Lessons Learned From the 2022 Viasat Hack: Evolution of Cyber Warfare

Nathan T. Rickett

University of South Florida

Course Number: ISM 6328-021301

12 December 2024

Abstract

In February of 2022, Russian hackers targeted the KA-SAT network, which is owned by the corporation known as Viasat. The affected network is used by Ukraine's military to facilitate communications and critical infrastructure as well as civilian infrastructure from multiple countries in Europe. The attack involved gaining unauthorized access to KA-SAT modems and installing malicious software on them. The malicious software, also known as AcidRain, wiped they modems of critical software needed to operate. Any endpoints connected to the KA-SAT network via these modems were then unable to communicate across the network, taking down thousands of systems, and giving the Russian military the foothold they needed to begin their invasion campaign against Ukraine. Collateral damage was also reported by non-Ukrainian Viasat customers such the German industrial controllers. This attack perfectly exemplifies how the nature of warfare has evolved from being fought almost entirely on a battlefield, to one that is fought in both physical space and a digital space. If one is proactive in securing their assets in all seven of the domains of IT infrastructure, the risk of threats such as this one being realized can be mitigated.

Lessons Learned From the 2022 Viasat Hack: Evolution of Cyber Warfare

Most of our daily life is now spent performing some activity that involves satellite communications. Whether you are using GPS to avoid traffic on your way to work, check the time on your phone, or you are living in a rural area where satellite internet is your only option for staying connected, chances are, you are not only utilizing satellite communication as a helpful tool, but rather you are reliant on it. As a society, we've become accustomed to the rapid advancement in technology and have been eager to take advantage of those advancements to improve our lives, but most of us don't stop to think about the potential risks involved with the technology we use, and what might happen if the threats they pose are realized. Satellite communication isn't necessarily new territory that we are stepping into, but the technology involved with it has developed to a point where it has become a contender for personal and private use, especially for home internet and civil infrastructure. Certainly, security was a forethought when starting to implement satellite internet into civil and military infrastructure, but organizations using it need to ensure that each of the seven domains are secured, especially when third parties are involved, or else that infrastructure could be compromised and potentially cost human lives.

In February of 2022, one hour before Russia invaded Ukraine, the American communications company Viasat noticed that thousands of their modems were being taken offline. These modems resided on the KA-SAT network, which was being used by the Ukrainian military, government, and civilians, as well as many other civilian entities across Easter Europe. This left Ukraine in a vulnerable state, allowing Russia to advance beyond the Ukraine-Russia border, affectively beginning the Russian

campaign to capture and control Ukraine. Collateral damage was also noted by other European customers, such as Nordex, a wind turbine manufacturer that noticed nearly 5,800 wind turbines had been taken offline in Germany. This perfectly outlines the importance of introducing a robust risk management framework into each system that we rely on to detect potential threats and ensure that some sort of plan for mitigation is created.

Reconnaissance

Every Cyber-attack begins with gathering information about a potential target. Russian adversaries were able to gather information about the infrastructure used by the Ukrainian government and military including the VPN provider used by Viasat administrators. Advanced persistent threats like this start their attack by gathering information on a target, which widens their attack surface and strengthens their understanding of the target's operations and weaknesses. With the information gathered, they no longer cast a wide net and see what works, instead, they can tailor the attack to their liking and reduce the amount of time to exploit, while minimizing time to detection. In a press release by the U.S. Department of State on May 10th, 2022, then Secretary of State Antony Blinken described the attack as nation state sponsored, specifically by Russia (U.S. Department of State, 2022), therefore, it likely had the support of one or more of the Russian Intelligence Agencies. There hasn't been any information released regarding how the nation state actors were able to gather information on Viasat, but we can assume Russia was able to gather intelligence through a reconnaissance campaign.

To minimize attack surface, an organization should limit the amount of publicly available information to reduce their public footprint. Data loss prevention should be integrated into IT infrastructure to identify sensitive information, and prevent it from exfiltration, leakage, and destruction. Regulations and policies on how to handle sensitive information are also key to maintaining data confidentiality. Regular audits of publicly available information such as social media, DNS records, domain information, web pages, geolocation, and more will help to improve the organization's security posture. Information regarding the internal infrastructure of an organization should not be known to the public, since it could be used for fingerprinting purposes.

Initial Foothold

The hackers created an initial foothold into the Viasat network by exploiting a Viasat VPN appliance manufactured by Teldat, a Spanish telecommunications company, which provided network access to administrators and operators. This exploit was key to the hackers' success in their attack, since it gave them access to internal assets which were then used as part of their attack framework.

Viasat has publicly stated that they still do not know how the exploit was performed, and even went as far as to say that it was not due to a 0-day exploit, or any known exploit, suggesting that it could have been enabled by an insider threat. In their book *Fundamentals of Information Systems Security* (Kim and Solomon, 2023, p. 39*)*, David Kim and Michael Solomon describe insider threats and humans in general as the weakest link in information security, and stated "Because no group can completely control any individual's behavior , every organization must be prepared for malicious users, untrained users, and careless users." While administrative controls aren't the

most effective in stopping adversaries, a training program for detecting insider threats and reporting them can sometimes mitigate malicious actions by employees.

Regardless of whether the human factor can be fully mitigated, there could have been preventative or detective security controls in place to mitigate the risk that someone were to gain unauthorized access to the management network. An example of a detective security control is a time-based signature in an intrusion detection system, which can detect when logon attempts are performed outside of normal operating hours. A location based signature is also a good way at identifying unusual or suspicious behavior in a network, by comparing the logon attempt location to a list of known good locations. When used in combination, an intrusion prevention system would be able to recognize the multiple failed logons attempts from an unusual location at an unusual time and determine that it is malicious, and therefore block any further access attempts.

Network Enumeration

While gaining network access is certainly a major step in carrying out a cyber-attack, it isn't the end goal for most adversaries. Having access to a local area network is like knowing treasure is nearby, you just need a treasure map to find it. The attackers were able to explore the network, most likely using a popular tool such as Nmap, and built their metaphorical treasure map, leading them to what they were looking for.

It's important to know how to stop adversaries from gaining unauthorized access to your network, but what many entities overlook is the importance of stopping one from causing any further damage once they have. Making use of a firewall to detect traffic used during network enumeration is important in stopping an adversary from doing that. Knowing what good network traffic looks like in your environment will allow you to create

fire rules that allow normal business operations, while also preventing anything that is unwanted. For example, if a device is trying to connect to another device on the LAN on 100 ports per minute, that is a good indication that someone is conducting a port scan. This kind of behavior can be detected and blocked by a network intrusion detection/prevention system. Segmentation of assets into multiple different network components via VLANs, subnets, and a DMZ would also make it more difficult for adversaries to perform network enumeration.

Lateral Movement & Data Collection

Its unclear which account credentials were compromised in the attack and what privileges it had, but the attackers were able to identify a critical network segment which was used for collecting data and executing the commands in the attack. The data that was exfiltrated contained details about the internal workings of Viasat modems as well as how many were online and more. This information was then used in crafting their exploit later.

There's no point in installing a maximum-security fence in your yard if you are going to remove the front door of your house. Similarly, you shouldn't allocate resources to secure the perimeter network just to allow all access to your network resources internally. To ensure control over network resources, an organization needs to protect account credentials and determine who needs access to what. User and administrator credentials need to be secured and properly stored. To achieve this, passwords should be complex, stored as a hash in a protected environment, and updated according to the organization's password expiration policy. Multi-factor authentication using a combination of something you have, something you know, or something you are is

another great way to ensure authenticity while authenticating. Failed logon attempt restrictions will also mitigate brute force attacks.

As stated above, Viasat did not release any information on the account that was used in the attack (Viasat, 2022), but it's important to acknowledge the possibility that appropriate access controls were not being used. Creating a policy for access controls ensures that even authorized users do not have read access to data that they aren't supposed to. Each section of the CIA triad influences the other sections, and in this example, data confidentiality was compromised, leading to a near total loss of availability.

Exploitation

Once all the data had been collected and a plan of attack was confirmed, the attackers exploited two different vulnerabilities. Initially Viasat reported that the cause of the denial of service was due to destructive commands which overwrote critical data in flash memory on the modems and denied all accusations that modems' software had been tampered with (Viasat, 2022), but security researchers found something different. Modems were analyzed and found to have wiper malware installed on them called AcidRain. AcidRain was deployed through a continuous integration (CI) server, which the attackers had gained access to during their lateral movement. The CI server was responsible for deploying new software to the modems as an update and was changed to include the malware in its next code deployment. After the modems were taken offline using AcidRain, the attackers flooded them with "destructive commands" from one of the management servers that they had gained access to, ensuring that in the case any of these modems hadn't received the new update, they would be taken offline anyways.

CISO at Viasat, Mark Colaluca**,** later confirmed the presence of the wiper malware in a demonstration at DEF CON 31. (Colaluca, 2022, 17:49)

A robust risk management framework helps to identify risks in your organization and determine an appropriate course of action to implement a mitigation. Threat analysis is a part of this framework, and serves to detect and document any vulnerabilities found, as well as their likelihood of being exploited. This can be done using a vulnerability scanner such as Nessus. Multiple vulnerabilities must have existed for these threats to be realized.

It is also apparent that Viasat did not have strong version controls with respect to their code repository for the modems. As a part of this version control, the code should have been thoroughly tested prior to deployment.

Recovery

Partial restoration of services following the attack took a few weeks, and full service was not restored until about a month after the attack. Prolonged downtime led to frustrated customers, and more importantly, left the Ukrainian military in a vulnerable state, allowing Russia to make advancements. The combination of limited communication from Viasat in early stages of recovery and geopolitical consequences resulted in criticism and negative reception of Viasat. Viasat did not publicly share the cost of the recovery, but they did state they had cyber-security insurance. Although cyber-security insurance did transfer some of the risks involved with an attack, it likely did not cover all the damages. Viasat did not release the total cost of recovery, but it can be speculated that the hack might have cost them millions of dollars.

Developing a business continuity and disaster recovery plan should be a high priority for any organization. Kim and Solomon explain this when they stated “A DRP enables an organization to make critical decisions ahead of time. That way, personnel can manage and review decisions without the urgency of an actual disaster. If these plans are not ready in advance, security professionals and managers will have to make best-guess decisions under huge pressure.” *(Kim and Solomon, 2023, p. 384*) The last thing that you want to do is make a best-guess decision while a country is relying on you for their communications as they are being invaded. Conducting a business impact analysis followed by a contingency and recovery plan will help to identify critical functions and make it easier to develop a contingency and recovery plan if they fail. It’s only a matter of time before disaster strikes, and when it does you want to be ready, especially when lives are at stake.

References

DEFCON Conference. (2021, August 8). DEF CON 31 - Defending KA-SAT - Mark Colaluca and Nick Saunders [Video]. YouTube. https://www.youtube.com/watch?v=qI_ICtX3Gm8&ab_channel=DEFCONConference

Kim, D., & Solomon, M. (2023). *Fundamentals of information systems security* (4th ed.). Jones & Bartlett Learning.

U.S. Department of State. (2022, July 19). *Attribution of Russia's malicious cyber activity against Ukraine*. U.S. Department of State. https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

Viasat. (2022, February 28). *KA-SAT network cyber attack overview*. Viasat. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview