Clop, Software S0611 | MITRE ATT&CK®

Archived: 2026-04-05 18:16:40 UTC

Clop is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high tech industries. Clop is a variant of the CryptoMix ransomware.[1][2][3]

ID: S0611

ⓘ

Type: MALWARE

ⓘ

Platforms: Windows

Version: 1.0

Created: 10 May 2021

Last Modified: 25 April 2025

Version Permalink

Live Version

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Clop can use cmd.exe to help execute commands on the system.[2]
Enterprise	T1486		Data Encrypted for Impact	Clop can encrypt files using AES, RSA, and RC4 and will add the ".clop" extension to encrypted files.[1][3][2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Clop has used a simple XOR operation to decrypt strings.[1]

Domain	ID		Name	Use
Enterprise	T1083		File and Directory Discovery	Clop has searched folders and subfolders for files to encrypt.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	Clop can uninstall or disable security products.[2]
Enterprise	T1490		Inhibit System Recovery	Clop can delete the shadow volumes with `vssadmin Delete Shadows /all /quiet` and can use bcdedit to disable recovery options.[1]
Enterprise	T1112		Modify Registry	Clop can make modifications to Registry keys.[2]
Enterprise	T1106		Native API	Clop has used built-in API functions such as WNetOpenEnumW(), WNetEnumResourceW(), WNetCloseEnum(), GetProcAddress(), and VirtualAlloc().[1][2]
Enterprise	T1135		Network Share Discovery	Clop can enumerate network shares.[1]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Clop has been packed to help avoid detection.[1][2]
Enterprise	T1057		Process Discovery	Clop can enumerate all processes on the victim's machine.[1]
Enterprise	T1489		Service Stop	Clop can kill several processes and services related to backups and security solutions.[3][1]

Domain	ID		Name	Use
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Clop can search for processes with antivirus and antimalware product names.[1][2]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	Clop can use code signing to evade detection.[3]
Enterprise	T1218	.007	System Binary Proxy Execution: Msiexec	Clop can use msiexec.exe to disable security tools on the system.[2]
Enterprise	T1614	.001	System Location Discovery: System Language Discovery	Clop has checked the keyboard language using the GetKeyboardLayout() function to avoid installation on Russian-language or other Commonwealth of Independent States-language machines; it will also check the `GetTextCharset` function.[1]
Enterprise	T1497	.003	Virtualization/Sandbox Evasion: Time Based Checks	Clop has used the `sleep` command to avoid sandbox detection.[3]

Source: https://attack.mitre.org/software/S0611