BADNEWS, Software S0128 | MITRE ATT&CK®

Archived: 2026-04-05 17:16:40 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

BADNEWS establishes a backdoor over HTTP.[3]

Enterprise T1119 Automated Collection

BADNEWS monitors USB devices and copies files with certain extensions to a predefined directory.[2]

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

BADNEWS installs a registry Run key to establish persistence.[1]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

BADNEWS is capable of executing commands via cmd.exe.[1][2]

Enterprise T1132 Data Encoding

After encrypting C2 data, BADNEWS converts it into a hexadecimal representation and then encodes it into base64.[1]

.001 Standard Encoding

BADNEWS encodes C2 traffic with base64.[1][3][2]

Enterprise T1005 Data from Local System

When it first starts, BADNEWS crawls the victim's local drives and collects documents with the following extensions: .doc, .docx, .pdf, .ppt, .pptx, and .txt.[1][3]

Enterprise T1039 Data from Network Shared Drive

When it first starts, BADNEWS crawls the victim's mapped drives and collects documents with the following extensions: .doc, .docx, .pdf, .ppt, .pptx, and .txt.[1]

Enterprise T1025 Data from Removable Media

BADNEWS copies files with certain extensions from USB devices to a predefined directory.[2]

Enterprise T1074 .001 Data Staged: Local Data Staging

BADNEWS copies documents under 15MB found on the victim system to is the user's `%temp%\SMB\` folder. It also copies files from USB devices to a predefined directory.[1][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

BADNEWS encrypts C2 data with a ROR by 3 and an XOR by 0x23.[1][2]

Enterprise T1083 File and Directory Discovery

BADNEWS identifies files with certain extensions from USB devices, then copies them to a predefined directory.[2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

BADNEWS typically loads its DLL file into a legitimate signed Java or VMware executable.[1][3]

Enterprise T1105 Ingress Tool Transfer

BADNEWS is capable of downloading additional files through C2 channels, including a new version of itself.[1][3][2]

Enterprise T1056 .001 Input Capture: Keylogging

When it first starts, BADNEWS spawns a new thread to log keystrokes.[1][3][2]

Enterprise T1036 .001 Masquerading: Invalid Code Signature

BADNEWS is sometimes signed with an invalid Authenticode certificate in an apparent effort to make it look more legitimate.[2]

.005 Masquerading: Match Legitimate Resource Name or Location

BADNEWS attempts to hide its payloads using legitimate filenames.[3]

Enterprise T1106 Native API

BADNEWS has a command to download an .exe and execute it via CreateProcess API. It can also run with ShellExecute.[1][2]

Enterprise T1120 Peripheral Device Discovery

BADNEWS checks for new hard drives on the victim, such as USB devices, by listening for the WM_DEVICECHANGE window message.[1][2]

Enterprise T1055 .012 Process Injection: Process Hollowing

BADNEWS has a command to download an .exe and use process hollowing to inject it into a new process.[1][2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

BADNEWS creates a scheduled task to establish by executing a malicious payload every subsequent minute.[3]

Enterprise T1113 Screen Capture

BADNEWS has a command to take a screenshot and send it to the C2 server.[1][3]

Enterprise T1102 .001 Web Service: Dead Drop Resolver

BADNEWS collects C2 information via a dead drop resolver.[1][3][2]

.002 Web Service: Bidirectional Communication

BADNEWS can use multiple C2 channels, including RSS feeds, Github, forums, and blogs.[1][3][2]
