Kevin, Software S1020 | MITRE ATT&CK®

Archived: 2026-04-05 18:14:13 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Variants of Kevin can communicate with C2 over HTTP.[1]

.004 Application Layer Protocol: DNS

Variants of Kevin can communicate over DNS through queries to the server for constructed domain names with embedded information.[1]

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

Kevin can use a renamed image of `cmd.exe` for execution.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Kevin can Base32 encode chunks of output files during exfiltration.[1]

Enterprise T1005 Data from Local System

Kevin can upload logs and other data from a compromised host.[1]

Enterprise T1001 .001 Data Obfuscation: Junk Data

Kevin can generate a sequence of dummy HTTP C2 requests to obscure traffic.[1]

Enterprise T1074 Data Staged

Kevin can create directories to store logs and other collected data.[1]

Enterprise T1030 Data Transfer Size Limits

Kevin can exfiltrate data to the C2 server in 27-character chunks.[1]

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

Kevin can compile randomly-generated MOF files into the WMI repository to persistently run malware.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Kevin can send data from the victim host through a DNS C2 channel.[1]

Enterprise T1008 Fallback Channels

Kevin can assign hard-coded fallback domains for C2.[1]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Kevin can hide the current window from the targeted user via the `ShowWindow` API function.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Kevin can delete files created on the victim's machine.[1]

Enterprise T1105 Ingress Tool Transfer

Kevin can download files to the compromised host.[1]

Enterprise T1036 .003 Masquerading: Rename Legitimate Utilities

Kevin has renamed an image of `cmd.exe` with a random name followed by a `.tmpl` extension.[1]

Enterprise T1106 Native API

Kevin can use the `ShowWindow` API to avoid detection.[1]

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

Kevin has Base64-encoded its configuration file.[1]

Enterprise T1572 Protocol Tunneling

Kevin can use a custom protocol tunneled through DNS or HTTP.[1]

Enterprise T1082 System Information Discovery

Kevin can enumerate the OS version and hostname of a targeted machine.[1]

Enterprise T1016 System Network Configuration Discovery

Kevin can collect the MAC address and other information from a victim machine using `ipconfig/all`.[1]

Enterprise T1497 Virtualization/Sandbox Evasion

Kevin can sleep for a time interval between C2 communication attempts.[1]
