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

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bumblebee-loader-cybercrime

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 older loaders, which suggests that it is the work of established actors and that the transition to Bumblebee was pre-planned.

By analysis of three other tools used in recent attacks involving Bumblebee, Symantec's Threat Hunter team, a part of Broadcom Software, has linked this tool to a number of ransomware operations including Conti, Quantum, and Mountlocker. The tactics, techniques, and procedures (TTPs) used in these older attacks support the hypothesis that Bumblebee may have been introduced as a replacement loader for 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,kXlNkCKgFC
```

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 then injected the Metasploit DLL into the legitimate process “ImagingDevices.exe”, which is a Windows Photo Viewer executable file.

In addition to this, using the “Dij” command Bumblebee injected the Cobalt Strike payload into the legitimate “wab.exe”, which is a Windows Mail executable file.

Bumblebee then dropped the AdFind tool using the “Dij” command and tried to enumerate domain-related information like domain trust, domain users, domain 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 tool; Splashtop, another remote desktop tool; and 7-Zip, the publicly available archiving tool. The attack was halted before a ransomware payload could be deployed.

During another abortive ransomware attack in May 2022, this variant of AdFind was also deployed. Again, the attackers used Atera in conjunction with Splashtop and AnyDesk. The widely used credential dumping tools Mimikatz and LaZagne were deployed, along with the NetScan network scanner. The attackers also made use of a 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. Once again the attackers used a number of publicly available tools, including Atera agent and Splashtop, along with Cobalt Strike. While the delivery mechanism wasn't uncovered, some of the infrastructure used had been previously linked to infrastructure used by BazarLoader, which along with Trickbot, was one of the primary pieces of malware used by the Miner cyber-crime group (aka Wizard Spider). Both were frequently used 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 seen attackers using the AvosLocker ransomware leveraging PDQ Deploy in their attacks. PDQ Deploy is a legitimate software package that allows users to manage patching on multiple software packages in addition to deploying custom scripts. At least one affiliate of AvosLocker is now using it to execute malicious PowerShell commands on multiple computers on victims' networks using PowerShell Empire to deploy the AvosLocker payload.

The Bumblebee threat

Bumblebee's links to a number of high-profile ransomware operations suggest that it is now at the epicenter of the cyber-crime ecosystem. Any organization that discovers a Bumblebee infection on its network should treat this incident with high priority since it could be the pathway to several dangerous ransomware threats.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

6804cff68d9824efeb087e1d6ff3f98ed947f002626f04cf8ae7ef26b51e394b – Bumblebee

daf055e5c7f843a3dbe34c3c7b848e5bbe9c53b65df2556b4b450390154af3bb - Bumblebee

7259b7a91df7c9bc78b0830808fe58c6ff66aa79bb856cf1bf50a107875b3651 – Bumblebee

ac20f3f9ed0c1e6b2160976a1dc4167e53fbb8c71b4824a640131acf24c71bfd - Bumblebee

71f91acc6a9162b600ff5191cc22f84a2b726050a5f6d9de292a4deeea0d9803 – Bumblebee

f06566e1e309123e03a6a65cdfa06ce5a95fdd276fb7fcbcb33f5560c0a3cd8c – Cobalt Strike

2e349b3224cc0d958e6945623098c2d28cc8977e0d45480c0188febbf7b8aa78 – Bumblebee

302a25e21eea9ab5bc12d1c5f9e5c119619e617677b307fe0e3044c19581faea – Likely Bumblebee

65e205b500160cbec44911080621d25f02ad7fcfcf2c3e75ce33f6f821a808b8 - Bumblebee-related DLL

905e87d8433fa58f3006ee685bb347024b46550a3ceda0777016f39e88519142 - Bumblebee-related DLL

6727d493d4ecc8cca83ed8bf7af63941175decff7218e599355065ae6c9563c4 - Bumblebee-related DLL

c8db63bfab805179a1297f8b70a90a043581c9260e8c97725f4920ab93c03344 - Bumblebee-related DLL

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

86c564e9fb7e45a7b0e03dd5a6e1c72b7d7a4eb42ebe6aa2e8f8a7894bed4cb5 – VBS file

1825e14e1ea19756b55b5ccec5afbb9c2dba0591403c553a83c842bb0dd14432 - ConnectWise

3dea930cfb0ea48c2ce9f7a8bd98ee37e2feca5fb4da8844890fa2d4f62dd105 - Atera

52f145a4ccc0f540a130bedbf04370a842daff1ee8d8361c75a8e0d21a88cf5a - Atera

update.exe 3b7512cfa21bd65bd5beecc8cb859ab4f7f5538f3caaf0703a68ec14389b357a - ConnectWise

4c6a865771fdb400456b1e8bc9198134ac9d2f66f1654af42b4b8fc67ae018f2 - ConnectWise

fef7d54d6c09a317d95300d10ffcc6c366dbb8f5ebf563dec13b509fff361dc1 - ConnectWise

165b491e5b9e273a61c16de0f592e5047740658c7a2e3047f6bf518a17e59eca - ConnectWise

a8faf08997e11a53f9d38797d997c51c1a3fcf89412c3da8dcca6631c6f314a8 - ConnectWise

01e22210e07708c0b9a0061d0f912041808e48bb8d59f960b545d0b9e11d42d2 - ConnectWise

f5218aaa046776a12b3683c8da4945a0c4c0934e54802640a15152d9dae15d43 - ConnectWise

bc41569c4c9b61f526c78f55993203806d09bb8c3b09dbbeaded61cd1dc2fcc2 - caexec.exe (likely similar to PAExec)

29767c912919cb38903f12c7f41cdd1c5f39fccb9641302c97b981e4b5e31ee5 - vSphere PowerCLI component

911c152d4e37f55bd1544794cc324364b6f03aff118cdf328127355ccc25282a - vSphere PowerCLI component

f5cd44f1d72ef8fc734c76ca62879e1f1cb4c0603cfdc0b85b5ad6ad8326f503 - vSphere PowerCLI component

0650722822e984da41d77b90fbd445f28e96a90af87043581896465c06ed1e44 – ConnectWise

f01a3f2186e77251acfac9d53122a1579182bde65e694487b292a8e09cf8d465 – Cobalt Strike

290b698d41525c4c74836ca934c0169a989a5eafde7208d90300a17a3f5bd408 – Ransom.Quantum

3d41a002c09448d74070a7eb7c44d49da68b2790b17337686d6dd018012db89d – Ransom.Quantum

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[.]hostedrmm[.]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[.]hostedrmm[.]com / 52.53.233.237 - AS16509 AMAZON-02

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

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

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

hxxp://adaptivenet[.]hostedrmm[.]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!gm1
- Trojan Horse
- Trojan.Bumblebee
- Trojan.Bumblebee!g1
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan.Gen.MBT

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

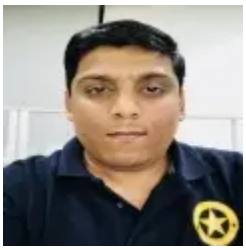
For the latest protection updates, please visit the Symantec Protection Bulletin.

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

Vishal Kamble

Principal Threat Analysis Engineer

Vishal is member of Symantec’s Security Technology and Response team where he is focused on researching future cyber threats.