Conti, Software S0575 | MITRE ATT&CK®

Archived: 2026-04-05 14:15:28 UTC

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

Conti can utilize command line options to allow an attacker control over how it scans and encrypts files.[2][4]

Enterprise T1486 Data Encrypted for Impact

Conti can use `CreateIoCompletionPort()`, `PostQueuedCompletionStatus()`, and `GetQueuedCompletionPort()` to rapidly encrypt files, excluding those with the extensions of .exe, .dll, and .lnk. It has used a different AES-256 encryption key per file with a bundled RAS-4096 public encryption key that is unique for each victim. Conti can use "Windows Restart Manager" to ensure files are unlocked and open for encryption.[1][2][3][5][4]

Enterprise T1140 Deobfuscate/Decode Files or Information

Conti has decrypted its payload using a hardcoded AES-256 key.[1][2]

Enterprise T1083 File and Directory Discovery

Conti can discover files on a local system.[2]

Enterprise T1490 Inhibit System Recovery

Conti can delete Windows Volume Shadow Copies using `vssadmin`.[2]

Enterprise T1106 Native API

Conti has used API calls during execution.[1][2]

Enterprise T1135 Network Share Discovery

Conti can enumerate remote open SMB network shares using `NetShareEnum()`.[2][5]

Enterprise T1027 Obfuscated Files or Information

Conti can use compiler-based obfuscation for its code, encrypt DLLs, and hide Windows API calls.[2][1][5]

Enterprise T1057 Process Discovery

Conti can enumerate through all open processes to search for any that have the string "sql" in their process name.[2]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Conti has loaded an encrypted DLL into memory and then executes it.[1][2]

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

Conti can spread via SMB and encrypts files on different hosts, potentially compromising an entire network.[1][2]

Enterprise T1018 Remote System Discovery

Conti has the ability to discover hosts on a target network.[5]

Enterprise T1489 Service Stop

Conti can stop up to 146 Windows services related to security, backup, database, and email solutions through the use of `net stop`.[2]

Enterprise T1016 System Network Configuration Discovery

Conti can retrieve the ARP cache from the local system by using the `GetIpNetTable()` API call and check to ensure IP addresses it connects to are for local, non-Internet, systems.[2]

Enterprise T1049 System Network Connections Discovery

Conti can enumerate routine network connections from a compromised host.[2]

Enterprise T1080 Taint Shared Content

Conti can spread itself by infecting other remote machines via network shared drives.[1][2]
