Five Threat Groups Target Industrial Systems: Dragos

By Eduard Kovacs

Published: 2018-03-01 · Archived: 2026-04-05 19:34:51 UTC

There are at least five sophisticated threat groups whose activities focus on industrial control systems (ICS), according to a report published on Thursday by industrial cybersecurity firm Dragos.

While it's not uncommon for non-targeted malware to make its way onto industrial systems, targeted attacks have also become increasingly common. Dragos currently tracks five threat actors that have either attacked ICS directly or have shown an interest in gathering information on these types of systems.

One of these groups is tracked by the security firm as Electrum. This is the actor behind the CRASHOVERRIDE/Industroyer malware used in December 2016 to cause a power outage in Ukraine. Electrum has been linked to Sandworm Team, which is believed to be responsible for a 2015 power outage in Ukraine. Russia has been accused for both attacks.

While it apparently hasn't launched any major attacks since the 2016 campaign targeting Ukraine's energy sector, Dragos says Electrum continues to be active, and evidence suggests it has expanded targets.

"While past ELECTRUM activity has focused exclusively on Ukraine, information from low- level ongoing events and the group's link to SANDWORM Dragos assesses that ELECTRUM could be 're-tasked' to other areas depending on the focus of their sponsor," Dragos said in its report.

Another gang tracked by Dragos is Covellite, which has been linked to North Korea's Lazarus group. Researchers started observing Covellite in September 2017, when it launched a highly targeted phishing campaign against a U.S. electric grid company. They later spotted attacks that may have been conducted by this group aimed at organizations in Europe, North America and East Asia.

Unlike Electrum, Covellite has yet to use malware specifically designed to target industrial systems in its campaigns.

Dragos' report also summarizes the activities of Dymalloy, a group whose attacks came to light during an investigation into Dragonfly, an actor that is also known as Crouching Yeti and Energetic Bear. Dragonfly, which is believed to be operating out of Russia, is known for its sophisticated Havex malware, and it was recently observed targeting control systems in U.S. energy firms.

Dragos believes Dymalloy is not linked – at least not directly – to Dragonfly and its tools are not as advanced as Havex. However, the hackers did manage to breach ICS organizations in Turkey, Europe and North America, gaining access to HMI devices.

Experts say Dymalloy appears to have become less active since early 2017, possibly in response to attention from the media and security researchers.

Learn More at SecurityWeek's ICS Cyber Security Conference

Since mid-2017, Dragos has been tracking a group it has named Chrysene, whose activity focuses on North America, Western Europe, Israel and Iraq, particularly organizations in the electricity generation and oil&gas sectors.

Chrysene, which continues to be active, has used a unique variation of a framework associated with the Iran-linked cyber espionage groups known as OilRig and Greenbug.

"While CHRYSENE's malware features notable enhancements over related threat groups using similar tools, Dragos has not yet observed an ICS-specific capability employed by this activity group. Instead, all activity thus

far appears to focus on IT penetration and espionage, with all targets being ICS-related organizations," Dragos said.

It's worth noting that the recently uncovered piece of malware known as Trisis/Triton, which is the first threat specifically designed to disrupt safety instrumented systems (SIS), has also been linked by some researchers to Iran.

The last ICS-focused threat group monitored by Dragos is Magnallium, which has also been linked to Iran. The security firm started tracking this actor following a report from FireEye on the activities of APT33.

While some media reports portrayed APT33 as a serious threat to ICS and critical infrastructure, Dragos' investigation showed that the group does not appear to possess any ICS-specific capabilities.

"While only one [of these groups] has demonstrated an apparent capability to impact ICS networks through ICS-specific malware directly, all have engaged in at least reconnaissance and intelligence gathering surrounding the ICS environment," Dragos said.

"These groups have remained relatively constant regarding overall activity throughout the year, and Dragos is confident that additional unknown events have occurred," the company added.

Related: DHS Warns of Malware Targeting Industrial Safety Systems

Related: DDoS Attacks More Likely to Hit Critical Infrastructure Than APTs

---