Bumblebee Loader Resurfaces in New Campaign

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-05 13:59:22 UTC

The deployment of file-encrypting ransomware by organized cybercriminal gangs is one of the largest cybersecurity risks facing organizations. A network breach that culminates with a ransomware infection often starts with an infection with a type of malware called a loader. This malware acts as a foothold into an organization's network and is subsequently used to install other payloads such as malware or tools. Bumblebee is a type of a loader that has increasingly been used by threat actors affiliated with ransomware, including the now-defunct Conti strain and a relative newcomer, Akira. Written in the C++ programming language, Bumblebee is used by multiple threat actors to secure initial footholds in high-value enterprise environments.

Bumblebee recently went on hiatus for two months, which often occurs as threat actors take a summer break. But at the end of August 2023, Bumblebee's operators resumed activity. Intel 471 Malware Intelligence systems have uncovered threat actors who are operating Bumblebee using new techniques to distribute it. They've also updated the malware to make it more difficult to disrupt. The update reduces Bumblebee's dependency on hard-coded command and control (C2) servers and instead uses a Domain Generation Algorithm (DGA) for creating new C2 touch points.

On Sept. 7, 2023, a new campaign was observed that leveraged Web Distributed Authoring and Versioning (WebDAV) servers to disseminate Bumblebee payloads. In this effort, threat actors utilized malicious spam emails to distribute Windows shortcut (.LNK) and compressed archive (.ZIP) files containing .LNK files. When activated by the user, these LNK files execute a predetermined set of commands designed to download Bumblebee malware hosted on WebDAV servers.

In this blog post, we will describe Bumblebee's recent activity and a threat actor currently using it. We will also discuss in more detail some of the malware's observed techniques, key updates to its code and mitigations that defenders can use to prevent infections.

BazarLoader's Replacement

The Bumblebee malware loader appeared in September 2021 and surged in popularity in late March 2022. This uptick came after threat actors who previously distributed a loader known as BazarLoader shifted their focus to Bumblebee (a compilation of vendor reports and resources related to Bumblebee can be found on Malpedia).

This shift coincided with the public release of the Conti ransomware gang's infrastructure chat logs and BazarLoader source code. Also released was control panel data that indicated victims of BazarLoader. This cumulative disclosure of information apparently put some threat actors off from further using it.

Since Bumblebee started operations, it has proved to be a relentless source of payloads from the Cobalt Strike, Metasploit and Sliver post-exploitation tools.

In addition to technical data, Intel 471 has collected intelligence related to how adversaries are employing Bumblebee in their operations. Bumblebee has links to threat actors who were formerly associated with the Conti and Trickbot operations. The usage of Bumblebee by skilled threat actors with a history of other ransomware activity means it should not be underestimated. One threat actor who has claimed to use Bumblebee sought a partner to run a malicious advertising (malvertising) campaign that would distribute Bumblebee and result in a victim pool that would include U.S.-based corporate users. The goal of the campaign appeared to be to gain access to those corporate users and then sell that access to ransomware affiliates and groups, a common scheme known as initial access brokering.

Distributing Bumblebee

On Sept. 7, 2023, the Intel 471 Malware Analysis team identified a new campaign that leveraged 4shared WebDAV services to distribute the Bumblebee malware loader. The 4shared aka 4shared.com file-hosting service allows users to upload and download files through both a web interface and the WebDAV protocol. WebDAV lets users manage and edit files on remote servers. Most operating systems support WebDAV, letting users treat a 4shared folder as a local network drive.

[Image: Fig 1 - This image depicts a screenshot highlighting the features of 4shared's WebDAV server Sept. 7, 2023.]

Using WebDAV isn’t a new technique. The SANS Internet Storm Center noted in a blog post Feb. 24, 2023, that WebDAV played a role in the distribution of the IcedID aka Bokbot malware. In this Bumblebee campaign, threat actors used malicious spam emails disguised as scans, notifications, invoices or numbered documents to lure victims into downloading attachments. Some examples of the file names used as lures in these attachments include:

- scan-document_2023(383).lnk
- notify-september_2023(309).lnk
- document-07september_2023(341).lnk
- invoice-07september_2023(231).lnk
- invoice-07september_2023 (262).zip
- [2-3 digit numbers].lnk

[Image: Figure 2 - This image depicts a screenshot of an email used in the Bumblebee campaign Sept. 7, 2023.]

While the majority of the observed samples were distributed as .LNK files, we noticed a subset was disseminated as .ZIP with .LNK files contained. Upon execution, the attached .LNK file initiates the Windows command processor, which then executes a preconfigured set of commands. The first command mounts a network drive to a WebDAV folder at **https://webdav.4shared[dot]com**, utilizing a specific username and password for authentication.

[Image: Figure 3 - This image depicts a screenshot of a 4shared panel hosting malware payloads connected to the WebDAV campaign Sept. 7, 2023, by X user @V3n0mStrike.]

Our analysis revealed variations in the specific command sets employed across different samples. Upon mounting the disk to the victim's device, subsequent commands varied depending on the particular sample analyzed. For

instance, in file manipulation, the first two commands employ **“expand**” to extract and copy files from the mounted drive, while the third employs “**replace.exe**” as an alternative method. Similarly, the approaches for executing these files also differ. The first example leverages the WMIC file **“wmic.exe**” to create a new process, the second utilizes “**conhost.exe**” and the third schedules a recurring task via “**schtasks**” for file execution.

Bumblebee payload

On Sept. 1, 2023, our monitoring system detected a new version of the Bumblebee loader featuring several alterations to its underlying architecture. Notably, the loader transitioned from utilizing the WebSocket protocol to employing a custom Transmission Control Protocol (TCP) for its communication mechanisms. The update also introduced DGA, a departure from the hard-coded list of C2 servers in earlier versions. Using a 64-bit static seed value, the DGA generated 100 new domains with a ".life" top-level domain (TLD). When the payload is executed, Bumblebee will iterate until it resolves a DGA domain to an IP address and successfully checks in. The use of DGA adds another layer of complexity, reducing dependency on hard-coded C2 servers and thereby making it more challenging to disrupt the malware’s operations.

In the observed WebDAV campaign, the following four domains were listed and the fourth domain was resolved successfully and contacted:

- 3v1n35i5kwx[dot]life
- cmid1s1zeiu[dot]life
- Itszko2ot5u[dot]life
- newdnq1xnl9[dot]life

On Sept. 7, 2023, our system detected a new sample labeled with the group name “**lnk1**,” potentially indicating the utilization of .LNK files, which aligns with the observed tactics in the recent WebDAV campaign.

Assessment

The Bumblebee loader received several key updates during its two-month pause in activity. These changes demonstrate a coordinated effort to enhance evasion tactics and bolster resilience against network-level scrutiny and domain takedown. Additionally, the use of 4shared's WebDAV services for distribution is a new attack vector. Analysis of the .LNK files shows calculated steps to evade detection. These include mounting a network drive to a WebDAV folder and utilizing varied command sequences and execution methods — from "wmic.exe" to "conhost.exe" and "schtasks" — all designed to bypass behavioral detection systems. The variation in these techniques suggests that threat actors are not only innovating but may also be attempting to determine which tactics are most effective for evasion.

Additional advancements in both the malware and its associated distribution methods indicate a growing sophistication within the global malware landscape. This escalation in complexity often is observed after a post-summer hiatus, suggesting that threat actors may utilize this period of reduced activity to refine and advance their operations. As threat actors consistently integrate advanced evasion techniques and exploit legitimate services, conventional security measures are becoming increasingly ineffective. Therefore, organizations continuously must stay up to date with emerging threats to adapt their cybersecurity strategies effectively. The Intel 471 team will

continue monitoring and reporting emerging threats to provide organizations with timely and actionable intelligence.

Recommendations

Intel 471 analysts recommend blocking the following known malicious domains associated with this campaign:

- If the “webdav.4shared[dot]com” domain normally is not used in your organization, blocking this domain is recommended.
- Additionally, organizations are advised to block other .life TLDs generated by the DGA.

The command line execution provides several threat hunting opportunities:

- Any command line event logs with “webdav.4shared[dot]com” likely are suspicious, unless this website is used by system administrators in your organization.
- Look for “replace.exe” in conjunction with “webdav.4shared[dot]com” in Windows command line event logs.
- Search for emails with attachments that match the following regular expressions (regex):

[a-z]+-[0-9a-z]+_2023\([0-9]{3}\).lnk

MITRE ATT&CK techniques

TECHNIQUE TITLE	ID	USE
Reconnaissance [TA0043]		
Gather Victim Host Information: Client Configurations	T1592.004	Malware lists the compromised host configuration that may include operating system or version, virtualization, architecture, language and/or time zone.
Resource Development [TA0042]		
Develop Capabilities: Malware	T1587.001	Adversaries develop malware to support and enhance their operations.
Obtain Capabilities: Malware	T1588.001	Adversaries purchase malware from third parties to enhance their operations.
Obtain Capabilities: Tool	T1588.002	Adversaries purchase or acquire stolen licenses to legitimate tools, which are abused during their operations.
Stage Capabilities: Upload Malware	T1608.001	Adversaries upload malware to third-party or adversary-controlled infrastructure to leverage it during operations.

Stage Capabilities: Upload Tool	T1608.002	Adversaries upload tools to third-party or adversary-controlled infrastructure to leverage it during operations.
Initial Access [TA0001]		
Phishing	T1566	Adversaries conduct mass malware spam campaigns to infect end users and increase botnet size.
Execution [TA0002]		
User Execution: Malicious Link	T1204.001	Spam operations rely on a user clicking a malicious link to gain execution.
User Execution: Malicious File	T1204.002	Spam operations rely on a user opening a malicious file to gain execution.
Scheduled Task/Job: Scheduled Task	T1053.005	Adversaries use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence.
Persistence [TA0003]		
Scheduled Task/Job: Scheduled Task	T1053.005	Adversaries use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence.
Credential access [TA0006]		
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	Adversaries acquire credentials from web browsers by reading files specific to the target browser. This is performed by the stealer plug-in.
Collection [TA0009]		
Data from Local System	T1005	Adversaries search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to exfiltration. This is performed by the stealer plug-in.
Command and Control [TA0011]		
Data Encoding	T1132	Adversaries encode data to make the content of C2 traffic more difficult to detect.

Data Obfuscation	T1001	Adversaries obfuscate C2 traffic to make it more difficult to detect.
Dynamic Resolution: Domain Generation Algorithms	T1568.002	Adversaries leverage DGAs to identify a destination domain for C2 traffic dynamically rather than relying on a list of static IP addresses or domains.
Non-Standard Port	T1571	Malware uses raw sockets and communicates over TCP on port 443, a commonly used port for Hypertext Transfer Protocol Secure (HTTPS) traffic.
Encrypted Channel: Symmetric Cryptography	T1573.001	Adversaries employ a known symmetric encryption algorithm to conceal C2 traffic.
Encrypted Channel: Asymmetric Cryptography	T1573.002	Adversaries employ a known asymmetric encryption algorithm to conceal C2 traffic.
Exfiltration [TA0010]		
Automated Exfiltration	T1020	Adversaries exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during collection. This is performed by the stealer plug-in.
Exfiltration Over C2 Channel	T1041	Adversaries steal data by exfiltrating it over an existing C2 channel. Stolen data is encoded into the normal communications channel using the same protocol as C2 communications.
