Koadic, Software S0250 | MITRE ATT&CK®

Archived: 2026-04-05 15:30:47 UTC

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

Koadic has 2 methods for elevating integrity. It can bypass UAC through `eventvwr.exe` and `sdclt.exe` .[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Koadic has used HTTP for C2 communications.[3]

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

Koadic has added persistence to the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` Registry key.[3]

Enterprise T1115 Clipboard Data

Koadic can retrieve the current content of the user clipboard.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Koadic has used PowerShell to establish persistence.[3]

.003 Command and Scripting Interpreter: Windows Command Shell

Koadic can open an interactive command-shell to perform command line functions on victim machines. Koadic performs most of its operations using Windows Script Host (Jscript) and to run arbitrary shellcode.[1][3]

.005 Command and Scripting Interpreter: Visual Basic

Koadic performs most of its operations using Windows Script Host (VBScript) and runs arbitrary shellcode .[1]

Enterprise T1005 Data from Local System

Koadic can download files off the target system to send back to the server.[1][3]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Koadic can use SSL and TLS for communications.[1]

Enterprise T1083 File and Directory Discovery

Koadic can obtain a list of directories.[3]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Koadic has used the command `Powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden` to hide its window.[3]

Enterprise T1105 Ingress Tool Transfer

Koadic can download additional files and tools.[1][3]

Enterprise T1046 Network Service Discovery

Koadic can scan for open TCP ports on the target network.[1]

Enterprise T1135 Network Share Discovery

Koadic can scan local network for open SMB.[1]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

Koadic can gather hashed passwords by dumping SAM/SECURITY hive.[1]

.003 OS Credential Dumping: NTDS

Koadic can gather hashed passwords by gathering domain controller hashes from NTDS.[1]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Koadic can perform process injection by using a reflective DLL.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Koadic can enable remote desktop on the victim's machine.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Koadic has used scheduled tasks to add persistence.[3]

Enterprise T1218 .005 System Binary Proxy Execution: Mshta

Koadic can use mshta to serve additional payloads and to help schedule tasks for persistence.[1][3]

.010 System Binary Proxy Execution: Regsvr32

Koadic can use Regsvr32 to execute additional payloads.[1]

.011 System Binary Proxy Execution: Rundll32

Koadic can use Rundll32 to execute additional payloads.[1]

Enterprise T1082 System Information Discovery

Koadic can obtain the OS version and build, computer name, and processor architecture from a compromised host.[3]

Enterprise T1016 System Network Configuration Discovery

Koadic can retrieve the contents of the IP routing table as well as information about the Windows domain.[1][3]

Enterprise T1033 System Owner/User Discovery

Koadic can identify logged in users across the domain and views user sessions.[1][3]

Enterprise T1569 .002 System Services: Service Execution

Koadic can run a command on another machine using PsExec.[1]

Enterprise T1047 Windows Management Instrumentation

Koadic can use WMI to execute commands.[1]
