BlackEnergy, Software S0089 | MITRE ATT&CK®

Archived: 2026-04-05 17:17:29 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

BlackEnergy attempts to bypass default User Access Control (UAC) settings by exploiting a backward-compatibility setting found in Windows 7 and later.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

BlackEnergy communicates with its C2 server over HTTP.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

The BlackEnergy 3 variant drops its main DLL component and then creates a .lnk shortcut to that file in the startup folder.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

The BlackEnergy 3 variant drops its main DLL component and then creates a .lnk shortcut to that file in the startup folder.[1]

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

One variant of BlackEnergy creates a new service using either a hard-coded or randomly generated name.[1]

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

BlackEnergy has used a plug-in to gather credentials from web browsers including FireFox, Google Chrome, and Internet Explorer.[1][2]

Enterprise T1485 Data Destruction

BlackEnergy 2 contains a "Destroy" plug-in that destroys data stored on victim hard drives by overwriting file contents.[3][4]

Enterprise T1008 Fallback Channels

BlackEnergy has the capability to communicate over a backup channel via plus.google.com.[2]

Enterprise T1083 File and Directory Discovery

BlackEnergy gathers a list of installed apps from the uninstall program Registry. It also gathers registered mail, browser, and instant messaging clients from the Registry. BlackEnergy has searched for given file types.[1][2]

Enterprise T1574 .010 Hijack Execution Flow: Services File Permissions Weakness

One variant of BlackEnergy locates existing driver services that have been disabled and drops its driver component into one of those service's paths, replacing the legitimate executable. The malware then sets the hijacked service to start automatically to establish persistence.[1]

Enterprise T1070 Indicator Removal

BlackEnergy has removed the watermark associated with enabling the `TESTSIGNING` boot configuration option by removing the relevant strings in the `user32.dll.mui` of the system.[1]

.001 Clear Windows Event Logs

The BlackEnergy component KillDisk is capable of deleting Windows Event Logs.[5]

Enterprise T1056 .001 Input Capture: Keylogging

BlackEnergy has run a keylogger plug-in on a victim.[2]

Enterprise T1046 Network Service Discovery

BlackEnergy has conducted port scans on a host.[2]

Enterprise T1120 Peripheral Device Discovery

BlackEnergy can gather very specific information about attached USB devices, to include device instance ID and drive geometry.[2]

Enterprise T1057 Process Discovery

BlackEnergy has gathered a process list by using Tasklist.exe.[1][2][4]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

BlackEnergy injects its DLL component into svchost.exe.[1]

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

BlackEnergy has run a plug-in on a victim to spread through the local network by using PsExec and accessing admin shares.[2]

Enterprise T1113 Screen Capture

BlackEnergy is capable of taking screenshots.[2]

Enterprise T1553 .006 Subvert Trust Controls: Code Signing Policy Modification

BlackEnergy has enabled the `TESTSIGNING` boot configuration option to facilitate loading of a driver component.[1]

Enterprise T1082 System Information Discovery

BlackEnergy has used Systeminfo to gather the OS version, as well as information on the system configuration, BIOS, the motherboard, and the processor.[1][2]

Enterprise T1016 System Network Configuration Discovery

BlackEnergy has gathered information about network IP configurations using ipconfig.exe and about routing tables using route.exe.[1][2]

Enterprise T1049 System Network Connections Discovery

BlackEnergy has gathered information about local network connections using netstat.[1][2]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

BlackEnergy has used a plug-in to gather credentials stored in files on the host by various software programs, including The Bat! email client, Outlook, and Windows Credential Store.[1][2]

Enterprise T1047 Windows Management Instrumentation

A BlackEnergy 2 plug-in uses WMI to gather victim host details.[3]

ICS T0865 Spearphishing Attachment

BlackEnergy targeted energy sector organizations in a wide reaching email spearphishing campaign. Adversaries utilized malicious Microsoft Word documents attachments. [6]

ICS T0869 Standard Application Layer Protocol

BlackEnergy uses HTTP POST request to contact external command and control servers. [6]

ICS T0859 Valid Accounts

BlackEnergy utilizes valid user and administrator credentials, in addition to creating new administrator accounts to maintain presence. [6]
