Critical Infrastructure Remains the Brass Ring for Cyber Attackers in 2024

oodaloop.com/archive/2024/01/02/critical-infrastructure-remains-the-brass-ring-for-cyber-attackers-in-2024/

Emilio Iasiello

Recent reporting reveals that both state and non state cyber actors are actively targeting critical infrastructures with impunity. Indeed, the Ukraine war, Palestine conflict, and other areas where geopolitical tension exists has created an environment where aggressive offensive cyber operations are unfolding and are even encouraged. What has become increasingly clear is that there seems to be very little that the global community is doing to deter these types of attacks, which have ranged from gaining access to more disruptive strikes designed to hamper operations, or the actors conducting them. This is disconcerting given how the volume of attacks against these targets has surged. According to one cybersecurity company's findings, in 2022 cyber attacks against critical infrastructures spiked 140% from the previous year. While many of these attacks can be linked to cybercriminals such as ransomware operators seeking to collect significant ransom payments for compromising vital networks, as many as 60% of attacks against infrastructures have been linked to nation states indicating that the potential intent behind them are for more nefarious purposes.

As we head toward the conclusion of 2023, the news has been rife with examples of such malfeasance, and from a variety of threat actors, which underscores that critical infrastructures are and will remain high-value targets for both state and nonstate groups. A quick review of media found four examples illustrating what the cyber environment looks like and what we can expect to transpire moving into 2024:

> **Oil/Gas**. Israeli hackers dubbed "The Predatory Sparrow" claimed responsibility for conducting a series of cyber attacks that created disruptions at 70% of Iran's gas stations and traffic light systems. Per reporting, the group provided visual evidence with screenshots taken of gas stations' computer systems, as well as payment information and management system data. The group asserted that the attack was retaliation for Iranian aggression in the region. The recent attack wasn't the first time this group conducted cyber attacks against Iran, having executed at least two of them previously that had disrupted Iran's rail networks and steel factories.

Telecommunications. Russian hacker group “Solntsepek” (a group tied to Russia’s military intelligence-linked Sandworm Team) claimed responsibility for a cyber attack against Ukraine’s largest telecommunications provider. The attack didn’t compromise customer data but did impact operations for at least a day causing outages and disrupting air raid sirens, some banks, ATMs, and point-of-sale terminals, making it one of the most impactful cyber attacks of the Ukraine war. It also had a causal effect by creating service surges for competitors not ready to accept an increase in user traffic. The ties to Sandstorm Team is noteworthy as that group has been very active against critical infrastructure targets such as Ukraine’s electrical grid in 2016 and 2017.

Hospitals/Medical. Israel’s National Cyber Directorate (NCD) attributed November 2023 cyber attacks against Safed Ziv Medical Center to the hacker group known as AGRIUS, and which is linked to the Iranian Intelligence Ministry. The NCD indicated that AGRIUS also had assistance from Lebanese Cedar, a group linked to Hezbollah. Though the attack was only partially successful, its intent appears to have been to disrupt hospital operations, which could create an impact in treating Israeli defense forces as it engages its conflict with HAMAS. More importantly, the attack shows how cyber attacks can play a role in supporting ground activities by achieving tactical objectives.

Water Facilities. Iranian cyber actors recently attacked a small Pennsylvania water authority, as well as other victims across the United States. But Iran is not alone. A recent news report revealed that hackers linked to China’s military had been gaining access into computer systems or more than 24 U.S. critical infrastructure organizations to include water utilities, a port, and at least one oil and gas pipeline. The article suggested that these intrusions were part of a plan to sow panic and hamper logistics in the event conflict should erupt between China and the United States over an issue like Taiwan. While it did not appear that these intrusions had made their way into accessing industrial control systems that operate critical functions, accesses gained could impact targets enough to disrupt services. Given that one of the targets supported U.S. Pacific Fleet in Hawaii, the attack provides another example of how cyber attacks could pre-position an adversary to affect ground operations in the event of a conflict.

Though there are no codified norms of state behavior in cyberspace, the targeting of critical infrastructures has always been considered taboo, largely because any such attack would directly impact services to civilians. Since the North Atlantic Treaty Organization (NATO) agreed that a cyber attack against a member state could trigger Article 5, it would appear that this would underscore the gravity with which any such attack could be viewed, interpreted, and be subject to retaliation. Indeed, in 2019, an article by NATO Secretary General Jens Stoltenberg asserted that NATO would guard its cyber domain and invoke collective defense if deemed necessary. Although criteria by which a serious cyber attack was never defined, given what has transpired in the realm of disruptive and destructive cyber attacks, one potentially severely impacting critical infrastructure certainly seems that it would fit the criteria.

Yet, despite this acknowledgement, nation states continue to test the boundaries and push the limits about the types of attacks they conduct against critical infrastructures raising the question if there is any real red line that will determine when action would be taken. Perhaps more worrisome is that continued failure to set any such conditions on nations states has freed up nonstate actors to target these vital networks for their own purposes, whether as a means of financial extortion or to support a benefacting state’s interests. Since the potential detrimental impact against critical infrastructures is not the sole purview of state actors, the Red Cross put forth ethical guidelines for hacktivists to consider before wading into cyber conflicts, though the effort has been a more symbolic gesture than one that has achieved any tangible results.

So where does this put us in 2024? Not in a favorable position. What’s evident is that there has been no threat of punishment, and certainly no repercussion, that has successfully discouraged threat actors from continuing to target critical infrastructures. Even when the attacks have been potentially detrimental, like the Iranian one that raised chlorinelevels in Israeli water facilities that could have had consequential effects on civilians, or the recent attack against the Israeli hospital disrupting potentially life-saving measures, there has been little effort by the international community to collaborate on going after these actors and/or punishing the states on whose behalf they may be acting.

Worse, heading into 2024 there is little evidence that the global community is trying to develop a strategy to deter such activity from happening in the first place. Therefore, it appears that states will be left up to their own judgement as to how they will respond to such activities, which risks quick escalation and entry for other actors – whether offensively or defensively – to join the fray.

Absent codified cyber norms and/or treaties, this does not improve cyber defense as much as exacerbate an already tense situation.

Continue the conversation on the OODA Network Slack channel. | Not a member? Join today!