Home (https://www.bleepingcomputer.com/) > News (https://www.bleepingcomputer.com/news/) > Security (https://www.bleepingcomputer.com/news/security/) > Massive Facebook Messenger phishing operation generates millions

23

Massive Facebook Messenger phishing operation generates millions

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

June 8, 2022 02:54 PM 0

Researchers have uncovered a large-scale phishing operation that abused Facebook and Messenger to lure millions of users to phishing pages, tricking them into entering their account credentials and seeing advertisements.

The campaign operators used these stolen accounts to send further phishing messages to their friends, generating significant revenue via online advertising commissions.

According to PIXM, a New York-based AI-focused cybersecurity firm, the campaign peaked in April-May 2022 but has been active since at least September 2021.

Top Articles
READ MORE
(https://www.bleepingcomputer.com/news/security/kali-linux-team-to-stream-free-penetration-testing-course-on-twitch/?traffic_source=Connatix)

PIXM was able to trace the threat actor and map the campaign due to one of the identified phishing pages hosting a link to a traffic monitoring app (whos.amung.us) that was publicly accessible ithout authentication.

Massive scale of abuse

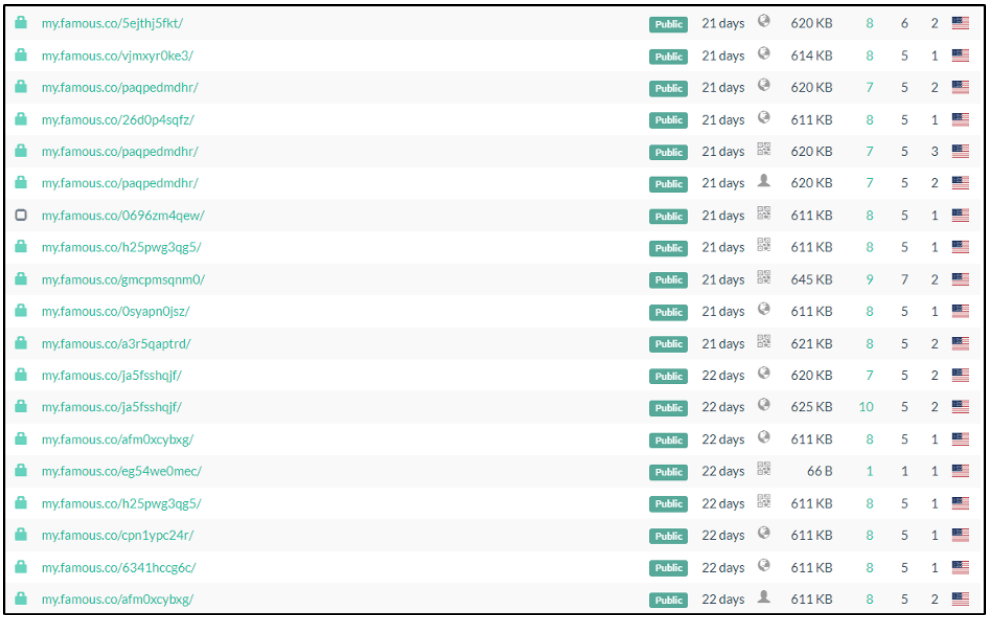
While it is unknown how the campaign initially started, PIXM states victims arrived at phishing landing pages from a series of redirects originating from Facebook Messenger.

As more Facebook accounts were stolen, the threat actors used automated tools to send further phishing links to the compromised account's friends, creating massive growth in stolen accounts.

"A user's account would be compromised and, in a likely automated fashion, the threat actor would log in to that account and send out the link to the user's friends via Facebook Messenger," explains PIXM in the report (https://pixmsecurity.com/blog/blog/phishing-tactics-how-a-threat-actor-stole-1m-credentials-in-4-months/).

While Facebook has protection measures to stop the dissemination of phishing URLs, the threat actors used a trick to bypass these protections.

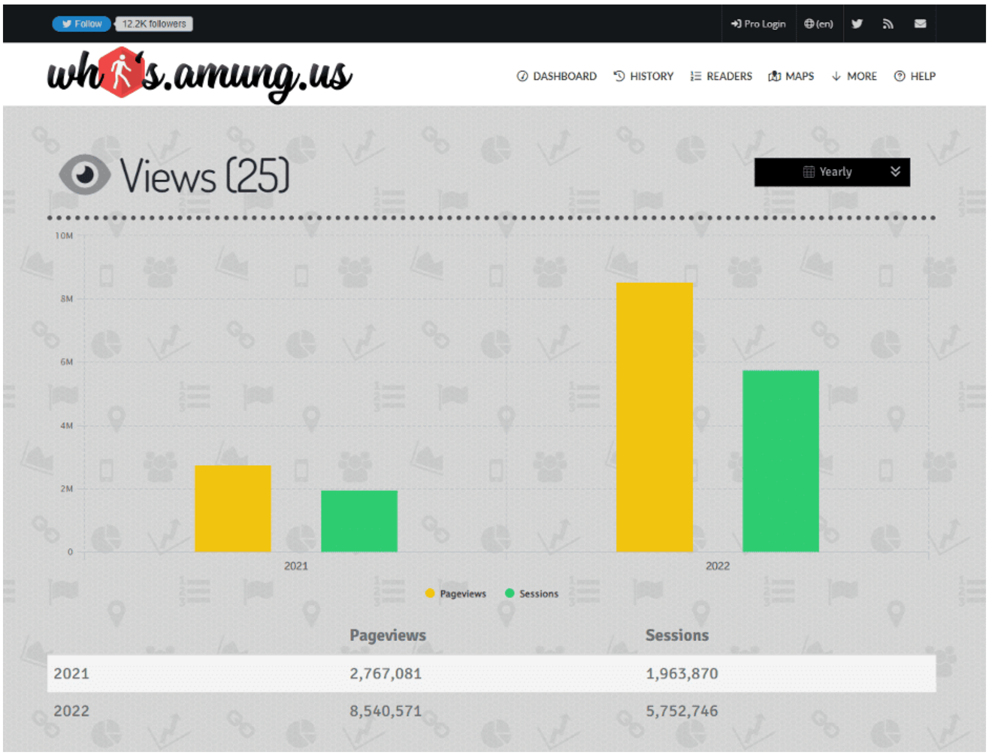
The phishing messages used legitimate URL generation services such as litch.me, famous.co, amaze.co, and funnel-preview.com, which would be a problem to block as legitimate apps use them.



my.famous.co/5ejthj5fkt/	Public	21 days	🌐	620 KB	8	6	2
my.famous.co/vjmxyr0ke3/	Public	21 days	🌐	614 KB	8	5	1
my.famous.co/paqpedmdhr/	Public	21 days	🌐	620 KB	7	5	2
my.famous.co/26d0p4sqfz/	Public	21 days	🌐	611 KB	8	5	1
my.famous.co/paqpedmdhr/	Public	21 days	▦	620 KB	7	5	3
my.famous.co/paqpedmdhr/	Public	21 days	👤	620 KB	7	5	2
my.famous.co/0696zm4qew/	Public	21 days	▦	611 KB	8	5	1
my.famous.co/h25pwg3qg5/	Public	21 days	▦	611 KB	8	5	1
my.famous.co/gmcpmsqnm0/	Public	21 days	▦	645 KB	9	7	2
my.famous.co/0syapn0jsz/	Public	21 days	🌐	611 KB	8	5	1
my.famous.co/a3r5qaptrd/	Public	21 days	▦	621 KB	8	5	2
my.famous.co/ja5fsshqjf/	Public	22 days	🌐	620 KB	7	5	2
my.famous.co/ja5fsshqjf/	Public	22 days	🌐	625 KB	10	5	2
my.famous.co/afm0xcybxg/	Public	22 days	🌐	611 KB	8	5	1
my.famous.co/eg54we0mec/	Public	22 days	▦	66 B	1	1	1
my.famous.co/h25pwg3qg5/	Public	22 days	▦	611 KB	8	5	1
my.famous.co/cpn1ypc24r/	Public	22 days	🌐	611 KB	8	5	1
my.famous.co/6341hccg6c/	Public	22 days	🌐	611 KB	8	5	1
my.famous.co/afm0xcybxg/	Public	22 days	👤	611 KB	8	5	2

Some of the URLs used in the phishing campaign *(PIXM)*

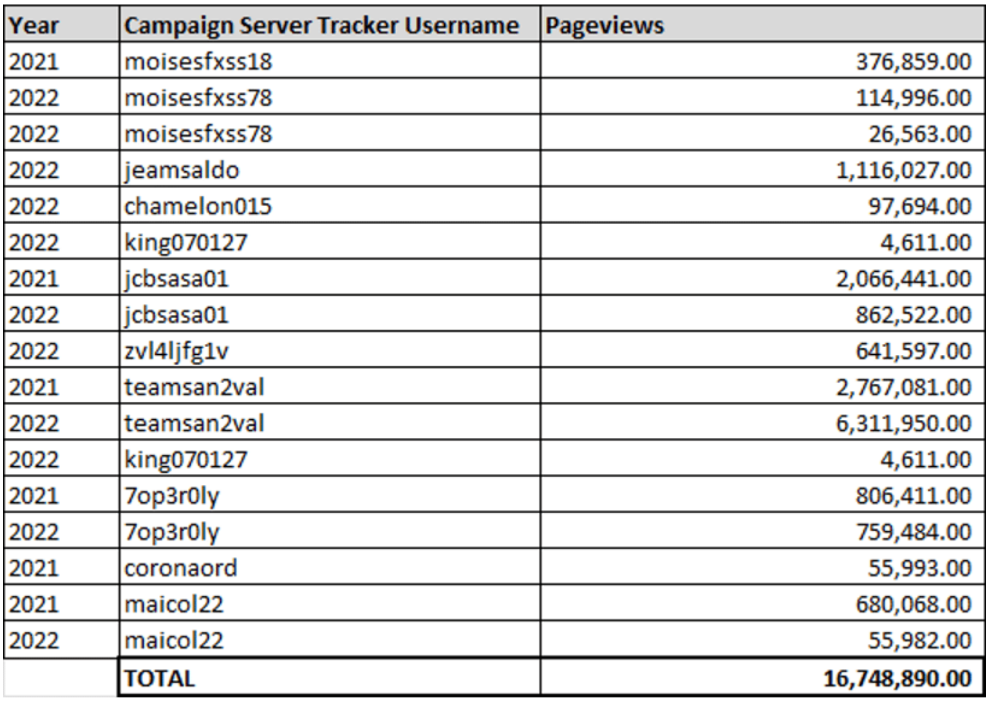
After discovering that they could gain unauthenticated access to the phishing campaign stats pages, the researchers found that in 2021, 2.7 million users had visited one of the phishing portals. This figure went up to 8.5 million in 2022, reflecting the massive growth of the campaign.



	Pageviews	Sessions
2021	2,767,081	1,963,870
2022	8,540,571	5,752,746

Snap from the dashboard of the exposed analytics service *(PIXM)*

By diving deeper, the researchers identified 405 unique usernames used as campaign identifiers, each having a separate Facebook phishing page. These phishing pages had page views ranging from only 4,000 views to some in the millions, with one as high as 6 million page views.

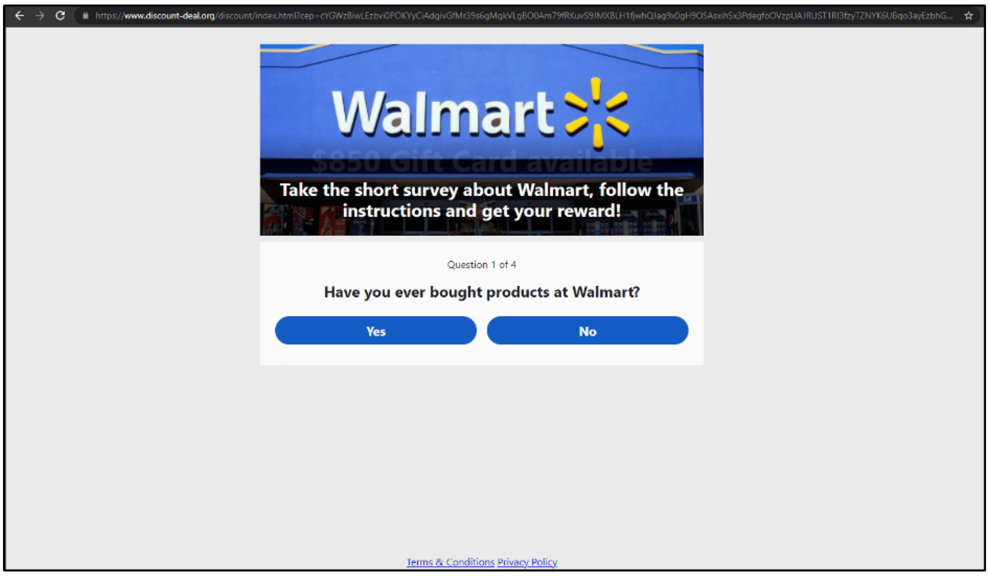


Year	Campaign Server Tracker Username	Pageviews
2021	moisesfxss18	376,859.00
2022	moisesfxss78	114,996.00
2022	moisesfxss78	26,563.00
2022	jeamsaldo	1,116,027.00
2022	chamelon015	97,694.00
2022	king070127	4,611.00
2021	jcbsasa01	2,066,441.00
2022	jcbsasa01	862,522.00
2022	zvl4ljfg1v	641,597.00
2021	teamsan2val	2,767,081.00
2022	teamsan2val	6,311,950.00
2022	king070127	4,611.00
2021	7op3r0ly	806,411.00
2022	7op3r0ly	759,484.00
2021	coronaord	55,993.00
2021	maicol22	680,068.00
2022	maicol22	55,982.00
	TOTAL	**16,748,890.00**

Sample of the identified dissemination users *(PIXM)*

The researchers believe that these 405 usernames represent only a fraction of the accounts used for the campaign.

After the victim enters their credentials on the phishing landing page, a new round of redirections begins, taking them to advertising pages, survey forms, etc.



https://www.discount-deal.org/discount/index.html?cep=cYGWzBiwLEzbvi0POKYyCiAdgivGfMr39s6gMgkVLgBO0Am79fRKuvS9JMXBLH1fjwhQJag9x0gH9OSAsxih5x3PdegfoOVzpUAJRUST1RI3fzyTZNYK6UBqo3ayEzbhG...

Take the short survey about Walmart, follow the instructions and get your reward!

Question 1 of 4

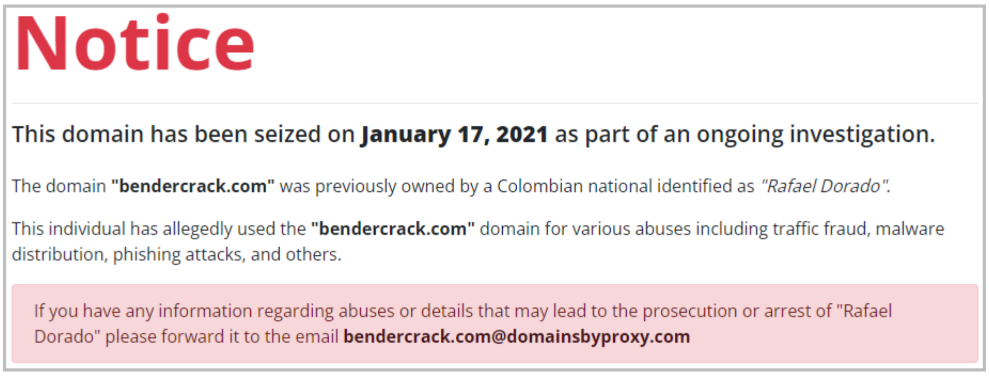
Have you ever bought products at Walmart?

One of the ads showed to phished users *(PIXM)*

The threat actors receive referral revenue from these redirects, which are estimated to be millions of USD at this scale of operation.

Tracing the threat actor

PIXM found a common code snippet on all landing pages, which contained a reference to a website that has been seized and constitutes part of an investigation against a Colombian man identified as Rafael Dorado.



Notice

This domain has been seized on **January 17, 2021** as part of an ongoing investigation.

The domain **"bendercrack.com"** was previously owned by a Colombian national identified as *"Rafael Dorado"*.

This individual has allegedly used the **"bendercrack.com"** domain for various abuses including traffic fraud, malware distribution, phishing attacks, and others.

If you have any information regarding abuses or details that may lead to the prosecution or arrest of "Rafael Dorado" please forward it to the email **bendercrack.com@domainsbyproxy.com**

Website belonging to the campaign operator

It is unclear who seized the domain and placed the notice on the site.

A reverse whois lookup revealed links to a legitimate web development company in Colombia and old sites offering Facebook "like bots" and hacking services.

PIXM shared the results of its investigation with the Colombian Police and Interpol, but as they note, the campaign is still ongoing, even though many of the identified URLs have gone offline.