# **Amazon Cookie Stealer**

## : 11/06/2022

https://rhomaniertaylor.com https://twitter.com/lotus\_infosec https://www.linkedin.com/in/rhomanietaylorcyber/ https://github.com/lotus-infosec

# Background

https://direct.supportamzac.beckyimhauser[.]com/s5nrsoV

The link being investigated ^



I'll start this off by explaining the interesting relationship me and my mom have with the spam messages she receives. My mother frequently sends/shows me suspicious emails or messages she receives to make sure they're safe. This Amazon link intrigued me and I wanted to take a deeper dive, so I rallied the troops (*Darryl Terrell*). We started our investigation by spinning up our virtual machines, *Remnux* and *Kali Linux*, then got to work discovering the secrets that lay behind the link.

# Analysis

As soon as you click the link it redirects the victim to Amazon's official website. The attack begins by allowing cookies to be shared with the attacker giving them access to any user data input into the site. Once you put the information in it exfiltrates it back to the attacker. - Darryl The attacker uses an XSS (Cross Site Scripting Vulnerability) to send cookies back to themselves. The link itself redirects you to Amazon.com where it embeds a PHP session ID and allows Amazon to generate and send cookies back to the attacking website.

Using Burpsuite we can see exactly what the packets are doing in transit and the responses.



0 matches ⑦ ۞ ← → Sea

🔸 Burp Suite Community Edition v20... 🛛 🎃 Server Not Found — Mozilla Firefox 🗌 💿 Amazon.com.

(2)(3) (+) 50

0 matches



Side Note: Cookies can be decoded to learn about the data they store.

Going to the link itself, without the attachment at the end proves less than useful...



We figured out a decent bit of information about the website itself. I used Securitytrails to look at historical DNS data.

(This screenshot got severely messed up, so as a summary the DNS records changed roughly 3 years ago so I don't believe that is the reason for the attack.)

of Interview Organization Free Lass Lear Lass Develop Lass   99120122003100 Jampiane Into 2000202100 200020100 3 prems   • • 2000202100 200020100 3 prems   • • 2000202100 200020100 3 days   • • • 2000202100 3 days   • • • 2000202100 3 days   • • • 200020100 3 days   • • • 20002010 3 days   • • • • •   • • • • •   • • • • •   • • • • •   • • • • •   • •	
HH 2012 2018 120     Jumpine Inv     2022 2014 120     2022 01 120     2 years       ·	
TRL2H2x8336 Jurgine Inc. 2015-07-05 2023-05-16 11 minites Charanta Charanta	
Chinese Chineses	
111.204.248.138 Junyaherinic 2018-07-00 2019-07-04 1 year (H years) D years	
999.204.208.138 Jumpine Inc. 2016.10.20 2018.07.64 3 years (5 years) (4 years)	
NO.218.102.41 Structure 2015-10-10 2016-10-22 1 year (7 years) (5 years)	
10.2 IL 10.41 ПомПой 2010.00.20 2010.10.17 22 барь. // ревец // ревец	
2010-09-24 2010-09-25 1-6ay (7-years) (7-years)	
902293-90246 Secondar 2015-05-02 2015-05-24 20.4455 27.95920 17.96930 20.4455	
2015-00-01 2015-03-02 1 бир Сутема) Сутема)	
NO.218.102.41 28440848 2015-03-18 2015-03-81 6 months (8 press) (7 press)	
41.162.154.5 Staudhart 2014-06-18 2015-03-18 Featros 20.41001 20.9101	
198.23 dt.74 Bradiel 2014.04.11 2014.04.01 3 meths. (8 prov) (8 prov)	
2014-02-10 2014-09-11 4 multitle (7 years) (7 years)	
- 2010/07/0 2010/07 4 middle (7 years) // 2010/07 1 4 middle (7 years) // 2010/07 1 1 pear (7 years) // 2010/07 1 1 pear	

We figured out the website was built on cPanel.

Kali Linux × 🔒 Amazon.com. Spend less. × 🏟 Settings × 🧬 cPanel Login × +	
$\leftarrow \rightarrow \mathbb{C}$ $\bigtriangleup$ $\mathbb{O}$ $\mathbb{A}$ https://direct.supportamzac.beckyimhauser.com/2083 $\diamondsuit$	⊚ ≡
cPanel"	
Username	
L Enter your username.	
Password	
Enter your account password.	
tesis	
Log III	
English العربيد бъятарски ćeština dansk Deutsch Ελληνικά español	
CopyrightO 2022 chaol, LLC. Privare Day	

We also noted that it stored the cookies in our Firefox browser. But when trying to view the database in. ~/.mozilla/firefox/<user>/cookies.sqllite we quickly learned that it doesn't actually store cookies in the database, it's held in a volatile Firefox cache.

<u>1</u> a										
	id	originAttributes	name	value	host	path	expiry	lastAccessed	creationTime	isSe
		Filter	Filter	Filter	Filter		Filter	Filter	Filter	Filt
1			i18n-prefs	USD	.amazon.com		1698964078	1667428079895851	1667428079895851	
2			sp-cdn	"L5Z9:NL"	.amazon.com		1698964079	1667428079895873	1667428079895873	
3		^partitionKey=%28https%2Camazon.com	abid	e8c21d3a-b771-420d-a036-f4f59c87c6f3	.associates-amazon.com		1669847288	1667428088605745	1667428088605745	
4			session-token	"dVVswxID3qMUhmEUz9UACUWQaIrWmm	.amazon.com		1698964096	1667428096065548	1667428096065548	
5	19		csm-hit	tb:	www.amazon.com		1697668106	1667428106285907	1667428086601742	
6	20		ubid-main	131-4157812-1094806	.amazon.com		1698964105	1667428107326760	1667428091513951	
7	21		session-id-time	2082787201	.amazon.com		1698964105	1667428107326847	1667428079895829	
8	22		session-id	143-4929396-8361966	.amazon.com		1698964105	1667428107326899	1667428079895763	
9	23	^partitionKey=%28https%2Camazon.com	ad-id	A5zAwhyclUzQpVj5MTVPw00	.amazon-adsystem.com		1688250514	1667428116298279	1667428115549037	
10	24	^partitionKey=%28https%2Camazon.com	ad-privacy		.amazon-adsystem.com		1830378514	1667428116298374	1667428116298374	
11	25	^partitionKey=%28https%2Camazon.com	pt	v2:ceba03f2e2a80ef448f1aff353026c3659	.ispot.tv		1730500117	1667428119373951	1667428119373951	
12	26	^partitionKey=%28https%2Camazon.com	sambapxid	103bd71b2ccbb9cbf	ads.samba.tv		1701556118	1667428120266430	1667428120266430	
13	28	^partitionKey=%28https%2Camazon.com		1667428119	.myvisualiq.net		1730500119	1667428121051266	1667428121051266	
14	29	^partitionKey=%28https%2Camazon.com	tuuid_lu	1667428119	.myvisualiq.net		1730500119	1667428121051341	1667428121051341	
15	30	^partitionKey=%28https%2Camazon.com	ndat	aO2WYGNi7xe+NBrROSZ9Ag==	.ninthdecimal.com		1682980119	1667428121399774	1667428121399774	

The following websites store cookies and site data on your computer. Firefox keeps data from websites with persistent storage until you delete it, and deletes data from websites with non-persistent storage as space is needed.

Site	Cookies	Storage	▼ Last Used
amazon.com	9	86.0 KB	8 seconds ago
beckyimhauser.com	3		52 seconds ago

We did try to view cached and session cookie storage but low and behold, that didn't work either.

🔻 🖶 Cache Storage							
https://s.amazon-adsystem.com	Кеу 🔺	Value					
https://www.amazon.com							
			/				
https://s.amazon-adsystem.com			/				
https://www.amazon.com							
		tb:9AVWQQ4G31661R7XXZQ2+s-9AVWQQ4G31661R7XXZQ2[1667428566690&t:1667428566690&adb:adbik_no	1				
▼ 🗄 Indexed DB			1				
https://s.amazon-adsystem.com			/				
https://www.amazon.com							
👻 🚍 Local Storage							
https://s.amazon-adsystem.com							
https://www.amazon.com							
🕶 🚍 Session Storage							
https://s.amazon-adsystem.com							
https://www.amazon.com			l .				
			7				

Another side note:

We also tried using dirbuster to see if we can enumerate more files on the system. But to be honest, that failed horribly... Maybe next time.

#### 

-(kali® kali)-[~/Documents/amazonscam] 🖵 s<u>udo</u> dirb https://beckyimhauser.com <u>/usr/share/wordlists/dirbuster/directory-list-1.0.txt</u> -w 255 DIRB v2.22 By The Dark Raver START\_TIME: Wed Nov 2 17:46:16 2022 URL\_BASE: https://beckyimhauser.com/ WORDLIST\_FILES: /usr/share/wordlists/dirbuster/directory-list-1.0.txt OPTION: Not Stopping on warning messages **GENERATED WORDS: 141600** (!) WARNING: Wordlist is too large. This will take a long time to end. (Use mode '-w' if you want to scan anyway) ---- Scanning URL: https://beckyimhauser.com/ ----==> DIRECTORY: https://beckyimhauser.com/cgi-bin/ ==> DIRECTORY: https://beckyimhauser.com/images/ -> Testing: https://beckyimhauser.com/artists

## Summary

This is pretty much where the story stops. We tried a few passwords on the CPanel login but ultimately deciding that it'll probably be super illegal if we actually gained access. (Also the passwords didn't really work). We weren't exactly sure what to do after this. We identified how the attack was being done and where the site was being hosted. We weren't exactly sure of how the website itself is being used because the author is definitely a real person who may have just lost control over her domain name servers.

Also, Darryl reached out to the owner via email to inform them that their site might be being utilized for malicious purposes. We have yet to receive response at the time of this writing.

Overall this little excursion was fun. It was one of the first websites Darryl and I did that wasn't protected by Cloudflare and we managed to learn a lot from it. Hopefully on the next one we can figure out how to take the scammer down!!

-- Darryl's LinkedIn (https://www.linkedin.com/in/darrylty/)

### As usual... THE LINKS

https://mxtoolbox.com/DNSLookup.aspx

https://whatismyipaddress.com/ip/199.204.248.138

https://www.inmotionhosting.com/support/edu/cpanel/how-to-log-into-cpanel/

https://unix.stackexchange.com/questions/82597/where-does-firefox-store-its-cookies-on-

linux#:~:text=Firefox%20stores%20cookies%20in%20sqlite,%2Fcookies.

https://stackoverflow.com/questions/151026/how-do-i-unlock-a-sqlite-database

https://support.mozilla.org/en-US/questions/1219653

https://firefox-source-docs.mozilla.org/devtools-user/storage\_inspector/index.html

https://securitytrails.com/domain/beckyimhauser.com/history/a

https://www.google.com/search?

<u>q=xss+using+cookies&oq=xss+using+cookies&aqs=chrome..69i57j0i22i30l5j0i390l3.2080j0j7&</u> <u>sourceid=chrome&ie=UTF-8</u>

.=.A.=. ، ر\_\_\_ر \\V//