ADVSTORESHELL, Software S0045 | MITRE ATT&CK®

Archived: 2026-04-05 15:37:53 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

ADVSTORESHELL connects to port 80 of a C2 server using Wininet API. Data is exchanged via HTTP POSTs. [1]

Enterprise T1560 Archive Collected Data

ADVSTORESHELL encrypts with the 3DES algorithm and a hardcoded key prior to exfiltration.[2]

.003 Archive via Custom Method

ADVSTORESHELL compresses output data generated by command execution with a custom implementation of the Lempel–Ziv–Welch (LZW) algorithm.[2]

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

ADVSTORESHELL achieves persistence by adding itself to the `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` Registry key.[1][2][3]

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

ADVSTORESHELL can create a remote shell and run a given command.[2][3]

Enterprise T1132 .001 Data Encoding: Standard Encoding

C2 traffic from ADVSTORESHELL is encrypted, then encoded with Base64 encoding.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

ADVSTORESHELL stores output from command execution in a .dat file in the %TEMP% directory.[2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

A variant of ADVSTORESHELL encrypts some C2 with 3DES.[3]

.002 Encrypted Channel: Asymmetric Cryptography

A variant of ADVSTORESHELL encrypts some C2 with RSA.[3]

Enterprise T1546 .015 Event Triggered Execution: Component Object Model Hijacking

Some variants of ADVSTORESHELL achieve persistence by registering the payload as a Shell Icon Overlay handler COM object.[2]

Enterprise T1041 Exfiltration Over C2 Channel

ADVSTORESHELL exfiltrates data over the same channel used for C2.[2]

Enterprise T1083 File and Directory Discovery

ADVSTORESHELL can list files and directories.[2][3]

Enterprise T1070 .004 Indicator Removal: File Deletion

ADVSTORESHELL can delete files and directories.[2]

Enterprise T1056 .001 Input Capture: Keylogging

ADVSTORESHELL can perform keylogging.[2][3]

Enterprise T1112 Modify Registry

ADVSTORESHELL is capable of setting and deleting Registry values.[3]

Enterprise T1106 Native API

ADVSTORESHELL is capable of starting a process using CreateProcess.[3]

Enterprise T1027 Obfuscated Files or Information

Most of the strings in ADVSTORESHELL are encrypted with an XOR-based algorithm; some strings are also encrypted with 3DES and reversed. API function names are also reversed, presumably to avoid detection in memory.[1][3]

Enterprise T1120 Peripheral Device Discovery

ADVSTORESHELL can list connected devices.[2]

Enterprise T1057 Process Discovery

ADVSTORESHELL can list running processes.[2]

Enterprise T1012 Query Registry

ADVSTORESHELL can enumerate registry keys.[2][3]

Enterprise T1029 Scheduled Transfer

ADVSTORESHELL collects, compresses, encrypts, and exfiltrates data to the C2 server every 10 minutes.[2]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

ADVSTORESHELL has used rundll32.exe in a Registry value to establish persistence.[3]

Enterprise T1082 System Information Discovery

ADVSTORESHELL can run Systeminfo to gather information about the victim.[2][3]

Source: https://attack.mitre.org/software/S0045/