

## 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.

**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.

**Announced** 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.fortiguards.com/threat-signal-report/5171/>

FortiGuard Labs has released Antivirus signatures for known malware and has behaviour detection engine service to detect other unknown and 0-day malware. FortiGuard Labs recommends organizations to review their OT/ICS security posture and always follow best practices for Operational Technology (OT) Security.  
<https://www.fortinet.com/resources/cyberglossary/ot-security-best-practices>

## PROTECT

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

### Reconnaissance

#### Lure


Detects CosmicEnergy Malware and prevents lateral movement in the network segment



FortiDeceptor  
v3.3+

#### Decoy VM

Detects CosmicEnergy Malware and prevents lateral movement in the network segment












FortiDeceptor  
v3.3+

### Weaponization

### Delivery




#### AV

Detects and blocks known CosmicEnergy Malware

 FortiGate DB 91.03626	 FortiWeb DB 91.03626	 FortiClient DB 91.03626	 FortiSASE DB 91.03626	 FortiMail DB 91.03626	 FortiCASB DB 91.03626	 FortiCWP DB 91.03626
 FortiADC DB 91.03626	 FortiProxy DB 91.03626					


#### AV (Pre-filter)

Detects and blocks known CosmicEnergy Malware

 FortiEDR DB 91.03626	 FortiSandbox DB 91.03626	 FortiNDR DB 91.03626
--	--	--

#### Behavior Detection

Behavior Detection Engine service detects unknown variants of the CosmicEnergy Malware



FortiSandbox  
v4.0+

### Exploitation

### Installation




### C2

### Action


## DETECT

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

#### IOC



 FortiAnalyzer	 FortiSIEM	 FortiSOCaaS
--	--	--

#### Outbreak Detection




FortiAnalyzer  
DB 2.00006

#### Threat Hunting

 FortiAnalyzer v6.4+	 FortiSIEM v6.4+
---	---

#### Content Update




FortiSIEM  
DB 316

## RESPOND

Develop containment techniques to mitigate impacts of security events:

#### Automated Response


Services that can automatically respond to this outbreak.



FortiXDR

#### Assisted Response Services

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



Incident Response

## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

#### InfoSec Services

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




Response Readiness

## IDENTIFY

Identify processes and assets that need protection:

#### Attack Surface Monitoring (Inside & Outside)

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



Security Rating

## Additional Resources

Mandiant	<a href="https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response">https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response</a>
Industrial Cyber	<a href="https://industrialcyber.co/ransomware/cosmicenergy-ot-malware-linked-to-russian-emergency-response-exercises-could-cause-power-disruption/">https://industrialcyber.co/ransomware/cosmicenergy-ot-malware-linked-to-russian-emergency-response-exercises-could-cause-power-disruption/</a>
Bleeping Computer	<a href="https://www.bleepingcomputer.com/news/security/new-russian-linked-cosmicenergy-malware-targets-industrial-systems/">https://www.bleepingcomputer.com/news/security/new-russian-linked-cosmicenergy-malware-targets-industrial-systems/</a>
Dark Reading	<a href="https://www.darkreading.com/ics-ot/cosmicenergy-malware-emerges-electric-grid-shutdown">https://www.darkreading.com/ics-ot/cosmicenergy-malware-emerges-electric-grid-shutdown</a>
The Hacker News	<a href="https://thehackernews.com/2023/05/new-cosmicenergy-malware-exploits-ics.html">https://thehackernews.com/2023/05/new-cosmicenergy-malware-exploits-ics.html</a>
Washington Post	<a href="https://www.washingtonpost.com/politics/2023/05/26/this-newly-discovered-malware-could-disrupt-power-generation-physical-damage/">https://www.washingtonpost.com/politics/2023/05/26/this-newly-discovered-malware-could-disrupt-power-generation-physical-damage/</a>

Learn more about [FortiGuard Outbreak Alerts](#)