VIASAT UKRAINE CASE STUDY

Jean-Jacques Halans
CSU April 18 2022

Introduction

Ukraine is in the news for all the wrong reasons. Over the last decade, it has suffered a barrage of cyber-attacks attributed to Russia, including NotPetya in June 27th, 2017 which spilled over and impacted non-Ukrainian targets, causing billions of dollars of damage around the globe (Perlroth, 2021). But earlier this year, on the morning of February 24th 2022, the Russian army commenced their "special military operation", a full scale invasion into Ukraine, while at the same time, between 3am and 9am, knocking out Ukrainian satellite communication (Pearson et al., 2022), as well as other Viasat satellite internet services across Europe. In this paper we review what is currently known about this recent Viasat cyber-attack.

Viasat KA-SAT AcidRain cyber-attack

Satellites play a vital role in our daily life, from weather predictions, global media consumption, GPS location, to communications, both civilian as well as military. Viasat is one such large global player in the satellite space. It provides information technology and communication services for both civilian as well as military purposes, in the US and globally, which makes it a "dual-use" carrier (Duffy, 2022), which comes with consequences.

First off, the February 24th attack was indeed a DoS cyber-attack on satellite communications, but not an attack on the communications satellite itself. I believe this distinction needs to be made as to how this affects any retaliatory action. As Brooks Tigner reported for Janes in June 2021, NATO's "*Article 5's tripwire would extend to all the NATO countries' space assets, whether in orbit or on the ground, whether within or beyond the geography of their collective home territory*" (Tigner, 2021).

In 2016, U.S. based Viasat went into a joint venture with French Eutelsat for the KA-SAT wholesale broadband service, known as Euro Broadband Infrastructure (EBI). Then end of 2020, Viasat acquired the whole operation, including KA-SAT satellite and ground stations, (*Viasat Completes Acquisition of Remaining Stake in its European Broadband Joint Venture, Inclusive of the KA-SAT Satellite and Ground Assets*, 2021). Until at least the end of this year, this service is commercialised by the Italy-based Skylogic, a subsidiary of Eutelsat. As you can see it is quite a complex commercial setup.

Two months on from the cyber-attack, in the fog of war, details are still missing as to what vulnerability was exploited, and where. Viasat released an incident report on March 30th with a high-level overview of the events that unfolded that morning. ReverseMode and SentinelOne provide more technical commentary as to the potential how.

Ka-band is the 26 GHz to 40 GHz satellite/microwave telecommunications frequency on which KA-SAT SATCOM operates (*Satellite frequency bands*, 2020), providing high-capacity broadband internet services to both government as well as private sector business and consumers. The service needs a dish and satellite modem, like the Viasat Surfbeam 2/2+ modem. These modems, the ones located in Ukraine, started misbehaving around 3:02 UTC on February 24th by sending malicious traffic across one of the KA-SAT *consumer-oriented network partitions* (*KA-SAT Network cyber attack overview*, 2022).

As Viasat and Skylogic forced those malicious terminals offline, others came online and continued the attack for several hours, denying service to other legitimate users on the network. Then on 4:45 UTC, for the next 45 minutes, Viasat and Skylogic notice a larger number of modems across Europe dropping of the network, never to connect again. Eventually tens of thousands of modems were affected. This includes most of the Ukrainian KA-SAT modems, as well as a significant number of modems across Europe (*KA-SAT Network cyber attack overview*, 2022).

Even though Viasat in their incident report highlighted, repeatedly, the fact that this happened on their consumer-oriented network/service partition, it also disconnected 5800 of Germany's Enercon wind turbines, good for 11 gigawatts of capacity, disabling its remote monitoring and control, but without any effect on the grid stability owing to their failover communication capabilities (*Satellite outage knocks out thousands of Enercon's wind turbines*, 2022).

The intended target of the cyber-attack was almost certainly the Ukrainian military, as the Ukrainian deputy chief of the "State Service of Special Communication and Information Protection", Victor Zhora, confirmed the satellite outage was "*a really huge loss in communications in the very beginning of war*" (Cattler & Black, 2022), which would have impacted their command and control capabilities as well as tactical missions like drone offenses on advancing Russian armoured vehicles (Nakashima, 2022).

Viasat officials explained this military use as a side effect of their distribution model using third parties, like Skylogic and others, and as such in the Ukrainian case they didn't have a direct relationship with those customers, and didn't know how their terminals were being used. (*Hackers Attacked Satellite Terminals Through Management Network, Viasat Officials Say*, 2022)

Viasat engaged Mandiant for incident response and forensic analysis. Through this investigation, they identified the point of intrusion as an exploit in a misconfigured VPN appliance, providing the attacker admission to the trusted management segment of the communication network. This allowed the attacker to send management commands to the terminals, which included overwriting flash memory, making the modem inoperable, although not permanently (*KA-SAT Network cyber attack overview*, 2022). Which VPN appliance, which misconfiguration or which exploit exactly?

On March 17 2022, CISA and the FBI jointly released CSA alert AA22-076A related to SATCOM network providers and their customers, highlighting specific mitigations (*Strengthening Cybersecurity of SATCOM Network Providers and Customers*, 2022). This document may include some clues as to what misconfigurations may have been in place at the Skylogic KA-SAT operations, like the presence of insecure remote access tools (like Telnet, FTP, SSH), default or weak credentials, or lack of vulnerability or patch management.

SentinelOne calls the second part of the attack where the terminals became inoperable, a supply chain attack, pushing out a wiper specifically developed for routers and modems. They first noticed a suspicious piece of software on March 15th, with the name "ukrop". SentinelOne calls this malware AcidRain (SentinelLabs, 2022), and it's the 7th wiper malware linked to the Russian invasion of Ukraine.

As per SentinelOne's analysis, AcidRain seems to be a general-purpose modem wiper, that looks for several device file identifiers and then overwrites it or wipes its data. SentinelOne found some superficial similarities to VPNFilter, another wiper malware that was attributed by the NSA to Russia's Sandworm APT, or rather one of VPNFilter's plugins named "dstr" (SentinelLabs, 2022).

Another security researcher, Ruben Santamarta, publishing on his ReverseMode blog, seems to confirm SentinelOne's plausible hypothesis. He obtained two Surfbeam 2 modems, one with original firmware, and another which was wiped, and compared the two. The targeted modem shows a destructive code pattern, applied through the AcidRain wiper, making it inoperable. He further on reverse engineered Viasat's TR069 data model, and concludes that there was no signature verification allowing the installation of arbitrary binaries or malicious command injections (Santamarta, 2022).

Additionally, through a Skylogic corporate video, Santamarta found a screenshot of an operator's desktop which, after further research, led him to believe they are using Fortigate VPN appliances. There is a known disclosure of SSL-VPN access credentials of 87000 Fortigate devices, published between 2019 and June 2021 (Windsor, 2021). Skylogic did make that list (which can be found on GitHub), though it is unconfirmed (but not unheard of) that they didn't patch their devices for two years, or update their credentials as per 2019 FortiGuard advisory (*FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests*, 2019). That advisory refers to the original DevCore research into 5 FortiOS vulnerabilities, including a "*Unauthenticated SSL VPN users password modification*" using a "magic" parameter, the almighty hardcoded password (Chang & Tsai, 2019).

Although U.S. government hasn't publicly announced the attribution, as per Washington Post, "*according to U.S. officials familiar with the matter*", U.S. intelligence analysts point to the GRU, the Russian military spy service being behind the compromise (Nakashima, 2022). Attribution isn't about accuracy or confidence, as Marcus Willett, a former director of the British GCHQ, explains it, but rather about protecting sources of information (Townsend, 2022). Of course, in this case, unlike previous cyber-attacks in Ukraine since 2014, there are also Russian boots on the ground in Ukraine.

Conclusion

Ironically, Viasat joined the U.S. CISA Enhanced Cybersecurity Services program as service provider, announced February 23 2021, a full 12 months to date before this cyber-attack (*CISA announces new enhanced cybersecurity services provider*, 2021), but their dependence in Europe on the inherited third party service provider Skylogic and Skylogic's network management security practices (or lack thereof) made them vulnerable to DDOS and supply-chain attacks. Confirmed details are still missing currently, and more research is required, but as with many other cyber-attacks, details will surface as months and years pass. In fact, additional details emerged as I was writing this report. We may know more about the how and who, possibly through Mandiant, when Viasat takes charge of operations later this year, at which point updated research is due. For now, I'm grateful for the excellent work of Ruben Santamarta and the SentinelOne researchers.

References

Cattler, D., & Black, D. (2022). *The Myth of the Missing Cyberwar*. Foreign Affairs. https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar

Chang, M., & Tsai, O. (2019). *Attacking SSL VPN - Part 2: Breaking the Fortigate SSL VPN*. DevCore. https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn/

CISA announces new enhanced cybersecurity services provider. (2021). CISA. https://www.cisa.gov/news/2021/02/23/cisa-announces-new-enhanced-cybersecurity-services-provider

Duffy, R. (2022). *LEO Megaconstellations Are…Dual-Use?* Payload. https://payloadspace.com/megaconstellations-dual-us/

FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests. (2019). FortiGuard. https://www.fortiguard.com/psirt/FG-IR-18-384

Hackers Attacked Satellite Terminals Through Management Network, Viasat Officials Say. (2022). Airforce Magazine. https://www.airforcemag.com/hackers-attacked-satellite-terminals-through-management-network-viasat-officials-say/

KA-SAT Network cyber attack overview. (2022). Viasat. https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

Nakashima, E. (2022). *Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say*. Washington Post. https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/

Pearson, J., Satter, R., Bing, C., & Schectman, J. (2022). *U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say*. Reuters. https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/

Perlroth, N. (2021). Prologue. In *This Is How They Tell Me the World Ends*. Bloomsbury Publishing.

Santamarta, R. (2022). *VIASAT incident: from speculation to technical details.* https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html

Satellite frequency bands. (2020). ESA. https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Satellite_frequency_bands

Satellite outage knocks out thousands of Enercon's wind turbines. (2022). Reuters. https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/

SentinelLabs. (2022). *AcidRain, A Modem Wiper Rains Down on Europe*. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

Strengthening Cybersecurity of SATCOM Network Providers and Customers. (2022). CISA Retrieved from https://www.cisa.gov/uscert/sites/default/files/publications/AA22-

076_Strengthening_Cybersecurity_of_SATCOM_Network_Providers_and_Customers.pdf

Tigner, B. (2021). NATO leaders extend Article 5 mutual defence clause to space domain. https://www.janes.com/defence-news/news-detail/nato-leaders-extend-article-5-mutual-defence-clause-to-space-domain

Townsend, K. (2022). *Russia, Ukraine and the Danger of a Global Cyberwar*. https://www.securityweek.com/russia-ukraine-and-danger-global-cyberwar

Viasat Completes Acquisition of Remaining Stake in its European Broadband Joint Venture, Inclusive of the KA-SAT Satellite and Ground Assets. (2021). ViaSat. https://www.viasat.com/about/newsroom/press-releases/viasat-completes-acquisition-remaining-stake-its-european/

Windsor, C. (2021). *Malicious Actor Discloses FortiGate SSL-VPN Credentials*. https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials