FlawedAmmyy, Software S0381 | MITRE ATT&CK®

Archived: 2026-04-05 14:47:46 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

FlawedAmmyy has used HTTP for C2.[1]

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

FlawedAmmyy has established persistence via the `HKCU\SOFTWARE\microsoft\windows\currentversion\run` registry key.[2]

Enterprise T1115 Clipboard Data

FlawedAmmyy can collect clipboard data.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

FlawedAmmyy has used PowerShell to execute commands.[2]

.003 Command and Scripting Interpreter: Windows Command Shell

FlawedAmmyy has used `cmd` to execute commands on a compromised host.[2]

Enterprise T1005 Data from Local System

FlawedAmmyy has collected information and files from a compromised machine.[2]

Enterprise T1001 Data Obfuscation

FlawedAmmyy may obfuscate portions of the initial C2 handshake.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

FlawedAmmyy has used SEAL encryption during the initial C2 handshake.[1]

Enterprise T1041 Exfiltration Over C2 Channel

FlawedAmmyy has sent data collected from a compromised host to its C2 servers.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

FlawedAmmyy can execute batch scripts to delete files.[2]

Enterprise T1105 Ingress Tool Transfer

FlawedAmmyy can transfer files from C2.[2]

Enterprise T1056 Input Capture

FlawedAmmyy can collect mouse events.[2]

.001 Keylogging

FlawedAmmyy can collect keyboard events.[2]

Enterprise T1120 Peripheral Device Discovery

FlawedAmmyy will attempt to detect if a usable smart card is current inserted into a card reader.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

FlawedAmmyy enumerates the privilege level of the victim during the initial infection.[1][2]

Enterprise T1113 Screen Capture

FlawedAmmyy can capture screenshots.[2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

FlawedAmmyy will attempt to detect anti-virus products during the initial infection.[1]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

FlawedAmmyy has been installed via `msiexec.exe`.[2]

.011 System Binary Proxy Execution: Rundll32

FlawedAmmyy has used `rundll32` for execution.[2]

Enterprise T1082 System Information Discovery

FlawedAmmyy can collect the victim's operating system and computer name during the initial infection.[1]

Enterprise T1033 System Owner/User Discovery

FlawedAmmyy enumerates the current user during the initial infection.[1][2]

Enterprise T1047 Windows Management Instrumentation

FlawedAmmyy leverages WMI to enumerate anti-virus on the victim.[1]
