Industroyer, Software S0604 | MITRE ATT&CK®

Archived: 2026-04-02 11:58:57 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Industroyer's main backdoor connected to a remote C2 server using HTTPS.[1]

Enterprise T1554 Compromise Host Software Binary

Industroyer has used a Trojanized version of the Windows Notepad application for an additional backdoor persistence mechanism.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Industroyer can use an arbitrary system service to load at system boot for persistence and replaces the ImagePath registry value of a Windows service with a new backdoor binary.[2]

Enterprise T1485 Data Destruction

Industroyer's data wiper module clears registry keys and overwrites both ICS configuration and Windows files.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Industroyer decrypts code to connect to a remote C2 server.[1]

Enterprise T1499 .004 Endpoint Denial of Service: Application or System Exploitation

Industroyer uses a custom DoS tool that leverages CVE-2015-5374 and targets hardcoded IP addresses of Siemens SIPROTEC devices.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Industroyer sends information about hardware profiles and previously-received commands back to the C2 server in a POST-request.[1]

Enterprise T1083 File and Directory Discovery

Industroyer's data wiper component enumerates specific files on all the Windows drives.[1]

Enterprise T1105 Ingress Tool Transfer

Industroyer downloads a shellcode payload from a remote C2 server and loads it into memory.[1]

Enterprise T1046 Network Service Discovery

Industroyer uses a custom port scanner to map out a network.[1]

Enterprise T1027 Obfuscated Files or Information

Industroyer uses heavily obfuscated code in its Windows Notepad backdoor.[1]

Enterprise T1572 Protocol Tunneling

Industroyer attempts to perform an HTTP CONNECT via an internal proxy to establish a tunnel.[2]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

Industroyer used Tor nodes for C2.[2]

Enterprise T1012 Query Registry

Industroyer has a data wiper component that enumerates keys in the Registry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`.[1]

Enterprise T1018 Remote System Discovery

Industroyer can enumerate remote computers in the compromised network.[1]

Enterprise T1489 Service Stop

Industroyer's data wiper module writes zeros into the registry keys in `SYSTEM\CurrentControlSet\Services` to render a system inoperable.[2]

Enterprise T1082 System Information Discovery

Industroyer collects the victim machine's Windows GUID.[2]

Enterprise T1016 System Network Configuration Discovery

Industroyer's 61850 payload component enumerates connected network adapters and their corresponding IP addresses.[1]

Enterprise T1078 Valid Accounts

Industroyer can use supplied user credentials to execute processes and stop services.[1]

ICS T0800 Activate Firmware Update Mode

The Industroyer SIPROTEC DoS module places the victim device into firmware update mode. This is a legitimate use case under normal circumstances, but in this case is used the adversary to prevent the SIPROTEC from performing its designed protective functions. As a result the normal safeguards are disabled, leaving an unprotected link in the electric transmission. [4]

ICS T0802 Automated Collection

Industroyer automatically collects protocol object data to learn about control devices in the environment. [5]

ICS T0803 Block Command Message

In Industroyer the first COM port from the configuration file is used for the actual communication and the two other COM ports are just opened to prevent other processes accessing them. Thus, the IEC 101 payload component is able to take over and maintain control of the RTU device. [5]

ICS T0804 Block Reporting Message

Industroyer uses the first COM port from the configuration file for the communication and the other two COM ports are opened to prevent other processes accessing them. This may block processes or operators from getting reporting messages from a device. [5]

ICS T0805 Block Serial COM

In Industroyer the first COM port from the configuration file is used for the actual communication and the two other COM ports are just opened to prevent other processes accessing them. Thus, the IEC 101 payload component is able to take over and maintain control of the RTU device. [5]

ICS T0806 Brute Force I/O

The Industroyer IEC 104 module has 3 modes available to perform its attack. These modes are range, shift, and sequence. The range mode operates in 2 stages. The first stage of range mode gathers Information Object Addresses (IOA) and sends select and execute packets to switch the state. The second stage of range mode has an infinite loop where it will switch the state of all of the previously discovered IOAs. Shift mode is similar to range mode, but instead of staying within the same range, it will add a shift value to the default range values. [5]

ICS T0807 Command-Line Interface

The name of the Industroyer payload DLL is supplied by the attackers via a command line parameter supplied in one of the main backdoors execute a shell command commands. [5]

ICS T0884 Connection Proxy

Industroyer attempts to connect with a hardcoded internal proxy on TCP 3128 [default Squid proxy]. If established, the backdoor attempts to reach an external C2 server via the internal proxy. [6]

ICS T0809 Data Destruction

Industroyer has a destructive wiper that overwrites all ICS configuration files across the hard drives and all mapped network drives specifically targeting ABB PCM600 configuration files. [6]

ICS T0813 Denial of Control

Industroyer is able to block serial COM channels temporarily causing a denial of control. [5]

ICS T0814 Denial of Service

The Industroyer SIPROTEC DoS module exploits the CVE-2015-5374 vulnerability in order to render a Siemens SIPROTEC device unresponsive. Once this vulnerability is successfully exploited, the target device stops responding to any commands until it is rebooted manually. [5] Once the tool is executed it sends specifically crafted packets to port 50,000 of the target IP addresses using UDP. The UDP packet contains the following 18 byte payload: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E. [5]

ICS T0815 Denial of View

Industroyer is able to block serial COM channels temporarily causing a denial of view. [5]

ICS T0816 Device Restart/Shutdown

The Industroyer SIPROTEC DoS module exploits the CVE-2015-5374 vulnerability in order to render a Siemens SIPROTEC device unresponsive. While the vulnerability does not directly cause the restart or shutdown of the device, the device must be restarted manually before it can resume operations. [5]

ICS T0827 Loss of Control

Industroyer's data wiper component removes the registry image path throughout the system and overwrites all files, rendering the system unusable. [5]

ICS T0837 Loss of Protection

Industroyer contained a module which leveraged a vulnerability in the Siemens SIPROTEC relays (CVE-2015-5374) to create a Denial of Service against automated protective relays. [4]

ICS T0829 Loss of View

Industroyer's data wiper component removes the registry image path throughout the system and overwrites all files, rendering the system unusable. [5]

ICS T0831 Manipulation of Control

Industroyer toggles breakers to the open state utilizing unauthorized command messages. [5]

ICS T0832 Manipulation of View

Industroyer's OPC module can brute force values and will send out a 0x01 status which for the target systems equates to a Primary Variable Out of Limits misdirecting operators from understanding protective relay status. [5]

ICS T0801 Monitor Process State

Industroyer's OPC and IEC 61850 protocol modules include the ability to send stVal requests to read the status of operational variables. [5]

ICS T0840 Network Connection Enumeration

Industroyer contains an IEC 61850 module that enumerates all connected network adapters to determine their TCP/IP subnet masks. [5]

ICS T0846 Remote System Discovery

The Industroyer IEC 61850 payload component has the ability to discover relevant devices in the infected host's network subnet by attempting to connect on port 102.[5]

Industroyer contains an OPC DA module that enumerates all OPC servers using the `ICatInformation::EnumClassesOfCategories` method with `CATID_OPCDAServer20` category identifier and `IOPCServer::GetStatus` to identify the ones running.

ICS T0888 Remote System Information Discovery

The Industroyer IEC 61850 component sends the domain-specific MMSgetNameList request to determine what logical nodes the device supports. It then searches the logical nodes for the CSW value, which indicates the device performs a circuit breaker or switch control function.[1]

Industroyer's OPC DA module also uses IOPCBrowseServerAddressSpace to look for items with the following strings: ctlSelOn, ctlOperOn, ctlSelOff, ctlOperOff, Pos and stVal.[1]

Industroyer IEC 60870-5-104 module includes a range mode to discover Information Object Addresses (IOAs) by enumerating through each.[1]

ICS T0881 Service Stop

Industroyer has the capability to stop a service itself, or to login as a user and stop a service as that user. [5]

ICS T0855 Unauthorized Command Message

Using its protocol payloads, Industroyer sends unauthorized commands to RTUs to change the state of equipment. [5]
