I

Industroyer Malware: How CrashOverride Targets Power Grid Operations

Industroyer, or CrashOverride, is an OT malware framework designed to disrupt electric-grid operations. Learn how it works, how Industroyer2 differs, and what defenders should monitor.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 Industroyer versus Industroyer2

02 What the original framework contained

03 What Industroyer cannot do automatically

04 Detection priorities for electric utilities

05 Incident response in an OT environment

06 Reducing exposure

07 Frequently asked questions

08 References

Industroyer, also called **CrashOverride**, is a modular malware framework built to disrupt industrial control systems used in electric-power substations. It was used in the December 2016 attack on Ukraine's power grid and is the first publicly known malware designed specifically to affect electric-grid operations.

Unlike ordinary Windows malware, Industroyer included components that could communicate using industrial protocols and issue legitimate-looking control messages. It still required attackers to compromise the operational environment, understand its design, and configure the malware for the target.

01 Industroyer versus Industroyer2

Feature	Industroyer / CrashOverride	Industroyer2
Publicly reported use	Ukraine, December 2016.	Attempted attack against Ukrainian energy infrastructure in 2022.
Design	Extensible framework with separate modules for several electric-grid communication protocols.	More focused, self-contained implementation for IEC 60870-5-104.
Target configuration	Modules and supporting configuration adapted to the environment.	Embedded configuration tied to specific intelligent electronic devices and control points.
Lesson for defenders	Protocol-aware OT malware can use normal control functions for malicious impact.	Known OT malware concepts can be tailored and redeployed against a new victim.

02 What the original framework contained

Public analysis describes a main backdoor for command and control, a secondary backdoor for persistence, a launcher, protocol-specific payload modules, and supporting denial-of-service or destructive components. The protocol modules supported technologies used in electrical automation, while a separate component targeted certain protective-relay communications.

The Windows backdoors provided access and orchestration. The industrial payloads were what made the framework unusual: instead of relying only on a software vulnerability, they could speak the same protocols used by control systems. This allowed malicious actions to resemble operator commands at the protocol level.

03 What Industroyer cannot do automatically

- It is not a universal program that can black out any grid after reaching one office computer.
- It does not eliminate the need for prior access to the OT environment and knowledge of its network, devices, protocols, and operational state.
- A module for one protocol or device profile does not automatically work against every vendor or substation.
- Traditional IT indicators alone do not describe the full physical-process risk.

This context matters because exaggerated descriptions hide the real defensive problem: an attacker who has already crossed into OT and can turn valid control functionality against the process.

04 Detection priorities for electric utilities

Exact sample hashes are useful for known artifacts, but behavioral and engineering context last longer. Defenders should combine:

- application allowlisting and integrity monitoring on engineering workstations, HMIs, SCADA servers, and jump hosts;
- alerts for unexpected services, altered binaries, persistence, remote administration, and command-and-control from OT Windows systems;
- passive monitoring for new protocol speakers, unusual control commands, scanning, repeated switching activity, or commands outside an approved time and workflow;
- comparison of network commands with operator actions, work orders, device state, alarms, and physical-process expectations;

- configuration and firmware baselines for relays, RTUs, gateways, and serial-to-network devices;
- central logging outside the affected zone so attackers cannot erase the only evidence.

OT monitoring must be engineered for the environment. Active scanning or automated blocking that is safe on an office network can disrupt fragile or safety-critical devices.

05 Incident response in an OT environment

1. **Put safety and reliable operation first.** Coordinate cyber responders with control-room staff, protection engineers, equipment owners, and incident command.
2. **Use approved isolation points.** Restrict remote access and unnecessary IT/OT paths without making unreviewed changes that could destabilize the process.
3. **Preserve multiple evidence sources.** Collect Windows, identity, firewall, remote-access, network, controller, and engineering records while maintaining safe operations.
4. **Validate device state independently.** Do not rely only on an HMI that may be compromised. Follow site procedures for confirming breaker, relay, and process state.
5. **Hunt for the whole intrusion.** Look beyond the final ICS payload to initial access, credentials, jump hosts, engineering files, reconnaissance, persistence, and supporting wipers.
6. **Recover from trusted baselines.** Validate software, device configuration, logic, firmware, protection settings, and credentials before returning systems to service.

06 Reducing exposure

- Separate business, DMZ, supervisory, and control zones with narrowly approved flows.
- Require phishing-resistant MFA and managed jump hosts for remote OT access.
- Remove direct internet access from control assets and tightly control portable media.
- Keep offline backups of configurations, logic, workstation images, and vendor installation media; test restoration.

- Inventory devices, protocols, trust paths, and safety dependencies before an incident.
- Exercise manual operation and loss-of-view scenarios with operations teams.
- Patch through an OT change-management process and apply compensating controls where immediate patching is unsafe.

07 Frequently asked questions

Is Industroyer the same as BlackEnergy?

No. Both are discussed in connection with attacks on Ukrainian energy organizations, but they are different malware families and campaigns. Do not merge their indicators or capabilities.

Does Industroyer exploit a protocol vulnerability?

Its key risk is that it can use legitimate, insecure-by-design control functions and protocol semantics. The decisive weakness is often unauthorized access to a trusted operational path, not one universal software flaw.

Can ordinary antivirus detect it?

Endpoint protection can detect known Windows components and behaviors, but it cannot replace OT network monitoring, engineering baselines, identity controls, and independent validation of process state.

08 References

- MITRE ATT&CK: Industroyer (S0604)
- US-CERT: CrashOverride Malware alert
- Mandiant: Industroyer.V2 analysis

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com