Feds Uncover a ‘Swiss Army Knife’ for Hacking Industrial Control Systems

The malware toolkit, known as Pipedream, is perhaps the most versatile tool ever made to target critical infrastructure like power grids and oil refineries.

Andy Greenberg Apr 13, 2022 3:50 PM

Photograph: JEFF PACHOUD/Getty Images

Malware designed to target industrial control systems like power grids, factories, water utilities, and oil refineries represents a rare species of digital badness. So when the United States government warns of a piece of code built to target not just one of those industries, but potentially all of them, critical infrastructure owners worldwide should take notice.

On Wednesday, the Department of Energy, the Cybersecurity and Infrastructure Security Agency, the NSA, and the FBI jointly released an advisory about a new hacker toolset potentially capable of meddling with a wide range of industrial control system equipment. More than any previous industrial control system hacking toolkit, the malware contains an array of components designed to disrupt or take control of the functioning of devices, including programmable logic controllers (PLCs) that are sold by Schneider Electric and OMRON and are designed to serve as the interface between traditional computers and the actuators and sensors in industrial environments. Another component of the malware is designed to target Open Platform Communications Unified Architecture (OPC UA) servers—the computers that communicate with those controllers.

"This is the most expansive industrial control system attack tool that anyone has ever documented," says Sergio Caltagirone, the vice president of threat intelligence at industrial-focused cybersecurity firm Dragos, which contributed research to the advisory and published its own report about the malware. Researchers at Mandiant, Palo Alto Networks, Microsoft, and Schneider Electric also contributed to the advisory. “It’s like a Swiss Army knife with a huge number of pieces to it.”

Dragos says the malware has the ability to hijack target devices, disrupt or prevent operators from accessing them, permanently brick them, or even use them as a foothold to give hackers access to other parts of an industrial control system network. He notes that while the toolkit, which Dragos calls “Pipedream,” appears to specifically target Schneider Electric and OMRON PLCs, it does so by exploiting underlying software in those PLCs known as Codesys, which is used far more broadly across hundreds of other types of

PLCs. This means that the malware could easily be adapted to work in almost any industrial environment. “This toolset is so big that it’s basically a free-for-all,” Caltagirone says. “There’s enough in here for everyone to worry about.”

The CISA advisory refers to an unnamed “APT actor” that developed the malware toolkit, using the common acronym APT to mean advanced persistent threat, a term for state-sponsored hacker groups. It's far from clear where the government agencies found the malware, or which country's hackers created it—though the timing of the advisory follows warnings from the Biden administration about the Russian government making preparatory moves to carry out disruptive cyberattacks in the midst of its invasion of Ukraine.

Dragos also declined to comment on the malware's origin. But Caltagirone says it doesn't appear to have been actually used against a victim—or at least, it hasn't yet triggered actual physical effects on a victim's industrial control systems. “We have high confidence it hasn’t been deployed yet for disruptive or destructive effects,” says Caltagirone.

While the toolkit's adaptability means it could be used against practically any industrial environment, from manufacturing to water treatment, Dragos points out that the apparent focus on Schneider Electric and OMRON PLCs does suggest that the hackers may have built it with power grid and oil refineries—particularly liquified natural gas facilities—in mind, given Schneider's wide use in electric utilities and OMRON's broad adoption in the oil and gas sector. Caltagirone suggests the ability to send commands to servo motors in those petrochemical facilities via OMRON PLCs would be particularly dangerous, with the ability to cause “destruction or even loss of life.”

The CISA advisory doesn't point to any particular vulnerabilities in the devices or software the Pipedream malware targets, though Caltagirone says it does exploit multiple zero-day vulnerabilities—previously unpatched hackable software flaws—that are still being fixed. He notes, however, that even patching those vulnerabilities won't prevent most of Pipedream's capabilities, as it's largely designed to hijack the intended functionality of target devices and send legitimate commands in the protocols they use. The CISA advisory includes a list of measures that infrastructure operators should take to protect their operations, from limiting industrial control systems' network connections to implementing monitoring systems for ICS systems, in particular, that send alerts for suspicious behavior.

When WIRED reached out to Schneider Electric and OMRON, a Schneider spokesperson responded in a statement that the company has closely collaborated with the US government and security firm Mandiant and that they together “identified and developed protective measures to defend against” the newly revealed attack toolkit. “This is an instance of successful collaboration to deter threats on critical infrastructure before they occur and further underscores how public-private partnerships are instrumental to proactively detect and counter threats before they can be deployed,” the company added. OMRON didn't immediately respond to WIRED's request for comment.

The discovery of the Pipedream malware toolkit represents a rare addition to the handful of malware specimens found in the wild that target industrial control systems (ICS) software. The first and still most notorious example of that sort of malware remains Stuxnet, the US- and Israeli-created code that was uncovered in 2010 after it was used to destroy nuclear enrichment centrifuges in Iran. More recently, the Russian hackers known as Sandworm, part of the Kremlin's GRU military intelligence agency, deployed a tool called Industroyer or Crash Override to trigger a blackout in the Ukrainian capital of

Kyiv in late 2016.

The next year, Kremlin-linked hackers infected systems at the Saudi Arabian oil refinery Petro Rabigh with a piece of malware known as Triton or Trisis, which was designed to target its safety systems—with potentially catastrophic physical consequences—but instead triggered two shutdowns of the plant's operations. Then, just last week, Russia's Sandworm hackers were detected using a new variant of their of Industroyer code to target a regional electrical utility in Ukraine, though Ukrainian officials say they managed to detect the attack and avert a blackout.

The Pipedream advisory serves as a particularly troubling new entry in the rogue's gallery of ICS malware, however, given the breadth of its functionality. But its revelation—apparently before it could be used for disruptive effects—comes in the midst of a larger crackdown by the Biden administration on potential hacking threats to critical infrastructure systems, particularly from Russia. Last month, for instance, the Justice Department unsealed indictments against two Russian hacker groups with a history of targeting power grids and petrochemical systems. One indictment named for the first time one of the hackers allegedly responsible for the Triton malware attack in Saudi Arabia and also accused him and his coconspirators of targeting US refineries. A second indictment named three agents of Russia's FSB intelligence agency as members of a notorious hacker group known as Berserk Bear, responsible for years of electric utility hacking. And then early this month the FBI took measures to disrupt a botnet of networking devices controlled by Sandworm, still the only hackers in history known to have triggered blackouts.

Even as the government has taken measures to call out and even disarm those disruptive hackers, Pipedream represents a powerful malware toolkit in unknown hands—and one from which infrastructure operators need to take measures to protect themselves, says Caltagirone. “This is not a small deal,” he says. “It’s a clear and present danger to the safety of industrial control systems.”

More Great WIRED Stories

- 📩 The latest on tech, science, and more: Get our newsletters!
- The race to rebuild the world's coral reefs
- Is there an optimal driving speed that saves gas?
- As Russia plots its next move, an AI listens
- How to learn sign language online
- NFTs are a privacy and security nightmare
- 👁️ Explore AI like never before with our new database
- 🏃🏽‍♀️ Want the best tools to get healthy? Check out our Gear team’s picks for the best fitness trackers, running gear (including shoes and socks), and best headphones