REvil, Software S0496 | MITRE ATT&CK®

Archived: 2026-04-05 16:58:47 UTC

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

REvil can obtain the token from the user that launched the explorer.exe process to avoid affecting the desktop of the SYSTEM user.[9]

.002 Access Token Manipulation: Create Process with Token

REvil can launch an instance of itself with administrative rights using runas.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

REvil has used HTTP and HTTPS in communication with C2.[6][7][9][2][1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

REvil has used PowerShell to delete volume shadow copies and download files.[7][8][2][3]

.003 Command and Scripting Interpreter: Windows Command Shell

REvil can use the Windows command line to delete volume shadow copies and disable recovery.[6][8][11][1]

.005 Command and Scripting Interpreter: Visual Basic

REvil has used obfuscated VBA macros for execution.[5][11]

Enterprise T1485 Data Destruction

REvil has the capability to destroy files and folders.[4][7][9][9][2][11][1]

Enterprise T1486 Data Encrypted for Impact

REvil can encrypt files on victim systems and demands a ransom to decrypt the files.[4][6][8][10][2][11][1][12]

Enterprise T1140 Deobfuscate/Decode Files or Information

REvil can decode encrypted strings to enable execution of commands and payloads.[5][4][6][9][2][1]

Enterprise T1189 Drive-by Compromise

REvil has infected victim machines through compromised websites and exploit kits.[1][9][11][7]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

REvil has encrypted C2 communications with the ECIES algorithm.[4]

Enterprise T1480 .002 Execution Guardrails: Mutual Exclusion

REvil attempts to create a mutex using a hard-coded value to ensure that no other instances of itself are running on the host.[13]

Enterprise T1041 Exfiltration Over C2 Channel

REvil can exfiltrate host and malware information to C2 servers.[1]

Enterprise T1083 File and Directory Discovery

REvil has the ability to identify specific files and directories that are not to be encrypted.[4][6][7][9][2][1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

REvil can connect to and disable the Symantec server on the victim's network.[6]

.009 Impair Defenses: Safe Mode Boot

REvil can force a reboot in safe mode with networking.[14]

Enterprise T1070 .004 Indicator Removal: File Deletion

REvil can mark its binary code for deletion after reboot.[2]

Enterprise T1105 Ingress Tool Transfer

REvil can download a copy of itself from an attacker controlled IP address to the victim machine.[8][9][11]

Enterprise T1490 Inhibit System Recovery

REvil can use vssadmin to delete volume shadow copies and bcdedit to disable recovery features.[4][6][7][8][9][2][11][1][12]

Enterprise T1680 Local Storage Discovery

REvil can identify system drive information on a compromised host.[4][6][7][9][9][2][3][1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

REvil can mimic the names of known executables.[11]

Enterprise T1112 Modify Registry

REvil can modify the Registry to save encryption parameters and system information.[6][7][9][2][1]

Enterprise T1106 Native API

REvil can use Native API for execution and to retrieve active services.[1][2]

Enterprise T1027 .011 Obfuscated Files or Information: Fileless Storage

REvil can save encryption parameters and system information in the Registry.[6][7][9][2][1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

REvil has used encrypted strings and configuration files.[5][7][9][2][3][11][1]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

REvil can identify the domain membership of a compromised host.[4][9][1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

REvil has been distributed via malicious e-mail attachments including MS Word Documents.[5][6][1][9][11]

Enterprise T1055 Process Injection

REvil can inject itself into running processes on a compromised host.[10]

Enterprise T1012 Query Registry

REvil can query the Registry to get random file extensions to append to encrypted files.[1]

Enterprise T1489 Service Stop

REvil has the capability to stop services and kill processes.[2][1]

Enterprise T1082 System Information Discovery

REvil can identify the username, machine name, system language, keyboard layout, and OS version on a compromised host.[4][6][7][9][9][2][3][1]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

REvil can check the system language using `GetUserDefaultUILanguage` and `GetSystemDefaultUILanguage`. If the language is found in the list, the process terminates.[4]

Enterprise T1007 System Service Discovery

REvil can enumerate active services.[2]

Enterprise T1204 .002 User Execution: Malicious File

REvil has been executed via malicious MS Word e-mail attachments.[5][10][11]

Enterprise T1047 Windows Management Instrumentation

REvil can use WMI to monitor for and kill specific processes listed in its configuration file.[7][3]

ICS T0828 Loss of Productivity and Revenue

The REvil malware gained access to an organizations network and encrypted sensitive files used by OT equipment. [15]

ICS T0849 Masquerading

REvil searches for whether the Ahnlab autoup.exe service is running on the target system and injects its payload into this existing process. [16]

ICS T0886 Remote Services

REvil uses the SMB protocol to encrypt files located on remotely connected file shares. [17]

ICS T0853 Scripting

REvil utilizes JavaScript, WScript, and PowerShell scripts to execute. The malicious JavaScript attachment has an obfuscated PowerShell script that executes the malware. [16]

ICS T0881 Service Stop

REvil searches for all processes listed in the prc field within its configuration file and then terminates each process. [18]

ICS T0869 Standard Application Layer Protocol

REvil sends HTTPS POST messages with randomly generated URLs to communicate with a remote server. [16] [13]

ICS T0882 Theft of Operational Information

REvil sends exfiltrated data from the victims system using HTTPS POST messages sent to the C2 system. [18] [13]

ICS T0863 User Execution

REvil initially executes when the user clicks on a JavaScript file included in the phishing emails .zip attachment. [16]
