PcShare, Software S1050 | MITRE ATT&CK®

Archived: 2026-04-05 12:54:06 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

PcShare has used HTTP for C2 communication.[1]

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

PcShare can execute `cmd` commands on a compromised host.[1]

Enterprise T1005 Data from Local System

PcShare can collect files and information from a compromised host.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

PcShare has decrypted its strings by applying a XOR operation and a decompression using a custom implemented LZM algorithm.[1]

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

PcShare has created the `HKCU\\Software\\Classes\\CLSID\\{42aedc87-2188-41fd-b9a3-0c966feabec1}\\InprocServer32` Registry key for persistence.[1]

Enterprise T1041 Exfiltration Over C2 Channel

PcShare can upload files and information from a compromised host to its C2 servers.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

PcShare has deleted its files and components from a compromised host.[1]

Enterprise T1056 .001 Input Capture: Keylogging

PcShare has the ability to capture keystrokes.[1]

Enterprise T1036 .001 Masquerading: Invalid Code Signature

PcShare has used an invalid certificate in attempt to appear legitimate.[1]

.005 Masquerading: Match Legitimate Resource Name or Location

PcShare has been named `wuauclt.exe` to appear as the legitimate Windows Update AutoUpdate Client.[1]

Enterprise T1112 Modify Registry

PcShare can delete its persistence mechanisms from the registry.[1]

Enterprise T1106 Native API

PcShare has used a variety of Windows API functions.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

PcShare has been encrypted with XOR using different 32-long Base16 strings.[1]

.015 Obfuscated Files or Information: Compression

PcShare has been compressed with LZW algorithm.[1]

Enterprise T1057 Process Discovery

PcShare can obtain a list of running processes on a compromised host.[1]

Enterprise T1055 Process Injection

The PcShare payload has been injected into the `logagent.exe` and `rdpclip.exe` processes.[1]

Enterprise T1012 Query Registry

PcShare can search the registry files of a compromised host.[1]

Enterprise T1113 Screen Capture

PcShare can take screen shots of a compromised machine.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

PcShare has used `rundll32.exe` for execution.[1]

Enterprise T1016 System Network Configuration Discovery

PcShare can obtain the proxy settings of a compromised machine using `InternetQueryOptionA` and its IP address by running `nslookup myip.opendns.comresolver1.opendns.com\r\n`.[1]

Enterprise T1125 Video Capture

PcShare can capture camera video as part of its collection process.[1]
