Goopy, Software S0477 | MITRE ATT&CK®

Archived: 2026-04-05 18:02:11 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Goopy has the ability to communicate with its C2 over HTTP.[1]

.003 Application Layer Protocol: Mail Protocols

Goopy has the ability to use a Microsoft Outlook backdoor macro to communicate with its C2.[1]

.004 Application Layer Protocol: DNS

Goopy has the ability to communicate with its C2 over DNS.[1]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Goopy has the ability to use cmd.exe to execute commands passed from an Outlook C2 channel.[1]

.005 Command and Scripting Interpreter: Visual Basic

Goopy has the ability to use a Microsoft Outlook backdoor macro to communicate with its C2.[1]

Enterprise T1005 Data from Local System

Goopy has the ability to exfiltrate documents from infected systems.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Goopy has used a polymorphic decryptor to decrypt itself at runtime.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Goopy has the ability to exfiltrate data over the Microsoft Outlook C2 channel.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Goopy has the ability to side-load malicious DLLs with legitimate applications from Kaspersky, Microsoft, and Google.[1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Goopy has the ability to disable Microsoft Outlook's security policies to disable macro warnings.[1]

Enterprise T1070 .008 Indicator Removal: Clear Mailbox Data

Goopy has the ability to delete emails used for C2 once the content has been copied.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Goopy has impersonated the legitimate goopdate.dll, which was dropped on the target system with a legitimate GoogleUpdate.exe.[1]

Enterprise T1106 Native API

Goopy has the ability to enumerate the infected system's user name via `GetUserNameW`.[1]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

Goopy has had null characters padded in its malicious DLL payload.[1]

.016 Obfuscated Files or Information: Junk Code Insertion

Goopy's decrypter have been inflated with junk code in between legitimate API functions, and also included infinite loops to avoid analysis.[1]

Enterprise T1057 Process Discovery

Goopy has checked for the Google Updater process to ensure Goopy was loaded properly.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Goopy has the ability to maintain persistence by creating scheduled tasks set to run every hour.[1]

Enterprise T1033 System Owner/User Discovery

Goopy has the ability to enumerate the infected system's user name.[1]
