Bumblebee, Software S1039 | MITRE ATT&CK®

Archived: 2026-04-02 11:46:27 UTC

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

Bumblebee has the ability to bypass UAC to deploy post exploitation tools with elevated privileges.[4]

Enterprise T1560 Archive Collected Data

Bumblebee can compress data stolen from the Registry and volume shadow copies prior to exfiltration.[4]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Bumblebee can use PowerShell for execution.[5]

.003 Command and Scripting Interpreter: Windows Command Shell

Bumblebee can use `cmd.exe` to drop and run files.[1][2]

.005 Command and Scripting Interpreter: Visual Basic

Bumblebee can create a Visual Basic script to enable persistence.[2][3]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Bumblebee has the ability to base64 encode C2 server responses.[2]

Enterprise T1005 Data from Local System

Bumblebee can capture and compress stolen credentials from the Registry and volume shadow copies.[4]

Enterprise T1622 Debugger Evasion

Bumblebee can search for tools used in static analysis.[5]

Enterprise T1140 Deobfuscate/Decode Files or Information

Bumblebee can deobfuscate C2 server responses and unpack its code on targeted hosts.[2][5]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Bumblebee can encrypt C2 requests and responses with RC4[2]

Enterprise T1041 Exfiltration Over C2 Channel

Bumblebee can send collected data in JSON format to C2.[1]

Enterprise T1008 Fallback Channels

Bumblebee can use backup C2 servers if the primary server fails.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Bumblebee can uninstall its loader through the use of a `Sdl` command.[2]

Enterprise T1105 Ingress Tool Transfer

Bumblebee can download and execute additional payloads including through the use of a `Dex` command.[1][2][3]

Enterprise T1559 .001 Inter-Process Communication: Component Object Model

Bumblebee can use a COM object to execute queries to gather system information.[2]

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

Bumblebee has named component DLLs "RapportGP.dll" to match those used by the security company Trusteer.[5]

Enterprise T1106 Native API

Bumblebee can use multiple Native APIs.[2][5]

Enterprise T1027 Obfuscated Files or Information

Bumblebee has been delivered as password-protected zipped ISO files and used control-flow-flattening to obfuscate the flow of functions.[2][4][5]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Bumblebee has gained execution through luring users into opening malicious attachments.[2][3][4][5]

.002 Phishing: Spearphishing Link

Bumblebee has been spread through e-mail campaigns with malicious links.[2][4]

Enterprise T1057 Process Discovery

Bumblebee can identify processes associated with analytical tools.[2][3][5]

Enterprise T1055 Process Injection

Bumblebee can inject code into multiple processes on infected endpoints.[4]

.001 Dynamic-link Library Injection

The Bumblebee loader can support the `Dij` command which gives it the ability to inject DLLs into the memory of other processes.[2][3]

.004 Asynchronous Procedure Call

Bumblebee can use asynchronous procedure call (APC) injection to execute commands received from C2.[2]

Enterprise T1012 Query Registry

Bumblebee can check the Registry for specific keys.[5]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Bumblebee can achieve persistence by copying its DLL to a subdirectory of %APPDATA% and creating a Visual Basic Script that will load the DLL via a scheduled task.[2][3]

Enterprise T1129 Shared Modules

Bumblebee can use `LoadLibrary` to attempt to execute GdiPlus.dll.[5]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Bumblebee can identify specific analytical tools based on running processes.[2][3][5]

Enterprise T1218 .008 System Binary Proxy Execution: Odbcconf

Bumblebee can use `odbcconf.exe` to run DLLs on targeted hosts.[4]

.011 System Binary Proxy Execution: Rundll32

Bumblebee has used `rundll32` for execution of the loader component.[2][3]

Enterprise T1082 System Information Discovery

Bumblebee can enumerate the OS version and domain on a targeted system.[1][2][3]

Enterprise T1033 System Owner/User Discovery

Bumblebee has the ability to identify the user name.[1]

Enterprise T1204 .001 User Execution: Malicious Link

Bumblebee has relied upon a user downloading a file from a OneDrive link for execution.[2][4]

.002 User Execution: Malicious File

Bumblebee has relied upon a user opening an ISO file to enable execution of malicious shortcut files and DLLs.[2][3][4][5]

Enterprise T1497 Virtualization/Sandbox Evasion

Bumblebee has the ability to perform anti-virtualization checks.[2]

.001 System Checks

Bumblebee has the ability to search for designated file paths and Registry keys that indicate a virtualized environment from multiple products.[5]

.003 Time Based Checks

Bumblebee has the ability to set a hardcoded and randomized sleep interval.[2]

Enterprise T1102 Web Service

Bumblebee has been downloaded to victim's machines from OneDrive.[2]

Enterprise T1047 Windows Management Instrumentation

Bumblebee can use WMI to gather system information and to spawn processes for code injection.[1][2][4]
