TLP WHITE

2022-015
07/03/2022

Report

Surfbeam2 blackout, what happened with KA-SAT?

Summary

At 6 a.m. on February 24th, 2022, satellite internet services associated with the Eutelsat 9E satellite, also known as "KA-SAT" and operated since April 2021 by Viasat, suffered a strong blackout. This KA-SAT service failure has spread outside Ukrainian borders, which caused a blackout of thousands of subscribers but also of industrial systems using this Internet link for communication purposes.

Several newspapers have taken over this event, often without technical elements regarding a possible cyber attack, announcing in some cases an attack directed against the KA-SAT satellite itself. Media also reported that in Germany, offshore wind farms experienced a network blackout with "*modems that would have burned*".

A SEKOIA.IO investigation has made it possible to uncover some motivations as well as possible technical attack vectors used during this attack.

What is KA-SAT?

KA-SAT is one of the multiple satellites allowing satellite Internet communications. Launched in December 2010, it communicates on the KA band (26 to 40GHz). It allows a much faster bandwidth than former generations that used the KU band (12 to 18GHz). Unlike satellites working on the KU band covering large geographic areas, the KA-SAT satellite splits these geographical areas in smaller areas called "cells".

With a cell diameter of approximately 250 kilometers, the beam concentration on these areas allows to significantly increase network speed but also makes interception harder by SIGINT ground stations that are not inside the cells.

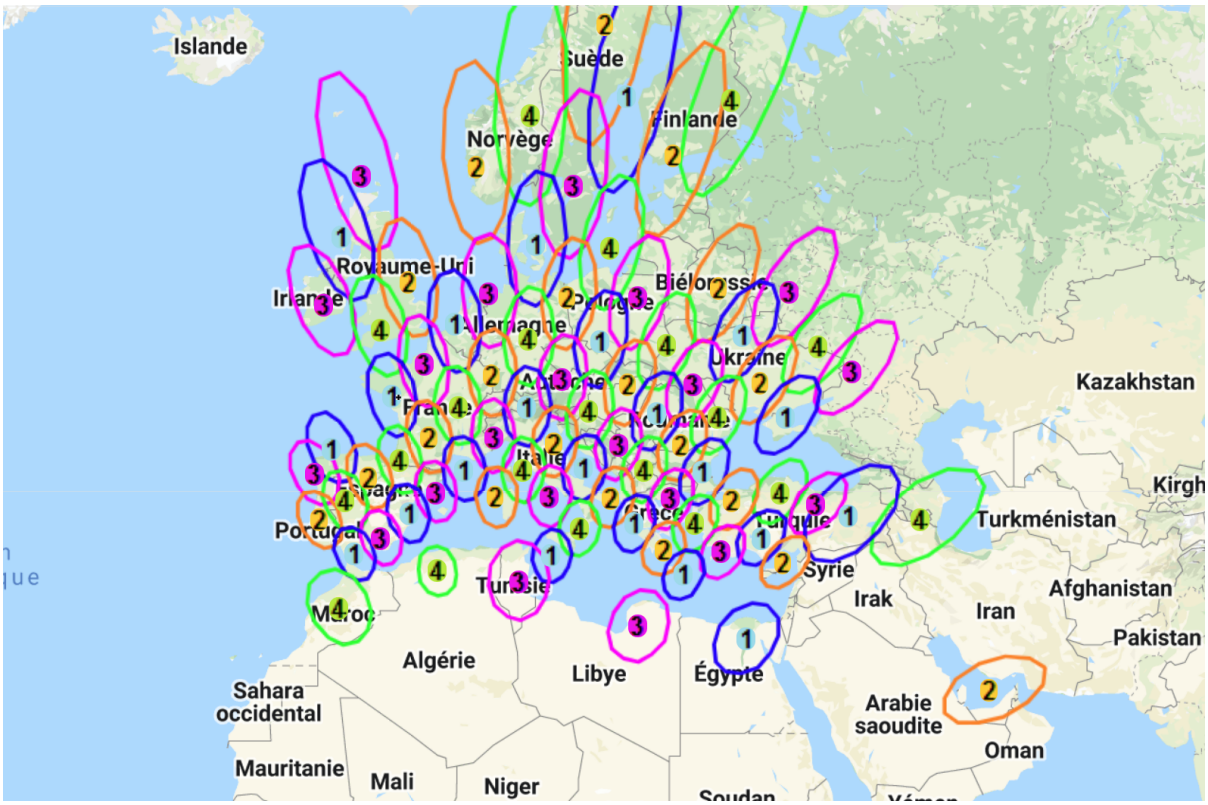

Figure 1. KA-SAT cells over Europe, including Ukraine.

Thanks to its ease of implementation in places that are difficult to reach and during natural disasters, **KA-SAT has become one of the leaders for satellite Internet communications through Europe**. Thenceforth, it has been used for almost 10 years by several military forces, emergency services, industrial companies and energy providers but also by regular subscribers living in white areas.

KA-SAT use in Ukraine

Thanks to OSINT investigations, **SEKOIA.IO is able to confirm that KA-SAT was used by the armed forces, the security services and the government of Ukraine** prior to the Russian invasion on February 24, 2022, date on which the incident took place. For proof, here is a screenshot from one of the Ukrainian armed forces websites presenting a mobile Tooway reception station using KA-SAT in 2016.

Засоби зв'язку

СУПУТНИКОВА АНТЕНА Tooway

22 Лютого, 2016 admin

ТАКТИКО ТЕХНІЧНІ ХАРАКТЕРИСТИКИ :

1. Антена Tooway забезпечує вихід в Інтернет, телефонні переговори в любому місці . Навіть там де не має наземних ліній зв'язку , кабельних мереж або телефонних комунікацій , покриття мобільних телефонів , де не працюють мережі 3G або мережі Wimax;
2. Комплект VSAT обладнання , куди входить супутниковий модем (інша назва "супутникова станція") установлюється в середині приміщення , в тому місці де стоїть комп'ютер , телефонна станція для роботи ;
3. Супутникова антенна Tooway виготовлена в США, компанії VIASAT;
4. Частина обладнання для супутникового зв'язку встановлюється на вулиці , на відкритій місцевості , щоб супутникова антена була направлена на супутник ka-sat 9E. (стінове кріплення, антенна Tooway, конвертор TRIA);
5. Полотно антени Tooway виготовлено з високолегірованої сталі (товщиною 1мм) покрашено порошковою краскою білого кольору . Логотип «Tooway» нанесений порошковою краскою голубого кольору по центру антени. Всі інші елементи і деталі антени Tooway покрашені в білий колір ;
6. Супутникова антенна Tooway призначена виключно для прийому і передачі інформації в мережі інтернет;
7. Супутникова антенна Tooway має діаметр 75см, загальна вага конструкції в в зборі складає 32кг;
8. Антена поставляється в картонній коробці з іншим обладнанням , в розібраному вигляді . В комплекті антенна Tooway мається зборочне креслення для самостійної установки.

Комплектація:

1. Уніфікований кронштейн для кріплення до стіни і др. -1 шт.
2. Фірмова антена "Tooway" діаметром 75см -1 шт.
3. Конвертор прийомо-передаючий TRIA – 1шт.
4. Спутніковий термінал ViaSat в комплекті с блоком живлення – 1 шт
5. Заземлюючий кабель – 1м.
6. Інструкція по самостійній установці – 1шт. (інструкція по монтажу);
7. Антена поставляється в картонній коробці з іншим обладнанням , в розібраному вигляді . В комплекті антенна Tooway мається зборочне креслення для самостійної установки

Figure 2. Ukrainian airborne forces article showing a Tooway/SurfBeam 2 modem

The use of Surfbeam2/Tooway modems is not limited to the Ukrainian army. Several public contacts listed on the government portal `prozorro.gov.ua` mentionned **KA-SAT ground stations purchases using Surfbeam2/Tooway modems**. Among other things, four important public contracts with the DataGroup Private Joint Stock Company - the only Ukrainian company that can respond to this public tender according prozorro.gov.ua - draw

our attention:

Contract ID	Amount	Description
UA-2020-12-23-008256-c	2 000 000,00 UAH	Contract related to the purchase of an unknown number of Tooway satellite network equipment by the Ukrainian security services.
UA-2019-12-27-002218-b	2 000 000,00 UAH	Contract related to the purchase of an unknown number of Tooway satellite network equipment by the Ukrainian security services.
UA-2019-06-14-003208-b	2 036 433,38 UAH	Contract related to technical support services (Maintenance, Repair) on satellite network equipment to ensure communications of the Ukrainian government.
UA-2016-12-23-001706-b	2 500 000,00 UAH	Contract related to the purchase of 51 Tooway satellite network equipments.

Table 1. Few contracts passed by the Ukrainian government mentioning Tooway

So what happened on February 24th, 2022 at 6am?

Despite the lack of information officially shared on the attack and given the significant media noise around it, several hypotheses can be considered with different levels of confidence.

First, it is highly unlikely that the KA-SAT satellite has been hacked and / or damaged following a cyber attack on February 24th, 2022. Although the "blackout" happened throughout Europe, some modems using this satellite, located in an area where the blackout happened, are still reachable and their users still have access to the Internet. Therefore the hypothesis of an attack directly conducted against KA-SAT itself or the ground infrastructure operating this satellite (teleports, SMTS etc.) can be removed.

However, several sources indicated thatTooway/SurfBeam2 modems may have undergone an attack on February 24th, 2022. Therefore, **the privileged hypothesis is an attack directed only against the Tooway/SurfBeam 2 modems**. These modems - used by Ukrainian forces and civilian facilities across Europe - also seem to have been used by the German wind farms. Indeed, an article from the Signalhorn company reports their connection to KA-SAT via Tooway technology around 2018. This could explain the communication breakdown suffered by the German wind farms on 24 February 2022.

As of today, it is known that to compromise such network equipments, four intrusion vectors can generally be used by attackers:

- **An attack via the WAN interface** where an attacker takes control of the modem by accessing the administration interface from the Internet (Telnet, SSH, HTTP(s)). The

main limitation here is the attack surface and the fact that many constructors prevent (thankfully) the accessibility of such interfaces from the Internet.

- **An attack via the LAN interface** by an attacker present on the local network or through a CSRF-like vulnerability (by visiting a website with a malicious script). This attack - as the one via the WAN interface - may also imply other vulnerabilities (command injection, privilege escalation, arbitrary file upload) to change the firmware to a malicious one.

- **A physical attack**, where the attacker opens the modem and flashes the existent firmware with the malicious one. Even if this attack is quite stealthy and can be done in few minutes, it requires physical access to the device and it's not scalable.

- **A supply-chain attack via the compromise of the modem's update mechanism**. It can be done - for example - just by putting a new firmware to download inside a repository owned by the constructor. Therefore if the modem regularly checks for new updates to be automatically installed, it will download and install the rogue firmware or a malicious binary which will install it and reboot the system.

Even if we still don't know how that attack was made, many external sources and hints (such as the attack's timing and its scale) point to the possible implication of the last intrusion vector, an "automatic update mechanism" which pushed a malicious firmware into thousands of modems. As this kind of automatic mechanism is not documented in the end-user Tooway documentation viewed by SEKOIA.IO.

However, **ViaSat documentation presents a system dubbed "EMS" for "Network Management System"**. According to the documentation "*The gateway element management system facilitates detection, isolation, notification, and correction of faults in the satellite network elements.* ***The EMS also manages configurations and software updates for the managed elements*** *and is capable of collecting and sending usage information to the NOC.*"

Therefore it is possible that the attackers have compromised and then used this system in order to push malicious software updates to the modems. The first vector can be also mentioned but we haven't been able to find such interfaces - except for extremely rare cases - on the Internet via specialized search engines.

If this hypothesis is proven, yet another question remains unanswered: what was the main objective of this attack? Today, **two distinct objectives** can be put on the table: **the sabotage of the modems** used by the Ukrainian forces by sending a blank firmware or an **attempt that would have failed to replace the existing firmware by a malicious one**. Even if this second objective seems less likely, we must not forget the strategic interest that can have an attacker in the interception (*via* a custom firmware) of communications passing through these modems in case of intelligence gathering during an armed conflict.

Whatever is the ultimate goal of this attack, its impact makes it one of the biggest cyber attacks disclosed and directly oriented against communications capabilities of an armed force. **Therefore, this event will act as a milestone for the next conventional conflicts.**

SEKOIA.IO reminds finally that **if a firmware is damaged and does not allow a boot sequence, it is impossible to update it without physical intervention** (firmware

flashing) on affected devices. Therefore, each modem impacted by this attack will probably have to be replaced by a new one.

REFERENCES

- [DSHV.MIL.GOV.UA] Ukraine airbone article mentioning Tooway
- [PROZORRO.GOV.UA] UA-2020-12-23-008256-c contract
- [PROZORRO.GOV.UA] UA-2019-06-14-003208-b contract
- [PROZORRO.GOV.UA] UA-2019-12-27-002218-b contract
- [PROZORRO.GOV.UA] UA-2016-12-23-001706-b contract
- [INAU.UA] KA-SAT technical presentation
- [SignalHorn] Press release mentioning Tooway
- [ZAUFANATRZECIASTRONA.PL] Article mentioning modem outages
- [VIASAT] VIASAT document mentioning the EMS technology

Our mailing address is:
SEKOIA
18-20 place de la Madeleine
Paris 75008
France