Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Seashell Blizzard, FROZENBARENTS, APT44, Group G0034

Archived: 2026-04-05 13:34:31 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

Sandworm Team has used a tool to query Active Directory using LDAP, discovering information about usernames listed in AD.[22]

.003 Account Discovery: Email Account

Sandworm Team used malware to enumerate email settings, including usernames and passwords, from the M.E.Doc application.[23]

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.[18]

Enterprise T1583 Acquire Infrastructure

Sandworm Team used various third-party email campaign management services to deliver phishing emails.[13]

.001 Domains

Sandworm Team has registered domain names and created URLs that are often designed to mimic or spoof legitimate websites, such as email login pages, online file sharing and storage websites, and password reset pages, while also hosting these items on legitimate, compromised network infrastructure.[1][24]

.004 Server

Sandworm Team has leased servers from resellers instead of leasing infrastructure directly from hosting companies to enable its operations.[1]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

Sandworm Team has scanned network infrastructure for vulnerabilities as part of its operational planning.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Sandworm Team's BCS-server tool connects to the designated C2 server via HTTP.[22]

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. [15]

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.[18]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Sandworm Team has used PowerShell scripts to run a credential harvesting tool in memory to evade defenses.[1] [18]

During the 2016 Ukraine Electric Power Attack, Sandworm Team used PowerShell scripts to run a credential harvesting tool in memory to evade defenses.[18]

During the 2022 Ukraine Electric Power Attack, Sandworm Team utilized a PowerShell utility called TANKTRAP to spread and launch a wiper using Windows Group Policy.[20]

.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. [18]

.005 Command and Scripting Interpreter: Visual Basic

Sandworm Team has created VBScripts to run an SSH server.[25][22][26][18]

During the 2015 Ukraine Electric Power Attack, Sandworm Team installed a VBA script called `vba_macro.exe`. This macro dropped `FONTCACHE.DAT`, the primary BlackEnergy implant; `rundll32.exe`, for executing the malware; `NTUSER.log`, an empty file; and desktop.ini, the default file used to determine folder displays on Windows machines. [15]

During the 2016 Ukraine Electric Power Attack, Sandworm Team created VBScripts to run on an SSH server.[18]

Enterprise T1586 .001 Compromise Accounts: Social Media Accounts

Sandworm Team creates credential capture webpages to compromise existing, legitimate social media accounts. [24]

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.[17]

Enterprise T1584 .004 Compromise Infrastructure: Server

Sandworm Team compromised legitimate Linux servers running the EXIM mail transfer agent for use in subsequent campaigns.[27][13]

.005 Compromise Infrastructure: Botnet

Sandworm Team has used a large-scale botnet to target Small Office/Home Office (SOHO) network devices.[28]

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. [15]

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.[18]

Enterprise T1543 .002 Create or Modify System Process: Systemd Service

During the 2022 Ukraine Electric Power Attack, Sandworm Team configured Systemd to maintain persistence of GOGETTER, specifying the `WantedBy=multi-user.target` configuration to run GOGETTER when the system begins accepting user logins.[20]

.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. [29]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Sandworm Team's CredRaptor tool can collect saved passwords from various internet browsers.[22]

Enterprise T1485 Data Destruction

Sandworm Team has used CaddyWiper, SDelete, and the BlackEnergy KillDisk component to overwrite files on victim systems. [30][26][20] Additionally, Sandworm Team has used the JUNKMAIL tool to overwrite files with null bytes.[14]

During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed CaddyWiper on the victim’s IT environment systems to wipe files related to the OT capabilities, along with mapped drives, and physical drive partitions.[20]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Sandworm Team's BCS-server tool uses base64 encoding and HTML tags for the communication traffic between the C2 server.[22]

Enterprise T1486 Data Encrypted for Impact

Sandworm Team has used Prestige ransomware to encrypt data at targeted organizations in transportation and related logistics industries in Ukraine and Poland.[11]

Enterprise T1213 .006 Data from Information Repositories: Databases

Sandworm Team exfiltrates data of interest from enterprise databases using Adminer.[13]

Enterprise T1005 Data from Local System

Sandworm Team has exfiltrated internal documents, files, and other data from compromised hosts.[1]

Enterprise T1491 .002 Defacement: External Defacement

Sandworm Team defaced approximately 15,000 websites belonging to Georgian government, non-government, and private sector organizations in 2019.[1][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Sandworm Team's VBS backdoor can decode Base64-encoded data and save it to the %TEMP% folder. The group also decrypted received information using the Triple DES algorithm and decompresses it using GZip.[22][23]

Enterprise T1587 .001 Develop Capabilities: Malware

Sandworm Team has developed malware for its operations, including malicious mobile applications and destructive malware such as NotPetya and Olympic Destroyer.[1]

Enterprise T1561 .002 Disk Wipe: Disk Structure Wipe

Sandworm Team has used the BlackEnergy KillDisk component to corrupt the infected system's master boot record.[30][26]

Enterprise T1484 .001 Domain or Tenant Policy Modification: Group Policy Modification

During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Group Policy Objects (GPOs) to deploy and execute malware.[20]

Enterprise T1499 Endpoint Denial of Service

Sandworm Team temporarily disrupted service to Georgian government, non-government, and private sector websites after compromising a Georgian web hosting provider in 2019.[1]

Enterprise T1585 .001 Establish Accounts: Social Media Accounts

Sandworm Team has established social media accounts to disseminate victim internal-only documents and other sensitive data.[1]

.002 Establish Accounts: Email Accounts

Sandworm Team has created email accounts that mimic legitimate organizations for its spearphishing operations. [1]

Enterprise T1041 Exfiltration Over C2 Channel

Sandworm Team has sent system information to its C2 server using HTTP.[22]

Enterprise T1190 Exploit Public-Facing Application

Sandworm Team exploits public-facing applications for initial access and to acquire infrastructure, such as exploitation of the EXIM mail transfer agent in Linux systems.[27][13]

Enterprise T1203 Exploitation for Client Execution

Sandworm Team has exploited vulnerabilities in Microsoft PowerPoint via OLE objects (CVE-2014-4114) and Microsoft Word via crafted TIFF images (CVE-2013-3906).[31][32][33]

Enterprise T1133 External Remote Services

Sandworm Team has used Dropbear SSH with a hardcoded backdoor password to maintain persistence within the target network. Sandworm Team has also used VPN tunnels established in legitimate software company infrastructure to gain access to internal networks of that software company's users.[25][26][34][14]

During the 2015 Ukraine Electric Power Attack, Sandworm Team installed a modified Dropbear SSH client as the backdoor to target systems.[15]

Enterprise T1083 File and Directory Discovery

Sandworm Team has enumerated files on a compromised host.[1][18]

Enterprise T1592 .002 Gather Victim Host Information: Software

Sandworm Team has researched software code to enable supply-chain operations, most notably for the 2017 NotPetya attack. Sandworm Team also collected a list of computers using specific software as part of its targeting efforts.[1]

Enterprise T1589 .002 Gather Victim Identity Information: Email Addresses

Sandworm Team has obtained valid emails addresses while conducting research against target organizations that were subsequently used in spearphishing campaigns.[1]

.003 Gather Victim Identity Information: Employee Names

Sandworm Team's research of potential victim organizations included the identification and collection of employee information.[1]

Enterprise T1590 .001 Gather Victim Network Information: Domain Properties

Sandworm Team conducted technical reconnaissance of the Parliament of Georgia's official internet domain prior to its 2019 attack.[1]

Enterprise T1591 .002 Gather Victim Org Information: Business Relationships

In preparation for its attack against the 2018 Winter Olympics, Sandworm Team conducted online research of partner organizations listed on an official PyeongChang Olympics partnership site.[1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

During the 2015 Ukraine Electric Power Attack, Sandworm Team modified in-registry internet settings to lower internet security. [15]

.002 Impair Defenses: Disable Windows Event Logging

During the 2016 Ukraine Electric Power Attack, Sandworm Team disabled event logging on compromised systems.[18]

Enterprise T1070 .004 Indicator Removal: File Deletion

Sandworm Team has used backdoors that can delete files used in an attack from an infected system.[22][23][20]

During the 2015 Ukraine Electric Power Attack, vba_macro.exe deletes itself after `FONTCACHE.DAT`, `rundll32.exe`, and the associated .lnk file is delivered. [15]

Enterprise T1105 Ingress Tool Transfer

Sandworm Team has pushed additional malicious tools onto an infected system to steal user credentials, move laterally, and destroy data.[22][1]

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. [15]

Enterprise T1490 Inhibit System Recovery

Sandworm Team uses Prestige to delete the backup catalog from the target system using: `C:\Windows\System32\wbadmin.exe delete catalog -quiet` and to delete volume shadow copies using: `C:\Windows\System32\vssadmin.exe delete shadows /all /quiet`. [11]

Enterprise T1056 .001 Input Capture: Keylogging

Sandworm Team has used a keylogger to capture keystrokes by using the SetWindowsHookEx function.[22]

During the 2015 Ukraine Electric Power Attack, Sandworm Team gathered account credentials via a BlackEnergy keylogger plugin. [15][35]

Enterprise T1570 Lateral Tool Transfer

Sandworm Team has used `move` to transfer files to a network share and has copied payloads--such as Prestige ransomware--to an Active Directory Domain Controller and distributed via the Default Domain Group Policy Object.[18][11] Additionally, Sandworm Team has transferred an ISO file into the OT network to gain initial access.[20]

During the 2015 Ukraine Electric Power Attack, Sandworm Team moved their tools laterally within the corporate network and between the ICS and corporate network. [15]

During the 2016 Ukraine Electric Power Attack, Sandworm Team used `move` to transfer files to a network share.[18]

During the 2022 Ukraine Electric Power Attack, Sandworm Team used a Group Policy Object (GPO) to copy CaddyWiper's executable `msserver.exe` from a staging server to a local hard drive before deployment.[20]

Enterprise T1036 Masquerading

Sandworm Team masqueraded malicious installers as Windows update packages to evade defense and entice users to execute binaries.[13]

.004 Masquerade Task or Service

During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Systemd service units to masquerade GOGETTER malware as legitimate or seemingly legitimate services.[20]

.005 Match Legitimate Resource Name or Location

Sandworm Team has avoided detection by naming a malicious binary explorer.exe.[22][1]

During the 2016 Ukraine Electric Power Attack, DLLs and EXEs with filenames associated with common electric power sector protocols were used to masquerade files.[29]

.008 Masquerade File Type

During the 2016 Ukraine Electric Power Attack, Sandworm Team masqueraded executables as `.txt` files.[18]

.010 Masquerade Account Name

During the 2016 Ukraine Electric Power Attack, Sandworm Team created two new accounts, "admin" and "система" (System).[18]

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. [15].

Enterprise T1106 Native API

Sandworm Team uses Prestige to disable and restore file system redirection by using the following functions: `Wow64DisableWow64FsRedirection()` and `Wow64RevertWow64FsRedirection()`.[11]

Enterprise T1040 Network Sniffing

Sandworm Team has used intercepter-NG to sniff passwords in network traffic.[22]

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. [36]

Enterprise T1095 Non-Application Layer Protocol

During the 2022 Ukraine Electric Power Attack, Sandworm Team proxied C2 communications within a TLS-based tunnel.[20]

Enterprise T1571 Non-Standard Port

Sandworm Team has used port 6789 to accept connections on the group's SSH server.[25]

Enterprise T1027 Obfuscated Files or Information

Sandworm Team has used Base64 encoding within malware variants.[31]

During the 2016 Ukraine Electric Power Attack, Sandworm Team used heavily obfuscated code with Industroyer in its Windows Notepad backdoor.[17]

.002 Software Packing

During the 2016 Ukraine Electric Power Attack, Sandworm Team used UPX to pack a copy of Mimikatz.[18]

.010 Command Obfuscation

Sandworm Team has used ROT13 encoding, AES encryption and compression with the zlib library for their Python-based backdoor.[22]

Enterprise T1588 .002 Obtain Capabilities: Tool

Sandworm Team has acquired open-source tools for their operations, including Invoke-PSImage, which was used to establish an encrypted channel from a compromised host to Sandworm Team's C2 server in preparation for the 2018 Winter Olympics attack, as well as Impacket and RemoteExec, which were used in their 2022 Prestige operations.[1][11] Additionally, Sandworm Team has used Empire, Cobalt Strike and PoshC2.[14]

.006 Obtain Capabilities: Vulnerabilities

In 2017, Sandworm Team conducted technical research related to vulnerabilities associated with websites used by the Korean Sport and Olympic Committee, a Korean power company, and a Korean airport.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Sandworm Team has used its plainpwd tool, a modified version of Mimikatz, and comsvcs.dll to dump Windows credentials from system memory.[22][26][11]

During the 2016 Ukraine Electric Power Attack, Sandworm Team used Mimikatz to capture and use legitimate credentials.[18]

.003 OS Credential Dumping: NTDS

Sandworm Team has used `ntdsutil.exe` to back up the Active Directory database, likely for credential access. [11]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Sandworm Team has delivered malicious Microsoft Office and ZIP file attachments via spearphishing emails.[31] [30][22][1][37][14]

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. [35]

.002 Phishing: Spearphishing Link

Sandworm Team has crafted phishing emails containing malicious hyperlinks.[1]

Enterprise T1598 .003 Phishing for Information: Spearphishing Link

Sandworm Team has crafted spearphishing emails with hyperlinks designed to trick unwitting recipients into revealing their account credentials.[1]

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. [15]

Enterprise T1572 Protocol Tunneling

During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the GOGETTER tunneler software to establish a "Yamux" TLS-based C2 channel with an external server(s).[20]

Enterprise T1090 Proxy

Sandworm Team's BCS-server tool can create an internal proxy server to redirect traffic from the adversary-controlled C2 to internal servers which may not be connected to the internet, but are interconnected locally.[22]

Enterprise T1219 Remote Access Tools

Sandworm Team has used remote administration tools or remote industrial control system client software for execution and to maliciously release electricity breakers.[30][11]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

Sandworm Team has copied payloads to the `ADMIN$` share of remote systems and run `net use` to connect to network shares.[18][11]

During the 2016 Ukraine Electric Power Attack, Sandworm Team utilized `net use` to connect to network shares. [18]

Enterprise T1018 Remote System Discovery

Sandworm Team has used a tool to query Active Directory using LDAP, discovering information about computers listed in AD.[22][18]

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. [36]

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.[18]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Sandworm Team leveraged SHARPIVORY, a .NET dropper that writes embedded payload to disk and uses scheduled tasks to persist on victim machines.[14]

During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Scheduled Tasks through a Group Policy Object (GPO) to execute CaddyWiper at a predetermined time.[20]

Enterprise T1593 Search Open Websites/Domains

Sandworm Team researched Ukraine's unique legal entity identifier (called an "EDRPOU" number), including running queries on the EDRPOU website, in preparation for the NotPetya attack. Sandworm Team has also researched third-party websites to help it craft credible spearphishing emails.[1]

Enterprise T1594 Search Victim-Owned Websites

Sandworm Team has conducted research against potential victim websites as part of its operational planning.[1]

Enterprise T1505 .001 Server Software Component: SQL Stored Procedures

During the 2016 Ukraine Electric Power Attack, Sandworm Team used various MS-SQL stored procedures.[18]

.003 Server Software Component: Web Shell

Sandworm Team has used webshells including P.A.S. Webshell to maintain access to victim networks.[34]

During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the Neo-REGEORG webshell on an internet-facing server.[20]

Enterprise T1489 Service Stop

Sandworm Team attempts to stop the MSSQL Windows service to ensure successful encryption of locked files.[11]

Enterprise T1072 Software Deployment Tools

Sandworm Team has used the commercially available tool RemoteExec for agentless remote code execution.[11]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

Sandworm Team staged compromised versions of legitimate software installers in forums to enable initial access to executing user.[14]

Enterprise T1539 Steal Web Session Cookie

Sandworm Team used information stealer malware to collect browser session cookies.[13]

Enterprise T1195 Supply Chain Compromise

Sandworm Team staged compromised versions of legitimate software installers on forums to achieve initial, untargetetd access in victim environments.[14]

.002 Compromise Software Supply Chain

Sandworm Team has distributed NotPetya by compromising the legitimate Ukrainian accounting software M.E.Doc and replacing a legitimate software update with a malicious one.[38][26][1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Sandworm Team used a backdoor which could execute a supplied DLL using rundll32.exe.[23]

During the 2015 Ukraine Electric Power Attack, Sandworm Team used a backdoor which could execute a supplied DLL using `rundll32.exe`. [15]

Enterprise T1082 System Information Discovery

Sandworm Team used a backdoor to enumerate information about the infected system's operating system.[23][1]

Enterprise T1049 System Network Connections Discovery

Sandworm Team had gathered user, IP address, and server data related to RDP sessions on a compromised host. It has also accessed network diagram files useful for understanding how a host's network was configured.[1][18]

Enterprise T1033 System Owner/User Discovery

Sandworm Team has collected the username from a compromised host.[1]

Enterprise T1199 Trusted Relationship

Sandworm Team has used dedicated network connections from one victim organization to gain unauthorized access to a separate organization.[1] Additionally, Sandworm Team has accessed Internet service providers and telecommunication entities that provide mobile connectivity.[14]

Enterprise T1204 .001 User Execution: Malicious Link

Sandworm Team has tricked unwitting recipients into clicking on malicious hyperlinks within emails crafted to resemble trustworthy senders.[1]

.002 User Execution: Malicious File

Sandworm Team has tricked unwitting recipients into clicking on spearphishing attachments and enabling malicious macros embedded within files.[22][1]

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. [35]

Enterprise T1078 Valid Accounts

Sandworm Team have used previously acquired legitimate credentials prior to attacks.[30]

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. [35]

.002 Domain Accounts

Sandworm Team has used stolen credentials to access administrative accounts within the domain.[1][11]

Enterprise T1102 .002 Web Service: Bidirectional Communication

Sandworm Team has used the Telegram Bot API from Telegram Messenger to send and receive commands to its Python backdoor. Sandworm Team also used legitimate M.E.Doc software update check requests for sending and receiving commands and hosted malicious payloads on putdrive.com.[22][26]

Enterprise T1047 Windows Management Instrumentation

Sandworm Team has used Impacket's WMIexec module for remote code execution and VBScript to run WMI queries.[18][11]

During the 2016 Ukraine Electric Power Attack, WMI in scripts were used for remote execution and system surveys. [18]

Mobile T1676 Linked Devices

Sandworm Team has used the linked devices feature to connect Signal accounts on devices captured on the battlefield to adversary-controlled infrastructure for follow-on exploitation.[39]

Mobile T1660 Phishing

Sandworm Team used SMS-based phishing to target victims with malicious links.[13]

Mobile T1409 Stored Application Data

Sandworm Team can collect encrypted Telegram and Signal communications.[14]

ICS T0895 Autorun Image

During the 2022 Ukraine Electric Power Attack, Sandworm Team used existing hypervisor access to map an ISO image named `a.iso` to a virtual machine running a SCADA server. The SCADA server's operating system was configured to autorun CD-ROM images, and as a result, a malicious VBS script on the ISO image was automatically executed.[20]

ICS T0803 Block 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. [35]

ICS T0804 Block 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. [35]

ICS T0805 Block 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. [15]

ICS T0807 Command-Line Interface

Sandworm Team uses the MS-SQL server xp_cmdshell command, and PowerShell to execute commands. [40]

During the 2016 Ukraine Electric Power Attack, Sandworm Team supplied the name of the payload DLL to Industroyer via a command line parameter.[17]

During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged the SCIL-API on the MicroSCADA platform to execute commands through the `scilc.exe` binary.[20]

ICS T0885 Commonly Used Port

During the 2015 Ukraine Electric Power Attack, Sandworm Team used port 443 to communicate with their C2 servers. [15]

ICS T0884 Connection Proxy

Sandworm Team establishes an internal proxy prior to the installation of backdoors within the network. [41]

During the 2015 Ukraine Electric Power Attack, Sandworm Team established an internal proxy prior to the installation of backdoors within the network. [15]

ICS T0813 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. [15][35]

ICS T0814 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. [35]

ICS T0816 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. [35][15]

ICS T0819 Exploit Public-Facing Application

Sandworm Team actors exploited vulnerabilities in GE's Cimplicity HMI and Advantech/Broadwin WebAccess HMI software which had been directly exposed to the internet. [42] [43]

ICS T0822 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. [15]

ICS T0823 Graphical User Interface

During the 2015 Ukraine Electric Power Attack, Sandworm Team utilized HMI GUIs in the SCADA environment to open breakers. [35]

ICS T0867 Lateral Tool Transfer

During the 2015 Ukraine Electric Power Attack, Sandworm Team moved their tools laterally within the ICS network. [15]

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` [18]

ICS T0826 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. [35][15]

ICS T0827 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. [35]

ICS T0828 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. [35][15]

ICS T0831 Manipulation of Control

During the 2015 Ukraine Electric Power Attack, Sandworm Team opened live breakers via remote commands to the HMI, causing blackouts. [35]

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.[18]

ICS T0886 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. [16]

During the 2016 Ukraine Electric Power Attack, Sandworm Team used MS-SQL access to a pivot machine, allowing code execution throughout the ICS network.[18]

ICS T0846 Remote System Discovery

During the 2015 Ukraine Electric Power Attack, Sandworm Team remotely discovered operational assets once on the OT network. [36] [15]

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.[18]

During the 2022 Ukraine Electric Power Attack, Sandworm Team utilizes a Visual Basic script `lun.vbs` to execute `n.bat` which then executed the MicroSCADA `scilc.exe` command.[20]

ICS T0894 System Binary Proxy Execution

During the 2022 Ukraine Electric Power Attack, Sandworm Team executed a MicroSCADA application binary `scilc.exe` to send a predefined list of SCADA instructions specified in a file defined by the adversary, `s1.txt`. The executed command `C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt` leverages the SCADA software to send unauthorized command messages to remote substations.[20]

ICS T0857 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. [35]

ICS T0855 Unauthorized Command Message

During the 2015 Ukraine Electric Power Attack, Sandworm Team issued unauthorized commands to substation breaks after gaining control of operator workstations and accessing a distribution management system (DMS) application. [35]

During the 2022 Ukraine Electric Power Attack, Sandworm Team used the MicroSCADA SCIL-API to specify a set of SCADA instructions, including the sending of unauthorized commands to substation devices.[20]

ICS T0859 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. [35][15]

During the 2016 Ukraine Electric Power Attack, Sandworm Team used valid accounts to laterally move through VPN connections and dual-homed systems.[18]
