

2015 Ukraine Electric Power Attack | MITRE ATT&CK®

Источник: <https://attack.mitre.org/campaigns/Co028/>

Сохранено в архиве decolonial.ist: 29.08.2026 · файлов в оригинале: 1

2015 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used BlackEnergy (specifically BlackEnergy3) and KillDisk to target and disrupt transmission and distribution substations within the Ukrainian power grid. This campaign was the first major public attack conducted against the Ukrainian power grid by Sandworm Team.

ID		Name		Description
G0034		Sandworm Team		[2] [3]
Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	During the 2015 Ukraine Electric Power Attack, Sandworm Team used BlackEnergy to communicate between compromised hosts and their command-and-control servers via HTTP post requests. [1]
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	During the 2015 Ukraine Electric Power Attack, Sandworm Team installed a VBA script called <code>vba_macro.exe</code> . This macro dropped <code>FONTCACHE.DAT</code> , the primary BlackEnergy implant; <code>rundll32.exe</code> , for executing the malware; <code>NTUSER.log</code> , an empty file; and <code>desktop.ini</code> , the default file used to determine folder displays on Windows machines. [1]
Enterprise	T1136	.002	Create Account: Domain Account	During the 2015 Ukraine Electric Power Attack, Sandworm Team created privileged domain accounts to be used for further exploitation and lateral movement. [1]
Enterprise	T1685		Disable or Modify Tools	During the 2015 Ukraine Electric Power Attack, Sandworm Team modified in-registry internet settings to lower internet security. [1]
Enterprise	T1133		External Remote Services	During the 2015 Ukraine Electric Power Attack, Sandworm Team installed a modified Dropbear SSH client as the backdoor to target systems.[1]

Enterprise	T1070	.004	Indicator Removal: File Deletion	During the 2015 Ukraine Electric Power Attack, vba_macro.exe deletes itself after FONTCACHE.DAT , rundll32.exe , and the associated .lnk file is delivered. [1]
Enterprise	T1105		Ingress Tool Transfer	During the 2015 Ukraine Electric Power Attack, Sandworm Team pushed additional malicious tools onto an infected system to steal user credentials, move laterally, and destroy data. [1]
Enterprise	T1056	.001	Input Capture: Keylogging	During the 2015 Ukraine Electric Power Attack, Sandworm Team gathered account credentials via a BlackEnergy keylogger plugin. [1][4]
Enterprise	T1570		Lateral Tool Transfer	During the 2015 Ukraine Electric Power Attack, Sandworm Team moved their tools laterally within the corporate network and between the ICS and corporate network. [1]
Enterprise	T1112		Modify Registry	During the 2015 Ukraine Electric Power Attack, Sandworm Team modified in-registry Internet settings to lower internet security before launching rundll32.exe , which in-turn launches the malware and communicates with C2 servers over the Internet. [1].
Enterprise	T1040		Network Sniffing	During the 2015 Ukraine Electric Power Attack, Sandworm Team used BlackEnergy's network sniffer module to discover user credentials being sent over the network between the local LAN and the power grid's industrial control systems. [5]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	During the 2015 Ukraine Electric Power Attack, Sandworm Team obtained their initial foothold into many IT systems using Microsoft Office attachments delivered through phishing emails. [4]
Enterprise	T1055		Process Injection	During the 2015 Ukraine Electric Power Attack, Sandworm Team loaded BlackEnergy into svchost.exe, which then launched iexplore.exe for their C2. [1]
Enterprise	T1018		Remote System Discovery	During the 2015 Ukraine Electric Power Attack, Sandworm Team remotely discovered systems over LAN connections. OT systems were visible from the IT network as well, giving adversaries the ability to discover operational assets. [5]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	

				During the 2015 Ukraine Electric Power Attack, Sandworm Team used a backdoor which could execute a supplied DLL using rundll32.exe . [1]
Enterprise	T1204	.002	User Execution: Malicious File	During the 2015 Ukraine Electric Power Attack, Sandworm Team leveraged Microsoft Office attachments which contained malicious macros that were automatically executed once the user permitted them. [4]
Enterprise	T1078		Valid Accounts	During the 2015 Ukraine Electric Power Attack, Sandworm Team used valid accounts on the corporate network to escalate privileges, move laterally, and establish persistence within the corporate network. [4]
ICS	T1695	.001	Block Communications: Serial COM	During the 2015 Ukraine Electric Power Attack, Sandworm Team overwrote the serial-to-ethernet converter firmware, rendering the devices not operational. This meant that communication to the downstream serial devices was either not possible or more difficult. [1]
ICS	T1691	.001	Block Operational Technology Message: Command Message	During the 2015 Ukraine Electric Power Attack, Sandworm Team blocked command messages by using malicious firmware to render serial-to-ethernet converters inoperable. [4]
		.002	Block Operational Technology Message: Reporting Message	During the 2015 Ukraine Electric Power Attack, Sandworm Team blocked reporting messages by using malicious firmware to render serial-to-ethernet converters inoperable. [4]
ICS	To885		Commonly Used Port	During the 2015 Ukraine Electric Power Attack, Sandworm Team used port 443 to communicate with their C2 servers. [1]
ICS	To884		Connection Proxy	During the 2015 Ukraine Electric Power Attack, Sandworm Team established an internal proxy prior to the installation of backdoors within the network. [1]
ICS	To813		Denial of Control	During the 2015 Ukraine Electric Power Attack, KillDisk rendered devices that were necessary for remote recovery unusable, including at least one RTU. Additionally, Sandworm Team overwrote the firmware for serial-to-ethernet converters, denying operators control of the downstream devices. [1][4]
ICS	To814		Denial of Service	During the 2015 Ukraine Electric Power Attack, power company phone line operators were hit with a denial of service attack so that they couldn't field customers' calls about outages. Operators were also denied service to their downstream devices when their serial-to-ethernet

				converters had their firmware overwritten, which bricked the devices. [4]
ICS	To816		Device Restart/ Shutdown	During the 2015 Ukraine Electric Power Attack, Sandworm Team scheduled the uninterruptable power supplies (UPS) to shutdown data and telephone servers via the UPS management interface. [4][1]
ICS	To822		External Remote Services	During the 2015 Ukraine Electric Power Attack, Sandworm Team used Valid Accounts taken from the Windows Domain Controller to access the control system Virtual Private Network (VPN) used by grid operators. [1]
ICS	To823		Graphical User Interface	During the 2015 Ukraine Electric Power Attack, Sandworm Team utilized HMI GUIs in the SCADA environment to open breakers. [4]
ICS	To867		Lateral Tool Transfer	During the 2015 Ukraine Electric Power Attack, Sandworm Team moved their tools laterally within the ICS network. [1]
ICS	To826		Loss of Availability	During the 2015 Ukraine Electric Power Attack, Sandworm Team opened the breakers at the infected sites, shutting the power off for thousands of businesses and households for around 6 hours. [4][1]
ICS	To827		Loss of Control	During the 2015 Ukraine Electric Power Attack, operators were shut out of their equipment either through the denial of peripheral use or the degradation of equipment. Operators were therefore unable to recover from the incident through their traditional means. Much of the power was restored manually. [4]
ICS	To828		Loss of Productivity and Revenue	During the 2015 Ukraine Electric Power Attack, power breakers were opened which caused the operating companies to be unable to deliver power, and left thousands of businesses and households without power for around 6 hours. [4][1]
ICS	To831		Manipulation of Control	During the 2015 Ukraine Electric Power Attack, Sandworm Team opened live breakers via remote commands to the HMI, causing blackouts. [4]
ICS	T1693	.001	Modify Firmware: System Firmware	During the 2015 Ukraine Electric Power Attack, Sandworm Team overwrote the serial-to-ethernet gateways with custom firmware to make systems either disabled, shutdown, and/or unrecoverable. [4]
ICS	To886		Remote Services	During the 2015 Ukraine Electric Power Attack, Sandworm Team used an IT helpdesk software to move the mouse on ICS control devices to maliciously release electricity breakers. [2]

ICS	To846		Remote System Discovery	During the 2015 Ukraine Electric Power Attack, Sandworm Team remotely discovered operational assets once on the OT network. [5] [1]
ICS	To859		Valid Accounts	During the 2015 Ukraine Electric Power Attack, Sandworm Team used valid accounts to laterally move through VPN connections and dual-homed systems. Sandworm Team used the credentials of valid accounts to interact with client applications and access employee workstations hosting HMI applications. [4][1]

- Booz Allen Hamilton. (2016). When The Lights Went Out. Retrieved December 18, 2024.
- Andy Greenberg. (2017, June 28). How an Entire Nation Became Russia's Test Lab for Cyberwar. Retrieved September 27, 2023.
- Scott W. Brady. (2020, October 15). United States vs. Yuriy Sergeyevich Andrienko et al.. Retrieved November 25, 2020.
- Electricity Information Sharing and Analysis Center; SANS Industrial Control Systems. (2016, March 18). Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case. Retrieved March 27, 2018.
- Charles McLellan. (2016, March 4). How hackers attacked Ukraine's power grid: Implications for Industrial IoT security. Retrieved September 27, 2023.