Destructive ICS Malware ‘Fuxnet’ Used by Ukraine Against Russian Infrastructure

By Eduard Kovacs

Published: 2024-04-15 · Archived: 2026-04-05 16:07:46 UTC

Industrial and enterprise IoT cybersecurity firm Claroty has conducted an analysis of Fuxnet, a piece of industrial control system (ICS) malware used recently by Ukrainian hackers in an attack aimed at a Russian underground infrastructure company.

In recent months, a hacker group named Blackjack, which is believed to be affiliated with Ukraine’s security services, has claimed to have launched attacks against several key Russian organizations. The hackers targeted ISPs, utilities, data centers and Russia’s military, and allegedly caused significant damage and exfiltrated sensitive information.

Last week, Blackjack disclosed the details of an alleged attack aimed at Moscollector, a Moscow-based company responsible for underground infrastructure, including water, sewage and communication systems.

“Russia’s industrial sensor and monitoring infrastructure has been disabled,” the hackers claimed. “It includes Russia’s Network Operation Center (NOC) [that] monitors and controls gas, water, fire alarm and many others, including a vast network of remote sensors and IoT controllers.”

The hackers claimed to have wiped database, email, internal monitoring and data storage servers.

In addition, they claimed to have disabled 87,000 sensors, including ones associated with airports, subway systems and gas pipelines. To achieve this, they claimed to have used Fuxnet, a malware they described as “Stuxnet on steroids”, which enabled them to physically destroy sensor equipment.

“Fuxnet has now started to flood the RS485/MBus and is sending ‘random’ commands to 87,000 embedded control and sensory systems (carefully excluding hospitals, airports, and other civilian targets),” the hackers said.

The hackers’ claims are difficult to verify, but Claroty was able to conduct an analysis of the Fuxnet malware based on information and code made available by Blackjack.

The cybersecurity firm pointed out that the actual sensors deployed by Moscollector, which are used to collect physical data such as temperature, were likely not damaged by Fuxnet. Instead, the malware likely targeted roughly 500 sensor gateways, which communicate with the sensors over a serial bus such as the RS485/Meter-Bus that was mentioned by Blackjack. These gateways are also connected to the internet to be able to transmit data to the company’s global monitoring system.

“If the gateways were indeed damaged, the repairs could be extensive given that these devices are spread out geographically across Moscow and its suburbs, and must be either replaced or their firmware must be individually reflashed,” Claroty noted.

Claroty’s analysis of Fuxnet showed that the malware was likely deployed remotely. Once on a device, it would start deleting important files and directories, shutting down remote access services to prevent remote restoration, and deleting routing table information to prevent communication with other devices. Fuxnet would then delete the file system and rewrite the device’s flash memory.

Once it has corrupted the file system and blocked access to the device, the malware attempts to physically destroy the NAND memory chip and then rewrites the UBI volume to prevent rebooting.

In addition, the malware attempts to disrupt the sensors connected to the gateway by flooding the serial channels with random data in an effort to overload the serial bus and the sensors.

“During the malware operation, it will repeatedly write arbitrary data over the Meter-Bus channel. This will prevent the sensors and the sensor gateway from sending and receiving data, rendering the sensor data acquisition useless,” Claroty explained. “Therefore, despite the attackers’ claim of compromising 87,000 devices, it seems that they actually managed to infect the sensor gateways only and were trying to cause further disruption by flooding the Meter-Bus channel connecting the different sensors to the gateway, similar to network fuzzing the different connected sensor equipment. As a result, it appears only the sensor gateways were bricked, and not the end-sensors.”

Related: Omron Patches PLC, Engineering Software Flaws Discovered During ICS Malware Analysis

Related: CosmicEnergy ICS Malware Poses No Immediate Threat, but Should Not Be Ignored

---