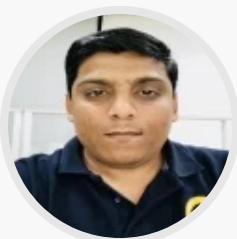




Threat Hunter Team
Symantec



Vishal Kamble
Principal Threat Analysis Engineer

POSTED: 28 JUN, 2022 | 11 MIN READ |
THREAT INTELLIGENCE

 SUBSCRIBE FOLLOW  

Bumblebee: New Loader Rapidly Assuming Central Position in Cyber-crime Ecosystem

New malware has links with multiple threat actors, including several high-profile ransomware operations.

Bumblebee, a recently developed malware loader, has quickly become a key component in a wide range of cyber-crime attacks and appears to have replaced a number of other loaders that the threat actors have used in the past.

By analyzing Symantec threat intelligence number of tactics, techniques and procedures (TTPs) used by threat actors, we have developed a hypothesis that Bumblebee may have been introduced as a replacement loader for



SHARE

×

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

Accept Cookies

[Cookies Settings](#)

Trickbot and BazarLoader, since there is some overlap between recent activity involving Bumblebee and older attacks linked to these loaders.

Bumblebee and Quantum: Bumblebee’s role in ransomware delivery

A recent attack involving the Quantum ransomware demonstrates how Bumblebee is now being leveraged by attackers to deliver ransomware.

The initial infection vector was a spear-phishing email with an attachment containing an ISO file. This ISO file contained a Bumblebee DLL file and an LNK file, which loaded the Bumblebee DLL file using rundll32.exe.

- rundll32.exe teas.dll,kXINkCKgFC

Bumblebee supports multiple commands like “Ins” for bot persistence, “Dij” for DLL injection, and “Dex” for downloading executables.

Bumblebee contacted a command-and-control (C&C) server (45.153.243.93) and created a copy in the %APPDATA% folder with a random name, and also created a VBS file at the same location to load the %APPDATA% DLL file.

A scheduled task was created using the Bumblebee “Ins” command to run a VBS file every 15 minutes.

- wscript.exe
CSIDL_COMMON_APPDATA\e147c18f9167cd0f\f30b25c870238567.vbs
- CSIDL_SYSTEM\rundll32.exe"
CSIDL_COMMON_APPDATA\e147c18f9167cd0f\f30b25c870238567.dll

After a couple of hours, Bumblebee used the “Dex” command to drop and run a Cobalt Strike payload named “wab.exe” in the %APPDATA% location. It also ran the “systeminfo” command.

- wmiprvse.exe --> wab.exe
- wmiprvse.exe --> wab.exe --> cmd.exe /C systeminfo

Using the “Dij” command, Bumblebee injected the Cobalt Strike payload into a legitimate process “Imagines” and created a new executable file.

In addition to this, using the “Dex” command, Bumblebee dropped the Cobalt Strike payload into the legitimate process “Imagines”.

Bumblebee then dropped the Cobalt Strike payload into the legitimate process “Imagines” and enumerated domain-related information like domain trust, domain users, domain

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

groups, and group permissions, etc.

At this point, Bumblebee dropped the Quantum ransomware using the “Dij” command. The attacker used both DLL and EXE payloads to encrypt files.

- rundll32.exe CSIDL_COMMON_APPDATA\2429189468.dll,start \shareall \nolog
- CSIDL_COMMON_APPDATA\2431789750.exe /shareall /NOLOG

Quantum collects system information and user information using WMI. It also checks for SQL-related services and stops them if found running. Quantum also checks for some processes related to malware analysis like procmon, wireshark, cmd, task manager, and notepad, and terminates them if found running.

Link 1: The AdFind connection

Tools used in recent Bumblebee attacks have appeared in older attacks, pre-dating Bumblebee’s appearance. In a number of attacks involving Bumblebee beginning in mid-May 2022, a version of AdFind (SHA256: b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682) was also deployed by the attackers. AdFind is a publicly available tool for querying Active Directory and has been widely used by a range of threat actors in recent years.

Similar to the previously mentioned example, malicious ISO files attached to phishing emails were the initial infection vector, with the attackers deploying legitimate ConnectWise remote desktop software (formerly known as ScreenConnect), along with Atera, another legitimate remote access tool, and Meterpreter, a Metasploit in-memory payload that provides a reverse shell to the attacker. In all cases, the attacks never reached the payload stage. However, similarities TTPs used in other attacks suggest that ransomware was the intended payload.

This version of AdFind used in these recent Bumblebee attacks has appeared in attacks dating back as far as June 2021, where it was being used in conjunction with Cobalt Strike to deliver the Avaddon ransomware.

In August 2021, it reappeared during an unsuccessful ransomware attack when it was used alongside a number of other legitimate software packages including AnyDesk, a publicly available remote desktop software, and WinRAR, a file archiving utility. In July 2021, 7-Zip, the publicly available file archiving utility, was used to deliver a ransomware payload called BlackCat.

During another abortive attack in June 2021, the attackers used a legitimate remote access tool, AnyDesk. The widely used network scanner, NetScan, was also deployed, along with the NetScan network scanner. The attackers also made use of a

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

PowerShell script named cve-2021-34527.ps1 that has previously been linked to Conti’s leaked attack playbook.

This version of AdFind also appeared in attacks involving Quantum ransomware during May 2022. The attackers also used Cobalt Strike; Ligolo, a publicly available tunneling tool created for penetration testing purposes, but which has been used by a number of espionage and ransomware actors; ProcDump for credential dumping; along with Rclone, a legitimate open-source tool that can legitimately be used to manage content in the cloud, but is frequently used by ransomware actors to exfiltrate data.

More recently, this same version of AdFind was used in an attack attempting to deliver the Diavol payload. The initial loader used by the attackers was not discovered, but the AdFind link with Bumblebee activity suggests it may have been used by the attackers.

Link 2: adf.bat

In early June 2022, Bumblebee was used in a thwarted attack. Although the payload wasn’t deployed, the TTPs used suggested ransomware. The attackers made use of a batch script called adf.bat (SHA256: 1e7737a57552b0b32356f5e54dd84a9ae85bb3acff05ef5d52aabaa996282dfb) along the previously mentioned version of AdFind (SHA256: b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682) and another version of AdFind (SHA256: 9d0fa4b88e5b36b8801b55508ab7bc7cda9909d639d70436e972cb3761d34eda).

This adf.bat script has been used in attacks since at least 2021. In September 2021, for example, the file was deployed in what appeared to be an attempted ransomware attack. It was used in conjunction with the previously mentioned version of AdFind (SHA256: b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682); Cobalt Strike; and PowerSploit, an exploitation framework originally developed for penetration testing.

The script was also used in another thwarted ransomware attack in November 2021, again alongside the previously mentioned version of AdFind. In this case, the attackers used a number of tools including Cobalt Strike, Splashtop, along with C&C servers. The attackers also used some of the infrastructure from the previous attack, including BazarLoader, which also appeared in the Conti attack. The attackers used by the Miner cybercriminal group.

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

as part of the delivery mechanism for the group’s ransomware families: Ryuk and Conti.

Link 3: find.exe/adfind.exe

A third version of AdFind (SHA256: 9d0fa4b88e5b36b8801b55508ab7bc7cda9909d639d70436e972cb3761d34eda) has also been used in recent attacks involving Bumblebee. This tool has been used in ransomware attacks for at least a year.

In May 2021, it was used alongside Cobalt Strike in an attempted ransomware attack against a large electronics organization. One feature of this attack was that the attackers installed a VirtualBox VM on some compromised computers. While a VM image was not retrieved, it appeared that the ransomware payload was located on the VM and ran once the operating system was fully booted. The VM likely had access to the host computer’s files and directories (via "SharedFolders" set up by runner.exe), allowing it to encrypt files on the host computer. While the payload wasn’t identified, there were some links to both the Conti and Mountlocker ransomware operations.

In another May 2021 attack it was again used in conjunction with Cobalt Strike in another abortive ransomware attack against an organization in the U.S. While the payload was not deployed, some of the TTPs had links to earlier Conti attacks.

Also in May 2021, this version of AdFind was leveraged along with Cobalt Strike in an attack against an organization in Canada. In this case, the Conti ransomware was used.

Increase in use of legitimate software

Aside from Bumblebee’s links to a range of ransomware attacks, another commonality between many of the attacks investigated is the preponderance of legitimate software tools now being deployed during ransomware attacks. Remote desktop tools such as ConnectWise, Atera, Splashtop, and AnyDesk frequently feature in ransomware investigations, in addition to Rclone, which is now widely leveraged for data exfiltration purposes.

More recently, Symantec has identified a new tool, PDQ Deploy, leveraging PDQ Deploy, a tool that allows users to manage and deploying custom scripts to execute malicious Powershell commands using PowerShell Empire.

The Bumblebee threat

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

261b06e30a4a9960e0b0ae173486a4e456c9bd7d188d0f1c9c109bb9e2281b59 -
Bumblebee-related DLL

24bf01c1a39c6fcab26173e285d226e0c2dcd8ebf86f820f2ba5339ac29086e5 -
Bumblebee-related DLL

86d7f7b265aae9eedb36bc6a8a3f0e8ec5fa08071e2e0d21774a9a8e3d4ed9e7 -
Bumblebee-related DLL

4c3d85e7c49928af0f43623dcbed474a157ef50af3cba40b7fd7ac3fe3df2f15 –
Unconfirmed, possible VM detection tool

b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682 -
AdFind

9d0fa4b88e5b36b8801b55508ab7bc7cda9909d639d70436e972cb3761d34eda -
AdFind

af.bat 1e7737a57552b0b32356f5e54dd84a9ae85bb3acff05ef5d52aabaa996282dfb
– af.bat

adf.bat
5a1b3f9589b468a06e9427eae6b0a855d1df6cb35ab71ddbfa05279579e9cda3 –
adf.bat

ee5fbc193f875a2b8859229508ca79a2ffe19d8a120ae8c5ca77b1d17233d268 -
wab.exe

5ad4fa74e71fb4ce0a885b1efb912a00c2ce3c7b4ad251ae67e6c3a8676ede02 -
wabmig.exe

02ea7b9948dfc54980fd86dc40b38575c1f401a5a466e5f9fbf9ded33eb1f6a7 -
wabmig.exe

b722655b93bcb804802f6a20d17492f9c0f08b197b09e8cd57cf3b087ca5a347 -
imagingdevices.exe

a60136d7377bc1ba8c161021459e9fe9f49c692bf7b397fea676211a2da4444d –
Malicious MSI file

86c564e9fb7e45a7b0
VBS file

1825e14e1ea19756b55
ConnectWise

3dea930cfb0ea48c2c
Atera

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

51.68.146.200 - AS16276 OVH SAS

154.56.0.221 - AS60602 Inovare-Prim SRL

3.85.198.66 - AS14618 AMAZON-AES

3.144.143.242 - AS16509 AMAZON-02

adaptivenet[.]hostedrm[.]com

hxxp://127.0.0.[.]1:[high-ephemeral-port]/

hxxps://ec2-3-144-143-242.us-east-2.compute.amazonaws[.]com

hxxps://ec2-3-85-198-66[.]compute-1.amazonaws[.]com

adaptivenet[.]hostedrm[.]com / 52.53.233.237 - AS16509 AMAZON-02

hxxp://adaptivenet[.]hostedrm[.]com/LabTech/Updates/LabtechUpdate_220.124.zip

hxxp://adaptivenet[.]hostedrm[.]com/LabTech/Updates/LabtechUpdate_220.77.zip

hxxp://adaptivenet[.]hostedrm[.]com/LabTech/transfer/tools/caexec.exe

hxxp://adaptivenet[.]hostedrm[.]com/LabTech/Deployment.aspx?
Probe=79EA559BB87BF3C8403C40586993D4AC&ID=660

URLs containing URI string "/LabTech/"

45.153.243.93 – Bumblebee C&C

Protection

Symantec Endpoint Protection (SEP) protects against ransomware attacks using multiple static and dynamic technologies.

AV-Protection

- Backdoor.Cobalt!gm1
- Backdoor.Cobalt!gm5
- Ransom.Quantum
- Ransom.Quantum
- Trojan.Horse
- Trojan.Bumblebee
- Trojan.Bumblebee
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan.Gen.MBT

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

Behavior Protection

- SONAR.SuspLoad!g12
- SONAR.Module!gen3
- SONAR.WMIC!gen13
- SONAR.WMIC!gen10
- SONAR.RansomGen!gen1
- SONAR.Ransomware!g13
- SONAR.RansomQuantm!g1
- SONAR.Dropper
- SONAR.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7

Intrusion Prevention System Protection

- 28589: Attack: Meterpreter Reverse HTTPS
- System Infected: Trojan.Backdoor Activity 373
- 32721: Audit: ADFind Tool Activity

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).




About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.



About the Author

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).



Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.



Related Blog Posts



POSTED: 22 OCT, 2024 | 5 MIN READ

Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps



POSTED: 17 OCT, 2024 | 3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter



POSTED: 2 OCT, 2024 | 5 MIN READ

Stonefly: Extortion Attacks Continue Against U.S. Targets



POSTED: 12 SEP, 2024 | 3 MIN READ

Ransomware: Attacks Once More Nearing Peak Levels

 SUBSCRIBE

FOLLOW



Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).