Daggerfly, Evasive Panda, BRONZE HIGHLAND, Group G1034

Archived: 2026-04-05 16:59:53 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Daggerfly uses HTTP for command and control communication.[4]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Daggerfly used PowerShell to download and execute remote-hosted files on victim systems.[1]

Enterprise T1584 .004 Compromise Infrastructure: Server

Daggerfly compromised web servers hosting updates for software as part of a supply chain intrusion.[4]

Enterprise T1136 .001 Create Account: Local Account

Daggerfly created a local account on victim machines to maintain access.[1]

Enterprise T1587 .002 Develop Capabilities: Code Signing Certificates

Daggerfly created code signing certificates to sign malicious macOS files.[4]

Enterprise T1189 Drive-by Compromise

Daggerfly has used strategic website compromise for initial access against victims.[4]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Daggerfly has used legitimate software to side-load PlugX loaders onto victim systems.[1] Daggerfly is also linked to multiple other instances of side-loading for initial loading activity.[4]

Enterprise T1105 Ingress Tool Transfer

Daggerfly has used PowerShell and BITSAdmin to retrieve follow-on payloads from external locations for execution on victim machines.[1]

Enterprise T1036 .003 Masquerading: Rename Legitimate Utilities

Daggerfly used a renamed version of rundll32.exe, such as "dbengin.exe" located in the `ProgramData\Microsoft\PlayReady` directory, to proxy malicious DLL execution.[1]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

Daggerfly used Reg to dump the Security Account Manager (SAM) hive from victim machines for follow-on credential extraction.[1]

Enterprise T1012 Query Registry

Daggerfly used Reg to dump the Security Account Manager (SAM), System, and Security Windows registry hives from victim machines.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Daggerfly has attempted to use scheduled tasks for persistence in victim environments.[4]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Daggerfly has used signed, but not notarized, malicious files for execution in macOS environments.[4]

Enterprise T1195 .002 Supply Chain Compromise: Compromise Software Supply Chain

Daggerfly is associated with several supply chain compromises using malicious updates to compromise victims.[2] [4]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Daggerfly proxied execution of malicious DLLs through a renamed rundll32.exe binary.[1]

Enterprise T1082 System Information Discovery

Daggerfly utilizes victim machine operating system information to create custom User Agent strings for subsequent command and control communication.[4]

Enterprise T1204 .001 User Execution: Malicious Link

Daggerfly has used strategic website compromise to deliver a malicious link requiring user interaction.[4]
