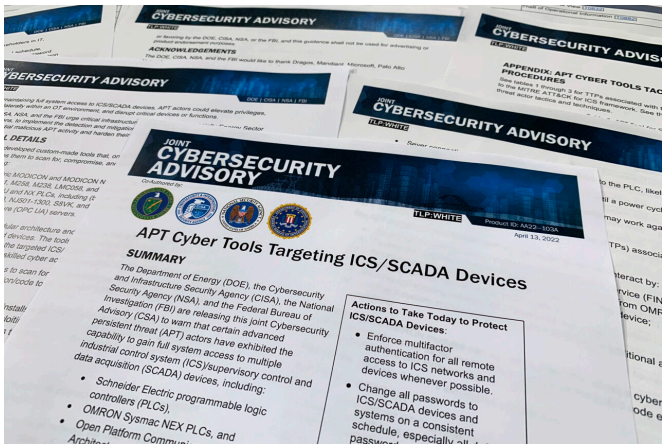
US agencies: Industrial control system malware discovered

14 April 2022, by Frank Bajak



A joint cybersecurity advisory released by the Department of Energy, the Cybersecurity and Infrastructure Security Agency, the National Security Agency and the FBI is photographed in Washington, Wednesday, April 13, 2022. The agencies issued the joint alert Wednesday announcing the discovery of malicious cyber tools capable of gaining "full system access" to multiple industrial control systems. Credit: AP Photo/Jon Elswick

Multiple U.S. government agencies issued a joint alert Wednesday warning of the discovery of a suite of malicious cyber tools created by unnamed advanced threat actors that are capable of sabotaging the energy sector and other critical industries.

The public alert from the Energy and Homeland Security Departments, the FBI and National Security Agency did not name the actors or offer details on the find. But their private sector cybersecurity partners said the evidence suggests Russia is behind the industrial control system-disrupting tools—and that they were configured to initially target North American energy concerns.

One of the cybersecurity firms involved, Mandiant, called the tools "exceptionally rare and dangerous."

In a report, it called the tools' functionality was "consistent with the malware used in Russia's prior physical attacks" though it acknowledged that the evidence linking it to Moscow is "largely circumstantial."

The CEO of another government partner, Robert M. Lee of Dragos, agreed that a state actor almost certainly crafted the malware, which he said was configured to initially target liquified natural gas and electric power sites in North America.

Lee referred questions on the state actor's identity to the U.S. government and would not explain how the malware was discovered other than to say it was caught "before an attack was attempted."

"We're actually one step ahead of the adversary. None of us want them to understand where they screwed up," said Lee. "Big win."

The Cybersecurity and Infrastructure Security Agency, which published the alert, declined to identify the threat actor.

The U.S. government has warned critical infrastructure industries the gird for possible cyberattacks from Russia as retaliation for severe economic sanctions imposed on Moscow in response to its Feb. 24 invasion of Ukraine.

Officials have said that Russian hacker interest in the U.S. energy sector is particularly high, and CISA urged it in a statement Wednesday to be especially mindful of the mitigation measures recommended in the alert. Last month, the FBI issued an alert saying Russian hackers have scanned at least five unnamed energy companies for vulnerabilities.

Lee said the malware was "designed to be a framework to go after lots of different types of

industries and be leveraged multiple times. Based on the configuration of it, the initial targets would be LNG and electric in North America."

Mandiant said the tools pose the greatest threat to Ukraine, NATO members and other states assisting Kyiv in its defense against Russian military aggression.

It said the malware could be used to shut down critical machinery, sabotage industrial processes and disable safety controllers, leading to the physical destruction of machinery that could lead to the loss of human lives. It compared the tools to Triton, malware traced to a Russian government research institute that targeted critical safety systems and twice forced the emergency shutdown of a Saudi oil refinery in 2017 and to Industroyer, the malware that Russian military hackers used the previous year to trigger a power outage in Ukraine.

Lee said the newly discovered malware, dubbed Pipedream, is only the seventh such malicious software to be identified that is designed to attack industrial control systems.

Lee said Dragos, which specializes in industrial control system protection, identified and analyzed its capability in early 2022 as part of its normal business research and in collaboration with partners.

He would offer no more specifics. In addition to Dragos and Mandiant, the U.S. government alert offers thanks to Microsoft, Palo Alto Networks and Schneider Electric for their contributions.

Schneider Electric is one of the manufacturers listed in the alert whose equipment is targeted by the malware. Omron is another.

Mandiant said it had analyzed the tools in early 2002 with Schneider Electric.

In a statement, Palo Alto Networks executive Wendi Whitmore said: ""We've been warning for years that our critical infrastructure is constantly under attack. Today's alerts detail just how sophisticated our adversaries have gotten."

Microsoft had no comment.

APA citation: US agencies: Industrial control system malware discovered (2022, April 14) retrieved 14 August 2022 from https://techxplore.com/news/2022-04-agencies-industrial-malware.html