Industroyer

By Contributors to Wikimedia projects

Published: 2017-07-04 · Archived: 2026-04-05 13:07:43 UTC

From Wikipedia, the free encyclopedia

Industroyer[1] (also referred to as **Crashoverride**) is a malware framework considered to have been used in the cyberattack on Ukraine's power grid on 17 December 2016.[2][3][4] The attack cut a fifth of Kyiv, the capital, off power for one hour and is considered to have been a large-scale test.[5][6] The Kyiv incident was the second cyberattack on Ukraine's power grid in two years. The first attack occurred on 23 December 2015.[7] Industroyer is the first ever known malware specifically designed to attack electrical grids.[8] At the same time, it is the fourth malware publicly revealed to target industrial control systems, after Stuxnet, Havex, and BlackEnergy.

Discovery and naming

[edit]

The malware was discovered by Slovak internet security company ESET. ESET and most of the cybersecurity companies detect it under the name "Industroyer".[9][10] Cybersecurity firm Dragos named the malware "Crashoverride".[8] In 2022, the Russian hacker group Sandworm initiated a blackout in Ukraine using a variant of Industroyer aptly dubbed Industroyer2.[11]

The detailed analysis of Industroyer[12] revealed that the malware was designed to disrupt the working processes of industrial control systems, specifically those used in electrical substations. Industroyer is modular malware; its main components are the following:

- **A main backdoor** is used to control all other components of the malware. It connects to its remote Command & Control servers in order to receive commands from the attackers.
- **An additional backdoor** provides an alternative persistence mechanism that allows the attackers to regain access to a targeted network in case the main backdoor is detected and/or disabled.
- **A launcher component** is a separate executable responsible for launching the payload components and the data wiper component. The launcher component contains a specific activation time and date; analyzed samples contained two dates: 17 December 2016 and 20 December 2016. (Note: the former date was the date the attack actually went ahead.)
- **Four payload components** target particular industrial communication protocols specified in the following standards: IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access (OPC Data Access). The functionalities of the payload components include mapping the network, and then issuing commands to the specific industrial control devices.
- **A data wiper component** is designed to erase system-crucial Registry keys and overwrite files to make the system unbootable and recovery from the attack harder.

- Control system security
- Cyberwarfare
- Ukraine power grid hack
- Pipedream (toolkit)

1. ^ *Spanish Video CCN-CERT STICS Conference 2017. "Video-Youtube" – via YouTube.* {{cite web}} : CS1 maint: numeric names: authors list (link)
2. ^ *"NPC Ukrenergo official statement". 18 December 2016 – via Facebook.*
3. ^ *Pavel Polityuk, Oleg Vukmanovic and Stephen Jewkes (18 January 2017). "Ukraine's power outage was a cyber attack: Ukrenergo". Reuters.*
4. ^ *Cherepanov, Anton (17 June 2017). "Industroyer: Biggest threat to industrial control systems since Stuxnet". welivesecurity.com. ESET.*
5. ^ *Zetter, Kim (17 January 2017). "The Ukrainian Power Grid Was Hacked Again". Motherboard.*
6. ^ *"'Crash Override': The Malware That Took Down a Power Grid". WIRED. Retrieved 22 January 2018.*
7. ^ *"Ongoing Sophisticated Malware Campaign Compromising ICS (Update E) | ICS-CERT". ics-cert.us-cert.gov. Retrieved 22 January 2018.*
8. ^ Jump up to: ***a*** ***b*** *Dragos Inc. (12 June 2017). "CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations" (PDF). Dragos.*
9. ^ *"Industroyer main backdoor detections". Virustotal. 27 June 2017.*
10. ^ *"Industroyer data wiper component detections". Virustotal. 27 June 2017.*
11. ^ *Greenberg, Andy. "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine". Wired. ISSN 1059-1028. Retrieved 13 April 2022.*
12. ^ *Cherepanov, Anton (12 June 2017). "WIN32/INDUSTROYER A new threat for industrial control systems" (PDF). welivesecurity.com. ESET.*

- ENISA *"Protecting Industrial Control Systems. Recommendations for Europe and Member States". 14 December 2011.*
- U.S. DEPARTMENT OF HOMELAND SECURITY *"Recommended Practice: Developing an Industrial Control Systems, Cybersecurity Incident Response Capability" (PDF). 1 October 2009.*
- *Andy Greenberg (20 June 2017). "How an Entire Nation Became Russia's Test Lab For Cyberwar". Wired.*
- *Michael McFail; Jordan Hanna; Daniel Rebori-Carretero (December 2021). "Detection Engineering in Industrial Control Systems- Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study". mitre.org. MITRE.*

Categories:

- Windows trojans
- Cyberattacks on energy sector
- 2010s in hacking
- 2016 crimes in Ukraine
- Malware targeting industrial control systems