StrongPity, Software S0491 | MITRE ATT&CK®

Archived: 2026-04-05 13:21:37 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

StrongPity can use HTTP and HTTPS in C2 communications.[2][1]

Enterprise T1560 .003 Archive Collected Data: Archive via Custom Method

StrongPity can compress and encrypt archived files into multiple .sft files with a repeated xor encryption scheme.[2][1]

Enterprise T1119 Automated Collection

StrongPity has a file searcher component that can automatically collect and archive files based on a predefined list of file extensions.[1]

Enterprise T1020 Automated Exfiltration

StrongPity can automatically exfiltrate collected documents to the C2 server.[2][1]

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

StrongPity can use the `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` Registry key for persistence.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

StrongPity can use PowerShell to add files to the Windows Defender exclusions list.[2]

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

StrongPity has created new services and modified existing services for persistence.[2]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

StrongPity has encrypted C2 traffic using SSL/TLS.[2]

Enterprise T1041 Exfiltration Over C2 Channel

StrongPity can exfiltrate collected documents through C2 channels.[2][1]

Enterprise T1083 File and Directory Discovery

StrongPity can parse the hard drive on a compromised host to identify specific file extensions.[2]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

StrongPity has the ability to hide the console window for its document search module from the user.[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

StrongPity can add directories used by the malware to the Windows Defender exclusions list to prevent detection.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

StrongPity can delete previously exfiltrated files from the compromised host.[2][1]

Enterprise T1105 Ingress Tool Transfer

StrongPity can download files to specified targets.[1]

Enterprise T1680 Local Storage Discovery

StrongPity can identify the hard disk volume serial number on a compromised host.[2]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

StrongPity has named services to appear legitimate.[2][1]

.005 Masquerading: Match Legitimate Resource Name or Location

StrongPity has been bundled with legitimate software installation files for disguise.[2]

Enterprise T1571 Non-Standard Port

StrongPity has used HTTPS over port 1402 in C2 communication.[1]

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

StrongPity has used encrypted strings in its dropper component.[2][1]

Enterprise T1057 Process Discovery

StrongPity can determine if a user is logged in by checking to see if explorer.exe is running.[2]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

StrongPity can use multiple layers of proxy servers to hide terminal nodes in its infrastructure.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

StrongPity can identify if ESET or BitDefender antivirus are installed before dropping its payload.[2]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

StrongPity has been signed with self-signed certificates.[1]

Enterprise T1016 System Network Configuration Discovery

StrongPity can identify the IP address of a compromised host.[2]

Enterprise T1569 .002 System Services: Service Execution

StrongPity can install a service to execute itself as a service.[2][1]

Enterprise T1204 .002 User Execution: Malicious File

StrongPity has been executed via compromised installation files for legitimate software including compression applications, security software, browsers, file recovery applications, and other tools and utilities.[2][1]
