has said, did not impact the satellite or its core network infrastructure and did not compromise user data.

“Throughout the whole time, we always had large numbers of users operating in the region,” Miller said. “Some were knocked offline, but we are repopulating all those terminals and within weeks we’ll have all the terminals replaced and every user back to capacity the way it was.”

While Viasat typically operates its own networks, Miller noted that the KA-SAT network is currently

operated by a subsidiary company called Skylogic and had a different set of security and tools than Viasat-operated networks.

“It was our estimation that the Viasat-operated networks were never vulnerable to an attack like this,” he said.

Normalizing incident reporting

Miller said Viasat supports CISA’s recommendation for companies to lower their cyber incident reporting threshold — largely because events like this are often accepted as business as usual rather than a serious security violation.

“I really applaud CISA for saying to lower the threshold for reporting because we should hold these actors accountable,” he said. “There’s sort of a perception that it’s just OK. But if I broke into your house and broke down your door, the police would show up.”

Neuberger echoed that sentiment this week, noting that while CISA has detected recent “preparatory activity” for a possible cyberattack, the call to action for network owners should continue even beyond the current heightened security environment.

“Every single day, there should be a call to action,” Neuberger told reporters. “We’re using the opportunity of this evolving threat intelligence regarding potential cyberattacks against critical infrastructure to reiterate . . . specifically to critical infrastructure owners and operators to say, ‘You have the responsibility to take these steps to protect the critical services Americans rely on.’”

Sam Costa, a space intelligence officer for the Director of National Intelligence, said Wednesday there may be a perception among the defense and commercial space industrial base that there would be repercussions for reporting cyber threats.

Speaking Wednesday on a panel at the Satellite 2022 Conference here, Costa said companies should remain engaged with the FBI and CISA in the future and continue reporting incidents.

In some cases, better collaboration between the government and SATCOM providers could improve incident reporting. Pete Hoene, CEO at SES Government Solutions, said the Combined Space Force Component Command’s Commercial Integration Cell at Vandenberg Space Force Base in California enables some of that partnership and information sharing on things like electromagnetic and radio frequency interference.

“We actually have a Commercial Integration Cell person on the [top secret/sensitive compartmentalized information] floor that’s working on observing EMI and RFI disruptions, trying to geolocate those and then trying to make sense of those,” Hoene said during a March 23 panel at the Satellite 2022 Conference. “That information is shared to a certain degree. There is some sensitivity there, but I think that’s an improvement and the interagency processes have improved over the last few years as well.”

Along with the growing partnership on the operations side, Hoene said there is a need for long-term cooperation when it comes to requirements and procurement so that companies can ensure they’re investing in the kinds of resilient capability the government needs. He praised the efforts of the Space

Force's Commercial SATCOM Office — the entity responsible for buying commercial SATCOM services — but said companies need more flexibility and appropriate contract structures in order to respond to the service's needs.

Improving resiliency

For SATCOM operators and users, resiliency measures can range from things like cyber hygiene and automated network monitoring to the availability of a diverse network of providers operating in multiple orbits.

Miller said that for the Department of Defense, having the "optionality" that comes with multiple providers operating on different frequency bands is a key line of defense against a range of threats – from cyber disruptions and satellite jamming to kinetic attacks.

"The more diverse you make it and the more optionality you create, the harder it is for the adversary," he said.

Viasat is on contract with the Air Force Research Laboratory to explore how hybrid, or diverse, satellite communications architectures can help make DoD systems more resilient. AFRL awarded the $50.8 million contract in 2021, and Miller said the company is developing multiple proof of concepts in the land and space domains.

Rick Lober, vice president and general manager of defense and intelligence systems at Hughes Network Systems, told C4ISRNET this week the company recently demonstrated the ability to switch internet traffic from a satellite based in geosynchronous orbit to one in low Earth orbit and to share traffic between multiple orbits.

The demonstration was for commercial users, but Lober noted that it has application for military customers as well, particularly when it comes to resiliency.

"The military can do that as a way to make it very difficult to figure out which path is the signal really going on," he said.

by Courtney Albon is C4ISRNET's space and emerging technology reporter. She previously covered the U.S. Air Force and U.S. Space Force for Inside Defense.

Category

1. Army-Wars-Conflict Zones-Military Tech.
2. Main
3. Politics-Geopolitics-Gov.-Events

Date Created
03/25/2022