ShadowPad, Software S0596 | MITRE ATT&CK®

Archived: 2026-04-05 14:57:01 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

ShadowPad communicates over HTTP to retrieve a string that is decoded into a C2 server URL.[3]

.002 Application Layer Protocol: File Transfer Protocols

ShadowPad has used FTP for C2 communications.[3]

.004 Application Layer Protocol: DNS

ShadowPad has used DNS tunneling for C2 communications.[3]

Enterprise T1132 .002 Data Encoding: Non-Standard Encoding

ShadowPad has encoded data as readable Latin characters.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

ShadowPad has decrypted a binary blob to start execution.[3]

Enterprise T1568 .002 Dynamic Resolution: Domain Generation Algorithms

ShadowPad uses a DGA that is based on the day of the month for C2 servers.[2][3][4]

Enterprise T1070 Indicator Removal

ShadowPad has deleted arbitrary Registry values.[3]

Enterprise T1105 Ingress Tool Transfer

ShadowPad has downloaded code from a C2 server.[2]

Enterprise T1680 Local Storage Discovery

ShadowPad has discovered system information including volume serial numbers.[3]

Enterprise T1112 Modify Registry

ShadowPad can modify the Registry to store and maintain a configuration block and virtual file system.[3][5]

Enterprise T1095 Non-Application Layer Protocol

ShadowPad has used UDP for C2 communications.[3]

Enterprise T1027 Obfuscated Files or Information

ShadowPad has encrypted its payload, a virtual file system, and various files.[2][5]

.011 Fileless Storage

ShadowPad maintains a configuration block and virtual file system in the Registry.[3][5]

Enterprise T1057 Process Discovery

ShadowPad has collected the PID of a malicious process.[3]

Enterprise T1055 Process Injection

ShadowPad has injected an install module into a newly created process.[3]

.001 Dynamic-link Library Injection

ShadowPad has injected a DLL into svchost.exe.[3]

Enterprise T1029 Scheduled Transfer

ShadowPad has sent data back to C2 every 8 hours.[2]

Enterprise T1082 System Information Discovery

ShadowPad has discovered system information including memory status, CPU frequency, and OS versions.[3]

Enterprise T1016 System Network Configuration Discovery

ShadowPad has collected the domain name of the victim system.[3]

Enterprise T1033 System Owner/User Discovery

ShadowPad has collected the username of the victim system.[3]

Enterprise T1124 System Time Discovery

ShadowPad has collected the current date and time of the victim system.[3]
