Constellations Podcast

Special Release – Threat Tracking, Information Sharing & the Watch Center

Speakers: Joel Francis, Watch Center Lead and Kevin Coggins, Senior Advisor, Space ISAC – 24 minutes

John Gilroy: Welcome to Constellations, the podcast from Kratos. My name is John Gilroy, and I will be your moderator. Today, we will be talking about Watch Center at the Space Information Sharing and Analysis Center, or Space ISAC. The Space ISAC serves to facilitate collaboration across the global space industry and to help respond to threats that could come from anywhere, such as cyber. They've even built their own Watch Center. I can't wait to dive into that. We have two guests today, Joel Francis is the Watch Center Lead at Space ISAC, and Kevin Coggins is a Senior Advisor to Space ISAC. Well, we're going to jump right in here. Joel, satellite ground stations are vulnerable to cyber and malware attacks as evidenced by a 2022 attack on ground station modems that crippled internet communications throughout Ukraine and much of Europe. Can you describe this attack that happened against mostly Ukrainian satellite modems?

Joel Francis: Sure thing, John. We know through extensive reporting from both the affected company and some other sources, including other threat researchers, that this was largely a denial of service attack, targeting those Ukraine based modems. The goal here was to cause disruption to the broadband services that were being provided. So when looking at the attack kill chain, we see that the attackers exploited a VPN connection to gain that initial access, which from what we've seen in the Watch Center is a very common technique that's used for accessing victim networks. Once they're able to gain that unauthorized access, they're able to exploit legitimate network pathways and move laterally to a specific segment of the network that had management privileges. This allowed them to stage a toolkit that scanned the network for connections and vulnerabilities which ultimately allowed them to execute malicious commands that wiped the flash memory of these modems. So what does this all mean? Well, this means that they utilized a wiper malware attack to disrupt these modems and as more and more information has come out, it's been clear that this was a very sophisticated and coordinated attack, meaning that attacker had to have extensive knowledge of the satellite networks.

John Gilroy: From a cybersecurity perspective, it's almost textbook. Compromise credentials, land and expand, escalation. Yeah, it's good, but it's done with a lot of finesse. It's an interesting sample to start off with here.

John Gilroy: Let's dive a little bit deeper into this, Joel, if we can. ISAC, we mentioned earlier, the Space Information Sharing and Analysis Center is one of more than two

dozen organizations tracking vulnerabilities and threats to U.S. critical infrastructure. Is the attack on Ukrainian ground station modems a type of attack or activity the Space ISAC would like to monitor and assess?

Joel Francis: Yeah, absolutely. This is really the exact kind of activity we're looking to watch for in the Watch Center. We're looking to monitor, analyze, and report this type of information for our members. We know that attacks like the one that we're talking about here that target the ground stations, that look at the ground segment and different enterprise networks, are the most likely to be targeted. We're coming up with this assumption based on the tactics and techniques that we've observed from the threat activity. In this specific example, we received a lot of early warnings from some of our government partners about increased cyber activity in Ukraine and for the first time actually mentioning that satellite architectures and satellite systems may be in jeopardy. So part of what we do at the Space ISAC is we're able to share that information with our members. We're also able to get more insights from our members as well. I want to emphasize too that it's not just the ground segment that we're looking at. When we look at the space attack surface, it's everything on the ground and more. We're also looking at different on-orbit effects, because there's a lot of different attack vectors when you're looking at potentially disrupting a satellite system.

John Gilroy: Wow. Kevin Coggins, we've got you to chip in here for us. When I read about the Space ISAC, it looks like it relies heavily on correlated and fused data driven by its own Watch Center. So Kevin, what kind of data is captured by the Watch Center, and how do you acquire it?

Kevin Coggins: All kinds of data. Our data comes from four main sources: commercial, government, open source, and most importantly from our members. So the Space ISAC has many members across the commercial space community and they have satellites deployed around the world, ground stations deployed around the world, user terminals around the world. Everywhere they have a capability or a network, we have the ability to pull in data. So we can get an amazing data set that gives us information from all over the world where space infrastructure is. We get it from our members through individual submissions to real-time data feeds. I tell you, the Space ISAC truly is a unique capability that can monitor a large space enterprise in real time.

John Gilroy: Joel, when Kevin just used the word open source, some people may jump up and down and worry or be concerned a little bit. So we know some of this data is from open source. So Joel, are you looking to capture any other types of data? I mean structured, unstructured, sensor information, or everything? I think that might enable the future version of the Watch to take advantage of other types of data, wouldn't it?

Joel Francis: Yeah, absolutely. To answer your question there, especially in the earlier phases of the Watch Center, we're really focused on gathering as much data as possible

so that is where some of the open source piece comes in. A lot of the information that we share has either been identified or confirmed through open source means, and a lot of the times the open source perspective will either give us a tip on a potential incident that we want to look into. Typically, we'll ask questions to our members or go through other reports we may have received to try to correlate that and provide a little bit higher confidence. But in terms of providing the eyes and giving us more things to see within the Watch Center, that open source element is very important.

John Gilroy: Well, Joel, you don't look like a boxer. But in boxing they have this thing called stick and move, stick and move. So let's talk about and apply this to the Watch Center. Does the Watch Center have a way to correlate data sets together? Is it possible to track adversaries as they move from one domain to another? For instance, across ground and space they stick and move, huh? Stick and jab.

Joel Francis: Yeah, exactly. This really falls in line with the mission and vision of the Space ISAC and our Watch Center. We want to be able to correlate what we're seeing in space to what we're seeing on the ground and vice versa. One specific example could be, let's say we're tracking a high volume of cyber activity in a particular geographical area. There are some open source feeds that we use for this, there are some other data feeds that we use to show ASN outages and just in general network activity around the globe. So let's say we see a particular conflict zone, and that may correlate with a particular satellite who's experiencing interference rather and whose beam spots fall within that same area. That's one example of how we're able to potentially correlate that data, and maybe potentially there is a multi-pronged attack in there.

That's one way and a lot of it is blending reports together and synthesizing information. But another more specific thing I want to call out is the MITRE ATT&CK Framework and now the SPARTA, the Aerospace SPARTA framework, which help us to look at a behavioral element to attacks. And so when we're looking at satellite data on orbit data maneuvers versus IP addresses, network traffic, it's really hard to blend those two together. But when you look at it from that behavioral element, then you create a common denominator. And that's how we're able to fuse that.

John Gilroy: I'm always amazed how MITRE came up with the spelling of ATT&CK, but that's a different podcast altogether. Simon Sinek, he says, "Start with why." I'm not going to start with why. I'm going to start with how. So Joel, here's the how question for you. Give us listeners, a deep dive into how the Watch Center works. So what types of threats are you seeing today or now?

Joel Francis: Yeah, so I guess a little bit more into how it works, giving a deep dive into how the Watch Center operates. On a day-to-day basis, we are monitoring feeds, we are cataloging information, and at the same time we're building out reports. So we send out daily, weekly, and monthly reports to our members. We also may

send out specific reports based on incidents. So we've developed playbooks on how to investigate these incidents, how to report that information out, and that also includes a process for how we sanitize information we may receive from our members to protect their anonymity and build that trust. In terms of what specific threats we're seeing right now, we are seeing a lot of ransomware activity. Specifically as we mentioned before, we're seeing a lot of external applications and software packages being targeted, and we're also seeing a lot of RF interference. The big piece with that is correlating to if it's intentional or unintentional, and that's another task that may fall within the line of our Watch Center analysts.

John Gilroy: Kevin Coggins, you are a senior advisor, so you have a catbird seat. You can see things from many different angles. So what's new at the Watch Center? Are peer adversaries and other nation states becoming more active, or do you see the goals of the Watch Center changing here?

Kevin Coggins: I don't see the goals changing at all. And yeah, adversaries are becoming more active. And we're also integrating capabilities that allow us to see where they're already active. So I mean, you've heard about cyber being a part of the attack surface. Joel just mentioned RF threats, but there's also orbital debris and satellites maneuvering around. And so we're paying attention to what's happening in space physically, where are the satellites supposed to be versus where they are. And there's all kinds of capabilities we're integrating to watch. Many satellites and users use GPS, for example, or some form of global navigation satellite system. So we're monitoring for interference and strange behaviors in that. While the attack surface for space continues to change and will continue to change, and threat actors will continue to adapt, I don't think the goal is going to change at all. The goal of the Center is to monitor for all the threats and all the hazards to space systems. However, we do have a list of priority intelligence requirements that help us identify emerging threats and focus on what's most important to the resilience of our community. And so we really pay attention to, for our members, what capabilities do they have and they're trying to provide. What are the top threats that matter to them? And so we review these at a minimum of once a year to facilitate this kind of activity.

John Gilroy: Kevin, you used the phrase that pays, attack surface. Let's maybe dive into that a little bit here. Satellite systems attack surfaces are complex with the satellites themselves only being a small part. Today's satellites feature more sensors. And the attack surface, ground stations, their uplinks, satellite downlinks and crosslinks are all vulnerable. Every component can be a sensor, and no single sensor knows everything. So Kevin, how does the Watch Center anticipate and keep pace with this threat?

Kevin Coggins: You just hit the main reason why the Watch Center exists, to anticipate and keep pace with this threat. The main method we use to keep up with the growing attack surface is characterizing the threat environment and identifying

use cases to deploy to the Watch Center. And so one of the threats is space weather. We've seen that affect satellite constellations. We have use cases to monitor space weather and look at how they might impact some of our commercial space systems. We have use cases for detecting GNSS interference. We have use cases for watching the orbits of satellites to make sure everyone's where they're supposed to be. And so we work with our members, and we define and refine these use cases and employ them in the Watch Center. And so that allows us to have use cases that are tailored to the priorities that we're trying to monitor.

John Gilroy: Joel, I think most people realize that the number of space systems is increasing. I think everyone knows that. Every Joe Six-Pack knows that. As the number of space systems increase here, supply chain information becomes important to sustain the production of nationally important space-based missions and services. It is a serious security issue. So Joel, can the Space ISAC help with the fidelity of this supply chain?

Joel Francis: Yeah, absolutely. Supply chain is one of the highest threats in terms of priority that we're looking at. We do have a supply chain working group that comes together to help gain visibility on the supply chain. And that's really at the core of the issue is gaining visibility on what are the dependencies in the supply chain, what are the vulnerabilities. The whole space timeline, or life cycle rather, has so many different players, suppliers, downstream providers, and stakeholders. There's a lot of different nodes that if you're an attacker, you could look to exploit. And this is especially true when we're looking at a lot of these space companies that have very mature cyber capabilities. But some of their vendors, some of those supply chain pieces, they may not be up to par for lack of a better term.

And so what we do is we look to identify components from an actual technology basis. We look to get insights from our members on what's most vulnerable and important. We look to track, in some cases, specific vendors if vulnerabilities come out targeting vendors that we know that this particular component or this particular piece of technology is widely used in the space domain. That helps us to prioritize what we're looking at. And a couple of specific examples is some of those data sets and other sources that we use in the Watch Center. Among those are the NIST Vulnerability Database, or the NVD, or DHS CISA's Known Exploited Vulnerabilities catalog, or the KEV. And so we look to keep up to date on what vulnerabilities are announced. But there are potentially around a hundred each week that come out. And so that prioritization piece is huge.

John Gilroy: Kevin, I got a senior advisor-type global question for you here. How do the Space ISAC initiatives support a national or international cyber strategy? Does it collaborate with the US government, and what about our international allies?

Kevin Coggins: Yeah, great question. The key to a national or international cyber strategy--one is cyber awareness, and one of the things that Space ISAC has really pushed across the community is cyber awareness. And that helps greatly align the community to the government initiatives. But we collaborate with government via information sharing and collaborative sessions. We have many collaborative groups that focus on implementing standards and best practices including CMMC and Space Policy Directive-5. We also work with DHS CISA in their Space Systems Critical Infrastructure Working Group. And one of the advantages of being in ISAC is our ability to collaborate with international business and governments as well. A success story in collaborating with the government is about a year or so ago, working with many government agencies, they invited the space ISAC in, CEOs of the companies that are part of the ISAC, gave them one-day security clearances and shared with them threat information that's not publicly available so that they could go back to their businesses and their enterprise and make informed decisions. That level of collaboration is incredible and has been a great help to our members in seeing that the government is on their side to solve some of these problems.

John Gilroy: Joel, we're going to walk down the hall to the lab here, the Vulnerability Lab. Vulnerability labs are basically research and development efforts that discover critical vulnerabilities in software and hardware products. You mentioned that just recently. Tell me about Watch Center's Cyber Vulnerabilities Lab. And what's the goal? Is it important that industry participate?

Joel Francis: Yeah, absolutely. The Cyber Vulnerability Lab or the CVL is really the counterpart to the Watch Center. It's that hands-on piece that helps to enable some of that real-time identification and also identifying of vulnerabilities. So that Cyber Vulnerability Lab is really intended to bring together government, academia, and industry to create a unique environment for hardware and software testing. The lab is actually managed by our members via our Cyber Vulnerability Lab Committee. And participation in the lab is included as a benefit to the Space ISAC members. We're currently running a pilot phase through the end of 2024. The idea is that members will be able to identify vulnerabilities exploited in the wild and potentially share the findings with our community. We think this is a really great benefit as well as it's one of the only commercial testing environments like this for the space community.

John Gilroy: Kevin, let's get down to business. Let's talk about the business of space. And it seems to be key to understanding its vulnerabilities. The commercialization of space means that its missions are growing far beyond NOAA weather reports, GPS, or even communications. Satellites are now also used for precision agriculture, maritime operations, supply chain tracking, and even emergency management. So how does the Space ISAC facilitate exchanging knowledge so that stakeholders can provide and benefit from the Watch Center?

Kevin Coggins: Yeah, that's also a great question. We know that adversary nations view commercial satellites as legitimate target for wartime operations, for just causing disruption even in commercial enterprises, regardless of the mission class that they fall under. So as these satellites and space systems take on more missions, it's more targets for the adversary. And the increased use of space capabilities, as you indicated, affects the space attack surface in two ways. Adversaries may look to target space systems as a way to disrupt supported critical infrastructure. There may be potential access vectors that attackers may look to exploit when targeting a space system that allow them to get into a system of interest. Those are two of the top ways, but this idea of access and disruption is key to what the adversary is trying to do. And because these space systems are connected in some cases through channels they can easily access, in some cases just sending signals up toward the satellite, it can be very accessible for the adversary.

So how does the Space ISAC facilitate exchanging knowledge so that people can provide and benefit from the Watch Center? Joel talked earlier about some of our daily and weekly activities and the information we push out to our members, but I tell you, it's through these use cases that our members inform, so that their interests are represented in what we're analyzing and what we're monitoring and how we're reporting data back. And they could get the data back in real time from the Watch Center through the methods we have for them to connect to it or through standard reporting that we do.

Joel Francis: And Kevin, I wanted to add on to that too. We, as an ISAC, are part of the National Council of ISACs. And so we have touch points to all of these other sector specific organizations. And for us, that really helps us to touch on some of the stakeholders in a lot of these interdependent architectures. We can talk to the Aviation ISAC, the Comms ISAC, even the Healthcare ISAC, if there's any overlap there. And we're all able to do that with some of the use of our tools. We use a member portal, and we also have an automated information sharing piece as well.

John Gilroy: Kevin Coggins, not your first day at the rodeo here. You've seen a lot of things over the years. Quite an impressive background I see on LinkedIn here. So if you put these things in perspective, what kind of cyber-attack events do you see being possible that have not happened yet?

Kevin Coggins: That's a great question. In cyber, you hear about a man-in-the-middle attack. And just on an IT computer network, that's pretty physically not impossible to do. It's just data. But when you have a satellite orbiting so high, what's a man-in-the-middle attack look like? It could be that you're on the ground receiving information, and you do a replay attack to impact the people that the satellite's trying to talk to. It could be you do a replay attack from the ground station and try to infiltrate the satellite. I think we're going to see more and more of these types of attacks where people are generating RF signals with cyber information

embedded to impact users or space systems. And then I think the big one that's coming, given the ability to launch satellites into orbit, CubeSats, and really inexpensive things in low earth orbit, you're going to start seeing attack vectors happen in space to other space systems. Either through things a small SAT can do to put RF on a satellite, to just bring the noise level up to some sophisticated cyber-attacks. Because I designed my space system to worry about satellites sitting next to me trying to do things to me. I worried about somebody trying to do it from the ground. And so when the paradigm changes, you can't update these space vehicles fast enough sometimes. We're going to see some new things.

John Gilroy: Oh, this has been a fascinating discussion. Kevin and Joel, I think what you've given our listeners is a better understanding of risk management as it applies to the world of satellites and space. I'd like to thank our guests, Joel Francis, Watch Center lead at Space ISAC, and Kevin Coggins, Senior Advisor to Space ISAC. Thank you, gentlemen.

Joel Francis: Thank you for having me, John. We appreciate it.

Kevin Coggins: Thank you so much.