

Fuxnet ICS Malware

 enigmasoftware.com/fuxneticsmalware-removal/



By **Mezo** in [Malware](#)

Information security researchers recently analyzed Fuxnet, a form of malware targeting Industrial Control Systems (ICS), which Ukrainian hackers deployed in a recent assault on a Russian underground infrastructure firm.

The hacking collective Blackjack, purportedly linked to Ukraine's security apparatus, has asserted responsibility for launching assaults on several critical Russian entities. Their targets included internet service providers (ISPs), utilities, data centers, and even Russia's military, resulting in substantial damage and the extraction of sensitive data.

Moreover, Blackjack hackers have divulged specifics regarding an alleged strike against Moscollector, a Moscow-based company overseeing underground infrastructure such as water, sewage, and communication systems.

[Table of Contents](#)

The Fuxnet Malware is Deployed in Attack Operations

According to the hackers, Russia's industrial sensor and monitoring infrastructure has been rendered inoperative. This infrastructure includes the Network Operation Center (NOC), responsible for overseeing gas, water, fire alarms, and various other systems, alongside a sprawling network of remote sensors and IoT controllers. The hackers asserted that they had wiped out databases, email servers, internal monitoring systems and data storage servers.

Furthermore, they alleged to have deactivated 87,000 sensors, including those vital to airports, subway systems, and gas pipelines. They claimed to have achieved this using Fuxnet, a malware they likened to a potent version of [Stuxnet](#), allowing them to damage sensor equipment physically.

The hackers stated that Fuxnet had initiated a flood of RS485/MBus and was issuing 'random' commands to 87,000 embedded control and sensory systems. They emphasized that they deliberately excluded hospitals, airports and other civilian targets from their actions.

While the hackers' claims are challenging to prove, researchers managed to analyze the Fuxnet malware based on information and code provided by the Blackjack group.

The Fuxnet Malware could Cause Severe Disruptions

Cybersecurity experts highlight that the physical sensors utilized by Moscollector, which are responsible for gathering data like temperature, likely remained unscathed by Fuxnet. Instead, the malware is believed to have targeted approximately 500 sensor gateways, which facilitate communication with the sensors via a serial bus like RS485/Meter-Bus, as mentioned by Blackjack. These gateways are also internet-connected to transmit data to the company's global monitoring system.

Should the gateways be compromised, repairs could prove extensive, given their geographical dispersion across Moscow and its outskirts. Each device would require either a replacement or individual firmware reflashing.

Analysis of Fuxnet suggests remote deployment of the malware. Once infiltrated, it initiates the deletion of crucial files and directories, disables remote access services to thwart restoration attempts, and wipes routing table data to hinder device-to-device communication. Subsequently, Fuxnet erases the file system and rewrites the device's flash memory.

Upon corrupting the file system and barring device access, the malware endeavors to physically damage the NAND memory chip and then rewrites the UBI volume to impede rebooting. Additionally, it seeks to disrupt sensors linked to the gateway by flooding serial channels with random data, aiming to overwhelm both the serial bus and the sensors.

Researchers Speculate that the Fuxnet Malware might Have Infected Sensor Gateways

The malware operation repeatedly adds arbitrary data to the Meter-Bus channel. This action obstructs the transmission and reception of data between the sensors and the sensor gateway, rendering the acquisition of sensor data ineffective. Hence, despite the attackers' claim of compromising 87,000 devices, it appears more practical that they had succeeded in infecting the sensor gateways. Their subsequent flooding of the Meter-Bus channel, akin to network fuzzing, aimed to disrupt the interconnected sensor equipment further. Consequently, it seems only the sensor gateways were rendered inoperable, leaving the end-sensors unaffected.

Your comment is awaiting moderation.

Please verify that you are not a robot.

Loading...