RogueRobin, Software S0270 | MITRE ATT&CK®

Archived: 2026-04-02 11:18:36 UTC

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

RogueRobin created a shortcut in the Windows startup folder to launch a PowerShell script each time the user logs in to establish persistence.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

RogueRobin establishes persistence by creating a shortcut (.LNK file) in the Windows startup folder to run a script each time the user logs in.[1][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

RogueRobin uses a command prompt to run a PowerShell script from Excel.[1] To assist in establishing persistence, RogueRobin creates `%APPDATA%\OneDrive.bat` and saves the following string to it: `powershell.exe -WindowStyle Hidden -exec bypass -File "%APPDATA%\OneDrive.ps1"` .[2][1]

.003 Command and Scripting Interpreter: Windows Command Shell

RogueRobin uses Windows Script Components.[2][1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

RogueRobin base64 encodes strings that are sent to the C2 over its DNS tunnel.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

RogueRobin decodes an embedded executable using base64 and decompresses it.[2]

Enterprise T1105 Ingress Tool Transfer

RogueRobin can save a new file to the system from the C2 server.[1][2]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

The PowerShell script with the RogueRobin payload was obfuscated using the COMPRESS technique in `Invoke-Obfuscation` .[1][3]

Enterprise T1057 Process Discovery

RogueRobin checks the running processes for evidence it may be running in a sandbox environment. It specifically enumerates processes for Wireshark and Sysinternals.[1]

Enterprise T1113 Screen Capture

RogueRobin has a command named `$screenshot` that may be responsible for taking screenshots of the victim machine.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

RogueRobin enumerates running processes to search for Wireshark and Windows Sysinternals suite.[1][2]

Enterprise T1218 .010 System Binary Proxy Execution: Regsvr32

RogueRobin uses regsvr32.exe to run a .sct file for execution.[2]

Enterprise T1082 System Information Discovery

RogueRobin gathers BIOS versions and manufacturers, the number of CPU cores, the total physical memory, and the computer name.[1]

Enterprise T1016 System Network Configuration Discovery

RogueRobin gathers the IP address and domain from the victim's machine.[1]

Enterprise T1033 System Owner/User Discovery

RogueRobin collects the victim's username and whether that user is an admin.[1]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

RogueRobin uses WMI to check BIOS version for VBOX, bochs, qemu, virtualbox, and vm to check for evidence that the script might be executing within an analysis environment. [1][2]

Enterprise T1102 .002 Web Service: Bidirectional Communication

RogueRobin has used Google Drive as a Command and Control channel. [2]

Enterprise T1047 Windows Management Instrumentation

RogueRobin uses various WMI queries to check if the sample is running in a sandbox.[1][2]
