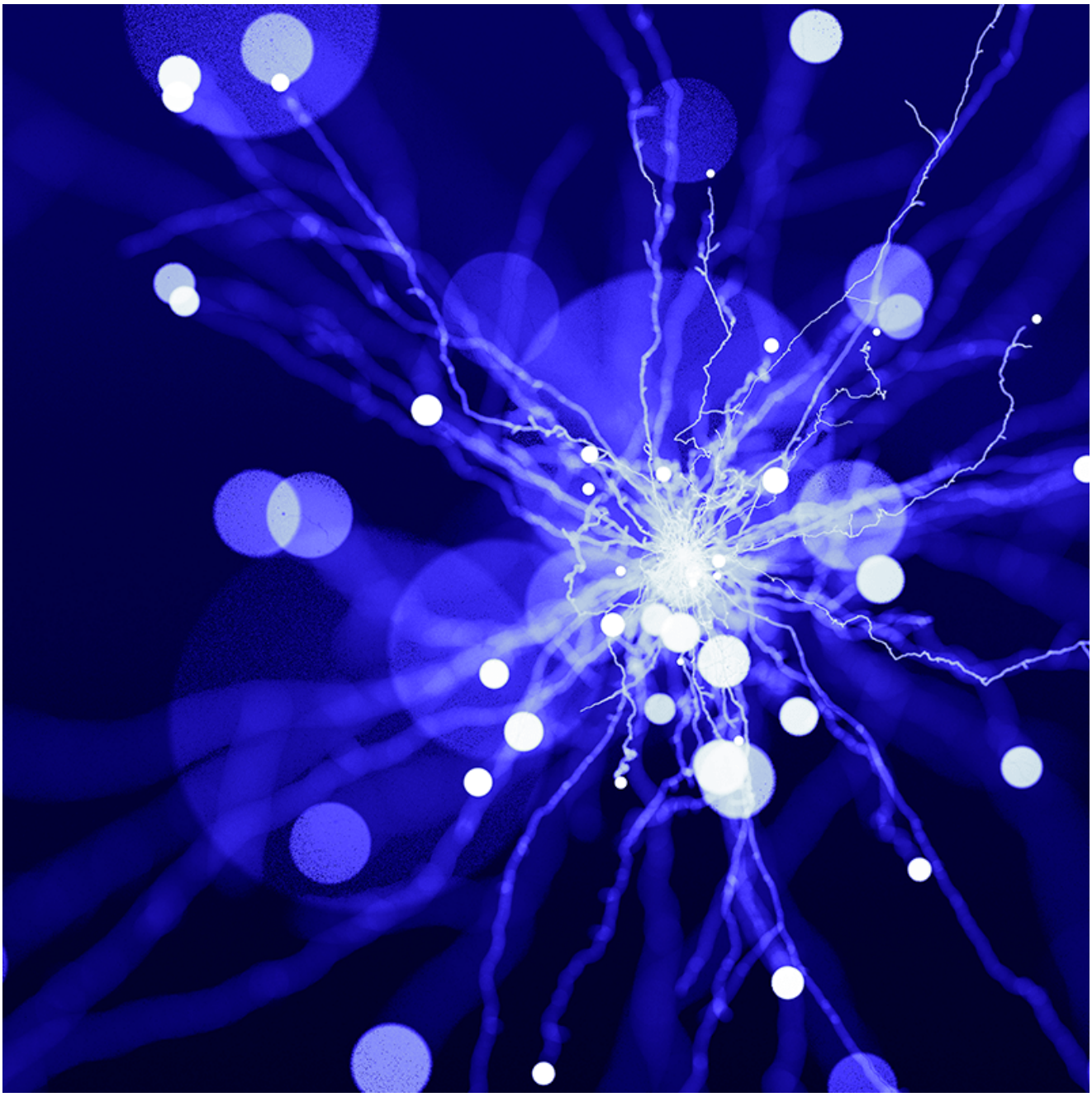
Ransoms Demanded for Hijacked Instagram Accounts

secureworks.com/blog/ransoms-demanded-for-hijacked-instagram-accounts

Counter Threat Unit Research Team



An extensive phishing campaign has targeted corporate Instagram accounts since approximately August 2021. The threat actors demand ransoms from the victims to restore access. Tuesday, January 25, 2022 *By: Counter Threat Unit Research Team*

Organizations typically focus on traditional enterprise cybersecurity threats. However, some threats are more subtle, targeting organizations on unexpected platforms. In October 2021, Secureworks® Counter Threat Unit™ (CTU) researchers identified a phishing campaign that

hijacks corporate Instagram accounts, as well as accounts of individual influencers who have a large number of followers. The threat actors then extort ransom payments from the victims. The activity continues as of this publication.

Baiting the hook

The phishing campaign begins with a message that purportedly originates from Instagram and alerts the victim to a potential copyright infringement issue (see Figure 1). The "Appeal As <*victim account username*>" link in the message is a shortened Bitly URL that resolves to an attacker-controlled phishing domain.

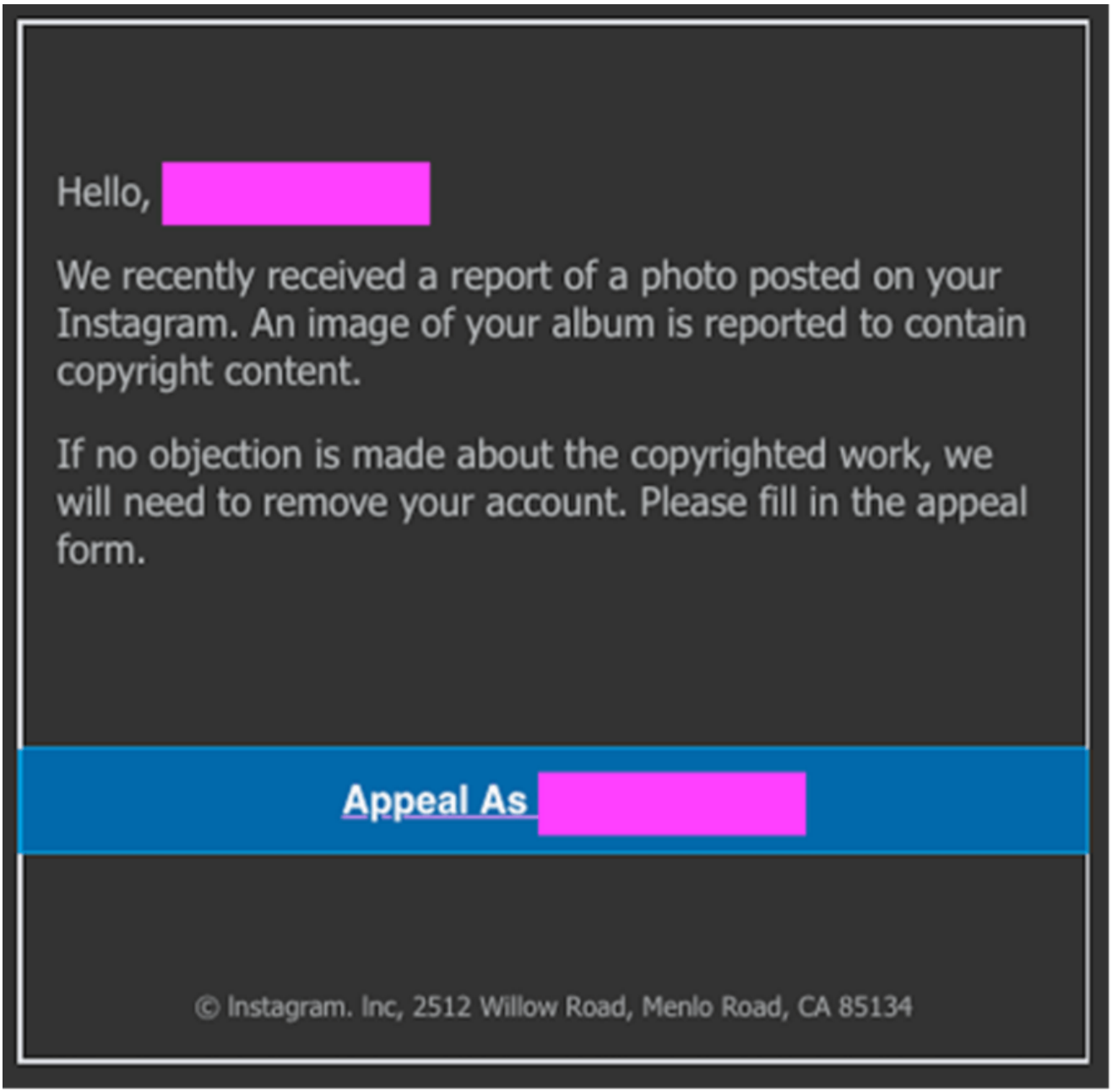


Figure 1. Fake Instagram notice about copyright infringement. (Source: Secureworks)

The phishing site is customized to mimic the victim's Instagram account (see Figure 2).

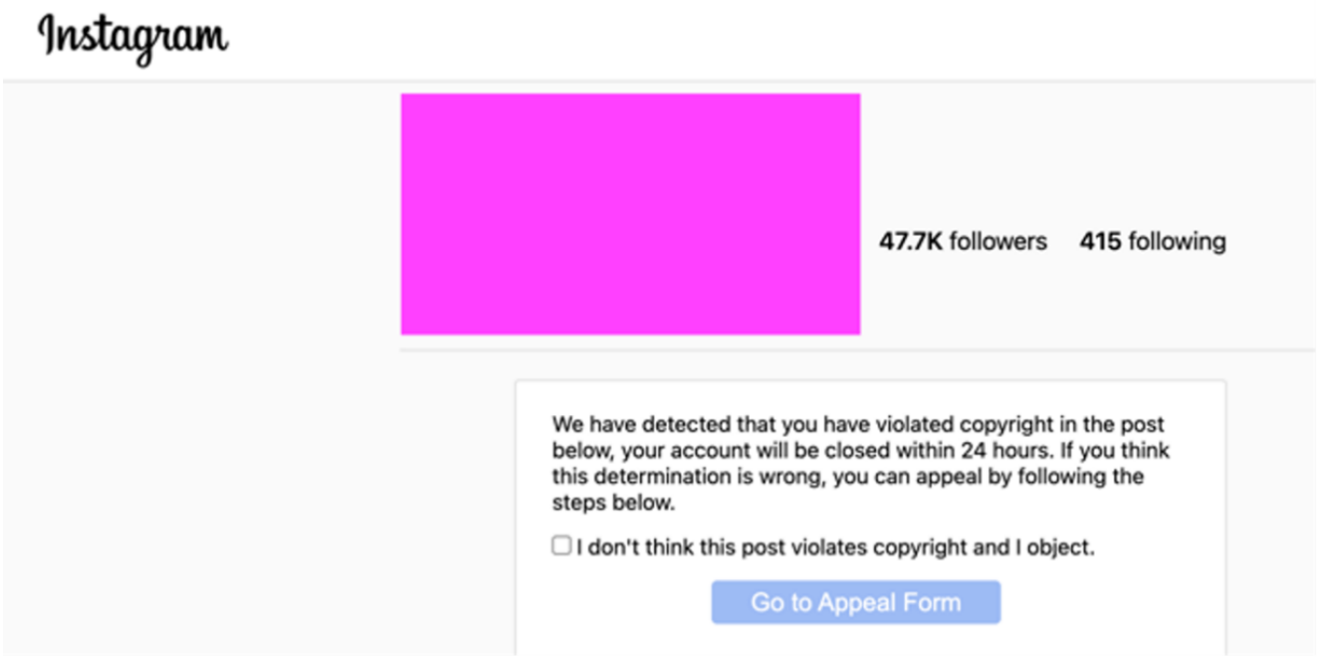


Figure 2. Fake Instagram page. (Source: Secureworks)

Reeling in the phish

When the victim checks the box indicating their objection, the "Go to Appeal Form" link becomes active. This link leads to a login screen (see Figure 3) that prompts for the victim's password. If the victim provides their password, the threat actors harvest the credentials and gain access to the account.

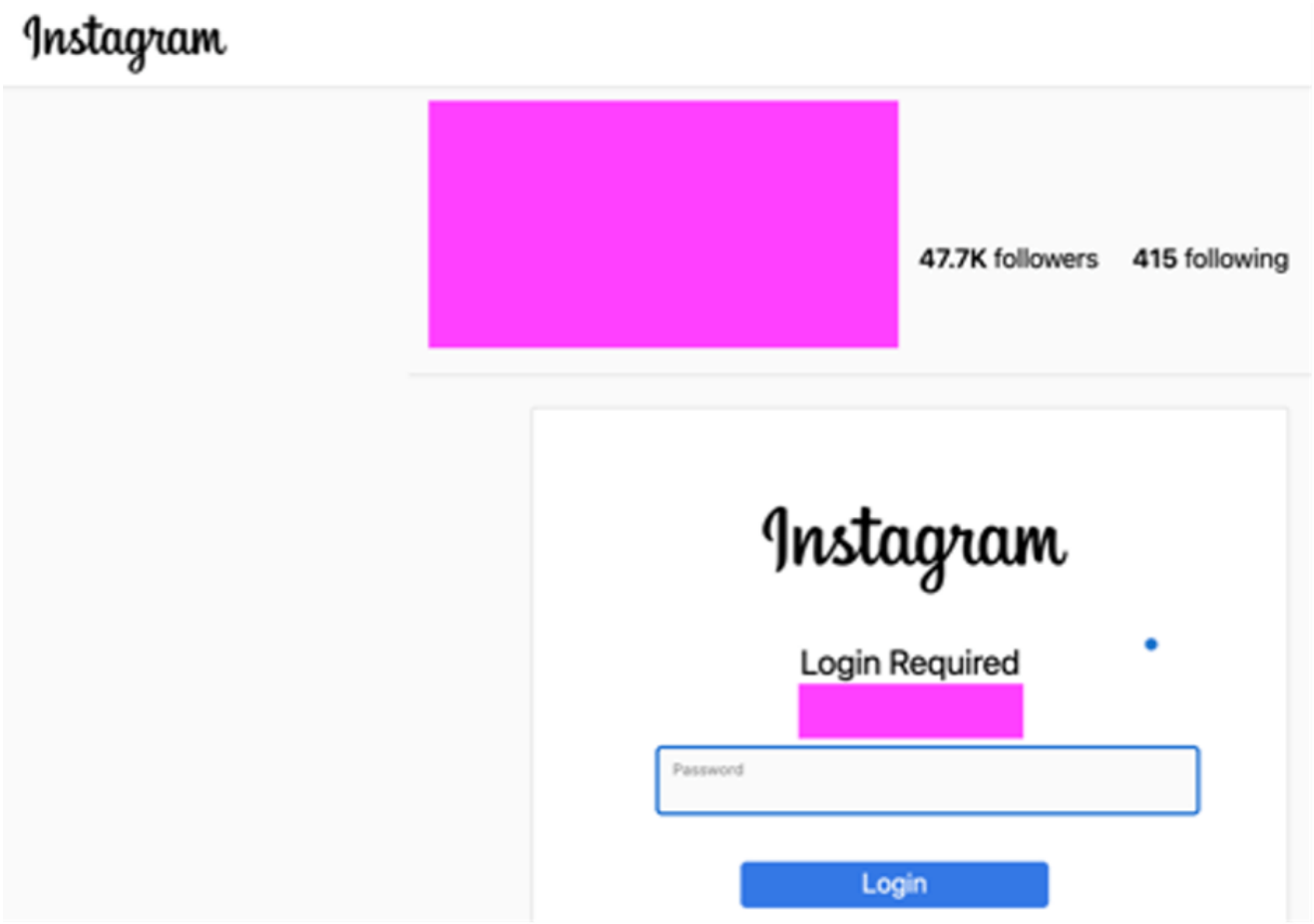


Figure 3. Password harvesting from fake login page. (Source: Secureworks)

Releasing the catch…for a price

After gaining control of the Instagram account, the threat actors change the password and username. The modified username is a variation of "pharabenfarway" followed by a number that appears to be the number of followers for the hijacked account (see Figure 4). The threat actors add a comment to the profile that "this Instagram account is held to be sold back to its owner." The comment includes a link composed of a shortened WhatsApp domain (wa . me) and a contact number. Clicking the link opens a WhatsApp chat conversation prompt with the threat actors. The threat actors also contact the victim via text message at the phone number listed on the account and start negotiating a ransom in exchange for access to the account.

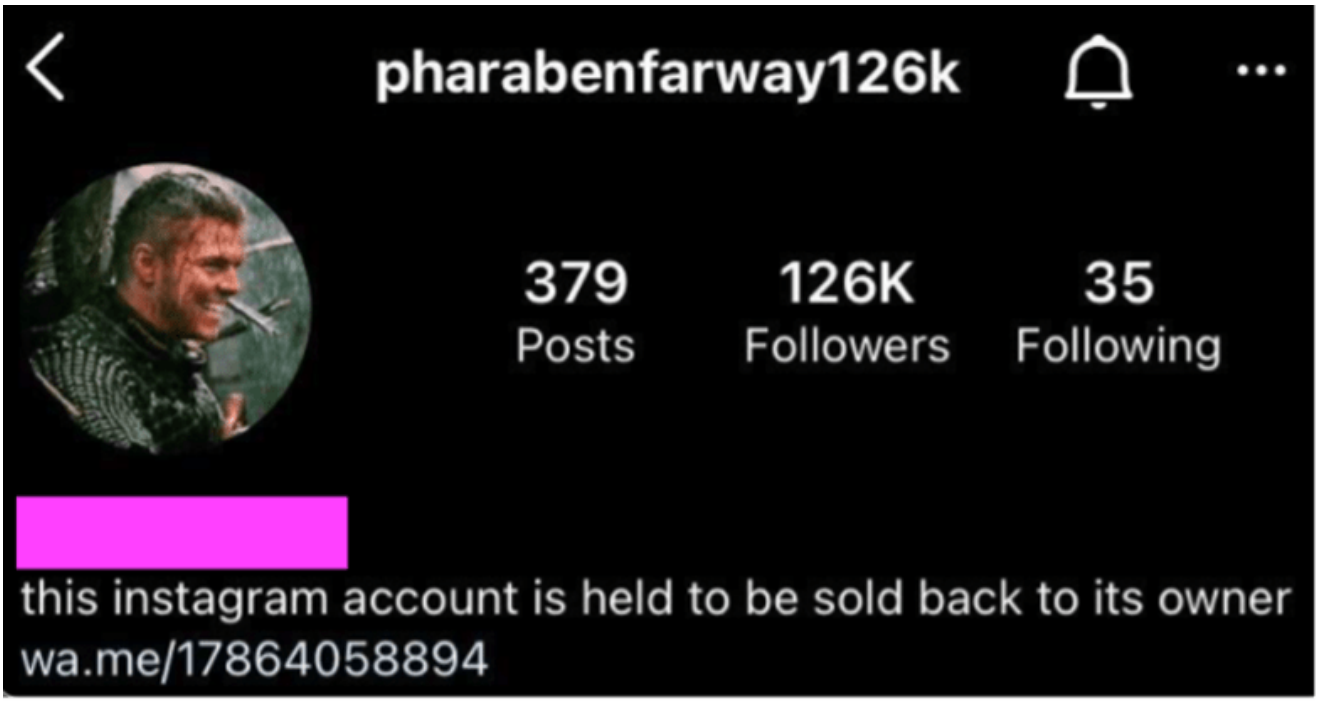


Figure 4. Hijacked Instagram account. (Source: Secureworks)

CTU™ researchers identified numerous Instagram accounts compromised by pharabenfarway, indicating this campaign is widespread. CTU analysis revealed a large list of domains used in the campaign. Based on the domain creation dates, the campaign likely started in August 2021. A September underground forum post references pharabenfarway and advertises hijacked Instagram accounts for up to $40,000 USD (see Figure 5).

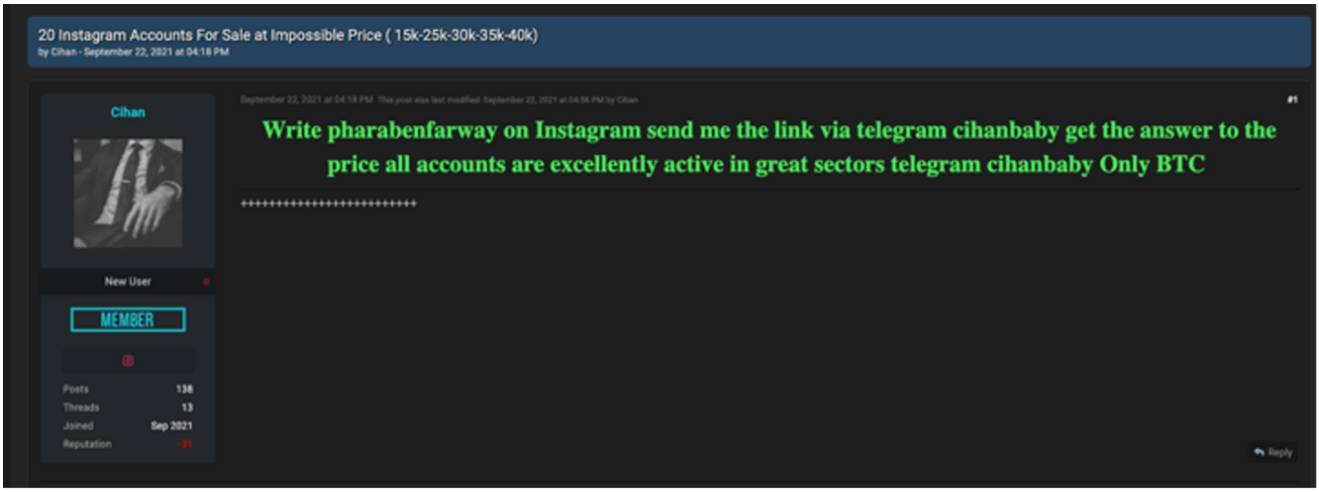


Figure 5. Instagram accounts for sale on underground forum. (Source: Secureworks)

Identifying the "phishermen"

Analysis of one of the IP addresses that hosts several of the phishing domains led CTU researchers to the 'pbfy . business' website. This website appears to belong to Pharaben and Farway, the threat actors likely operating this campaign (see Figure 6). The threat actors self-

identify as "advanced experts in social media and hacking" and provide their Instagram handles along with WhatsApp contact numbers. Pharaben's contact number uses a Russian country code, and Farway's uses a Turkish country code.

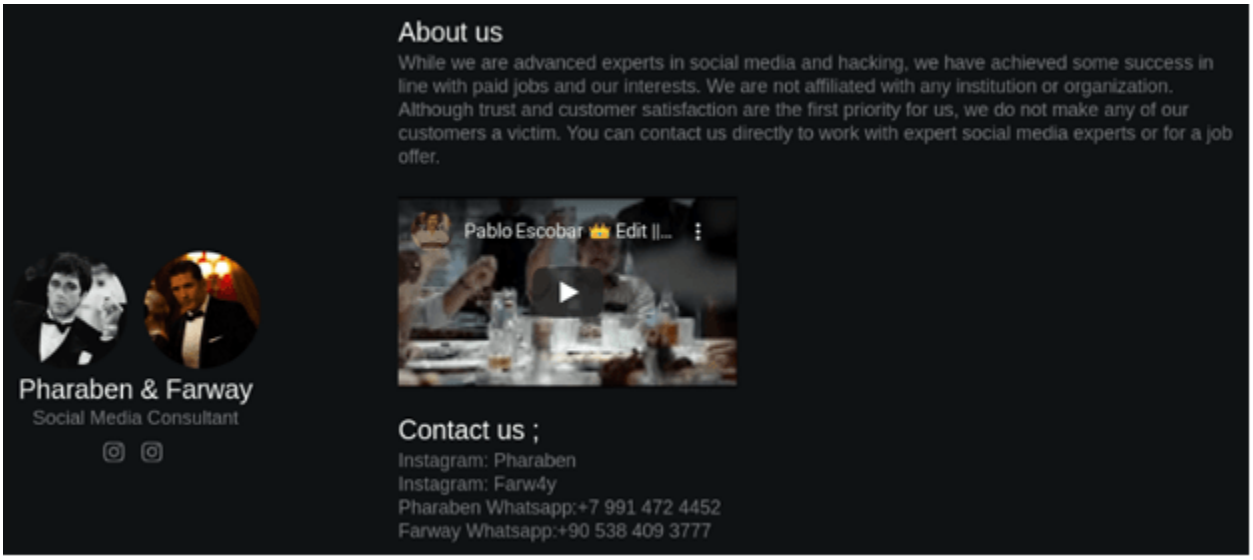


Figure 6. Pharaben & Farway website. (Source: Secureworks)

In addition to the Turkish country code, other aspects of this campaign also suggest that at least one of the threat actors could be located in Turkey. In one incident, threat actor communications originated from a Turkish-language version of Instagram. Additionally, the page source of one of the phishing websites references the Turkish hizliresim . com file-sharing service. The infrastructure associated with this campaign is based in Turkey and other countries.

Conclusion

Organizations should include social media accounts for the company and high-profile staff members in their risk assessment models. Mobile apps are a common attack vector. Use of multi-factor authentication can limit unauthorized access. While social media account takeover may seem insignificant, threat actors could access email accounts or other corporate resources if passwords were reused. Additionally, threat actors could abuse hijacked accounts to damage the organization's brand as further leverage to obtain a ransom payment.

Review the Emerging Cybersecurity Trends in 2022 report to learn about other threats that organizations should consider.

Threat indicators

To mitigate exposure to this threat, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be reallocated. The domains and IP addresses in the table may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
195.85.205.15	IP address	Hosting Instagram phishing domains
198.38.86.93	IP address	Hosting Instagram phishing domains
51.254.6.251	IP address	Hosting Instagram phishing domains
78.135.85.92	IP address	Hosting Instagram phishing domains
ig-contactform.com	Domain name	Instagram phishing site
ig-contactservices.com	Domain name	Instagram phishing site
ig-copyrightsobjection.com	Domain name	Instagram phishing site
ig-mailservices.com	Domain name	Instagram phishing site
ig-mailservicesupport.com	Domain name	Instagram phishing site
lg-supportservices.com	Domain name	Instagram phishing site
objectionservices.org	Domain name	Instagram phishing site
supportcomminity.com	Domain name	Instagram phishing site
supportercontacts.com	Domain name	Instagram phishing site
supporterviolation.com	Domain name	Instagram phishing site
supportscommunity.com	Domain name	Instagram phishing site
supportsnotification.com	Domain name	Instagram phishing site
supportviolationform.com	Domain name	Instagram phishing site
wfarway@gmail.com	Email Address	Threat actor contact information in Instagram phishing campaign
+7 991 472 4452	Phone number	Threat actor contact information in Instagram phishing campaign

Indicator	Type	Context
+90 538 409 3777	Phone number	Threat actor contact information in Instagram phishing campaign
Pharaben	Username	Threat actor contact information in Instagram phishing campaign
Farw4y	Username	Threat actor contact information in Instagram phishing campaign
bc1qgpukcptnyfyejmalpqzzz0fwg2w727ur6r4fvf	Cryptocurrency wallet ID	Bitcoin account for Instagram phishing ransom payments

Table 1. Indicators for this threat.