Helminth, Software S0170 | MITRE ATT&CK®

Archived: 2026-04-05 13:15:11 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Helminth can use HTTP for C2.[1]

.004 Application Layer Protocol: DNS

Helminth can use DNS for C2.[1]

Enterprise T1119 Automated Collection

A Helminth VBScript receives a batch script to execute a set of commands in a command prompt.[1]

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

Helminth establishes persistence by creating a shortcut in the Start Menu folder.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Helminth establishes persistence by creating a shortcut.[1]

Enterprise T1115 Clipboard Data

The executable version of Helminth has a module to log clipboard contents.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

One version of Helminth uses a PowerShell script.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

Helminth can provide a remote shell. One version of Helminth uses batch scripting.[1]

.005 Command and Scripting Interpreter: Visual Basic

One version of Helminth consists of VBScript scripts.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

For C2 over HTTP, Helminth encodes data with base64 and sends it via the "Cookie" field of HTTP requests. For C2 over DNS, Helminth converts ASCII characters into their hexadecimal values and sends the data in cleartext.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Helminth creates folders to store output from batch scripts prior to sending the information to its C2 server.[1]

Enterprise T1030 Data Transfer Size Limits

Helminth splits data into chunks up to 23 bytes and sends the data in DNS queries to its C2 server.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Helminth encrypts data sent to its C2 server over HTTP with RC4.[1]

Enterprise T1105 Ingress Tool Transfer

Helminth can download additional files.[1]

Enterprise T1056 .001 Input Capture: Keylogging

The executable version of Helminth has a module to log keystrokes.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

The Helminth config file is encrypted with RC4.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

Helminth has checked the local administrators group.[2]

.002 Permission Groups Discovery: Domain Groups

Helminth has checked for the domain admin group and Exchange Trusted Subsystem groups using the commands `net group Exchange Trusted Subsystem /domain` and `net group domain admins /domain`.[2]

Enterprise T1057 Process Discovery

Helminth has used Tasklist to get information on processes.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Helminth has used a scheduled task for persistence.[3]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Helminth samples have been signed with legitimate, compromised code signing certificates owned by software company AI Squared.[3]
