Threats Against Satellite Ground Infrastructure: A retrospective analysis of sophisticated attacks

Jessie Hamill-Stewart
University of Bristol, University of Bath
jessie.hamill-stewart@bristol.ac.uk

Awais Rashid
University of Bristol
awais.rashid@bristol.ac.uk

***Abstract*—Satellite services are vital for many types of critical infrastructure, including electricity, finance and transportation. Sophisticated attackers therefore may target satellites, in order to create widespread disruption. The ground infrastructure of satellite systems offers attackers direct access to satellite systems, as this is where satellites are operated and monitored. We investigate the tactics and technology utilised by attackers of satellite ground systems, through analysis of previous attacks conducted against satellite ground infrastructure. Through this investigation, we contribute to growing literature surrounding cyber attacks against satellite systems, by providing empirical analysis of techniques and tactics used to attack ground infrastructure. Analysis of attack cases is presented, and then we discuss key findings and implications for future research.**

I. Introduction

Satellites are innately vulnerable to cyber attacks and attacks against the ground segment are especially concerning. This is where satellites and wider satellite services are managed. Within satellite ground infrastructure, a satellite operations centre with one or more ground terminals communicates with satellites and the system processes satellite bus and payload information [1]. Operation centres vary in size, with larger ones operating many different types of satellites or a constellation of similar satellites, such as Iridium ™ [1]. These may have external interfaces that provide significant amounts of data, and they are geographically dispersed, so that data sharing takes place among various sites [1]. Ground systems also contain the distribution of infrastructure which relies on satellites, such as unmanned air vehicle (UAV) intelligence mission products, NOAA and NASA weather images, SaaS end-user services and PaaS storage [1].

The ground infrastructure of satellite systems is uniquely vulnerable to cyber attacks both physically and remotely. With the commercialization of space infrastructure, companies may prioritise profit and invest less in security tools for command and control systems and related ground stations [16]. This may result in lower security levels in ground infrastructure.

Cyber attacks pose a specific threat to satellite systems, due to a dependence on timing and direct management of connected services. Satellites rely on synchronization with one another to function properly. Satellite constellations are perfectly timed, and if a satellite alters timing or positioning, the entire constellation may start to omit incorrect timing data. Satellites rely on synchronization with one another to function properly. If synchronization and orbit determination are interleaved in a strict sense due to relativistic corrections [7], a problem with one satellite's positioning could disrupt the entire constellation. The same applies to constellations for other services, such as satellite communications, and impact is worsened with low earth orbit satellites, which require a large number of satellites in order to function [5]. Timing data needs to be accurate so that if something goes wrong, satellite operators know exactly when it happened, and because many other industries rely on accurate timing too. The Global Positioning System is a global navigation satellite system (GNSS) which provides accurate timing for other constellations, as well as wider industries. Therefore, if attackers altered a satellite's positioning and impacted its timing, there would be wider implications. A satellite which is wrongly timed, resulting in a wrong position, also poses a physical threat of collision with other satellites in space and this physical risk is not replicated in other types of critical infrastructure.

In addition to the dependence on timing, wider satellite services are managed and operated from ground infrastructure with direct impact on end users, such as satellite broadband. If attackers access functionalities which control wider components, such as internet modems, they can make them malfunction and directly disrupt many peoples' lives. Satellite infrastructure directly creates timing services and is critically dependent on them, and directly manages wider services for users, making them more vulnerable to attacks with wide implications, compared to other types of critical infrastructure.

The novel contributions of this research are as follows:

- Further development of literature surrounding cyber attacks against satellite systems.
- Further exploration of ground infrastructure as an important attack vector within satellite systems with empirical evidence.
- Aiding in the development of defensive measures which protect satellite infrastructure from the ground.
- Providing initial input for national risk strategies regarding satellite security by demonstrating weak points within infrastructure.

Workshop on Security of Space and Satellite Systems (SpaceSec) 2024
1 March 2024, San Diego, CA, USA
ISBN 979-8-9894372-1-4
https://dx.doi.org/10.14722/spacesec.2024.23087
www.ndss-symposium.org

II. BACKGROUND AND RELATED WORK

A. Ground infrastructure vulnerabilities

Scholars have established that satellite systems are vulnerable to cyber attacks, due to the uplink and downlink of data, ground system software and hardware, and physical inaccessibility of satellites.

Some research looks at securing the uplink and downlink of data. Space operators work off console systems and ground terminals link satellite feeds with customer communication networks [3]. This research does not consider additional cyber security threats posed directly to ground infrastructure. In this paper, we explore how attackers access and launch attacks against ground systems, in order to recognise a wide range of threats.

Additional literature more broadly acknowledges the vulnerability of ground systems. The network vulnerabilities of ground stations are comparable to computers [5]. The situation is worsened for satellites because some constellations are more challenging to supervise, as they are constantly changing, for instance with the openness of LEO satellites' orbit [5]. In addition, many ground systems use widely available components, and attackers can more easily analyse vulnerabilities of these and also insert vulnerabilities like backdoors into software [5]. Ground terminals are also easily identified remotely [13]. Scholars have also recognised vulnerabilities within the hardware of ground infrastructure. Commercial off-the-shelf hardware is often coupled with bespoke systems, so that vulnerabilities may apply widely but applying patches is a bespoke process [13]. This is a more detailed analysis of ground infrastructure cyber vulnerabilities, and our research builds upon this by demonstrating how attackers exploit weaknesses.

Finally, it has also been recognised that if a problem occurs, it is virtually impossible to physically maintain satellites and other spacecraft [8]. This specific vulnerability of ground infrastructure, makes it harder to respond quickly to attacks which impact satellites and connected ground infrastructure. We build upon the research by systematically demonstrating additional ways in which ground infrastructure is vulnerable.

B. Ground infrastructure as an attack vector

Some research already documents how attackers exploit the weaknesses in ground infrastructure, by demonstrating attacker motivations and methods. Sophisticated attackers may target satellite systems due to their significance for other types of critical infrastructure [13], such as finance, transportation and communication. In particular, satellite communication is vital for both commercial and military systems [16]. This analysis indicates methods which may be used, as well as the perceived sophistication of attackers. However, this area of research is not specific to satellite ground infrastructure.

Academics also recognise that ground infrastructure is important for the functioning of satellite systems. Ground systems improve the performance parameters of satellite services, for instance positioning, and consequently infrastructure is often distributed globally [7]. This further demonstrates why attackers would disrupt satellites via the ground segment. We further demonstrate how attackers target ground systems, and also how they can reach satellites this way. Some scholars have already recognised tactics used to access ground infrastructure. They include information systems access control, injection and execution of malicious software and denial-of-service (DoS) [16]. Attackers can therefore utilise similar attack approaches as for other types of critical infrastructure. This is a helpful acknowledgement but research should also recognise the nuances of attacks against satellite ground infrastructure.

Some research looks further into these nuances, with exploration of theoretical attack scenarios, including how attackers can send false data to the server of a compromised ground node, and claim that it was downloaded from the spacecraft [20]. Another scholar outlines how backdoor trojans could allow attackers to gain full control of a satellite system network without a user realising, through a reverse connection to the attacker on the target machine [9]. NASA also outlines threats to ground systems, including a subversion of command authority, or impact to space missions by targeting key system dependencies, such as GNSS, ground stations or an external service [12]. We build upon these theoretical scenarios by conducting systematic analysis of empirical examples of attacks against ground systems, to identify the tactics used by attackers, at different attack stages. Existing research recognises some of these threats, but a more systematic review, with empirical evidence will help to further recognise how ground infrastructure can be targeted, and therefore should be protected.

C. Mitre ATT&CK

In order to systematically analyse attacks, we draw upon the Mitre ATT&CK framework. This established framework provides a layout of tools, techniques and procedures utilised by attackers to target enterprise, mobile devices and industrial control systems (ICS). We utilised Mitre ATT&CK for ICS, because satellite ground infrastructure shares characteristics with ICS, including operational technology. SPARTA is another attack framework which focuses closely on cyber attacks against the space and aerospace industry. We chose the Mitre framework as it focuses more broadly on cyber attacks and therefore facilitates extensive analysis of attack stages and techniques within them.

III. METHODS

The attacks analysed were found through an online open source search. We created a long list of cyber attacks against ground infrastructure of satellite systems between January 2018 and January 2024. Cases of spoofing and jamming were not considered as they typically take place within the user segment, and have smaller, more localised targets than attacks targeting ground infrastructure which operates and manages satellites and wider systems.

We chose attacks for analysis which were:

- Intended to be large scale.

- Conducted by a nation state.
- Sophisticated due to having the resources and capabilities of a state actor.

The attack cases were chosen from a longer list of attacks which only met some of the criteria. The attacks which were not analysed were; a ransomware attack on SpaceX-supplier Maximum Industries in March, 2023; attack on Dozer-Teleport, Russian satellite communications firm in June, 2023; attacker group SiegedSec attack on satellite receivers around July 2023; and an unauthorized access attack to a network server on Japan's space agency in November 2023. An overview of the chosen attacks follows.

In 2018 the Thrip Campaign was discovered targeting management and admin segments within ground infrastructure of two US-based satellite companies [4]. Attackers developed a custom backdoor, Hannotog [6] and then enumerated directories. They tried to install Infostealer.Catchamas on computers within the network of a satellite communications operator [17]. The attackers looked for and infected computers which were running software that monitors and controls satellites, as well as running MapXtreme GIS, Google Earth Server and Garmin imaging software.

In 2022 attackers targeted the Ka-Sat network of Viasat's satellite broadband [19]. They exploited a vulnerability to gain access to the initial network and then laterally moved through, to reach management and admin segments. They utilised access to send malicious commands to thousands of modems, in some cases irreversible. The Ukrainian military's ground communications were disrupted, alongside further disrupted infrastructure across Europe, including wind turbines in Germany.

In 2022, Fancy bear (APT28) was discovered to have persistent access into a satellite communications provider network with US critical infrastructure customers [18]. They exploited a vulnerability within an unpatched virtual private network in order to scrape credentials with active sessions [18]. Attackers accessed emergency accounts and could also access unencrypted SCADA traffic, including the state of industrial devices and commands [18].

In 2023 Volt Typhoon installed code onto telecommunication systems in Guam and across US [14]. They also attacked the emergency management services and geographic information system of a major US city and satellite service providers. Targeting these infrastructure providers would allow attackers to disrupt major portions of US electrical infrastructure.

In 2023 Peach Sandstorm was found to have targeted many companies within the satellite industry worldwide [2]. Attackers utilised password spray attacks to compromise an intermediate environment and attack downstream environments. Attackers also utilised AnyDesk to maintain access and conducted a golden SAML attack. They minted an SAML token in order to bypass AD FS authentication and access federated services. They also tunnelled traffic between actor-controlled systems and target systems. And finally FalseFont helped attackers to remotely access an infected system, launch files and send information to command and control servers.

A. Discussion

Mapping the attacks against Mitre ATT&CK for ICS revealed common attack types and vulnerabilities within satellite systems and the key findings are in Table I. Our analysis revealed similar vulnerabilities between satellite ground infrastructure and other types of ICS. For instance, attackers accessed networks and escalated their privileges in order to access sensitive data. This was helpful for demonstrating how defensive measures utilised to protect other critical infrastructure, could also help protect satellite ground systems.

Attackers also specifically targeted the operational side of satellite ground infrastructure, referring to an operation within systems and software. The nature of operation varied greatly, due to multiple functionalities within satellite ground systems, resulting in a variety of techniques and tools within this attack stage.

IV. Findings

Each attack was analysed in terms of the attack stages, in order to identify significant stages for ground infrastructure cyber attacks. Key findings from the Mitre ATT&CK mapping is in Table I. The most significant Mitre Attack steps were initial access, persistence, privilege escalation, lateral movement, discovery and collection. An additional step was added, labelled Satellite Operations Access. Attackers specifically targeted the operational side of satellite ground infrastructure.

We found that attackers targeted computers running software with operational elements, as well as control commands. Even though attackers mostly only observed operations in the attacks we analysed, they could potentially use this access and data collected to disrupt operations in future attacks. Attackers were likely not utilising their full capacity to conduct attacks, as nation state actors often have the resources and capabilities to more severely impact operations and create widespread disruption.

Despite sharing vulnerabilities, attacks against satellite systems have different manifestations and consequences. Satellite infrastructure has legacy systems, such as SCADA which were not designed with cyber security in mind. Access to associated data enables attackers to identify the state of operational devices and in particular those monitoring and controlling the movements and positions of satellites and connected infrastructure. Another vulnerability is complex supply chains, in terms of the software and hardware related to satellites and connected systems, influenced by the scale of satellite infrastructure. A variety of software contributes towards infrastructure of satellite systems, including GIS which integrates geographic based location into other applications. In addition, hardware and software is also closely connected within satellite systems, in terms of ground infrastructure monitoring satellites, and linked systems. Attackers used conventional attack methods such as password spraying to access systems and exploited vulnerabilities in a virtual private network initially to identify credentials for initial access. In one case, the credentials were the same for emergency accounts and the

	Key Insights
Initial Access	Methods such as spear phishing [15], password spraying [10] and scraping credentials [18] to access infrastructure without detection.
Persistence	Maintaining access into target networks, and both malware, Sednit [15] and Web Shell [14] and legitimate software, PsExec [17] were used.
Privilege Escalation	Gained privileged access within networks, commonly utilising privileged credentials to access networks [18] [11].
Lateral Movement	Laterally moving throughout networks and appearing legitimate, such as potentially accessing unencrypted SCADA data using "emergency" accounts [18], using a remote desktop protocol (RDP) [10] and also PsExec for admin access [17].
Discovery	Legitimate tools were further used, including PowerShell [17],ping commands [11]and other publicly available tools [10].
Collection	Collection or exfiltration of data, including security certificates [17] with AzureHound [10] and WinSCP [17].
Satellite Operations Access	Attackers targeted infrastructure related to operational sides of satellite ground infrastructure, including computers running MapXtreme GIS [17], industrial device statuses and control center commands [18] and AzureArc which can be used to operate infrastructure [10].

TABLE I
MITRE ATT&CK MAPPING

attacker could then reach a variety of systems due to having privileged access.

These factors are worsened by the nuances of satellite systems. The first is that satellites cannot be physically modified or monitored, compared to other ICS which is predominantly on or near the ground. This makes it hard to physically monitor satellites and quickly recover should hardware need replacing, so that monitoring and repairing needs to be done remotely. The same applies to physical infrastructure which is distributed on a wide scale to users. Following the ViaSat attack, thousands of replacement modems were sent out when they stopped working, as that large scale of infrastructure could not be fixed manually.

Satellite systems are also centrally managed, including constellations of multiple satellites and extensive ground infrastructure distributed to users globally. Management takes place in few locations considering their global nature, so that if attackers target ground infrastructure, they can have widespread implications. Attackers targeted management and admin segments of the KaSat network and sent commands to thousands of modems. Attackers also accessed monitoring infrastructure in other attacks. Other ICS are engineered to prevent national or international outages, making it harder for attackers to achieve the same level of widespread disruption as satellite systems.

Using Mitre ATT&CK for ICS to analyse cyber attacks chronologically revealed how satellite ground infrastructure is vulnerable to different attacks at different stages. For instance, attackers initially used techniques such as password spraying and spear phishing to steal credentials, in order to obtain network access. When attackers gained access to networks, they would conduct different attacks. This is helpful for demonstrating how satellite ground infrastructure is vulnerable in different ways and at different points. It is vital to protect satellite ground infrastructure, due to its role as a gateway for accessing other related systems, including satellites and other dependent components. Defending ground infrastructure provides additional barriers for attackers seeking to access other critical areas. Attackers are motivated to access operational aspects within satellite ground systems and also to remain on the network for a long period of time. These motivations may evolve over time, making sustained awareness of this threat vital.

Therefore, continuous monitoring of networks to ensure users are acting legitimately is vital, to detect attackers even when they are using legitimate credentials and software. This would help to achieve more secure satellite infrastructure. Increased security around operational functions such as additional authentication and higher standards for passwords, would also make these important areas harder to access. Analysis of attacks against satellite ground infrastructure should continue, in order to monitor their evolution and especially how they can be better defended against. Resilience can then be developed within satellite infrastructure, which is crucial because attackers may conduct more disruptive attacks in the future.

V. CONCLUSION

Ground infrastructure is expanding and continues to be vital for maintaining satellite operations. Attackers target satellite ground systems and are most interested in accessing and monitoring networks over a longer period. As a result of attacker focus on operational side of satellite ground services, we added an additional step to Mitre ATT&CK for ICS, Satellite Operations Access. This step encapsulates the focus on software and devices which contribute to operations. Attackers may target this area for data exfiltration, but also with more severe objectives.

This research has identified vulnerabilities within satellite ground infrastructure which attackers exploit. The findings could contribute towards national risk strategies, by highlighting where there are significant risks of intrusion and disruption. For instance recommendations could be made to monitor use of legitimate tools and also prevent sophisticated attackers from maintaining long-term access to networks.

Going forwards, there should be further systematic research which considers attacks and techniques used to target the ground infrastructure of satellite systems. Perhaps use of alternative attack frameworks, including SPARTA and Mitre ATT&CK for enterprise will highlight additional vulnerabilities. Considering the significance of nation state actors, it is important for this to be interdisciplinary research, in order to also consider the wider context surrounding attacks. It is out of the scope for this short paper, but analysis of wider context is vital for understanding attacker motivations, and resulting attacks. Further attack research contributes to maintaining high security standards within the satellite industry.

ACKNOWLEDGMENT

This work is funded by the Engineering and Physical Sciences Research Council through the EPSRC Centre for Doctoral Training in Trust, Identity, Privacy and Security at Scale (EP/S022465/1).

REFERENCES

[1] R. Anthony, J. Fritz, and D. Barnhart, "Cloud computing applications for large-scale satellite ground systems," in *2011 - MILCOM 2011 Military Communications Conference*. Baltimore, MD, USA: IEEE, Nov. 2011, pp. 1894–1898. [Online]. Available: http://ieeexplore.ieee.org/document/6127590/

[2] D. Antoniuk, "Iranian state hackers targeted satellite, defense organizations worldwide," *The Record*, 2023. [Online]. Available: https://therecord.media/iranian-hackers-target-satellite-defense-orgs

[3] S. Bichler, "Mitigating Cyber Security Risk in Satellite Ground Systems," *US Air Force*, pp. 1–33, 2015. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1012754.pdf

[4] C. Bing, "Chinese hacking group resurfaces, targets U.S. satellite companies and systems," *CyberScoop*, 2018. [Online]. Available: https://cyberscoop.com/symantec-thrip-satellite-hacking-trojans/

[5] H. Cao, L. Wu, Y. Chen, Y. Su, Z. Lei, and C. Zhao, "Analysis on the Security of Satellite Internet," in *Cyber Security*, W. Lu, Q. Wen, Y. Zhang, B. Lang, W. Wen, H. Yan, C. Li, L. Ding, R. Li, and Y. Zhou, Eds. Singapore: Springer Singapore, 2020, vol. 1299, pp. 193–205. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-33-4922-3_14

[6] D. Fratini, "Chinese APT "Thrip" Identified," *University of Hawai'i-West O'Ahu*, 2019. [Online]. Available: https://westoahu.hawaii.edu/cyber/uncategorized/chinese-apt-thrip-identified/

[7] C. Günther, "Kepler Satellite Navigation without Clocks and Ground Infrastructure," in *Insitute of Navigation*, Miami, Florida, Oct. 2018, pp. 849–856. [Online]. Available: https://www.ion.org/publications/abstract.cfm?articleID=15997

[8] C. J. Kotze, "Ground Systems to Connect Small-Satellite Constellations to Underserved Areas," in *Handbook of Small Satellites*, J. Pelton, Ed. Cham: Springer International Publishing, 2019, pp. 1–22. [Online]. Available: http://link.springer.com/10.1007/978-3-030-20707-6_31-1

[9] S. Lohani and R. Joshi, "Satellite Network Security," in *2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3)*. Lakshmangarh, India: IEEE, Feb. 2020, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/9117553/

[10] Microsoft Threat Intelligence (1), "Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets," *Microsoft*, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-\\collection-at-high-value-targets/

[11] Microsoft Threat Intelligence (2), "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," *Microsoft*, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land\\-techniques/

[12] NASA, "11.0 Ground Data Systems and Mission Operations within State-of-the-Art of Small Spacecraft Technology." *NASA*, 2023. [Online]. Available: https://www.nasa.gov/smallsat-institute/sst-soa/ground-data-systems-and-mission-operations/#11.4

[13] J. Pavur and I. Martinovic, "SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research," *arXiv.org*, 2020. [Online]. Available: https://www.semanticscholar.org/paper/SOK%3A-Building-a-Launchpad-for-Impactful-Satellite-Pavur-Martinovic/6c505622fc25708ffbd2157dc072987715b039d3

[14] D. Sanger, "Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target? The New York Times," *The New York Times*, 2023.

[15] E. Sayegh, "APT28 Aka Fancy Bear: A Familiar Foe By Many Names," *Forbes*, 2023.

[16] S. M. Shah, A. Nasir, H. Ahmed, and J. Shah, "A Survey Paper on Security Issues in Satellite Communication Network infrastructure," *International Journal of Engineering Research and General Science*, vol. 2, no. 6, 2014. [Online]. Available: https://www.researchgate.net/publication/316924176_A_Survey_Paper_on_Security_Issues_in_Satellite_Communication_Network_infrastructure

[17] Symantec, "Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies," *Symantec Corp*, 2018. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

[18] C. Vasquez, "CISA researchers: Russia's Fancy Bear infiltrated US satellite network," *Cyberscoop*, 2022. [Online]. Available: https://cyberscoop.com/apt28-fancy-bear-satellite/

[19] Viasat, "KA-SAT Network cyber attack overview," *Viasat*, 2022. [Online]. Available: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

[20] B. Zufelt, "CloudSat: IoT Approach to Small Satellite Ground Infrastructure," 2018. [Online]. Available: https://digitalrepository.unm.edu/cgi/viewcontent.cgi?article=1458&context=ece_etds