SOFTWARE

XLoader for Android
XLoader for iOS
XTunnel
YAHOYAH
YiSpecter
yty
Zebrocy
Zen
ZergHelper
Zeroaccess
ZeroT
Zeus Panda
ZLib
Zox
zwShell
ZxShell

WhisperGate

WhisperGate is a multi-stage wiper designed to look like ransomware that has been used in attacks against Ukraine since at least January 2022.[1][2][3]

ID: S0689
ⓘType: MALWARE
ⓘPlatforms: Windows
Contributors: Phil Taylor, BT Security
Version: 1.0
Created: 10 March 2022
Last Modified: 10 April 2022

Version Permalink

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	WhisperGate can make an HTTPS connection to download additional files.[2][4]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	WhisperGate can use PowerShell to support multiple actions including execution and defense evasion.[2][5][4]
		.003	Command and Scripting Interpreter: Windows Command Shell	WhisperGate can use `cmd.exe` to execute commands.[2]
		.005	Command and Scripting Interpreter: Visual Basic	WhisperGate can use a Visual Basic script to exclude the `C:\` drive from Windows Defender.[2][5]
Enterprise	T1485		Data Destruction	WhisperGate can corrupt files by overwriting the first 1 MB with `0xcc` and appending random extensions.[3][6][1][2][5][4]
Enterprise	T1140		Deobfuscate/Decode Files or Information	WhisperGate can deobfuscate downloaded files stored in reverse byte order and decrypt embedded resources using multiple XOR operations.[5][4]
Enterprise	T1561	.001	Disk Wipe: Disk Content Wipe	WhisperGate can overwrite sectors of a victim host's hard drive at periodic offsets.[6][5][4]
		.002	Disk Wipe: Disk Structure Wipe	WhisperGate can overwrite the Master Book Record (MBR) on victim systems with a malicious 16-bit bootloader.[3][6][1][2][5][4]
Enterprise	T1083		File and Directory Discovery	WhisperGate can locate files based on hardcoded file extensions.[3][2][5][4]