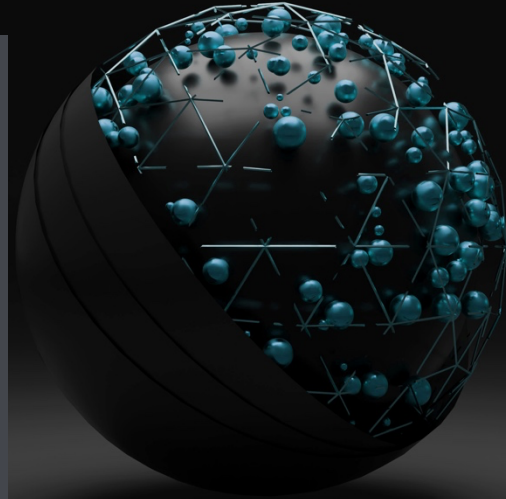


Buzz of the Bumblebee – A new malicious loader

Emerging Threats Protection Report



Every other week a new vulnerability is discovered and becomes public. Some customers know how to deal with them, others – don't.

Logpoint Security Research team researches and investigates new major vulnerabilities discovered, and builds SIEM rules and SOAR playbooks for investigation and response.

This report is the outcome of Logpoint's Security Research team and Global Services, as part of our Emerging Threat Protection service to provide Logpoint's customers with up-to-date detection rules, Investigation and Response playbooks, and security best practices.

This time, the talk of the town is Bumblebee, a malware loader, that is hard to detect, being used by multiple ransomware threat groups as a replacement to the infamous Bazarloader.

Analysis of the used tactics, techniques, and procedures

The TTP most commonly used among all known attack vectors follows a pattern that we are going to use to detect any potential that might be brewing in our network.

Initial access

As with any initial access attempt, the bumblebee has been known to perform both spearphishing and whaling attacks to get the victim to download the malware loader. In this case, it is the bumblebee loader.

URLs and HTML attachments

The first line of email phishing campaigns started with a DocuSign-branded email campaign with two alternate paths designed to lead the victim into downloading a malicious ISO file.

The first path begins with the victim clicking on "REVIEW THE DOCUMENT". Once clicked, a zipped ISO hosted on Onedrive would download onto the victim's computer.

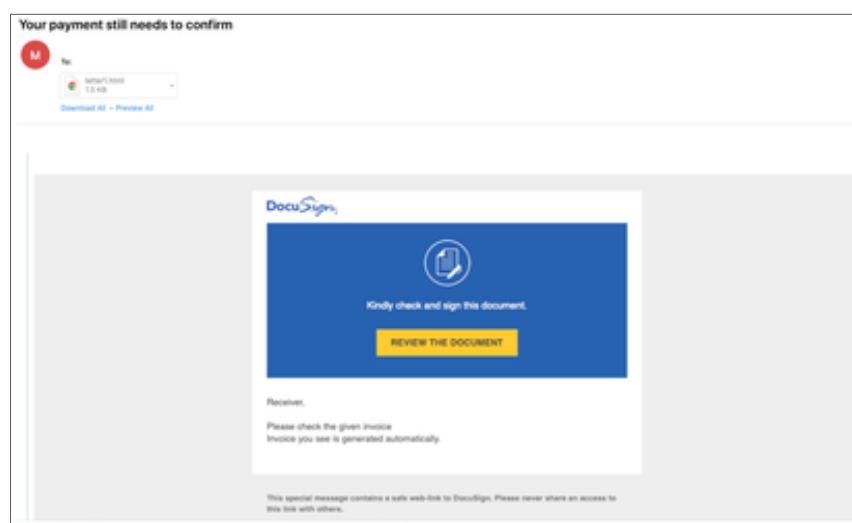
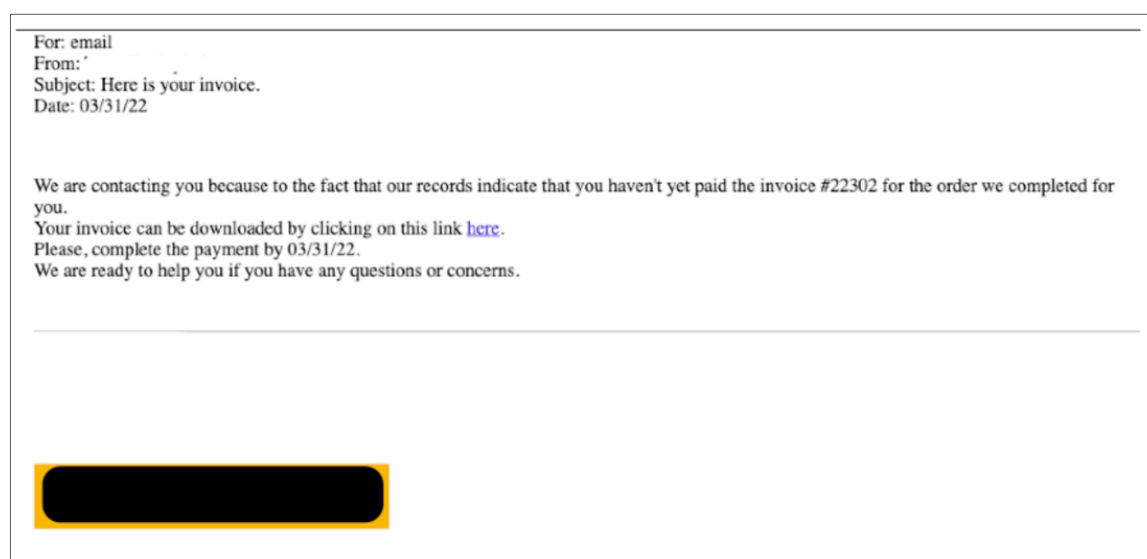


Image courtesy of [Proofpoint](#).

The second path begins with the HTML file attached to the email. The file is created to resemble an email. The content might vary, but the user is prompted to click on a link that would eventually lead to the downloading of the same malicious ISO file.



For alerts against phishing, Logpoint comes out of the box with vendor-specific phishing alerts. Please check the vendor list if any of your devices are supported. However, an alert can be created to detect a phishing attack and modified as per required. This however requires some sort of email security application that hashes the receiving file.

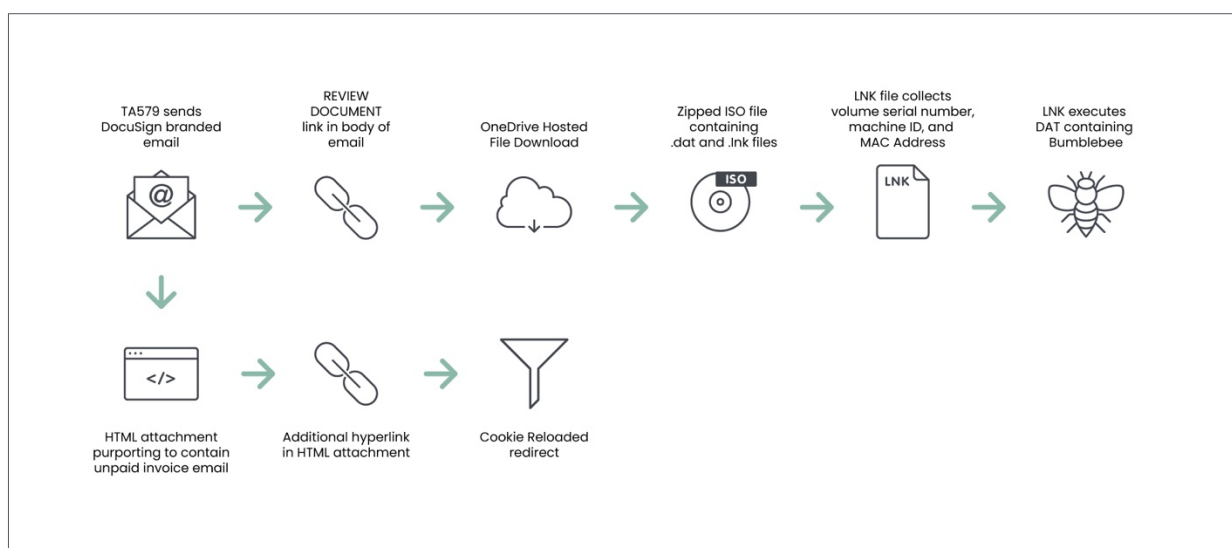
Alerts can be created to detect a phishing attack and modified as per required based on pre-existing alerts. Bumblebee detection, however, requires some sort of email security application that hashes the receiving file. An example could be:

```
1 label=File file=* sender=* receiver=* hash IN BUMBLEBEE_HASHES
```

Thread hijacking: Zipped ISO attachments

The researchers this month observed a campaign that delivered emails that appeared to reply to existing and legitimate email conversations and also included malicious zipped ISO attachments. The Proofpoint researchers said they are highly confident "based on malware artifacts" that "all the tracked threat actors using Bumblebee are receiving it from the same source."

The loader is unusual in that most of it is pulled together into a single function. Most malware breaks out initialization, request sending, and response handling into different functions. In addition, its configuration is stored in plaintext, though the Proofpoint researchers expect obfuscation features will be used in the future.




What's more, the embedded URL in the HTML attachment makes use of a traffic direction system (TDS) dubbed Prometheus — which is available for sale on underground platforms for \$250 a month — to redirect the URLs to the archive files based on the time zone and cookies of the victims.

Contact forms: Stolen images

Late August to March 2022 saw a rise in another campaign, wherein emails were generated by submitting a message to a contact form on the target organization's website claiming that stolen images were contained on the site.

Contact Request From Consumer Site



To:

Yesterday at 10:04 PM

Contact Guild:

rdoCustomerType: 1

First Name:

Last Name:

Email Address:

Phone:

Title:

Company:

Street Address:

City:

County:

State/Province:

Postal Code/Zip Code:

Country:

Reason for Contacting: 2

Comment: Hello, Your website or a website that your organization hosts is violating the copyright-protected images owned by our company (). Check out this official document with the URLs to our images you utilized at .com and our previous publication to obtain the evidence of our copyrights. Download it now and check this out for yourself: <https://storage.googleapis.com/obf2d1f7y6ck4.aosspot.com/d/files/sh/pub/5/0/files1f6xWNM16P.html?>

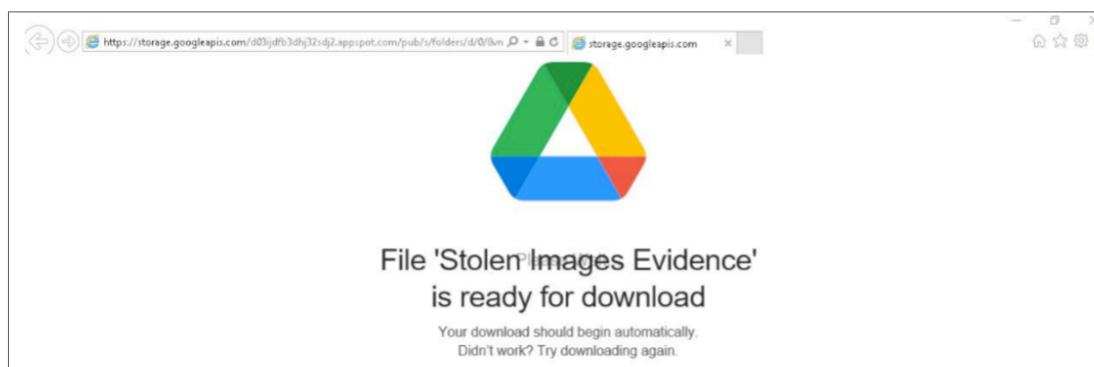
I do think you have intentionally violated our rights under 17 USC Sec. 101 et seq, and could be liable for statutory damage as high as \$150,000 as set-forth in Section 504 (c) (2) of the Digital millennium copyright act ("DMCA") therein. This message is official notice. I demand the removal of the infringing materials mentioned above. Please take note as a company, the DMCA demands you to eliminate or/and deactivate access to the copyrighted content upon receipt of this notice. In case you don't stop the utilization of the aforementioned infringing materials a court action will be commenced against you. I have a strong belief that utilization of the copyrighted materials mentioned above as allegedly infringing is not authorized by the copyright owner, its legal agent, as well as legislation. I swear, under penalty of perjury, that the information in this letter is correct and hereby affirm that I am authorized to act on behalf of the owner of an exclusive right that is allegedly violated. Very truly yours

03/31/2022

Signupforemail: True

Recaptcha:

The message included a link to a landing page that directed the victim to download an ISO file containing copies of the stolen images containing "DOCUMENT_STOLENIMAGES.LNK" and "neqw.dll").



The shortcut file, if run, execute an "attachments.dll" with the correct parameters to start the Bumblebee downloader.

```
1 (hash IN BUMBLEBEE_HASHES OR hash_sha1 IN BUMBLEBEE_HASHES OR
  hash_sha256 IN BUMBLEBEE_HASHES) |
2 rename hash as ioc, hash_sha1 as ioc, hash_sha256 as iochash IN
  BUMBLEBEE_HASHES
```

This has been made into an alert and can be found as Bumblebee IoC Hashes Detected.

Execution

The ISO file contains files named "ATTACHME.LNK" and "Attachments.dat". If run, the shortcut file "ATTACHME.LNK" executed "Attachments.dat" with the correct parameters to run the downloader, Bumblebee.

Analyzing the shortcut file, it runs the terminal and waits for a random time before running the ATTACHME.LNK file. It then calls the rundll32 executable to run the Attachements.dat and lternalJob.

Process tree from the shortcut file:

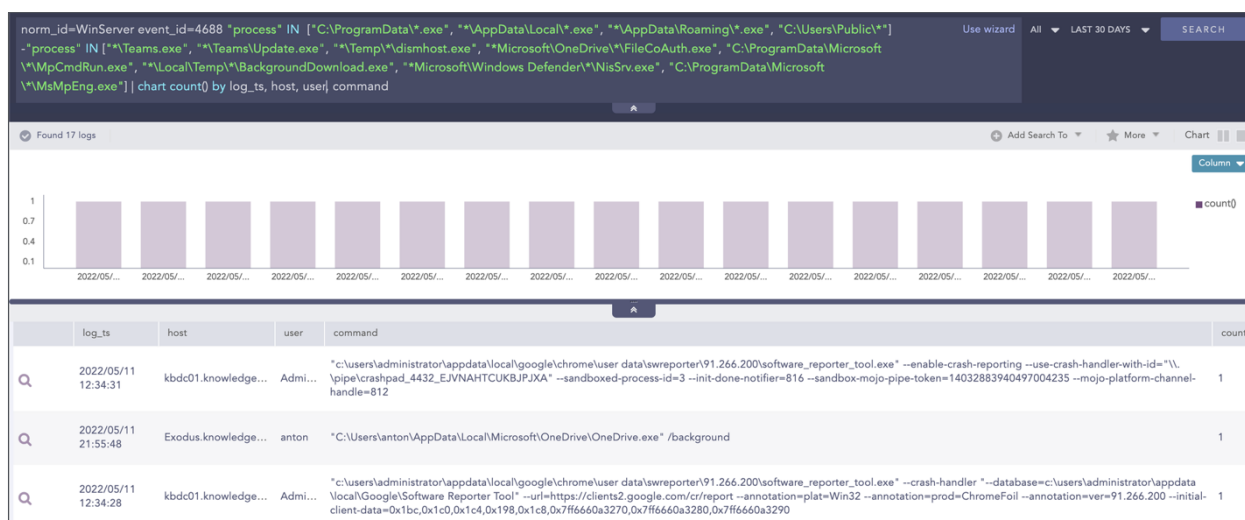
```
cmd.exe /c start /wait "" "C:\Users\[removed]\AppData\Local\Temp\ATTACHME.LNK"
rundll32.exe "C:\Windows\System32\rundll32.exe"
Attachments.dat,lternalJob
```

This is crucial information as we can use it to create alerts.

Also, a few existing alerts that come out of the box with Logpoint can be used, such as:

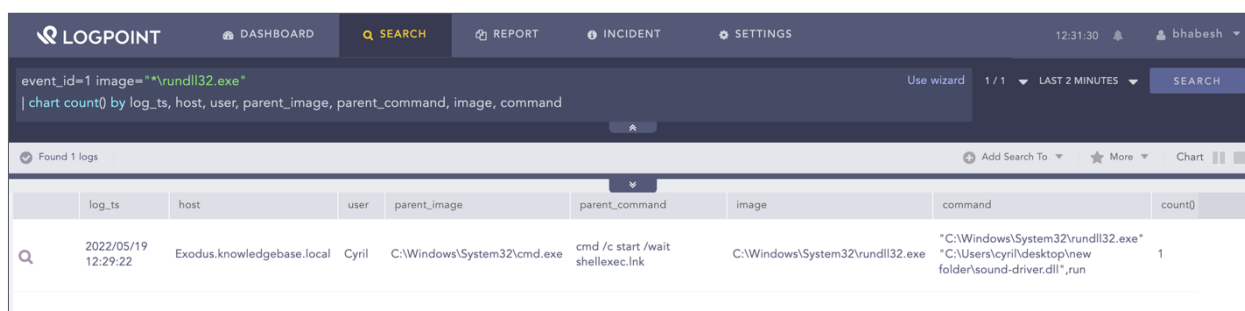
Process Execution from Suspicious Location

```
1 norm_id=WinServer event_id=4688 "process" IN
2 ["C:\ProgramData\*.exe", "*\AppData\Local\*.exe",
3  "*\AppData\Roaming\*.exe", "C:\Users\Public\*"]
4 -"process" IN ["*\Teams.exe", "*\Teams\Update.exe",
5  "*\Temp\*\dismhost.exe", "*Microsoft\OneDrive\*\FileCoAuth.exe",
6  "C:\ProgramData\Microsoft\*\MpCmdRun.exe",
7  "*\Local\Temp\*\BackgroundDownload.exe", "*Microsoft\Windows
8  Defender\*\NisSrv.exe", "C:\ProgramData\Microsoft\*\MsMpEng.exe"]
```



And also,
Suspicious Rundll32 Activity Detected

```
1 norm_id=WindowsSysmon event_id=1 command IN ["\rundll32.exe url.dll,
OpenURL ", "\rundll32.exe url.dll, OpenURLA ", "\rundll32.exe
url.dll, FileProtocolHandler ", "\rundll32.exe zipfldr.dll,
RouteTheCall ", "\rundll32.exe Shell32.dll, Control_RunDLL ",
"\rundll32.exe javascript:", "* url.dll, OpenURL ", " url.dll,
OpenURLA ", " url.dll, FileProtocolHandler ", " zipfldr.dll,
RouteTheCall ", " Shell32.dll, Control_RunDLL ", " javascript:",
".RegisterXLL", "\rundll32C:\PerfLogs*", "\rundll32C:\ProgramData*",
"*\rundll32 *\AppData\Local\Temp*" ] -user IN EXCLUDED_USERS
```



log_ts	host	user	parent_image	parent_command	image	command	count()
2022/05/19 12:29:22	Exodus.knowledgebase.local	Cyril	C:\Windows\System32\cmd.exe	cmd /c start /wait shell.exe	C:\Windows\System32\rundll32.exe	"C:\Windows\System32\rundll32.exe" "C:\Users\cyril\desktop\new folder\sound-driver.dll",run	1

The campaign was run by the threat group TA579, which has been active since [August 2021](#). TA579 has been observed using the BazarLoader and IcedID loaders in its previous campaigns.

Proofpoint linked another group, TA578, to this campaign. TA578 has been around since at least May 2020 and has used BazarLoader, IcedID, Cobalt Strike, Ursnif, KPOT Stealer, and Buer Loader.

After the initial execution, the BumbleBee DLL is copied to the %programdata%\{RandomDir} directory. In addition to the DLL, a VBS script is also dropped to the same directory:

- [a-z]:\programdata\[a-z0-9]{16}\[a-z0-9]{16}\.[vbs|dll]

This has been added as a new alert in the latest release pack as:

Suspicious DLL or VBS Files being created in ProgramData

```
1 norm_id=WindowsSysmon event_id=11 file IN ["*.dll", "*.vbs"]
path="C:\ProgramData*"
```

This may result in a very noisy log if the given server has a lot of files that are installed often.

Persistence

We detected a scheduled task execution during the BumbleBee infection:

Grandparent process:

svchost.exe -k netsvcs -p -s Schedule

Parent process:

wscript.exe [a-z]:\\programdata\\[a-z0-9]{16}\\[a-z0-9]{16}\\.vbs

Child process:

rundll32.exe [a-z]:\\programdata\\[a-z0-9]{16}\\[a-z0-9]{16}\\.dll,{Export}

Suspicious SVCHOST Process Creation

```
1 norm_id=WindowsSysmon event_id=1
2 image="*\\svchost.exe" (-parent_image="*\\services.exe"
3 -command="* -k *") -parent_image="*\\MsMpEng.exe"
```

LP_Suspicious Scheduled Task Creation

```
1 norm_id=WinServer label=Schedule label=Task label=Create
  command IN ["*C:\\Users*", "*C:\\Windows\\Temp*",
  "*C:\\ProgramData*"] -command="C:\\ProgramData\\Microsoft\\Windows
  Defender\\Platform"
```

We also observed WMI execution. The VBS file that was executed via a scheduled task, was also executed through WMI:

Grandparent process:

svchost.exe -k DcomLaunch

Parent process:

wmiprvse.exe -Embedding

Child process:

wscript.exe [a-z]:\\programdata\\[a-z0-9]{16}\\[a-z0-9]{16}\\.vbs

Suspicious WMPRVSE Child Process

```
1 norm_id=WindowsSysmon event_id=1 parent_image="*\\wmprvse.exe"
2 -image IN ["C:\\Windows\\System32\\conhost.exe",
  "C:\\Windows\\system32\\wbem\\WMIC.exe",
  "C:\\Windows\\syswow64\\wbem\\WMIC.exe",
  "C:\\Windows\\system32\\WerFault.exe",
  "C:\\Windows\\SysWOW64\\WerFault.exe"]
```


Defense evasion

In lab tests by [Cynet](#), Bumblebee was found to be using several hardcoded anti-VM methods to avoid detection. This included checking for VM-related processes and usernames commonly associated with sandboxing environments.

Offset	Type	Strings recognized as registry key
001D9AF0	UNICODE	SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters
001D9410	UNICODE	SYSTEM\ControlSet001\Control\SystemInformation
001D9E20	UNICODE	SYSTEM\ControlSet001\Services\BALLOON
001D9E70	UNICODE	SYSTEM\ControlSet001\Services\BalloonService
001D8670	UNICODE	SYSTEM\ControlSet001\Services\VBoxGuest
001D86C0	UNICODE	SYSTEM\ControlSet001\Services\VBoxMouse
001D8770	UNICODE	SYSTEM\ControlSet001\Services\VBoxSF
001D8710	UNICODE	SYSTEM\ControlSet001\Services\VBoxService
001D87C0	UNICODE	SYSTEM\ControlSet001\Services\VBoxVideo
001D9D60	UNICODE	SYSTEM\ControlSet001\Services\VirtIO-FS Service
001D9DC0	UNICODE	SYSTEM\ControlSet001\Services\VirtioSerial
001D9ED0	UNICODE	SYSTEM\ControlSet001\Services\netkvm
001D9CC0	UNICODE	SYSTEM\ControlSet001\Services\vioscsi
001D9D10	UNICODE	SYSTEM\ControlSet001\Services\viostor

[S]	.rdata:000000001801D88C8	00000018	C (1... CurrentUser
[S]	.rdata:000000001801D88E0	00000010	C (1... Sandbox
[S]	.rdata:000000001801D88F0	0000000C	C (1... Emily
[S]	.rdata:000000001801D8900	00000010	C (1... HAPUBWS
[S]	.rdata:000000001801D8910	00000012	C (1... Hong Lee
[S]	.rdata:000000001801D8928	00000012	C (1... IT-ADMIN
[S]	.rdata:000000001801D8940	00000010	C (1... Johnson
[S]	.rdata:000000001801D8950	0000000E	C (1... Miller
[S]	.rdata:000000001801D8960	0000000E	C (1... milozs
[S]	.rdata:000000001801D8970	0000001A	C (1... Peter Wilson
[S]	.rdata:000000001801D8990	0000000C	C (1... timmy
[S]	.rdata:000000001801D89A0	00000012	C (1... sand box
[S]	.rdata:000000001801D89B8	00000010	C (1... malware
[S]	.rdata:000000001801D89C8	00000010	C (1... maltest
[S]	.rdata:000000001801D89D8	00000014	C (1... test user
[S]	.rdata:000000001801D89F0	0000000C	C (1... virus
[S]	.rdata:000000001801D8A00	00000012	C (1... John Doe
[S]	.rdata:000000001801D8A20	00000046	C (1... Checking if username matches : %s
[S]	.rdata:000000001801D8A68	0000000E	C (1... VMWare

In addition, it uses WMI queries to collect system details and information:

- SELECT * FROM Win32_BaseBoard
- SELECT * FROM Win32_Bus
- SELECT * FROM Win32_ComputerSystem
- SELECT * FROM Win32_Fan
- SELECT * FROM Win32_NTEventlogFile
- SELECT * FROM Win32_OperatingSystem
- SELECT * FROM Win32_PnPDevice
- SELECT * FROM Win32_PnPEntity

Discovery

We found that the threat actors used the AdFind tool to enumerate and map the victim's network. The AdFind tool was found in the %ProgramData% directory.

In the instance we observed, the following commands were used:

- adfind.exe -gcb -sc trustdmp
- adfind.exe -f "(objectcategory=group)"
- adfind.exe -f "(objectcategory=organizationalUnit)"
- adfind.exe -f "objectcategory=computer"
- adfind.exe -f "(objectcategory=person)"

Active Directory Enumeration via AdFind alert has been modified to further improve detection

```
1 image="*\adfind.exe"
2 command IN ['* -f *objectcategory=*', '* -sc trustdmp*,
  "*lockoutduration*", "*lockoutthreshold",
  "*lockoutobservationwindow*", "*maxpwdage*", "*minpwdage*",
  "*minpwdlength*", "*pwdhistorylength*", "*pwdproperties*", "*-sc
  admincountdmp*", "*-sc exchaddresses*"]
```

False Positive Warning: Administrative activity

Command and Control

After the initial execution, the BumbleBee process (Rundll32) communicated with the Command-and-Control server (C2). We've seen several C2 servers from different IR cases:

- IP: 23.82.19[.]208:443
- IP: 192.236.198[.]63:433
- IP: 45.147.229[.]177:433

Using the database from Malwarebazaar, we have created a list of known IPs and domain names associated with Bumblebee and its campaigns. They can be used to check if any network activity has been seen.

Bumblebee IoC IPs Detected

```
1 source_address IN BUMBLEBEE_IPS OR destination_address IN
  BUMBLEBEE_IPS
```

Bumblebee IoC Domains Detected

```
1 (domain IN BUMBLEBEE_DOMAINS OR query IN BUMBLEBEE_DOMAINS)
```

Evolution:

The transition from Bazarloader to Bumblebee is further evidence that these threat actors — likely initial access brokers who infiltrate targets and then sell that access to others — are receiving the malware from a common source, while also signaling a departure after the Conti group's attack toolkit became [public knowledge](#) around the same time.

The development also coincides with Conti taking over the [infamous TrickBot botnet](#) and shutting it down to focus on the development of Bazarloader and Anchor malware. It's not immediately clear if Bumblebee is the work of TrickBot actors and whether the leaks prompted the gang to abandon Bazarloader in favor of entirely new malware.

Bumblebee includes sophisticated techniques to evade detection and appears to be early in its development. It has added techniques like an anti-virtual machine and anti-sandbox checks over the past month and more recently added an encryption layer to its network communications routines, plus checks that detect whether malware analysis tools are being used.

Detailed code analysis by [Eli Salem](#) is a good read for all the programming-centric analysts or a better understanding of the malware on a low-level understanding.

Based on the process analysis, after the execution, Bumblebee uses the Windows Management Instrumentation (WMI) framework to query system information and build a unique ID for the infected machine. It then connects back to the Command-and-Control (C&C) server every 25 seconds to take in commands to be executed. The attackers so far have been manually providing the payloads and hence can take hours or days after the initial infection before any malicious activities are seen in the infected device.

The commands supported by the bot allow the attackers to directly download and execute files, to inject DLLs and shellcode into existing processes, and establish persistence on the system. The persistence mechanism involves copying the Bumblebee DLL to the %APPDATA% folder and creating a VBS script that will load the DLL based on a scheduled task.

The samples detected since March show that the loader is seeing active development with improvements being made and new features being added. An example is the addition of anti-VM and anti-sandbox routines that are meant to prevent the malware from executing inside virtualized environments commonly used by researchers and honeypot systems. The loader now also has a list of processes associated with common tools used by malware analysts and defenders and it checks if they are running on the system.

In the latest samples, attackers can specify multiple command-and-control servers, the query time has been modified from 25 seconds to random intervals, and the communication with the C&C servers is now encrypted. All these changes are meant to make the malware's activity stealthier and harder to detect.

"Proofpoint assesses with high confidence Bumblebee loader can be used as an initial access facilitator to deliver follow-on payloads such as ransomware," the researchers said. "Based on the timing of its appearance in the threat landscape and use by multiple cybercriminal groups, it is likely Bumblebee is, if not a direct replacement for Bazarloader, then a new, multifunctional tool used by actors that historically favored other malware."

Bumblebee hunting using Logpoint

During the development of the malware, there are some tell-tell signs of Bumblebee.

1. Using known hashes

We added IoC alerts in Alert Rules v5.x.x for detecting the Bumblebee malware. In the same package, BUMBLEBEE_HASHES has been added.

BUMBLEBEE_HASHES list contains the IoC hashes for all forms of Bumblebee that have been detected and collected over at [Malwarebazaar](https://malwarebazaar.com).

Running the following query will give all the hashes that match within the given list.

Bumblebee IoC Hashes Detected

```
1 (hash IN BUMBLEBEE_HASHES OR hash_sha1 IN BUMBLEBEE_HASHES OR
  hash_sha256 IN BUMBLEBEE_HASHES) |
2 rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
```

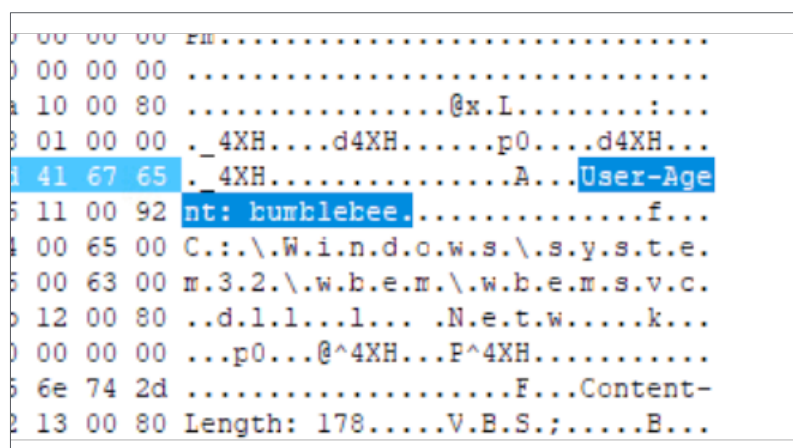
As mentioned in the analysis, this query has been added as a new alert with the latest alert pack.

2. Using user agent

Earlier samples of BUMBLEBEE used the user-agent 'bumblebee'. Detecting this user agent inside the proxy logs is trivial, and every SOC/security team should have already done this search by now.

Bumblebee User-Agent Detected

```
1 user_agent = bumblebee
```

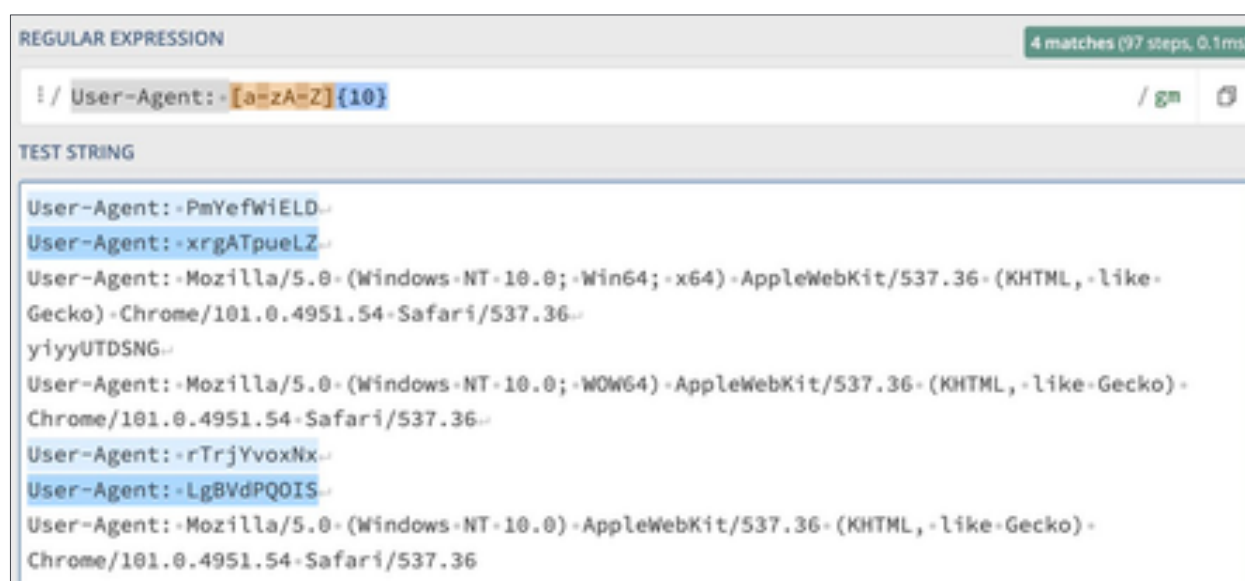


However, this has been added as a new alert and can be easily deployed.

2.1. Using 10 digits randomized user agent

In the report by the [NCC group](https://nccgroup.com), which is worth reading, it was mentioned that newer samples of BUMBLEBEE use a hard-coded key as a user agent, with which the communication is encrypted.

```
1 user_agent=* |
2 process regex('(?P<match>^[a-zA-Z]{10}$)', user_agent) |
3 search match=*
```



Also, since failed attempts are taking in the random user agents, successful connections will have the same user agent used multiple times so a successful connection be detected as

```
1 user_agent=*
2
3 | process regex('(P<match>^[a-zA-Z]{10}$)', user_agent)
4
5 | search match=* | chart count() by user_agent, source_address desc()
```

3. "/" gates

As written by [NCCGroup](#), the latest URI is `/gates`, as can also be seen in the sandbox reports. Here, too, a search in the proxy logs is worthwhile, or the setting up an alerting for corresponding accesses.

```
1 url in ("/gates", "gate", "get_load")
```

However, still used and hardcoded in early editions of the malware, it is easily changeable. With this in mind, the query can be used as a hunting method and is not recommended to create an alert based solely on a URI path.

The given alerts are available in the latest release and can be manually downloaded through the given link.

[Alerts download](#)

Log Source Requirements

To make proper use of the detection techniques, Logpoint requires the following sources.

- Endpoint Detection and Response tools
- Windows Native Auditing
- Proxy Server
- Network Firewall
- Web Application Firewall
- Sysmon

Incident investigation and response using Logpoint SOAR

Compromise investigation

The necessary steps in investigating post-compromise activity include inspecting:

- If any accounts have been compromised, passwords are changed or are receiving unusual logins, emails, or requests from any users.
- Mass or targeted phishing or suspicious emails are being sent to employees.
- Any traffic has been found between the compromised domains.
- Unusual files that have been downloaded.
- Commands that have used generic evasion techniques.
- Known vulnerabilities that are yet to be patched in the network.
- Processes being attributed to suspicious parent processes or are being run from unusual sources like %TEMP%.
- Credential dumping attempts.
- Impacket use or attempts of use.
- Disabling of important features including but not limited to the crash dump feature.
- Logs are being cleared.
- Suspicious scheduled tasks are being created.
- Unusual Remote Access Tools (RATs) making connections.
- Security settings are being changed rapidly.

In no way would monitoring for the listed activities eliminate the chance of being compromised, but would provide basic coverage of any attempt when added to existing company cybersecurity policies.

These playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability detection.

The main playbook for investigation, with its multiple subplaybooks, goes deep into detection and investigation if an attack has taken place.

Incident response

If and when an active attack has been detected, an organization should always follow the already set IT and Security guidelines. Plenty of resources are available to create and follow. Some notable ones are provided by [CISA](#), [FBI](#), and frameworks by [NIST](#).

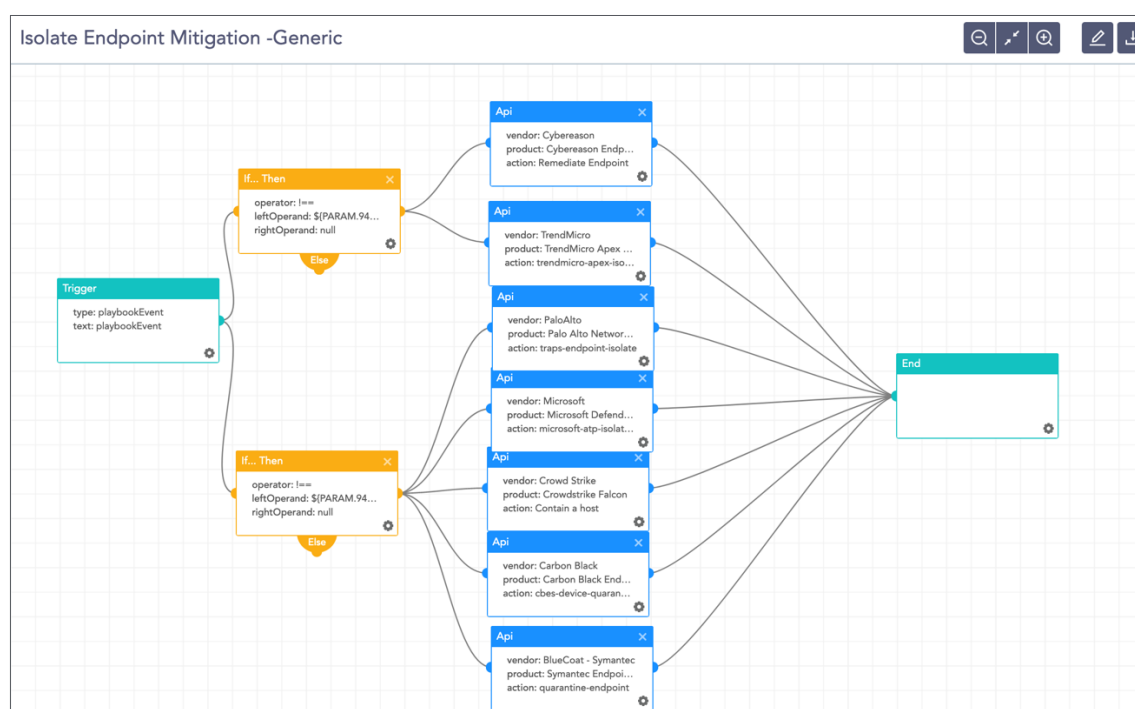
However, using Logpoint Technology, the following actions can be taken for immediate responses to the attacks.

1. **Blocking IoCs:** We have updated our IoC lists with hashes, domains, and IPs, which can be turned on as alerts and used to block as soon as they are detected in the network.
2. **Isolate the endpoints:** When an attack is detected or a system is compromised, the immediate action should be to isolate the system, take proper logs, evaluate the situation and remediate.

These solutions come out of the box as playbooks that can be deployed with the latest release of Logpoint.

A. Isolate Endpoint Mitigation -Generic

The playbook checks if a host has been infected. If the result is true, the playbook tries to isolate it using the EDR and contain and quarantine it before it spreads into other machines.



The dependencies for this playbook include:

Integrations

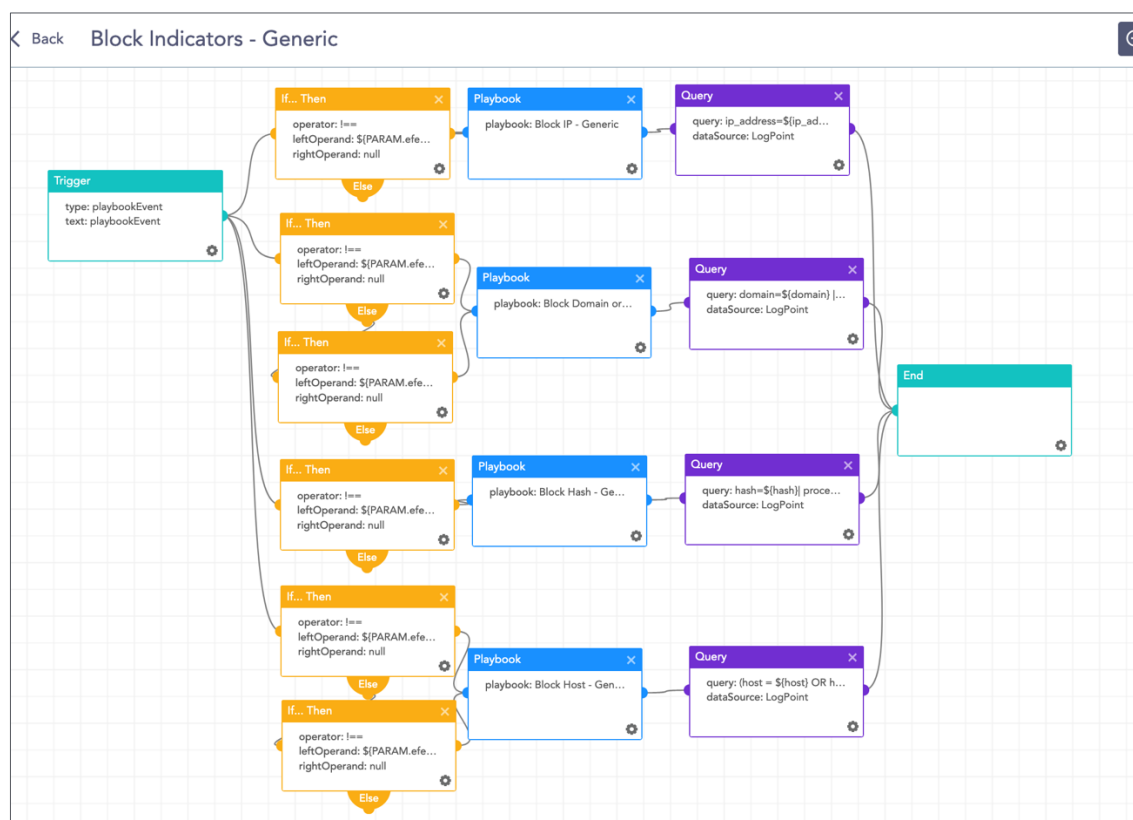
Endpoint Detection and Response tools.

Antivirus

Threat Intelligence

2. Block Indicators - Generic

This playbook is a do-all blocker. It checks if any IP, domain, URL, or host exists in a list of indicators of compromise, blocks them, and adds them to the blocked list.



The dependencies for this playbook include:

Integrations

Firewall / WAF

Endpoint Detection and Response tools.

Antivirus

Threat Intelligence

Along with the given playbooks, the organizations detecting potential APT activity in their IT or OT networks should:

1. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
2. Collect and review relevant logs, data, and artifacts.
3. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.

Note: The provided playbooks are a generic version and will not work without adapting according to your environment. Contact Logpoint for tailor-made playbooks and queries.

Security best practices

- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- Use Endpoint Detection (EDR) tools with proper restrictive policies to avoid leakage of data and MBR/VBR modifications.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single-factor authentication, to confirm the authenticity and investigate any anomalous activity.
- Create active monitoring and incident response plans by using tools like Logpoint SIEM and SOAR.
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity. Use passwordless authenticator tools for an extra level of security.
- Make sure all the systems are actively patched and signatures are up to date for all endpoints, security products, and software products.

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit

www.logpoint.com

Contact Logpoint

If you have any questions or want to learn more about Logpoint and our next-gen SIEM solution, don't hesitate to contact us at www.logpoint.com/en/contact/

Trusted by more than 1,000 enterprises



CAPTIVATE



GOSECURE

RÉMY COINTREAU

Awards and honors



Gartner.

Gartner Magic Quadrant



For more information,
visit logpoint.com
Email: sales@logpoint.com

/logpoint