RansomHub, Software S1212 | MITRE ATT&CK®

Archived: 2026-04-05 17:57:29 UTC

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

RansomHub has created an autorun Registry key through the `-safeboot-instance -pass` command line argument.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

RansomHub can use PowerShell to delete volume shadow copies.[2]

.003 Command and Scripting Interpreter: Windows Command Shell

RansomHub can use `cmd.exe` to execute multiple commands on infected hosts.[2]

Enterprise T1486 Data Encrypted for Impact

RansomHub can use Elliptic Curve Encryption to encrypt files on targeted systems.[1] RansomHub can also skip content at regular intervals (ex. encrypt 1 MB, skip 3 MB) to optomize performance and enable faster encryption for large files.[2]

Enterprise T1491 .001 Defacement: Internal Defacement

RansomHub has placed a ransom note on comrpomised systems to warn victims and provide directions for how to retrieve data.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

RansomHub can use a provided passphrase to decrypt its configuration file.[2]

Enterprise T1480 Execution Guardrails

RansomHub will terminate without proceeding to encryption if the infected machine is on a list of allowlisted machines specified in its configuration.[2]

Enterprise T1083 File and Directory Discovery

RansomHub has the ability to only encrypt specific files.[2]

Enterprise T1562 .009 Impair Defenses: Safe Mode Boot

RansomHub can reboot targeted systems into Safe Mode prior to encryption.[2]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

RansomHub can delete events from the Security, System, and Application logs.[2]

.004 Indicator Removal: File Deletion

RansomHub has the ability to self-delete.[2]

Enterprise T1490 Inhibit System Recovery

RansomHub has used `vssadmin.exe` to delete volume shadow copies.[1][2]

Enterprise T1135 Network Share Discovery

RansomHub has the ability to target specific network shares for encryption.[2]

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

RansomHub has an encrypted configuration file.[2]

Enterprise T1057 Process Discovery

RansomHub can stop processes associated with files currently in use to maximize the impact of encryption.[1]

Enterprise T1090 Proxy

RansomHub can use a proxy to connect to remote SFTP servers.[2]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

RansomHub can use credentials provided in its configuration to move laterally from the infected machine over SMBv2.[2]

Enterprise T1018 Remote System Discovery

RansomHub can enumerate all accessible machines from the infected system.[2]

Enterprise T1489 Service Stop

RansomHub has the ability to terminate specified services.[2]

Enterprise T1082 System Information Discovery

RansomHub can retrieve information about virtual machines.[2]

Enterprise T1497 .003 Virtualization/Sandbox Evasion: Time Based Checks

RansomHub can sleep for a set number of minutes before beginning execution.[2]
