Honeypotting for National Security

How a fake critical infrastructure network shed light on real live cyberthreats.

Amanda Ziadeh
Thu, 08/23/2018 - 13:20

Illustration: fstop123/iStock

In July, cybercriminals broke into a network belonging to what they thought was a powerful electricity provider’s infrastructure, through backdoors installed by a black market seller. These hackers snaked through the IT environment, looking for a path to the operating systems delivering power, natural gas and water.
But what could have ended with a blacked-out power grid instead left the hackers empty handed. That’s because the system they breached was being watched by Ross Rustici, Israel Barak and their team at Cybereason, a cybersecurity software provider, who were surveying the hackers as they were leaving behind a trail of digital breadcrumbs.

The team had set up a honeypot that masqueraded as a major electricity provider to observe tactics, techniques and procedures of hackers targeting critical infrastructure, and to find the threat industrial control systems actually face.

“You see a lot of governments . . . talking about nation-state-level actors going after industrial control systems,” said Rustici, Cybereason’s senior director of intelligence services and former technical lead at the Defense Department. “It’s always focused on big, bad governments across the world, and we had a sneaking suspicion that while that is an important part of the threat to pay attention to, that isn’t the only part.”

The network was set up to look like a power transmission substation using doppelganger naming conventions to appear like a very large East Coast electricity provider. It had a large IT network, smaller operational technology network, and layered defenses to make it seem as real as possible. The only difference was the remote desktop protocol was weak — usernames and passwords were as easy as “useruser.”

The Cybereason team members didn’t care how the hackers got in; they wanted to know what the hackers did once they understood what network they were in and how they operated in it, Rustici said.

Within two days of exposing the network to the internet, Rustici saw a lot of generic cyberactivity — people trying to run botnets for cryptomining and spamming, for instance.

“But one piece of activity stood out, and that was somebody who was running a playbook for prepping an environment for sale on the dark market,” Rustici said, because the hacker installed a toolset commonly found in assets sold on the black market.

Once in the network, these hackers changed passwords, created new usernames
and passwords for remote desktop services, installing a patch that would allow for multiple people to be logged into the service at the same time without kicking each other off. Now, other hackers could operate on it without detection.

And then, that environment went quiet.

Days after, Rustici saw a completely new group access the network through one of the usernames created by the first hacker, and it set out for the OT environment.

“The first actor had unveiled some stuff to clarify that it was an ISC-connected network, and this group was focused on that like a laser,” Rustici said.

The group began laterally moving in a way that allowed it to triangulate where the relays between the IT and OT networks were, systematically moving from one machine to the next, trying to get to those gateway boxes.

And what was even more intriguing, Rustici said, was that these hackers operated without using any malware, employing only inherent system capabilities built into modern operating systems. Their footprint was incredibly small. Hadn’t someone like Rustici and his team watched this network, this activity could have been missed.

**So What is the Threat?**

There were many factors that led Rustici and his team to think this was a sub-nation-state-level actor, falling more into the category of cybercrime. These hackers were very quick and knew what they were doing — they even had a playbook and went after the OT network.

But they made some “really stupid mistakes,” Rustici said.

For example, the hackers immediately tried to uninstall all the security products when they accessed the network. This activity raises a red flag because anyone monitoring the environment will notice when a sensor goes offline.

“If a box goes dark, that’s a big problem from a security perspective,” Rustici said.

So, it was probably mid-tier cybercrime: The hackers know what they’re doing and they have an objective, but they don’t have the technical sophistication to feed false information into logging systems and fool security products, or bypass them on a technical level. That’s why the hackers reverted to uninstalling sensors and
security and tried to move faster than the security operations center response team.

“They were trading noisiness for opportunity,” and that's something nation-state actors typically don't do, Rustici said.

**What Does this Mean?**

“You’re not just dealing with the nation-state actors, you’re not just dealing with the top tier, and you need to defend the lower half as well,” Rustici said. The nation-state threat is there, it’s important and the tools the hackers use are far more advanced than what most SOCs are used to. But they’re also not necessarily the most pressing threats, he added.

Because the goal of nation-state actors, outside of some very select regions and targets, is to build capabilities within an infiltrated network and quietly lay down tools for future use, they’re trained on ISC systems and advanced enough to try find the vulnerabilities that allow them access so they can stay for years. They’re very careful and cautious.

These cybercriminals, on the other hand, were not vigilant or concerned about being quiet.

“As the industrial control systems are out there connected to the web, and as you’re dealing with critical infrastructure providers, the big takeaway is: Your threat is not just the cautious, careful, really sophisticated, and you need to be paying attention to the cybercrime element as well,” Rustici said.

The hackers' motivation was hard for Cybereason to determine, because the attackers never reached the OT system. But based on the speed at which they operated and their tech-savvy, Rustici’s guessed they were either looking to take a trophy and prove they could operate against these types of systems so they could get work in the future, or demand a ransom.

“Those are the types of threats that I think need to be highlighted more for the critical infrastructure sector,” Rustici said. “You’re not just dealing with nation-states; you’re dealing with people who have a clear profit motivation.” And if attackers get in, you either lose access, rebuild it, or you pay the ransom.

And refocusing on that level of actor and those motivations gives critical
infrastructure providers a threat they can deal with, Rustici said. A well-equipped SOC will catch them and boot them off the network before they do damage, so when it comes to cybercrime, it’s a fight the defenders can actually win.

But with nation-states, “it’s easier to throw up your hands and say, ‘well, it’s the Russian military, how can I be expected to defend against those guys?’” Rustici said.

**Educating the Masses**

Spinning up a honeypot is expensive, so Cybereason is talking with the right industries and with the government about the evolution and different types of the threat, how hackers are operating and if current recommendations will remediate that activity.

“Because on one hand, if you focus solely on the nation-state actors, and you build a good defense against them, you’ll clear out pretty much everybody else who goes against that network,” Rustici said. He said he feels the overall trend when receiving [Homeland Security Department](https://www.dhs.gov) bulletins is to go talk with those who control the infrastructure.

“It’s a really good conversation, and then nothing really changes because it costs too much, it’s too hard, they have other priorities regarding reliability on the grid,” Rustici said. “Everybody agrees this is a problem that needs to be addressed, and there’s no movement.”

So, Rustici is hoping with this type of research, agencies won’t have to tackle the entire mountain in one day, “even if you get a mile up it, you’re going to be demonstrably more secure,” he said.