2016 Ukraine Electric Power Attack | MITRE ATT&CK®

2016 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used Industroyer malware to target and disrupt distribution substations within the Ukrainian power grid. This campaign was the second major public attack conducted against Ukraine by Sandworm Team.[1] [2]

ID	Name	Description
G0034	Sandworm Team	[3][4]

Domain	ID		Name	Use
Enterprise	T1098		Account Manipulation	During the 2016 Ukraine Electric Power Attack, Sandworm Team used the `sp_addlinkedsrvlogin` command in MS-SQL to create a link between a created account and other servers in the network.[2]
Enterprise	T1110		Brute Force	During the 2016 Ukraine Electric Power Attack, Sandworm Team used a script to attempt RPC authentication against a number of hosts.[2]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	During the 2016 Ukraine Electric Power Attack, Sandworm Team used PowerShell scripts to run a credential harvesting tool in memory to evade defenses.[2]
		.003	Command and Scripting Interpreter: Windows Command Shell	During the 2016 Ukraine Electric Power Attack, Sandworm Team used the `xp_cmdshell` command in MS-SQL.[2]
		.005	Command and Scripting Interpreter: Visual Basic	During the 2016 Ukraine Electric Power Attack, Sandworm Team created VBScripts to run on an SSH server.[2]
Enterprise	T1554		Compromise Host Software Binary	During the 2016 Ukraine Electric Power Attack, Sandworm Team used a trojanized version of Windows Notepad to add a layer of persistence for Industroyer.[1]

Enterprise	T1136		Create Account	During the 2016 Ukraine Electric Power Attack, Sandworm Team added a login to a SQL Server with `sp_addlinkedsrvlogin` .[2]
		.002	Domain Account	During the 2016 Ukraine Electric Power Attack, Sandworm Team created two new accounts, "admin" and "система" (System). The accounts were then assigned to a domain matching local operation and were delegated new privileges.[2]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	During the 2016 Ukraine Electric Power Attack, Sandworm Team used an arbitrary system service to load at system boot for persistence for Industroyer. They also replaced the ImagePath registry value of a Windows service with a new backdoor binary. [5]
Enterprise	T1685	.001	Disable or Modify Tools: Disable or Modify Windows Event Log	During the 2016 Ukraine Electric Power Attack, Sandworm Team disabled event logging on compromised systems.[2]
Enterprise	T1570		Lateral Tool Transfer	During the 2016 Ukraine Electric Power Attack, Sandworm Team used `move` to transfer files to a network share.[2]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	During the 2016 Ukraine Electric Power Attack, DLLs and EXEs with filenames associated with common electric power sector protocols were used to masquerade files.[5]
		.008	Masquerading: Masquerade File Type	During the 2016 Ukraine Electric Power Attack, Sandworm Team masqueraded executables as `.txt` files.[2]
		.010	Masquerading: Masquerade Account Name	During the 2016 Ukraine Electric Power Attack, Sandworm Team created two new accounts, "admin" and "система" (System).[2]
Enterprise	T1027		Obfuscated Files or Information	During the 2016 Ukraine Electric Power Attack, Sandworm Team used heavily obfuscated code with Industroyer in its Windows Notepad backdoor.[1]
		.002	Software Packing	During the 2016 Ukraine Electric Power Attack, Sandworm Team used UPX to pack a copy of Mimikatz.[2]
Enterprise	T1003	.001		

			OS Credential Dumping: LSASS Memory	During the 2016 Ukraine Electric Power Attack, Sandworm Team used Mimikatz to capture and use legitimate credentials.[2]
Enterprise	T1021	.002	Remote Services: SMB/ Windows Admin Shares	During the 2016 Ukraine Electric Power Attack, Sandworm Team utilized `net use` to connect to network shares.[2]
Enterprise	T1018		Remote System Discovery	During the 2016 Ukraine Electric Power Attack, Sandworm Team checked for connectivity to resources within the network and used LDAP to query Active Directory, discovering information about computers listed in AD.[2]
Enterprise	T1505	.001	Server Software Component: SQL Stored Procedures	During the 2016 Ukraine Electric Power Attack, Sandworm Team used various MS-SQL stored procedures.[2]
Enterprise	T1047		Windows Management Instrumentation	During the 2016 Ukraine Electric Power Attack, WMI in scripts were used for remote execution and system surveys.[2]
ICS	T0807		Command-Line Interface	During the 2016 Ukraine Electric Power Attack, Sandworm Team supplied the name of the payload DLL to Industroyer via a command line parameter.[1]
ICS	T0867		Lateral Tool Transfer	During the 2016 Ukraine Electric Power Attack, Sandworm Team used a VBS script to facilitate lateral tool transfer. The VBS script was used to copy ICS-specific payloads with the following command: `cscript C:\Backinfo\ufn.vbs C: \Backinfo\101.dll C:\Delta\101.dll` [2]
ICS	T0849		Masquerading	During the 2016 Ukraine Electric Power Attack, Sandworm Team transferred executable files as .txt and then renamed them to .exe, likely to avoid detection through extension tracking.[2]
ICS	T0886		Remote Services	During the 2016 Ukraine Electric Power Attack, Sandworm Team used MS-SQL access to a pivot machine, allowing code execution throughout the ICS network.[2]
ICS	T0853		Scripting	During the 2016 Ukraine Electric Power Attack, Sandworm Team utilized VBS and batch scripts for file movement and as wrappers for PowerShell execution.[2]
ICS	T0859		Valid Accounts	During the 2016 Ukraine Electric Power Attack, Sandworm Team used valid accounts to laterally move through VPN connections and dual-homed systems.[2]

ID	Name	Description
S0604	Industroyer	Within the 2016 Ukraine Electric Power Attack, Industroyer was used to target and disrupt the Ukrainian power grid substation components.[2][1]

- Anton Cherepanov. (2017, June 12). Win32/Industroyer: A new threat for industrial controls systems. Retrieved December 18, 2020.
- Joe Slowik. (2018, October 12). Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE. Retrieved December 18, 2020.
- Scott W. Brady. (2020, October 15). United States vs. Yuriy Sergeyevich Andrienko et al.. Retrieved November 25, 2020.