WarzoneRAT, Software S0670 | MITRE ATT&CK®

Archived: 2026-04-05 13:49:19 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

WarzoneRAT can use `sdclt.exe` to bypass UAC in Windows 10 to escalate privileges; for older Windows versions WarzoneRAT can use the IFileOperation exploit to bypass the UAC module.[1][2]

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

WarzoneRAT can add itself to the `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UIF2IS20VK` Registry keys.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

WarzoneRAT can use PowerShell to download files and execute commands.[1][2]

.003 Command and Scripting Interpreter: Windows Command Shell

WarzoneRAT can use `cmd.exe` to execute malicious code.[1]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

WarzoneRAT has the capability to grab passwords from numerous web browsers as well as from Outlook and Thunderbird email clients.[1][2]

Enterprise T1005 Data from Local System

WarzoneRAT can collect data from a compromised host.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

WarzoneRAT can use XOR 0x45 to decrypt obfuscated code.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

WarzoneRAT can encrypt its C2 with RC4 with the password `warzone160\x00`.[1]

Enterprise T1546 .015 Event Triggered Execution: Component Object Model Hijacking

WarzoneRAT can perform COM hijacking by setting the path to itself to the `HKCU\Software\Classes\Folder\shell\open\command` key with a `DelegateExecute` parameter.[1]

Enterprise T1041 Exfiltration Over C2 Channel

WarzoneRAT can send collected victim data to its C2 server.[1]

Enterprise T1083 File and Directory Discovery

WarzoneRAT can enumerate directories on a compromise host.[1]

Enterprise T1564 Hide Artifacts

WarzoneRAT can masquerade the Process Environment Block on a compromised host to hide its attempts to elevate privileges through `IFileOperation`.[1]

.003 Hidden Window

WarzoneRAT has the ability of performing remote desktop access via a hVNC window for decreased visibility.[3]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

WarzoneRAT can disarm Windows Defender during the UAC process to evade detection.[1]

Enterprise T1105 Ingress Tool Transfer

WarzoneRAT can download and execute additional files.[1]

Enterprise T1056 .001 Input Capture: Keylogging

WarzoneRAT has the capability to install a live and offline keylogger, including through the use of the `GetAsyncKeyState` Windows API.[1][2]

Enterprise T1112 Modify Registry

WarzoneRAT can create `HKCU\Software\Classes\Folder\shell\open\command` as a new registry key during privilege escalation.[2][1]

Enterprise T1106 Native API

WarzoneRAT can use a variety of API calls on a compromised host.[2]

Enterprise T1095 Non-Application Layer Protocol

WarzoneRAT can communicate with its C2 server via TCP over port 5200.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

WarzoneRAT has been distributed as a malicious attachment within an email.[1][4]

Enterprise T1057 Process Discovery

WarzoneRAT can obtain a list of processes on a compromised host.[1]

Enterprise T1055 Process Injection

WarzoneRAT has the ability to inject malicious DLLs into a specific process for privilege escalation.[1]

Enterprise T1090 Proxy

WarzoneRAT has the capability to act as a reverse proxy.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

WarzoneRAT has the ability to control an infected PC using RDP.[1]

.005 Remote Services: VNC

WarzoneRAT has the ability of performing remote desktop access via a VNC console.[1]

Enterprise T1014 Rootkit

WarzoneRAT can include a rootkit to hide processes, files, and startup.[1]

Enterprise T1082 System Information Discovery

WarzoneRAT can collect compromised host information, including OS version, PC name, RAM size, and CPU details.[1]

Enterprise T1221 Template Injection

WarzoneRAT has been install via template injection through a malicious DLL embedded within a template RTF in a Word document.[4]

Enterprise T1204 .002 User Execution: Malicious File

WarzoneRAT has relied on a victim to open a malicious attachment within an email for execution.[1][4]

Enterprise T1125 Video Capture

WarzoneRAT can access the webcam on a victim's machine.[1][2]
