F#RTINET.

OUTBREAK ALERTS





CosmicEnergy Malware New OT Malware designed to cause electric power disruption

A new malware called CosmicEnergy has been discovered that targets operational technology sector. According to the reports, the malware is

designed to cause electric power disruption by exploiting IEC 60870-5-104 (IEC-104) protocol, which are commonly used in electric transmission and distribution operations in Europe, the Middle East, and Asia.

Announced

Background

CosmicEnergy is similar in its capabilities to previous OT malware families Industroyer and Industroyer 2.0, as both variants aim to cause electric power disruption through targeting devices commonly used in electric transmission and distribution operations. According to the reports, CosmicEnergy is possibly associated with Russian government-funded power disruption and emergency response exercises.

May 25, 2023: Mandiant released a blog on CosmicEnergy Malware. https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response

Latest Developments May 25, 2023: FortiGuard Labs released a Threat Signal. https://www.fortiguard.com/threat-signal-report/5171/

FotiGuard Labs has released Antivirus signatures for known malware and has behaviour detection engine service

security posture and always follow best practices for Operational Technology (OT) Security. https://www.fortinet.com/resources/cyberglossary/ot-security-best-practices

to detect other unknown and 0-day malware. FortiGuard Labs recommends organizations to review their OT/ICS

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Detects CosmicEnergy Malware and prevents lateral movement in the network segment

Lure

Decoy VM Detects CosmicEnergy Malware and prevents lateral movement in the network segment

FortiDeceptor

v3.3+

FortiSASE

DB 91.03626

FortiMail

DB 91.03626

FortiCASB

DB 91.03626

FortiCWP

DB 91.03626

FortiDeceptor v3.3+ Weaponization

AV

DB 91.03626

Delivery

FortiGate FortiWeb FortiClient

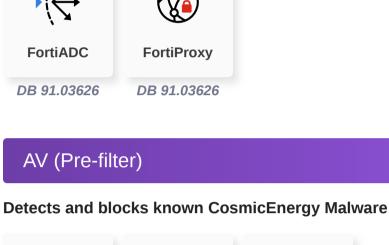
DB 91.03626

FortiNDR

DB 91.03626

DB 91.03626

Detects and blocks known CosmicEnergy Malware



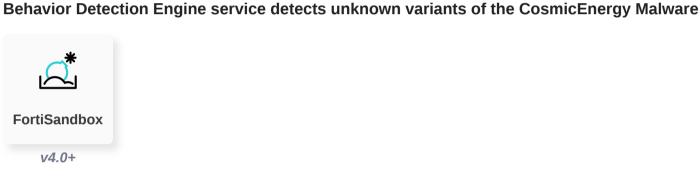
DB 91.03626

FortiEDR

Behavior Detection

FortiSandbox

DB 91.03626



IOC

FortiAnalyzer

FortiAnalyzer

DB 2.00006

Installation C2 **Action**

Exploitation

FortiSIEM

FortiSIEM

v6.4+

FortiSOCaaS

DETECT

alert and generate reports:

Outbreak Detection

Find and correlate important information to identify an outbreak, the following updates are available to raise



Content Update

DB 316

RESPOND

Services that can automaticlly respond to this outbreak.

Automated Response

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

RECOVER Improve security posture and processes by implementing security awareness and training, in preparation for

Develop containment techniques to mitigate impacts of security events:



Identify processes and assets that need protection:

Security readiness and awareness training for SOC teams, InfoSec and general employees.



Additional Resources

Dark Reading https://www.darkreading.com/ics-ot/cosmicenergy-malware-emerges-electric-grid-shutdown **The Hacker News** https://thehackernews.com/2023/05/new-cosmicenergy-malware-exploits-ics.html

physical-damage/

Learn more about FortiGuard Outbreak Alerts







Incident

3

FortiXDR







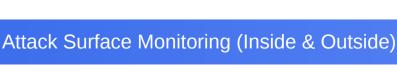


Mandiant

Industrial Cyber

Bleeping Computer

Washington Post



Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.



https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response https://industrialcyber.co/ransomware/cosmicenergy-ot-malware-linked-to-russian-emergency-response-exercises-couldcause-power-disruption/

https://www.washingtonpost.com/politics/2023/05/26/this-newly-discovered-malware-could-disrupt-power-generation-do-

https://www.bleepingcomputer.com/news/security/new-russian-linked-cosmicenergy-malware-targets-industrial-systems/

F#RTINET.