ELECTRUM Targeted Ukrainian Electric Entity Using Custom Tools and CaddyWiper Malware, October 2022

⋮ 12/11/2023

12.11.23 | 3 min read

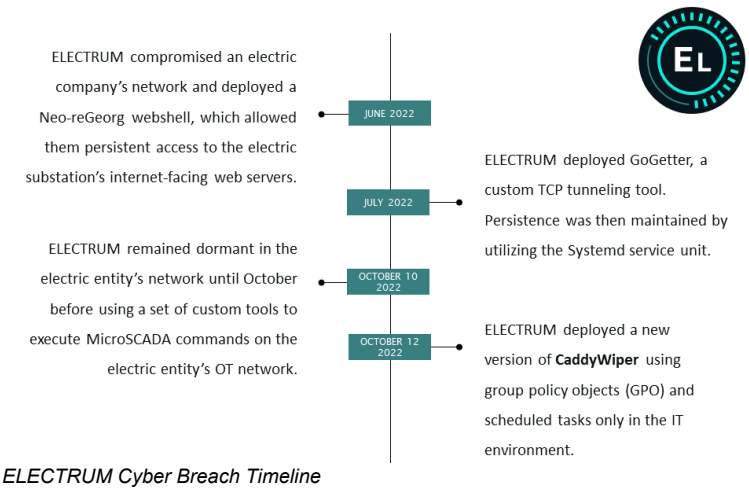
Dragos, Inc.

On November 9, 2023, Mandiant released new details from forensic investigations following a disruptive attack against Ukraine electric substation which started in June 2022 and culminated in two events on October 10 and 12, 2022. Dragos associates this activity with the ELECTRUM threat group (has technical overlaps with SANDWORM Advanced Persistent Threat (APT)). ELECTRUM is responsible for several cyber attacks on Ukrainian electric utilities and a 2016 power outage that resulted in the disruption of power to ¼ million homes, and this newly disclosed attack shares similarities with previous attacks.

Understanding the tactics and tools employed by ELECTRUM from an intelligence perspective and the ability to hunt and monitor for their known behaviors and indicators in OT environments should be prioritized for ICS assets located in Ukraine, and where the European electric industry is concerned.

ELECTRUM Cyber Breach Timeline

In June of 2022, ELECTRUM gained access to a hypervisor running an end-of-life (EOL) version of MicroSCADA software in the electric substation's OT environment. ELECTRUM then attempted to execute a set of custom living off the land (LOTL) scripts to impact the availability and control of the substation. ELECTRUM also utilized a new version of CaddyWiper to remove their operational footprint from the electric substation's compromised IT systems. These actions by ELECTRUM satisfy Stage 1 and Stage 2 of the ICS Cyber Kill Chain.



ELECTRUM Cyber Breach Timeline

At that same time in October, Russia attacked Ukraine with massive missile strikes targeting key energy infrastructure, damaging 30 percent of the energy infrastructure in Ukraine with power supply interruptions in many locations.

Currently, Dragos is unsure of exactly what ELECTRUM's dormancy suggests other than potential system reconnaissance and collections activities. Dragos cannot confirm whether this attack was successful in interrupting the substation and thus impacting power in Ukraine. The initial compromise vector for the June-October events has not been identified.

ELECTRUM Attacks on the Ukraine Electric Sector

The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) reported that Ukraine's Computer Emergency Response Team (CERT-UA) recorded 2,100 cyber incidents in 2022. While only a subset of incidents is associated with ELECTRUM, the energy sector was a particular focus in the region and ELECTRUM has been responsible for several major attacks on the electric sector going back to 2015.

In April 2022, the security firm ESET identified multiple malware capabilities at a Ukrainian utility provider. During the incident, ELECTRUM remained dormant on the electric entity's network for at least one month before the attack was to occur. This is a consistent pattern for ELECTRUM: gain access to a network, remain dormant, potentially collect system details, and then build custom scripts and tools prior to executing a destructive cyber attack. This attack used a new version of CaddyWiper, other custom wipers, and Industroyer2 (a scaled-back version of CRASHOVERRIDE). This marked the third time ELECTRUM had attacked a Ukrainian utility provider.

Given ELECTRUM's destructive history, ELECTRUM's likely objectives were to execute the commands against the MicroSCADA utility to impact the availability and control of the electric substation. It is interesting that MicroSCADA software, designed for legitimate purposes in operational technology environments, was used during this incident. While the effect of use remains unclear, this tactic is noteworthy and should be used to update and inform threat models for future cyber attacks.

MicroSCADA has been deployed in more than 10,000 substations and monitors the electric supply for more than 10 percent of the world's population. In addition, the compromised version of MicroSCADA was considered end-of-life (EOL), which means that it was software that the manufacturer or vendor no longer supported. Similarly, the creation of the PIPEDREAM ICS-specific malware involved the implementation and use of known industrial protocols OPC-UA and Modbus. This reinforces the importance of considering the role of native software and capabilities in OT-focused cyber attacks.

Recommendations

Dragos recommends referencing the five critical controls for OT cybersecurity identified by the SANS Institute for a framework for defending against adversary activity directed against ICS/OT system environments.

Among the critical controls is ensuring OT network monitoring. In addition to scanning for known indicators of compromise (IOCs), Dragos also recommends monitoring in the form of proactive threat hunting to identify potentially malicious tactics, techniques, and procedures (TTPs) in the environment. If an adversary somehow gains access to a network, threat hunting serves as an essential last line of defense to find and stop a breach before significant impacts occur, like execution of a wiper or causing physical effects in a process control environment.

As noted above, ELECTRUM attacks against electric utilities have typically involved long dwell times between initial access and finally turning out the lights. In the latest attack reported by Mandiant, threat hunting for the following types of suspicious behaviors in the OT network during that dwell time could have helped uncover the adversary before they achieved their objectives:

- Unexpected file transfers from the enterprise network (or an external sever) into to the OT/ICS network, specifically, the transfer of an .iso file to a "Crown Jewel" SCADA system
- Transfer and execution of unexpected scripts like PowerShell (.ps1), Visual Basic (.vbs), and Batch (.bat) files on a SCADA server
- Unexpected commands issued from SCADA servers to RTUs

These are just a few examples of the wide range of behaviors that proactive threat hunting can help reveal to thwart an intrusion. The Dragos OT Watch team provides managed threat hunting and serves as a force multiplier for existing security teams seeking assistance with threat hunting in their OT environments. Threat-based detections for ELECTRUM TTPs are codified in the Dragos Platform for enhanced visibility of threats to ICS assets.