Social Media Phishing: Expanding the List of IoCs for Recent Facebook Page Impersonation Attacks

Posted on March 2, 2021

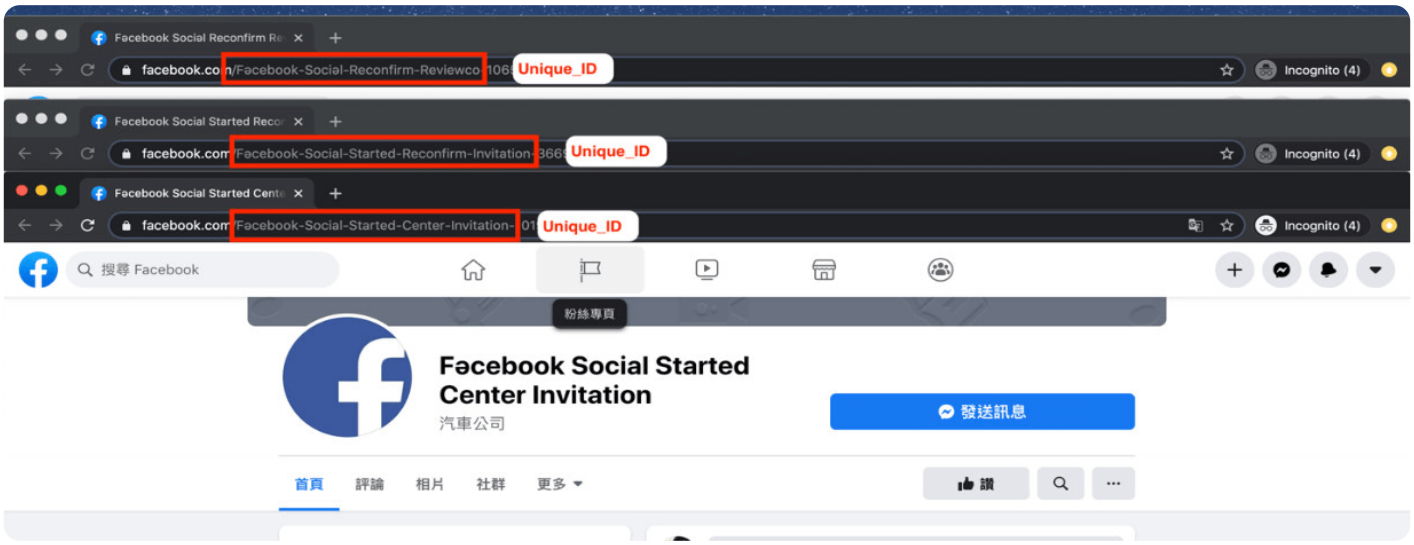
A few months back, security researchers noticed a spike in the volume of social media phishing attacks. Cybercriminals had been impersonating the Facebook pages of various influential personalities proactively in hopes of luring their followers into parting with their account credentials. The social media campaign focused on the Facebook pages of influencers with tons of followers.

A researcher from security firm Trend Micro believed an average of three pages were being spoofed per day. The personalities targeted were from Taiwan, India, Australia, Canada, and the Philippines.

The attackers began by stealing the target pages' administrative account credentials. Once done, they sent a malicious link to all of the page's followers for the potential victims to give out their own account credentials. As a common practice among phishers, the cybercriminals mimicked the pages down to their profile photos. As of August last year, 120–180 fake Facebook pages believed to be part of the campaign were seen.

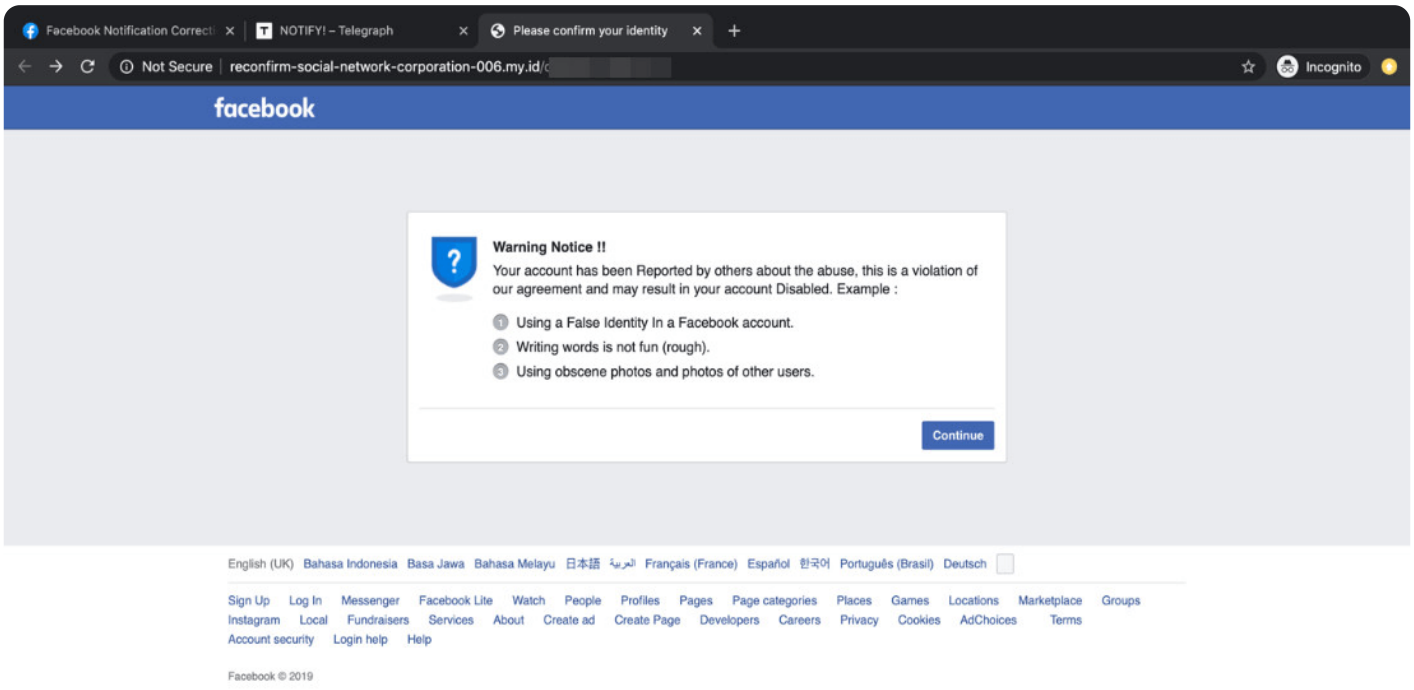
How Was the Attack Constructed?

The bogus Facebook pages used non-ASCII characters in the links sent to potential victims for various official-looking strings, such as "P??vacy Policy," "F?cebook Soci?l Reconfirm Center Invitation," and "Re-confi?m Fac?book." The "r" in "Privacy" is actually an "?" and the "a" in "Facebook" and "Social" is actually an "?." This use of non-Latin characters is suspicious, as Facebook does not use them in its communications.



Source: Trend Micro

Also typical of phishing attacks, the campaign scares potential victims into thinking their pages have violations and were reported by users. Instructions that include clicking on the malicious link are also included in the fake notifications. Users should realize the message is fake since it is riddled with grammatical errors but some still fall for the ruse.



Source: Trend Micro

Once a victim's credentials are obtained, they are used to create a fake Facebook page. To make it more credible, the cybercriminals use a vanity URL to mimic the official page's link. Victims only realize their pages have been compromised when they start seeing bogus posts (not coming from them) spread. In the worst cases, the personalities' pages are sold to other users.

Another telltale sign of compromise is the use of the domain telegra[.]ph followed by the string "/notify" in the malicious links.

What Can Cyberthreat Intelligence Sources Tell Us about telegra[.]ph?

Given the indicators of compromise (IoCs) mentioned in the Trend Micro post, we sought to find other related artifacts that Facebook users should be wary of using a variety of domain and IP intelligence tools—in particular, looking at telegra[.]ph as a starting point for our analysis.

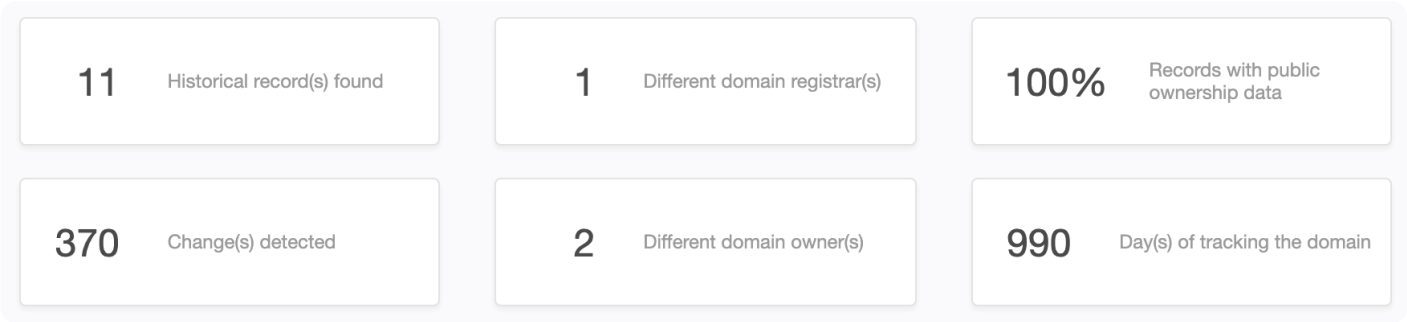
WHOIS Search Results

A WHOIS search for the domain telegra[.]ph revealed that it is privately registered and none of its record details, save for its registrar (dotPH Domains, Inc.), WHOIS server, and nameservers, are publicly available.

A screenshot of the website using the domain, meanwhile, shows the following:

The domain seems to be hosting a blog that at this point in time (around five months since the threat surfaced) doesn't contain even a single post.

Deepening our search using WHOIS History Search to see if telegra[.]ph is a newly registered domain (NRD) showed that it is not. The domain, as it turns out, is at least 6 years old, having been first registered on 11 July 2009 by a privacy-protected registrant. Since then, it has had 11 historical records and undergone 370 changes, including two domain ownership modifications.



Domains & Subdomains Discovery API

A search for telegra[.]ph on Domains & Subdomains Discovery API revealed 20+ subdomains, a few of which are shown below.

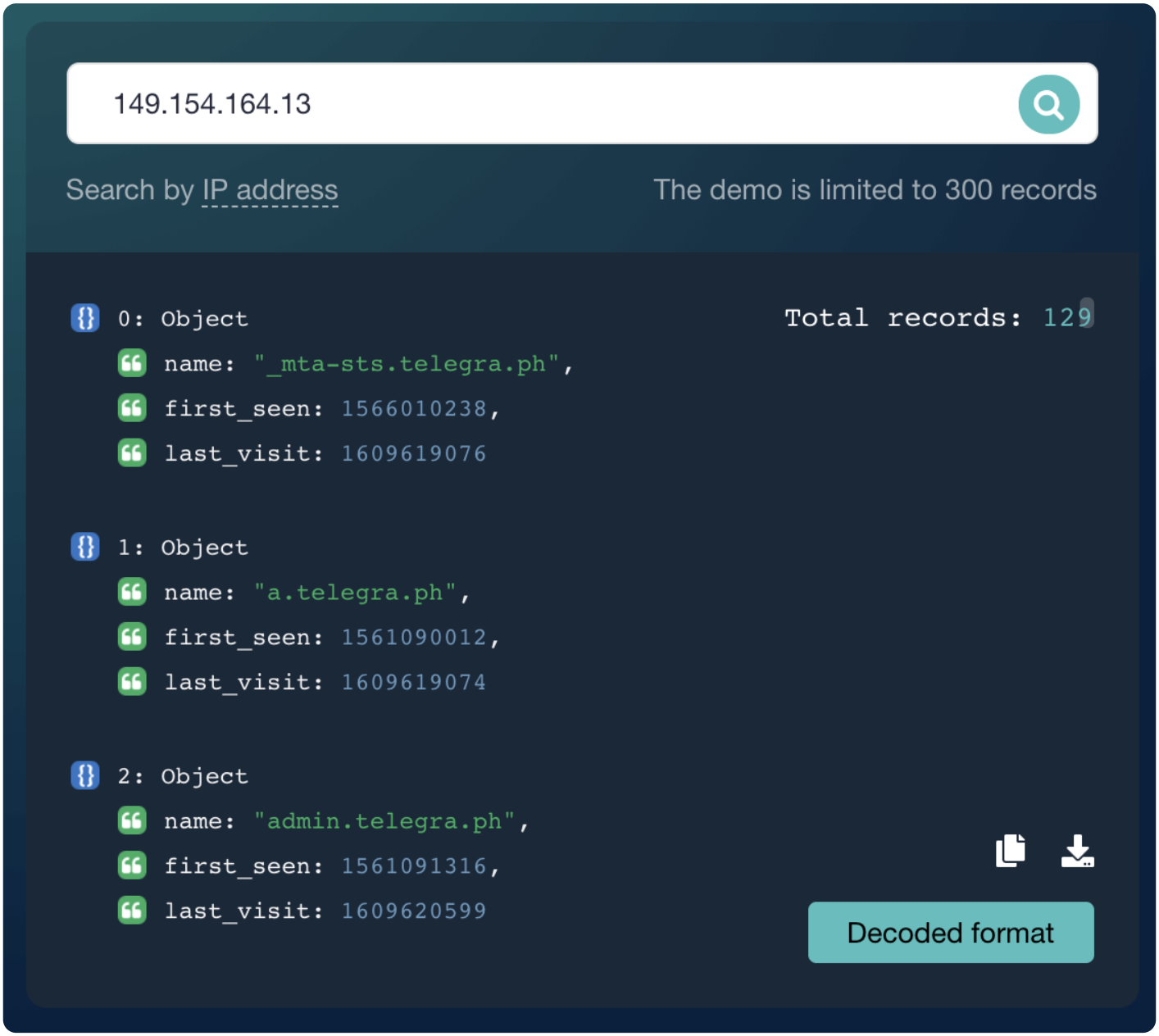
- telegra[.]ph[.]outerstats[.]com
- telegra[.]ph[.]3s3s[.]ru
- telegra[.]ph[.]mcas[.]ms
- telegra[.]ph[.]freeadsgroups[.]com
- telegra[.]ph[.]admin-mcas[.]ms
- telegra[.]ph[.]ghostly[.]in
- telegra[.]ph[.]whoisbucket[.]com
- telegra[.]ph[.]cutestat[.]com

While none of these are dubbed malicious as of this writing, some or all of them could figure in similar attacks.

DNS Lookup API, IP Geolocation API, and Reverse IP/DNS API

A DNS Lookup API query for telegra[.]ph gave us the IP address 149[.]154[.]164[.]13. Keying this into IP Geolocation API, we find that it is a U.K.-based IP address owned by Telegram Messenger Amsterdam Network.

In our effort to identify all other possible artifacts, we queried the IP address on Reverse IP/DNS API. That resulted in the identification of 129 domains.



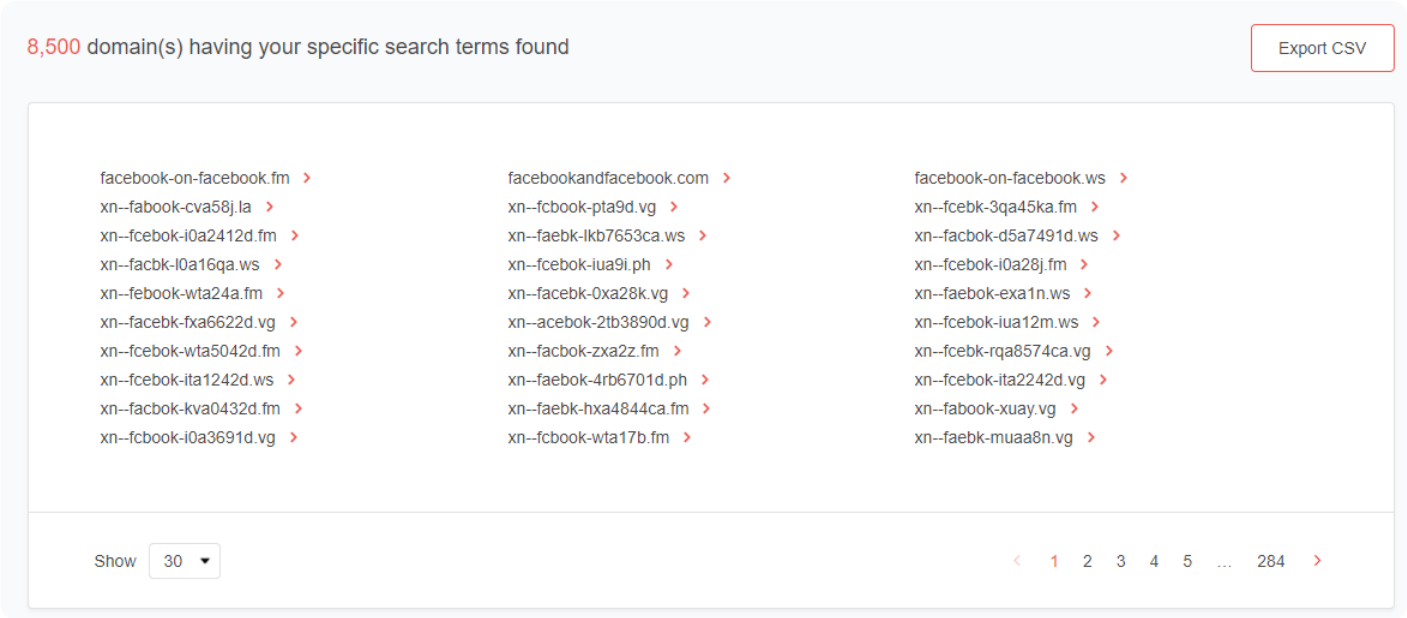
Telegra[.]ph seems to be using a dedicated IP address since all of the resulting domains appear to be under the same domain infrastructure. Given that, it may be wise for users to avoid all domains and subdomains related to telegra[.]ph, as they may all be under cybercriminal control.

Beyond Social Media Phishing: How about Domain and Subdomain Footprints?

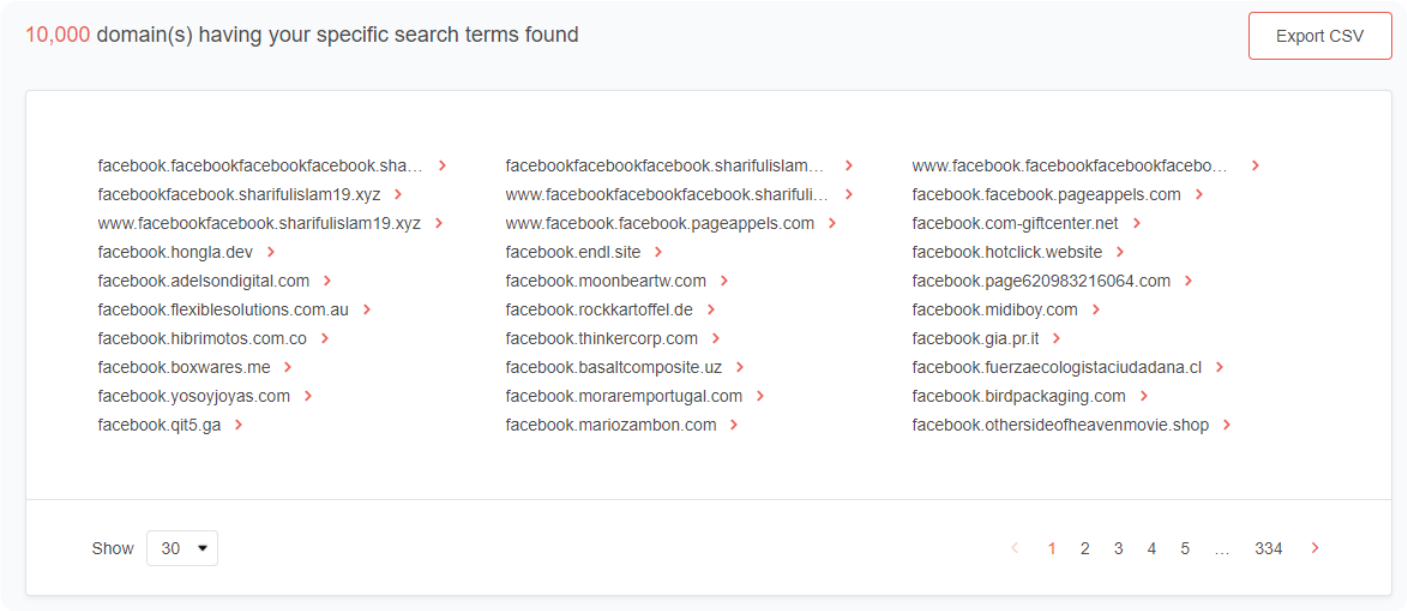
Hijacking the social media accounts of personalities is not the only way in which threat actors can execute phishing campaigns. In fact, we often identify domains and subdomains which could credibly be used to host copycat websites or send phishing emails.

Case in point, we subjected the string “facebook” to a domains and subdomains discovery query, which yielded a list of:

- 8,500 domains added since August 17, 2020 (when the TrendMicro’s research was published)



- Over 10,000 subdomains added since August 17, 2020



Checks on VirusTotal confirmed that dozens of the subdomains on the list turn out to be malicious. Some examples include the following;

- facebook[.]facebook-sukurity[.]ml
- facebook[.]facebook-sukurity-co[.]tk
- facebook[.]facebook-sukurity--id[.]ml
- facebook[.]facebook-sukurity--id[.]ga
- facebook[.]facebook-sukurity--id[.]tk

As shown in this post, social media phishing is an important threat affecting some of the largest social media platforms. Gathering intelligence on established IoCs can give more context around threats and help identify lists of related artifacts that may be worth investigating for greater enterprise cybersecurity.

Are you a cybersecurity researcher or security product developer? Contact us to learn more about the IP and threat intelligence sources used in this post and the artifacts we identified.