INTELLIGENCE BRIEF

Strategic Overview of the Fuxnet Malware

BRYCE LIVINGSTON | SENIOR ADVERSARY HUNTER II

SAM HANSON | SENIOR VULNERABILITY ANALYST

DRAGOS, INC

MAY 2024

Summary

In April 2024, the pro-Ukrainian hacktivist persona Blackjack claimed responsibility for a cyberattack on Moskollektor, a Russian organization managing Moscow's municipal infrastructure. Blackjack allegedly used a malware called Fuxnet, designed to disrupt sensor operations within Moskollektor's operational technology (OT) monitoring network.

This incident highlights a trend of increasing hacktivist activity targeting civilian OT infrastructure. The attention garnered by the Blackjack claims suggests that other personas may seek to replicate such attacks. Dragos has observed a rise in the number of claims targeting ICS/OT and civilian critical infrastructure, indicating that hacktivist groups are learning from each other and converging on similar strategies.

Hacktivism, defined as hacking to promote a political or social agenda, is often portrayed as grassroots activism. However, many of these groups may be influenced or directly controlled by nation-state intelligence agencies. For defenders and decision makers at industrial organizations, the distinction between grassroots and state-sponsored activity is less critical than understanding the threat landscape. It's crucial to comprehend the tactics these groups employ against industrial organizations and assets. Defenders need visibility into OT environments, ICS-specific incident response plans, and a thorough understanding of their external attack surface to mitigate the associated risks effectively.

Key Findings

- Fuxnet, if validated, would qualify as the 8th known ICS-specific malware due to its Meter-bus fuzzing capabilities.
- The malware's ICS-specific component is likely usable but may be tailored to Moskollektor's environment, limiting its functionality in other settings without further modification.
- Dragos analyzed the evidence provided by Blackjack and engaged with the persona directly. Based on this investigation, Dragos assesses with moderate confidence that Moskollektor was compromised. However, the extent of the damage or data exfiltration currently remains unclear.

Fuxnet Malware

In April 2024, the hacktivist persona Blackjack claimed to have successfully conducted a cyberattack targeting Moskollektor, an organization responsible for the OT network overseeing Moscow's infrastructure sensor system. In addition to claiming to have disrupted 87,000 sensors using the Fuxnet malware, Blackjack claimed to have accessed the Russian 112 emergency services number, invalidated key cards to office buildings, defaced websites and social media pages, and more. In support of these claims, Blackjack posted information stolen during the alleged operation and screenshots of the Fuxnet malware's source code to a data leak site.

Joint Stock Company (JSC) "Moskollektor" is a municipal entity in Moscow responsible for overseeing the city's communication "collectors." These collectors are underground tunnels reinforced with concrete, housing essential utilities like power and communication cables, hot and cold water, and natural gas lines. Their primary purpose is to centralize the maintenance and management of these utilities, safeguarding Moscow's infrastructure and conserving urban real estate. Moskollektor oversees a vast network of numerous sensors, monitoring the tunnels' health and function and the associated infrastructure.

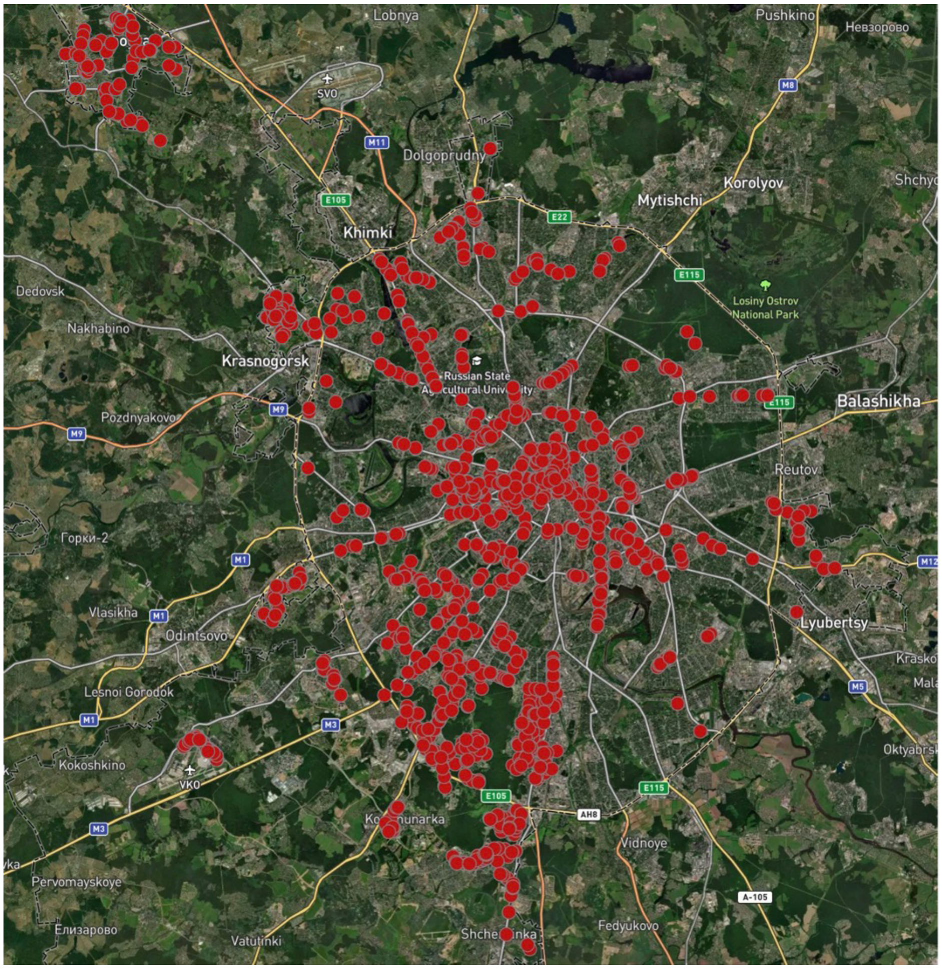

Figure 1: Image Of Underground Communication Collector. Image Retrieved From Moscow Urban Services Complex Website

Blackjack posted code screenshots of key functionality of the Fuxnet malware, along with limited screenshots of its claimed deployment. The screenshots describe two capabilities designed to destroy Moskellektor's network of sensors: a sensor gateway destructor component and a sensor denial of service (DoS) component.

The sensor gateway destructor attempts to destroy the gateways by:

- removing critical files,
- stopping services,
- isolating the device from the internet
- writing an incomplete amount of junk data to the UBI volume leaving it in a corrupted state,
- wearing out locations of flash memory to the point of corruption.

The sensor denial of service component "floods" the sensor by repeatedly sending Meter-Bus requests, thus overwhelming the sensor and facilitating DoS conditions. These Meter-Bus requests contain randomly generated junk data conforming to the requirements of a Meter-Bus packet with the objective of triggering a denial-of-service vulnerability in the sensor.

Assessing the Impact

As noted earlier, no compiled version of the Fuxnet malware has been released, and no observed direct evidence supports the claims of disruption within Moskollektor's network. Russian media outlets have not reported the incident, and Moskollektor has neither acknowledged nor responded to Blackjack's claims.

Despite the absence of direct evidence from the incident or the malware, other elements lend some credence to the adversary's assertions. Moskollektor's website was defaced, confirmed by an archived snapshot dated 09 April. Furthermore, Blackjack claimed responsibility for altering Moskollektor's Facebook profile picture and cover image. While Dragos did not directly observe these changes, the sudden change in both images on April 09 back to the original photos, following nearly two years of inactivity, suggests a possible compromise.

The track record of the Blackjack persona adds another layer of complexity. This incident marks their 11th claimed attack against Russian targets. Dragos found supporting evidence for at least one prior claim: a disruptive New Year's Day attack on the Russian ISP "Siberian Bear". This lends some weight to the authenticity of Blackjack's operations, though many of its exploits go unpublicized according to the persona.

Given the lack of detailed information about the malware or its deployment, accurately judging the potential impact remains challenging. If Fuxnet was deployed as described, its effectiveness is still uncertain. The sensor DoS component aimed to induce a denial of service during sensor operation, but whether it succeeded is unknown. Regardless, while not ICS-specific, the sensor gateway destructor component would have severed the connection between the sensor gateways and Moskollektor's central monitoring system. The precise impact on Moskollektor's and Moscow's operations is difficult to determine without detailed infrastructure knowledge. However, given Moskollektor's role, it likely caused a temporary loss of visibility rather than an immediate or catastrophic danger.

Blackjack's screenshots, showing sensor locations in critical infrastructure, are concerning as they indicate the potential for disrupting essential services, such as gas and electrical supplies to hospitals. Even if the impact was not immediately catastrophic, targeting civil infrastructure in this manner underscores the urgent need for robust cybersecurity measures to protect ICS/OT environments from such threats.

Recommendations

To effectively defend against these threats, ICS/OT defenders need comprehensive visibility into their environments, ICS-specific incident response plans, and secure remote access. This visibility includes understanding the attack surface and ensuring robust cybersecurity measures are in place to mitigate the risks from increasingly sophisticated hacktivist groups.

Dragos recommends organizations implement the 5 Critical Controls for World-Class OT Cybersecurity identified by the SANS Institute. These controls present a framework for implementing a world-class OT cybersecurity program to defend against adversary activity directed against OT networks, be it intellectual property theft, ransomware, or targeted cyber-physical effects.

1. ICS Incident Response
The Fuxnet malware included a sensor denial of service (DoS) component specifically targeting ICS environments, indicating that if deployed, it could cause operational disruptions. An operations-informed incident response plan would ensure system integrity and recovery capabilities are in place to address such disruptions and restore normal operations quickly..

2. Defensible Architecture
The Fuxnet malware exploited vulnerabilities in Moskollektor's infrastructure, particularly by gaining root access to IoT routers using default passwords. Dragos recommends implementing strict network segmentation between IT and OT environments to limit the lateral movement of adversaries and contain potential intrusions. Additionally, OT defenders should consider conducting security audits of the organization's external attack surface. Defenders can use low-cost tools like Censys and Shodan to identify glaring security issues. These tools can identify exposed PLCs and provide detailed information, such as specific PLC versions, highlighting the extent of discoverability and exposure risk.

3. ICS Network Visibility Monitoring
The incident revealed the adversary's detailed understanding of Moskollektor's network, including various devices' IP addresses and functions. Continuous network security monitoring with protocol-aware toolsets allows for early detection of suspicious activities and unauthorized access and timely intervention before significant damage occurs. Dragos recommends ensuring network visibility and monitoring are in place for north-south and east-west network traffic in enterprise IT and OT. Dragos Platform threat detections have been updated to alert customers of the presence of Fuxnet in their environments.

4. Secure Remote Access
The deployment of the Fuxnet malware likely involved exploiting default device passwords and unsecured remote access points. Organizations can significantly reduce the risk of unauthorized access and potential malware deployment by identifying and inventorying all remote access points and implementing multi-factor authentication and secure access methods.

5. Risk-Based Vulnerability Management
The malware's capability to exploit specific vulnerabilities within Moskollektor's sensor gateways underscores the need for risk-based vulnerability management. Understanding the cyber digital controls and operating conditions helps prioritize patching and mitigation efforts for the most critical vulnerabilities, ensuring that resources are effectively allocated to protect against the highest risks.

Takeaways for Defenders

Dragos assesses with moderate confidence that if the claims are proven, Fuxnet qualifies as the 8th ICS-specific malware due to its Meter-bus functionality. However, self-claimed hacktivist personas such as Blackjack have an inherent incentive to exaggerate their claims to increase awareness of their "success," one must be careful when taking them at their word. Further evidence of Fuxnet's effects or the Fuxnet binary itself must be uncovered before stating unequivocally that Fuxnet is the 8th ICS-specific malware.

The increasing visibility and attention towards ICS/OT environments and incidents involving relatively simple hacktivism, set worrying precedents for targeting infrastructure. ICS/OT operations are increasingly targeted by "hacktivist" personas, either through rhetoric (making false or unverifiable claims of impacting ICS/OT assets) or genuine attacks. The anti-Israel CyberAv3ngers persona conducted an exploitation campaign targeting Unitronics PLCs in November 2023, resulting in operational disruptions to water treatment systems in Ireland as well as impacting systems in the U.S. Additionally, the pro-Russian CyberArmyofRussia_Reborn persona has claimed disruptive attacks on water utilities across the globe, causing disruptions in at least one confirmed case in the United States.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo   Contact Us