HOW TO CHECK MALICIOUS/ PHISHING LINKS

How to check if the links/URLs are malicious/phishing or not?

Malicious URL: http://rxqsd.com/9n4fbg (URL Sample (link is dead), can use your own)

Tools: URL Scan io, BrightCloud, Browserling

We need to answer all the questions below:

- Check the URL behaviour using https://urlscan.io/ Result:
- 2. Check domain reputation using https://www.brightcloud.com/tools/url-ip-lookup.php Result:
- 3. Interact with URL using virtual sandboxed browser from https://www.browserling.com/ Result:

Investigation

First, we need to check the URL behaviour using URLScan (<u>https://urlscan.io/</u>). Open the website.

	urlscan.io 🔒 Home 🔍 Search	🚯 Live	罷 API	🗲 Blog	Docs	C Pricing	ing 👤 Login			SecurityTrails			
		u	rls(A sandba	can	io								
	URL to scan I						▶ Pul	blic Scan	٥	Options			
Red	cent scans 🖑 Updates every 10s - Last upd	late: 00:55:5	7										
	URL					Age			Size	₽	IPs	*	ŧ
0	iqbroker.com/lp/regulated/?aff=283168					25 se	conds	<u>1</u> 4	38 KB	33	19	7	•
	www.youtube.com/?feature=youtu.be					28 se	conds	<u>#</u>	3 MB	76	9	2	-
	zenwriting.net/streetactor7/what-is-a-sales-manage	er				32 se	conds	1	75 KB	8	4	4	
	seguro.blueshopbrasil.com.br/cart					33 se	conds	0	1 MB	44	18	4	۲
	www.bigpanda.io/privacy-policy/?mkt_tok=Nzc4LVV	OSS05NjUA	AGBRMJ63	3hBji5eBOy2	ri-w	34 se	conds	题 9	95 KB	96	29	4	
	www.gettyimages.co.uk/						conds	82	6 MB	114	31	5	•
	www.vaillant.be/professionnels/?j=430192&sfmc_su	ub=11716607	&l=249_HTI	ML&u=1207	257	40 se	conds	822	4 MB	16	2	2	-
	www.vaillant.be/a-propos/information-generale/con	ditions-d-utili	sation/?j=43	8019		43 se	conds	82	3 MB	8	3	2	-
	myemail.constantcontact.com/We-now-have-Canad	lian-projects	html?soid=1	127600303.		45 se	conds	器 3	22 KB	20	8	2	

Then put the URL address that you want to check and click "Public Scan".

	urlscan.io 🕈 Home			Q Search	ه Live	醌 API	🗲 Blog	Docs	C Pricing	💄 Login		Seci	urity	rityTrails			
					u	rls(A sandba	can	io									
		http://rxqsd.co	om/9n4fbg							Public Sc	an 🌻	Options					
Re	cent s	cans 🔿 Upd	lates every 10)s - Last updat	e: 00:56:0	7											
	URL								A	ge	Size	₽	IPs	-	ŧ		
	consent.	youtube.com/m?	continue=http:	s%3A%2F%2Fv	www.youtub	e.com%2Fu	er%2FVailla	antb	18	seconds	356 KB	25	6	2	-		
	www.so	larwinds.com/ser	vice-desk						23	3 seconds 💄	2 MB	200	91	8	-		
	thekeyre	ewards.com/tc/							23	3 seconds	428 KB	63	14	3			
	ccmail.k	ofyksh.club/login							24	seconds 💄	102 KB	12	1	1			
	hvac-bo	ston.org/							24	seconds 💄	1 MB	60	4	3			
	visitor.co	onstantcontact.co	om/do?p=un&n	n=001l4sO-Qsl	MF7MDnB)	<610x00g%3	D&ch=c560	aa40	24	seconds	367 KB	10	6	3			
	get4click.ru/coupons/097c853f279b6bf87fed63e9083e2706f88bea					ea210f156/			28	8 seconds 💄	5 MB	162	15	4	-		
	www.big	panda.io/?mkt_t	ok=Nzc4LVVO	SSO5NjUAAAG	BRMJ63vb	F_Jb9uQ7rg	VQzWEhos	wdJFMBVTF.		seconds 🗟	2 MB	130	28	4			
	iqbroker	.com/lp/regulate	d/?aff=283168						34	seconds	438 KB	33	19	7	۲		

After you click the "Public Scan" it's take some time to complete the scanning.

🝳 urlscan.io 🕈 Home Q Search 🏼 Live 🐯 API 🗲 Blog 🗖 Docs 🖸 Pricing 💄 Login Secur	rityTrails
---------------------------------------------------------------------------------	------------

http://rxqsd.com/9n4fbg

We're browsing to your website...

We're waiting for this website to finish loading. Depending on our load, this might take a minute. You will automatically be redirected to the result, you do **not** have to refresh this page! Now, we got the result. As we can see it stated this URL is "Malicious Activity!". The URLScan io verdic this as potentially malicious.

Q urlscan.io	ft Home	Q Search	ه Live	鬷 API	🗲 Blog	Docs	🖒 Prie	ing 👤	Login	sponsored by SecurityTrails
itemtt.chk 2606:4700:303 Submitted URL: https:/ Effective URL: https:/ Submission: On June 2	SO::ac43:da //rxqsd.com/9 //itemtt.chkpa ?7 via manual	tt.top a5c Ma n4fbg rceltt.top/bank (June 27th 20	(3/ch/swsps) 23, 7:26:01	t/?p=200& 9 pm UTC)	cep=ygmeY	SunrOtpP-so — Scanned	dMUO-5Y	OCr0yht1ts	Q Looks	up • 🔗 Go To 🛛 Report CRescan
☆ Summary ≓ HTT	P 17 🏕 Redi	rects @Links	1 📮 Beh	aviour 🙆	Indicators	Ø Similar	DOM	Content	88 API	
Summary							Scr	eenshot		Live screenshot
This website conta The main IP is 2600 CLOUDFLARENET TLS certificate: Issu	This website contacted 4 IPs in 2 countries across 6 domains to perform 17 HTTP transaction The main IP is 2606:4700:3030::ac43:da56 , located in United States and belongs to CLOUDFLARENET , US. The main domain is itemtt.chkparceltt.top . TLS certificate: Issued by <i>Cloudflare Inc ECC CA-3</i> on November 15th 2021. Valid for: a year.									
itemtt.chkparceltt.to	p scanned 5 ti	mes on urlscan	io		Sho	w Scans 5				244-0120128
urlscan.io Verd	ict: Potentia	ally Maliciou	ıs 🕖							And the second se
Targeting these bra	nds: 💽 Swis	ss Post (Transpo	ortation)							
Generic Track	ing (Transport	ation)								
Live informatio	n						Pag	e URL Hi	story	Show full URLs
Google Safe Brows Current DNS A rec	ing: ONo clas	8.86 (AS1333)	emtt.chkpar 5 - CLOUDF	celtt.top LARENET, I	US)		1. h	ttp:// rxqsd . ttps:// track	.com/9n4fbg	нттр 302 nder.com/d6532c1e-b4c7-4f21-9726-04

We also can see this URL targeting which brand. In this case, they are targeting Swiss Post (National postal service of Switzerland).

🝳 urlscan.ig 🔶 Users 🖸 s	inarch 🖓 Live 😤 A	PL & Plas Door C Printer	C Login	sponsored by urityTrails
itemtt.ch 2606:4700:3 Submitted URL: htt Effective URL: htt Submission: On Dece Mainmary		AUSSTEHENDE LIEFERUNG CONSTITUTION AUSSTEHENDE LIEFERUNG AUSSTEHENDE AUSSTEHENDE LIEFERUNG AUSSTEHENDE AUSSTEHENDE LIEFERUNG AUSSTEHENDE LIEFERUNG AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE LIEFERUNG AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AUSSTEHENDE AU		ort CRescan qrdw9w
This website con The main IP is 2: CLOUDFLAREN TLS certificate: H itemtLchkparcel		Con gue annua		
Targeting these Generic Tr Live informa	(f)	(in)	۲	
Google Safe Bro Current DNSA		•	U	c7-4f21-9726-04

Now, we have an answer for Questions 1.

Check the URL behaviour using https://urlscan.io/ Result: Potential Malicious

Next, we check the domain reputation using BrightCloud

(<u>https://www.brightcloud.com/tools/url-ip-lookup.php</u>). Copy the "Effective URL" from the precious URL scan.



Then put the URL address that you want to check and click "LOOK UP".



Now, we got the result. As we can see it stated that web reputation is suspicious (40 of 100).

Look up URL or IP:		ELTT.TOP
I'm not a robot	Web Reputation:	
LOOK UP	Request a reputation change	
If you have a mutually executed agreement with Vebroot, bose terms apply to your use of the BrightCloud Service. If you do not have a mutually executed agreement with Vebroot, by closing "LOOK UP", you agree to the terms and conditions of the BrightCloud Thread Intelligence Service for Entreprise Agreement.	Web Category: - Uncategorized Request a category change	
Request a Change:		
URL or IP: *	Web Reputation Influences:	Impact:
Optional: I would like to suggest a category	- No infections past 12 months	
for this URL	- 0 months old (not established)	

Now, we have an answer for Questions 2.

Check domain reputation using https://www.brightcloud.com/tools/url-ip-lookup.php Result: Suspicious Finally, we interact with URL using Browserling (<u>https://www.browserling.com/</u>). This virtual sandboxed browser allows us to running web applications in isolated environments to prevent browser-based malware from spreading to the network. Copy the URL.



Then put the URL address that you want to check.

< → C O ●	i browserling.com Q టి చి	🄰 🛪 🛞 Incognito 🗄
	Pricing Live API About Us Sign In Sign Up	
	000	
000		
	Online cross-browser testing	
	http://rxqsd.com/9n4fbg Test now!	
	Vindows 7 - Kinternet Explorer	
	Get a browser and start testing in 5 seconds!	

Choose the browser that you prefer and click "Test now!". For me, I like to use Chrome.



After clicking "Test now!", you need to wait for a moment for the browser to establish the connection.



Now, we are in the isolated mode. Let's observed and analyse this website.

← → C ☆ 🕯 browserling.com	/browse/win/7/chrome/92/http%3A%2F%2Frxqsd.e	om%2F9n4fbg			이, 숫 🏮 🆈 🙆 Incognito 🚦
	😵 https://demtt.chkparceltt.top/be 🗴 🕂			0 60 11	
		nk3/ch/swspst/7p=200&cep=KtzPRmfHiFtRbipzWqH3ihCZnhr	rzCamfy9g8pQik9fo0kmKreWi	1 4 4 4	
() 02:40 remaining		SWISS POST	German English	: ×	
use all browsers and all system with no time limits.	5	AUSSTEHENDE LIEFERUNG			
Operating System		_0			
🚝 Windows 7	~				
Browser		-			
Chrome 92	 Image: A set of the set of the	Du hast eine ausstehende Lieferung, Benutze dein einziaartia Verfolaunascode zu verfolaan			
URL		und zu empfangen ihr artikel.			
http://rxqsd.com/9n4fbg	>	Ihre Verfolgungscode			
Display options C Capture s	reen	SWP001836759			
>_ Local testing Show key	oard				
	back	4	-		
× End session		Spur ihre artikel			

The content is in German language. Translate the website content to English to make sure we understand all the details.

→ C O m b	rowserling.com/browse/v	n/T/chrome/92/http%3A%2F%2Fnqsd.com%2F9n4fbg	् 🖈	•	🖈 🎯 Incognito	1
		📀 https://depatchippereittopiles x +				
		C & KemtLchkparcelt.top/bank3/ch/swspst//p=2008ccep=Kt2PRmtHiFiRblgzWqH3hCzhvzCunf/9g8pQ89fo8mKreW8				
O2:34 remaining Upgrade to a premium plan to use all browsers and all systems with no time limits.		SWISS POST				
		PENDING DELIVERY				
Operating System		-0				
🖅 Windows 7 🗸						
Browser						
Chrome 92	~	You have a delivery pending. Use your unique				
URL		inducing court o nock and receive your rem.				
http://rxqsd.com	n/9n4fbg →	Yourtracking code				
Display options	Capture screen	SWP001836759				
>_ Local testing	Show keyboard					
⊘ Share browser	Send feedback					
× En	d session	Track your Hern				

So, we want to observe what the threat actor trying to trick us with this website. First click the button "Track your item".

→ C & @ E	browserling.com/browse/v	vin/7/chrome/92/http%3A%2F%2Frxc	asd.com%2F9n4fbg				@ ☆	🟮 🖈 🛞 Incognito 🗄
		https://itemtt.chkparceltt.top/bo X	+			0 00 2		
			op/bank3/ch/swspst/7p=2	2008.cep=KtzPRmfHlFtRblpzWq	H3ihCZntvzCxntj9g8pQik9fo0kmKre	wna \$ ☆ 🛋 i		
() 02:23 rama	aining			SWISS POST		1		
Upgrade to a <u>premium plan</u> to use all browsers and all systems with no time limits.			۲	-0-	C			
Operating System								
💐 Windows 7	7 ~		Package	information:				
Browser		Status: Held in the depot (unpoid impert duity)						
Chrome 92	2 👻		Shipping via: Intl tracked courier					
URL			Customs fee	es: 2.00 CHF				
http://rxqsd.com	m/9n4fbg →							
Display options	Capture screen			edule the dislivery no				
>_ Local testing	Show keyboard							
Ø Share browser	Send feedback							
× Er	nd session							
		(f	in	(a)			

Next click "Enter shipping information".

C A	/7/chrome/92/http%3A%2F%2Fnxqpd.com%2F9n4fbg	🔍 🕁 🏮 🛪 🌚 Incognito 🚦
	O https://temtt.chkpacetit.top/los x +	
	🗧 -> C 🔹 itemti.chiparcelit.top/bank3/ch/wspst//p=2008.cep=KtzPRmtHER8bipzWqH3ihCZnhrzCunl/pg8pQikHo0kmKreWi8 💐 🏚 🛓 I	
	SWISS POST	
Upgrade to a <u>premium plan</u> to use all browsers and all systems with no time limits.	●—●—●	
Operating System		
鸄 Windows 7 🗸 🗸	DELIVERY CONFIRMATION	
Browser	DELIVERT CONFIRMATION	
Chrome 92 V	Expected delivery time:	
URL	Between 8:30 a.m. and 8:00 p.m.	
http://rxqsd.com/9n4fbg →	* Enter your contact information on the next page and pay 2.00 CHF the customs fee	
Display options Capture screen		
>_ Local testing Show keyboard	Enter the shipping information	
× End session	P P	

Finally, we are on the page that we need to fill all the details. From here we know this is phishing.

→ C & (m b	rowserling.com/browse/w		Q 🖈	•	* 6	Incognito	
		Stylecopenhagen CH Check out X +					
(01:59 remain Upgrade to a use all browse with no time in	ining premium plan to rs and all systems imits.	Delivery address and payment information					
Operating System		Your first pame					
🐉 Windows 7	~	last name .					
Browser		L. F. mail address					
Chrome 92	~	Phone number					
URL		Address fine 1					
http://rxqsd.com	n/9n4fbg →						
Display options	Capture screen	Choose State					
>_ Local testing	Show keyboard	Switzerland 🗸					
P Share browser	Send feedback	Postal code					
V Endersten		Delivery address as billing address					
A En	M BESSION	Credit card:					
		Credit card #					
		CW/code					

They also ask for our credit card details. This is red flag.

 Interspensages Cirl Cleck and x + Interspensa	→ C & (m b	् 🛧 🚺 🛧 🛞 Incognito 🗄		
O 11:46 remaining Upgrade to a greating india to use all browsers and all systems with no time limits. Operating System Invoser Or throws 7 Invoser Or throws 92 URL URL Integrade com/9n4lbg → 2. Local testing Show keyboard Share browser Send feedback X End session Subjector Subjector 2. Local testing Show keyboard Share browser Send feedback X End session Subjector Subjector 2. Local testing Show keyboard 3. Send feedback X End session Subjector 2. Source			⊘ Σι/κορκηλαχην CH1Check out x +	
Cperating System Cover and	O 01:46 remaining Upgrade to a premium plan to use all browsers and all systems with no time limits.		Postal code Delivery address as billing address Delivery address Delivery address	
Iterwise Iterw	Operating System		Credit card # CWCode	
Chrome 92 URL http://nxqsd.com/9n4lbg → Display options C Capture screen >_ Local testing © Show keyboard Ø Share browser Send feedback X End session Suscettal 2000#	Browser		Of (Jan) 2000 C	
http://rxqsd.com/9n4fbg → Display options Capture screen >_ Local testing Show keyboard Ø Share browser Send feedback X End session Subrotest Subrotest 2000+# aetwery 0.000-#	Chrome 92 VIII		KEEP GOING	
□ Display options ① Capture screen >_ Local testing □ Show keyboard Ø' Share birowser □ Send feedback × End session Subtrata Subtrata 2000+#	http://rxqsd.com/9n4fbg →		0	
>_ Local testing Image: Show keyboard ⊘ Share browser Image: Show keyboard X End session Subtrata subtrata 2.000+# aelivery 0.000+#	Display options	C Capture screen	VISA 🔤	
	>_ Local testing	Show keyboard		
X End session Subtots 200CHF delivery 0.00CHF		Send feedback		
delivery 0.00CH#	× End session		Subtratol 2,00CHF	
			delivery 0.00CH#	

Now, we have an answer for Question 3

Interact with URL using virtual sandboxed browser from https://www.browserling.com/ Result: Phishing URL to harvest credit card info and personal data | Phishing link

So, we already have answered all the questions:

- 1. Check the URL behaviour using https://urlscan.io/ Result: Potential Malicious
- 2. Check domain reputation using https://www.brightcloud.com/tools/url-ip-lookup.php Result: Suspicious
- 3. Interact with URL using virtual sandboxed browser from https://www.browserling.com/ Result: Phishing URL to harvest credit card info and personal data | Phishing link

Now, we can conclude that links/URLs are malicious. The threat actor used the phishing method to harvest credit card info and personal data.