NETWIRE, Software S0198 | MITRE ATT&CK®

Archived: 2026-04-05 17:33:11 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

NETWIRE has the ability to communicate over HTTP.[4][5]

Enterprise T1010 Application Window Discovery

NETWIRE can discover and close windows on controlled systems.[4]

Enterprise T1560 Archive Collected Data

NETWIRE has the ability to compress archived screenshots.[4]

.003 Archive via Custom Method

NETWIRE has used a custom encryption algorithm to encrypt collected data.[6]

Enterprise T1119 Automated Collection

NETWIRE can automatically archive collected data.[4]

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

NETWIRE creates a Registry start-up entry to establish persistence.[2][4][7][5]

.013 Boot or Logon Autostart Execution: XDG Autostart Entries

NETWIRE can use XDG Autostart Entries to establish persistence on Linux systems.[4]

.015 Boot or Logon Autostart Execution: Login Items

NETWIRE can persist via startup options for Login items.[4]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

The NETWIRE binary has been executed via PowerShell script.[6]

.003 Command and Scripting Interpreter: Windows Command Shell

NETWIRE can issue commands using cmd.exe.[4][5]

.004 Command and Scripting Interpreter: Unix Shell

NETWIRE has the ability to use `/bin/bash` and `/bin/sh` to execute commands.[4][5]

.005 Command and Scripting Interpreter: Visual Basic

NETWIRE has been executed through use of VBScripts.[6][5]

Enterprise T1543 .001 Create or Modify System Process: Launch Agent

NETWIRE can use launch agents for persistence.[4]

Enterprise T1555 Credentials from Password Stores

NETWIRE can retrieve passwords from messaging and mail client applications.[4]

.003 Credentials from Web Browsers

NETWIRE has the ability to steal credentials from web browsers including Internet Explorer, Opera, Yandex, and Chrome.[6][4][5]

Enterprise T1074 .001 Data Staged: Local Data Staging

NETWIRE has the ability to write collected data to a file created in the `./LOGS` directory.[6]

Enterprise T1573 Encrypted Channel

NETWIRE can encrypt C2 communications.[4]

.001 Symmetric Cryptography

NETWIRE can use AES encryption for C2 data transferred.[4]

Enterprise T1083 File and Directory Discovery

NETWIRE has the ability to search for files on the compromised host.[5]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

NETWIRE can copy itself to and launch itself from hidden folders.[4]

Enterprise T1105 Ingress Tool Transfer

NETWIRE can downloaded payloads from C2 to the compromised host.[6][5]

Enterprise T1056 .001 Input Capture: Keylogging

NETWIRE can perform keylogging.[2][3][6][4][5]

Enterprise T1036 .001 Masquerading: Invalid Code Signature

The NETWIRE client has been signed by fake and invalid digital certificates.[2]

.005 Masquerading: Match Legitimate Resource Name or Location

NETWIRE has masqueraded as legitimate software including TeamViewer and macOS Finder.[4]

Enterprise T1112 Modify Registry

NETWIRE can modify the Registry to store its configuration information.[4]

Enterprise T1106 Native API

NETWIRE can use Native API including `CreateProcess` `GetProcessById`, and `WriteProcessMemory`.[6]

Enterprise T1095 Non-Application Layer Protocol

NETWIRE can use TCP in C2 communications.[4][7]

Enterprise T1027 Obfuscated Files or Information

NETWIRE has used a custom obfuscation algorithm to hide strings including Registry keys, APIs, and DLL names.[6]

.002 Software Packing

NETWIRE has used .NET packer tools to evade detection.[4]

.011 Fileless Storage

NETWIRE can store its configuration information in the Registry under `HKCU:\Software\Netwire`.[4]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

NETWIRE has been spread via e-mail campaigns utilizing malicious attachments.[7][5]

.002 Phishing: Spearphishing Link

NETWIRE has been spread via e-mail campaigns utilizing malicious links.[7]

Enterprise T1057 Process Discovery

NETWIRE can discover processes on compromised hosts.[6]

Enterprise T1055 Process Injection

NETWIRE can inject code into system processes including notepad.exe, svchost.exe, and vbc.exe.[4]

.012 Process Hollowing

The NETWIRE payload has been injected into benign Microsoft executables via process hollowing.[6][4]

Enterprise T1090 Proxy

NETWIRE can implement use of proxies to pivot traffic.[4]

Enterprise T1053 .003 Scheduled Task/Job: Cron

NETWIRE can use crontabs to establish persistence.[4]

.005 Scheduled Task/Job: Scheduled Task

NETWIRE can create a scheduled task to establish persistence.[6]

Enterprise T1113 Screen Capture

NETWIRE can capture the victim's screen.[2][6][4][5]

Enterprise T1082 System Information Discovery

NETWIRE can discover and collect victim system information.[2]

Enterprise T1016 System Network Configuration Discovery

NETWIRE can collect the IP address of a compromised host.[4][5]

Enterprise T1049 System Network Connections Discovery

NETWIRE can capture session logon details from a compromised host.[6]

Enterprise T1204 .001 User Execution: Malicious Link

NETWIRE has been executed through convincing victims into clicking malicious links.[6][7]

.002 User Execution: Malicious File

NETWIRE has been executed through luring victims into opening malicious documents.[6][7][5]

Enterprise T1102 Web Service

NETWIRE has used web services including Paste.ee to host payloads.[6]
