I

# Industroyer Malware: Power Grid Attack Framework

What it is Industroyer, also called CrashOverride, is a malware framework designed to interact with industrial control systems used in electric-power environments. It is associated with a 2016 disruption in Ukraine. Unlike ordinary...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
2 min

## What it is

Industroyer, also called CrashOverride, is a malware framework designed to interact with industrial control systems used in electric-power environments. It is associated with a 2016 disruption in Ukraine. Unlike ordinary Windows malware, parts of the framework understand specific grid communication protocols and can issue commands to field equipment.

## How it works

The attackers first need access to the operational environment and knowledge of its architecture. Industroyer components can communicate using industrial protocols, map or control equipment, and include supporting functions for denial of service or destructive cleanup. A later related tool known as Industroyer2 showed a more targeted implementation.

## Key points

- The malware does not automatically work against every power network; configuration and protocol details matter.
- Traditional antivirus on office endpoints cannot replace monitoring and controls designed for operational technology.
- Safety, availability, and controlled recovery take priority over rapid removal in an active industrial incident.

## What to do

- Separate business and operational networks and strictly control remote engineering access.
- Baseline legitimate industrial commands so unusual control activity can be detected.
- Maintain tested manual operations and restoration procedures independent of compromised systems.
- Coordinate containment with control engineers and specialized incident responders.

## Why ordinary cleanup guidance is not enough

Industroyer is relevant to operational technology and electric-power environments, where an unplanned shutdown or scan can affect safety and service availability. Suspected activity should be coordinated with control engineers, incident responders, and the equipment owner. Preserve engineering-workstation, remote-access, and network evidence; isolate only through an approved operational procedure. Validate controller logic and trusted configurations before restoration. Home users are unlikely to encounter this family. For general endpoint containment, use the malware guide, but do not apply consumer remediation steps blindly to an industrial control system.

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**