Understanding BumbleBee Loader: The Delivery

Understanding BumbleBee:

The delivery of Bumblee

Let’s explore how the malicious loader BumbleBee employs different delivery methods including OneNote documents, LNK, ISO and PDf files and HTML smuggling to deliver the payload.

BUMBLEBEE BLOG SERIES – 1

09 August 2023

DOWNLOAD THE E-BOOK

Table of Contents

BumbeBee loader: an overview

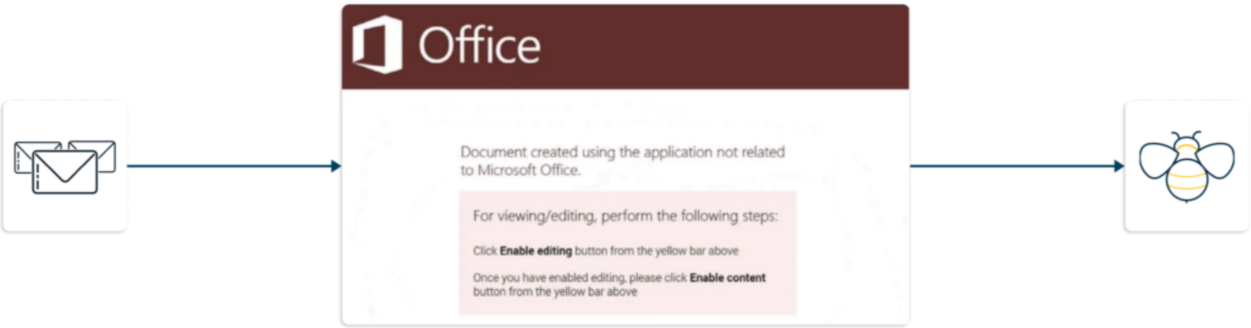
In March of 2022 a new loader equipped with more than 50 evasion techniques was spotted in the wild: BumbleBee employs a variety of methods to escape detection – from complex delivery chains and hooking-based loading to iterating through a collection of evasion techniques to detect manual and dynamic analysis. This demonstrates the strong focus attackers have recently put on escaping ever-evolving monitoring tools.

BumbleBee, named after the user-agent it used during C2 communication in the original version, can be regarded as the successor to the popular BazarLoader. Similar to BazarLoader, attackers employing BumbleBee showcase an interesting variety in delivery chains, from common methods of delivering executables inside ZIP attachments via email, to more sophisticated attacks involving password-protected ZIP archives containing an ISO file and Windows shortcuts to execute a malicious binary which is heavily packed and protected to hinder manual analysis.

Recently, we have been tracking BumbleBee and its code changes starting from one of the first samples spotted in the wild to more recent variants. Our analysis shows significant changes in network functionality and evasion techniques with constants updates that are likely to continue. Our analysis also shows that BumbleBee is currently in the top ten malware families that we see on VMRay Platform on a daily basis, suggesting that it might gain even more in popularity in the future.

Unveiling BumbleBee’s delivery methods

The most popular and widely known method for delivering malware is through email attachments containing a malicious executable, document or script, see Figure 1.



Document created using the application not related to Microsoft Office.

For viewing/editing, perform the following steps:

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

Figure 1: Simple delivery chain commonly observed for malware requires users to open an attachment and execute the malicious file (e.g. an Office document with macros).

BumbleBee, however, often goes much further and adds additional layers of obfuscation.

One interesting delivery chain starts with an email containing a **password-protected ZIP archive,** which already complicates the analysis of the malware if the password is not extracted properly from the email body. The main reason for this approach is that it is not possible to decrypt a ZIP archive without the accompanying password (if the password is of sufficient strength). First, this prevents analysis by virus scanners triggered either automatically by the email provider or the email client, and second, this prevents analysis in a dynamic, behavior-based analysis engine if the submission misses the email containing the password.

In one case we observed, the archive itself did not contain an executable, document or script – rather, it contained an **ISO file which is commonly used as a filesystem for optical disks,** such as CD-ROM's. While these ISO files on their own are not malicious in nature, malware developers, in their effort to find new obscure techniques to evade analysis and infect systems, have opted to embed their malicious files inside these rather uncommon file systems. In the final step, opening the ISO file presents the user with a folder containing a Windows shortcut which executes a hidden DLL file. Some of this variety in delivery chains is demonstrated in Figure 2.

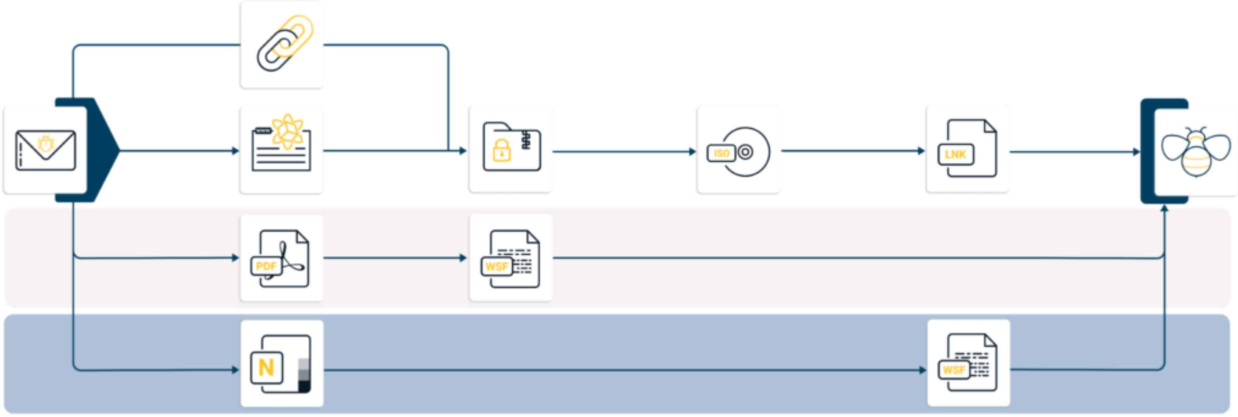


Figure 2: Excerpt of the complex delivery chain observed for BumbleBee showing PDF documents, HTML smuggling, ISO files, LNK fils and OneNote attachments

HTML Smuggling

Some attackers make use of a technique called HTML smuggling where the payload for the next stage is directly embedded in an HTML file. This avoids the need for a remote server as no download is required.

These HTML files are delivered via email attachments and typically drop either **ZIP archives (sometimes password-protected) or ISO files.** This attack scenario is likely the result of file extension blocking: many email providers have block-listed potentially risky file extensions, e.g., executable files with an "exe" extension or script files with the "vbs". However, most providers allow ZIP files and many allow HTML files to be attached to an email.

ISO File

Threat actors are always on the hunt for lesser known file formats in the hope that a lack of support for such file types in malware scanners can be used as a means to evade analysis. In this regard, QBot, BazarLoader and BumbleBee (among others) have been observed to use **ISO files to store their malware** in a similar fashion to how ZIP archives have been commonly used before.

ISO files are widely known as image formats representing the content of CD-ROM's, that's why they are mounted as drives when they are double-clicked (see Figure 3). This simulates the insertion of an actual CD or DVD-ROM.

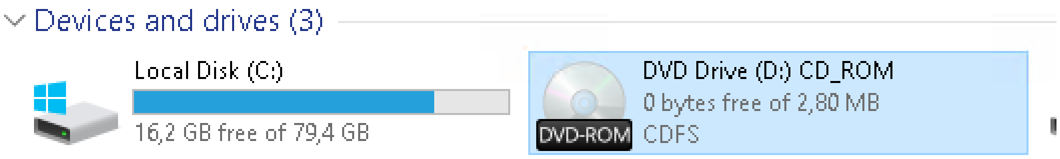
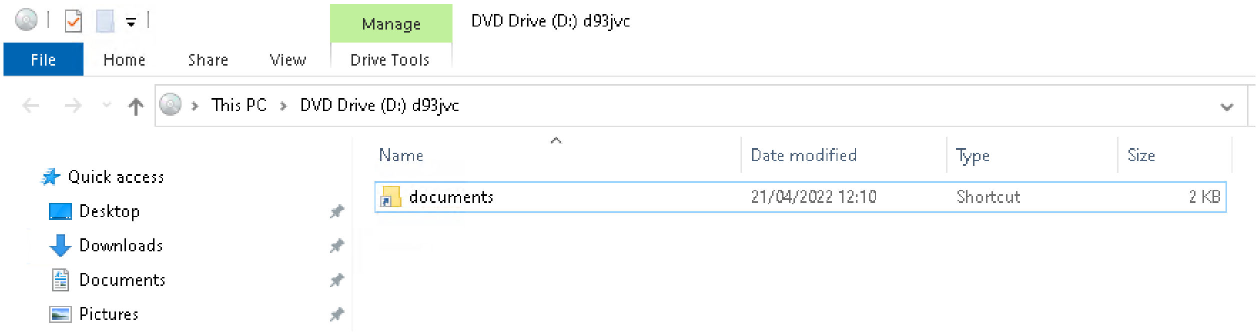


Figure 3: Double-clicking on an ISO file mounts the file as a CD or DVD-ROM drive.

Once the user has unpacked the content of the archives, a double click on the ISO file opens a window with the content of a new drive: here, the user is presented with a single file using the directory icon to masquerade as a folder (see Figure 4). This **gives the user a false sense of security** as double-clicking on a folder is a far more secure action than double-clicking on an executable. However, the file on this drive is actually a Windows shortcut **which finally executes BumbleBee.**

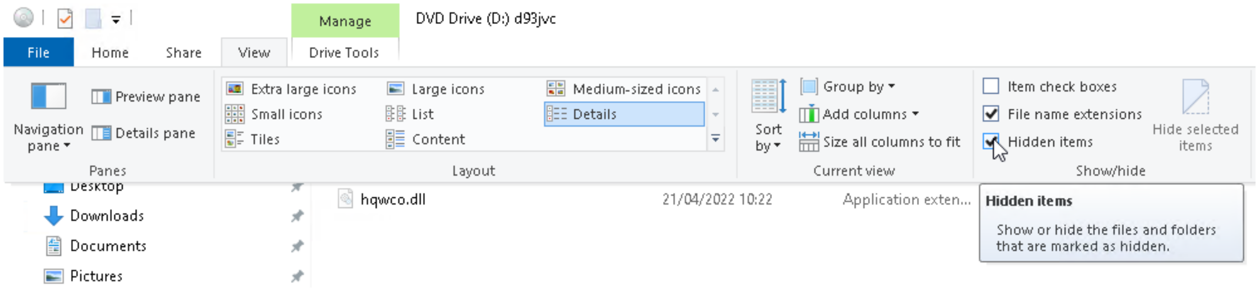
Previously, victims have noted that Windows does not prompt the user for confirmation before executing the malware, which is usually the case for ZIP files downloaded from the web. Before late 2022, Windows did not use the so-called Mark-of-the-Web to track ISO files and their content, a hidden marker to classify files as coming from the Internet and thus requiring more caution (additional AV scans, Microsoft Office documents are opened in protected mode, etc.) This allowed ISO files to fly under the radar.



Name	Date modified	Type	Size
documents	21/04/2022 12:10	Shortcut	2 KB

Figure 4: Once the ISO file is mounted, a popup automatically reveals the content. In this case, it's a shortcut abusing the folder icon and the name "documents" to fool the user into thinking a double-click will not execute an application but just open a folder which is a far safer action, when in fact this file will infect the system.

One additional advantage of ISO files (which is not possible with ZIP files) is the ability to contain hidden files. Windows users are not presented with those by default. BumbleBee abuses this to **hide a DLL file which contains the actual malicious code** (see Figure 5).



□ Item check boxes
☑ File name extensions
☑ Hidden items

hqwco.dll 21/04/2022 10:22 Application exten...

Hidden items
Show or hide the files and folders that are marked as hidden.

Figure 5: Activating the display of hidden items reveals an otherwise invisible DLL file in the same folder.

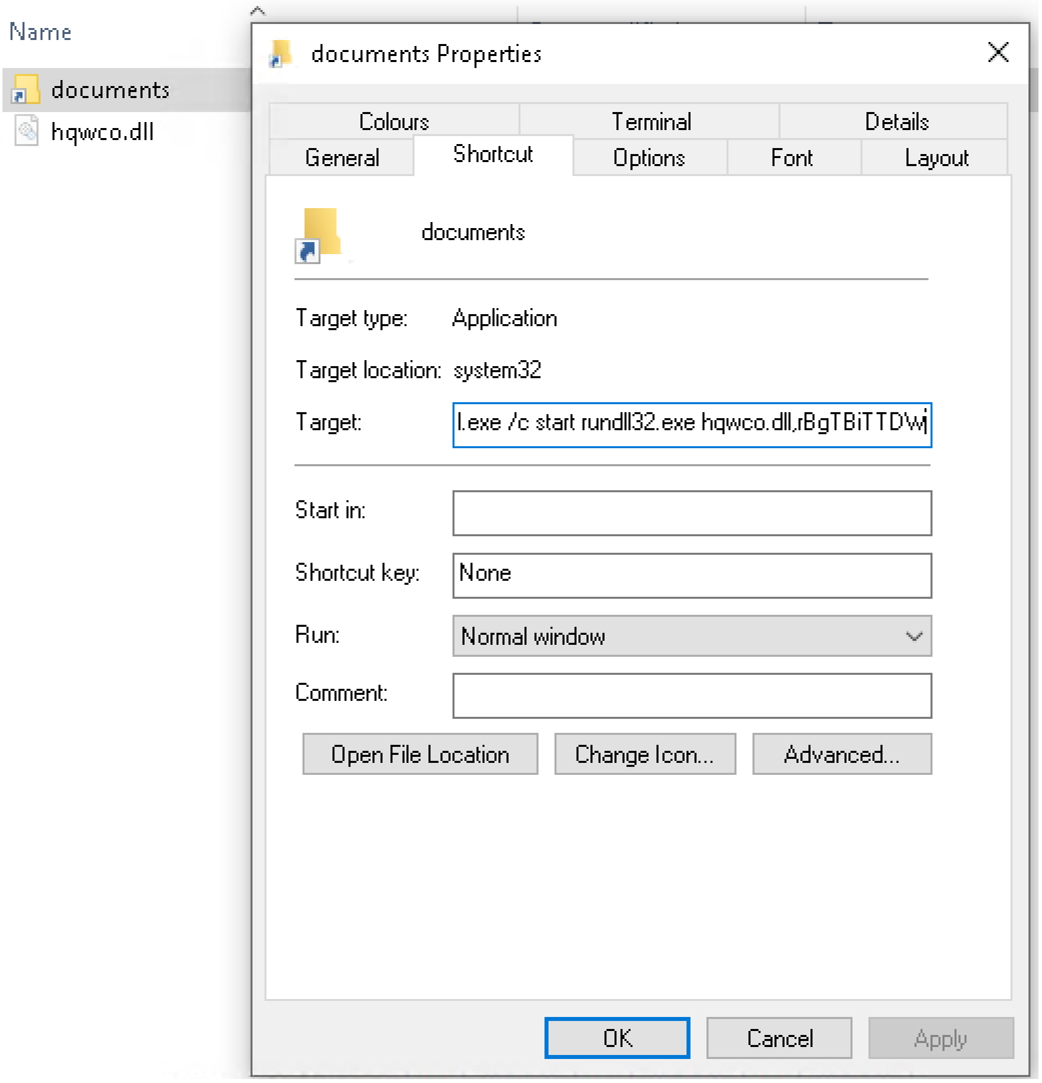
Features like these, i.e., an obscure file format supported by Windows by default and the ability to hide files, make ISO files a perfect tool to deliver malware.

LNK File

Similar to ISO files, Windows shortcuts (also known as LNK files) are usually not associated with malicious activity which is why threat actors are increasingly making use of this file type.

Basically, **LNK files are just shortcuts** (i.e., references) to other files on the system, so a double-click on a shortcut executes the linked target. As LNK files are not script files or executables themselves, attacks involving this type of method rely on executables that are already on the system, such as cmd.exe, powershell.exe or wscript.exe.

These are popular targets for malicious Windows shortcuts as their location is predictable for most users (i.e., cmd.exe is often found at “C:\Windows\system32\cmd.exe”). In this case, BumbleBee is delivered as a DLL file, and as libraries can not be executed directly, the Windows shortcut points to “rundll32.exe”, a helpful tool on Windows systems to execute specific functions in DLL files (see Figure 6).



documents

Target type: Application

Target location: system32

Target: l.exe /c start rundll32.exe hqwco.dll,rBgTBiTTDWj

Start in:

Shortcut key: None

Run: Normal window

Comment:

Figure 6: The "documents" file, masquerading with a folder icon, is actually a Windows shortcut pointing to rundll32.exe which again points to the hidden DLL file.

If this delivery chain sounds too complicated to work, note that the target does not see much of it – **they are only expected to open the attachment** and click on the file presented to them.

At the same time, analyzing any of these files (the password protected ZIP file, the ISO file or the LNK file) may break the automated analysis of the delivery chain for some malware analysis engines and thus the malware could potentially avoid detection.

Video: Step-by-step analysis of an LNK file

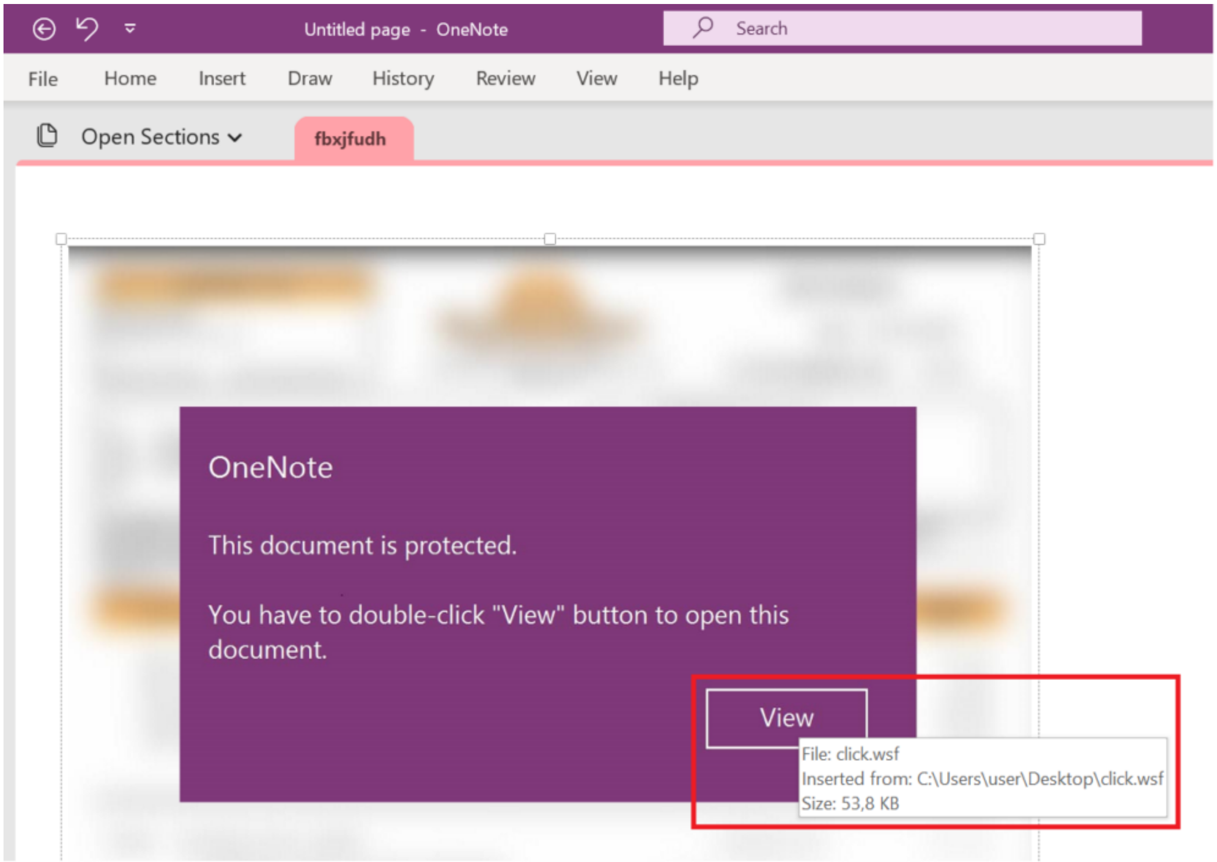
OneNote Document

Another delivery method abuses files for OneNote, a Microsoft Office application for note-taking.

There are multiple ways to deliver malware via OneNote, one interesting approach we have witnessed for the **Emotet malware family involves an embedded malicious script file.** When the OneNote file is opened, the user is presented with a fake interface containing instructions to **click on an image pretending to be a button.** However, this button is actually hiding a malicious script file just below (see Figure 7).

A double-click does not activate the button but actually instructs OneNote to extract and e**xecute the embedded executable file beneath.** Read our report here for more details.

Read the report: From OneNote to Emotet



OneNote

This document is protected.

You have to double-click "View" button to open this document.

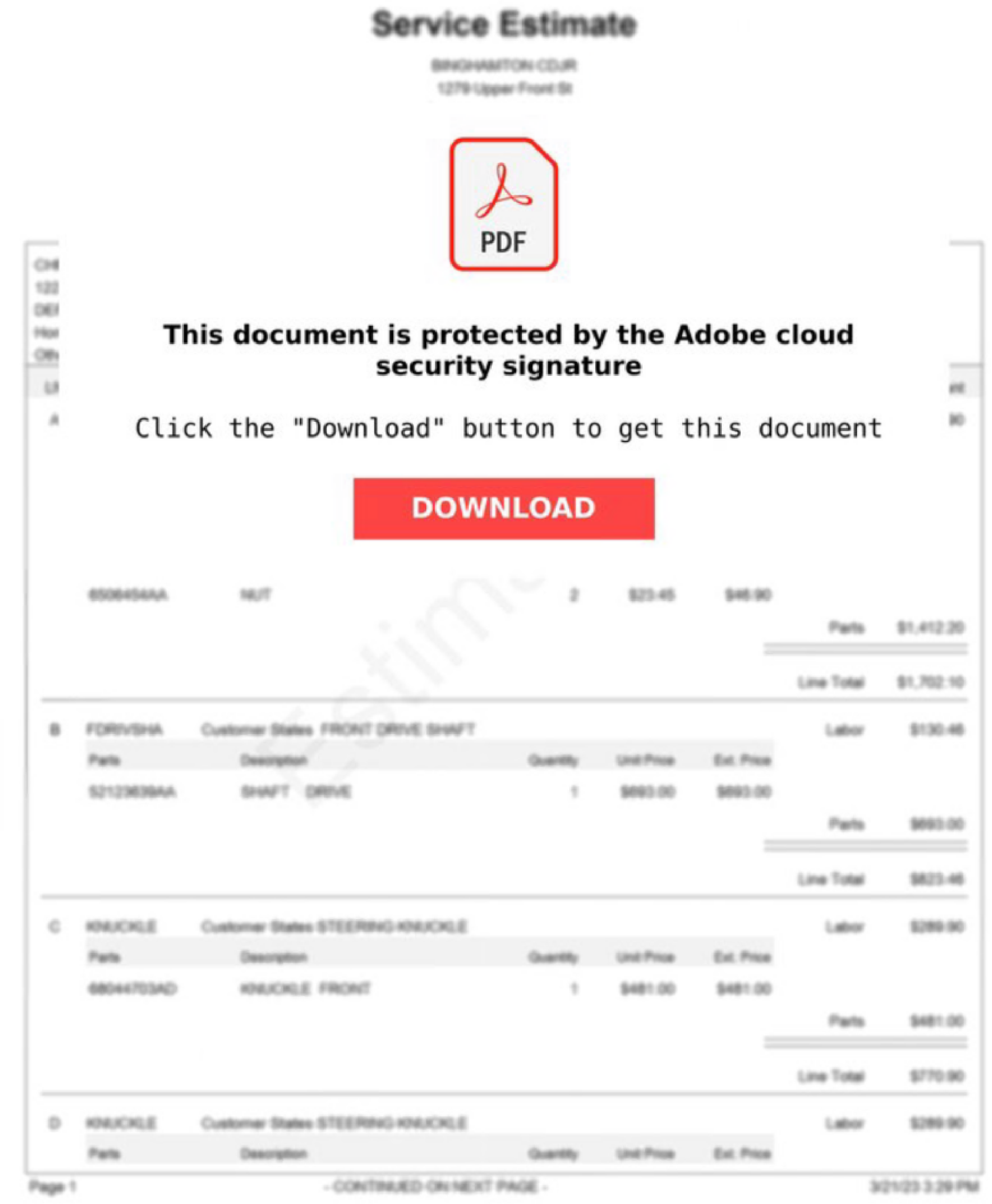
File: click.wsf
Inserted from: C:\Users\user\Desktop\click.wsf
Size: 53,8 KB

Figure 7: A malicious "WSF" script file hides behind a fake button in a OneNote document, which infects the system once the button is double-clicked.

PDF Document

Similar to the OneNote technique, another one involving PDF documents urges the user to click on a button which leads to a direct download. In this case too the button is actually an image pretending to belong to the PDF viewer.

This method can then be combined with the techniques illustrated above, e.g., the downloaded archive could in turn contain another ISO archive.



Service Estimate

This document is protected by the Adobe cloud security signature

Click the "Download" button to get this document

Figure 8: A malicious PDF document pretending to contain a button to download the next stage.

Conclusion

In conclusion, the intricate delivery methods employed by BumbleBee underscore the evolving sophistication of modern malware attacks.

Its multifaceted approach, leveraging a spectrum of attack vectors, highlights a significant departure from traditional tactics. BumbleBee’s proclivity for elaborate delivery chains, often involving techniques surpassing standard file attachments, demonstrates the lengths to which threat actors go to evade detection.

From password-protected ZIP archives and ISO files to HTML smuggling and Windows shortcuts, BumbleBee strategically employs a diverse array of strategies to infiltrate systems. By exploring and dissecting these innovative delivery mechanisms, we gain valuable insights into the evolution of malware, offering a unique perspective that is crucial for effective threat detection and mitigation strategies.

As we delve deeper into the subsequent segments of this blog series, we will uncover the intricacies of BumbleBee’s evasion techniques and the evolution of its configuration, enabling us to forge a comprehensive understanding of this persistent and evolving threat.

Emre Güler
Threat Researcher

BumbleBee Series – 2:
The malicious behavior

BumbleBee Series – 3:
The malware configuration and clusters