Advance Fee Fraud: The Emergence of Elaborate Crypto Schemes

proofpoint.com/us/blog/threat-insight/advance-fee-fraud-emergence-elaborate-crypto-schemes

August 31, 2021

Blog

Threat Insight

Advance Fee Fraud: The Emergence of Elaborate Crypto Schemes

September 08, 2021 Davide Canali, Crista Giering, Tim Kromphardt, and Sam Scholten

Key Takeaways

- Proofpoint researchers have observed email fraud campaigns that send functioning sets of login credentials to fake cryptocurrency exchange platforms.
- Proofpoint researchers explored one of the platforms in depth and determined it is well crafted, appearing fully functional to victims.
- Victims are tempted by the promise of a considerable amount of cryptocurrency. Cashing out the full balance, however, requires the victim to first deposit some Bitcoin to the platform, which is the point of the scheme.
- The campaigns are not targeting any specific vertical or geography and are instead being distributed worldwide.

Overview

Proofpoint researchers have identified an intriguing Advance Fee Fraud scheme sending low volume email campaigns and employing advanced social engineering tactics to swindle unsuspecting victims out of Bitcoin. This scheme spreads credentials to alleged private Bitcoin investment platforms and lures victims with the promise of withdrawing hundreds of thousands of dollars worth of cryptocurrency from an already established account on the platform(s).

While being very similar to traditional Advance Fee Fraud schemes, this set of campaigns is much more sophisticated from a technical standpoint, is fully automated, and requires substantial victim interaction. The use of cryptocurrency, in this case, is also notable for the following reasons:

- It provides anonymity for both the attacker and the victim. Specifically for the victim, they may find it appealing that the money would be acquired anonymously and tax-free.

- It indicates that the threat actor is targeting individuals that are somewhat technically savvy as they will need to be comfortable handling Bitcoin and a digital wallet.

Campaign Details

Proofpoint researchers detected the first of these campaigns in May 2021 using a coins45[.]com landing page while the most recent version started in July 2021 and directs potential victims to securecoins[.]net.

According to Proofpoint visibility, each of the email campaigns has been sent to anywhere from tens to hundreds of recipients around the globe, and emails from the same campaign contain the same credential pairs—user id and password—for all recipients. It appears that multiple people can log in with the same user id and password if they log in from a different IP address and browser. However, once they change the password, as detailed in the next section, and add in a phone number, the account becomes unique, and victims will not see any trace of other victims' activities.

A Walkthrough of the Scheme

This cluster of Advance Fee Fraud activity begins like any other type of business email compromise, with an email designed to get the attention of the recipient. The emails all appear similar to the one shown in Figure 1, which attempts to lure victims with the promise of a hefty amount of money. In this case, that amount is 28.85 Bitcoin or about $1,350,119 USD (as of 26 August 2021).

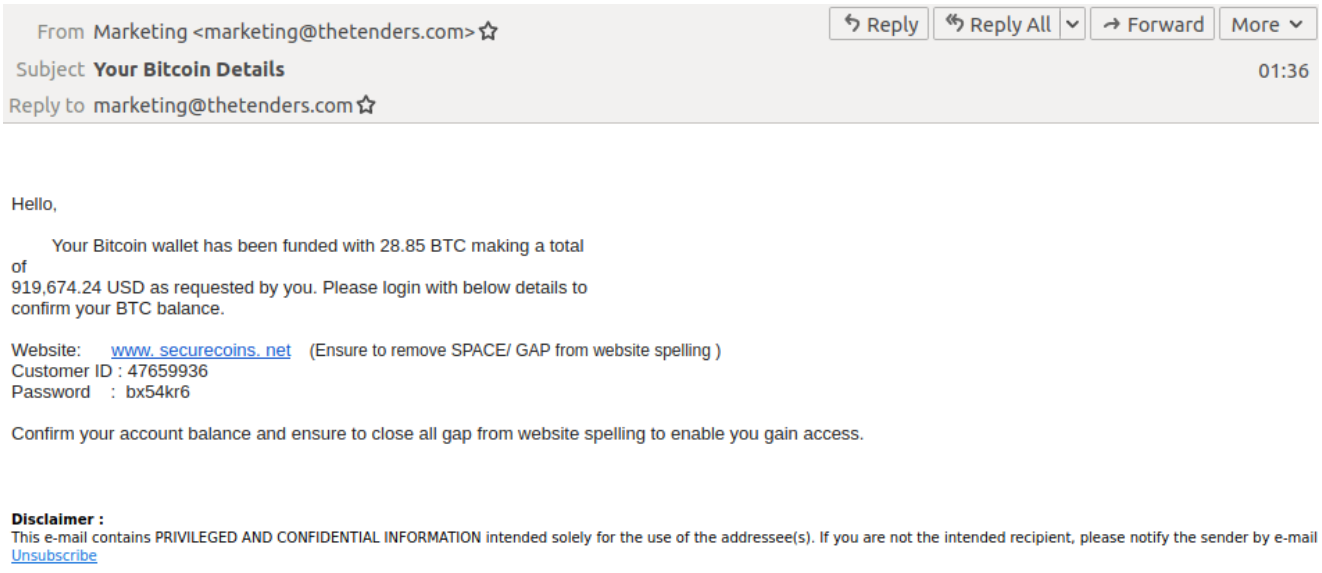

Figure 1. Sample of the initial email sent to intended victims.

Step 1 - Logging In

Once a victim is successfully enticed by the monetary promise in the email, they will be tempted to try to log in to the noted Bitcoin wallet website using the provided credentials. The customer ID and password work to access the site; however, as soon as a victim logs in, they are prompted to change the password and add a recovery phone number for security (Figure 2).

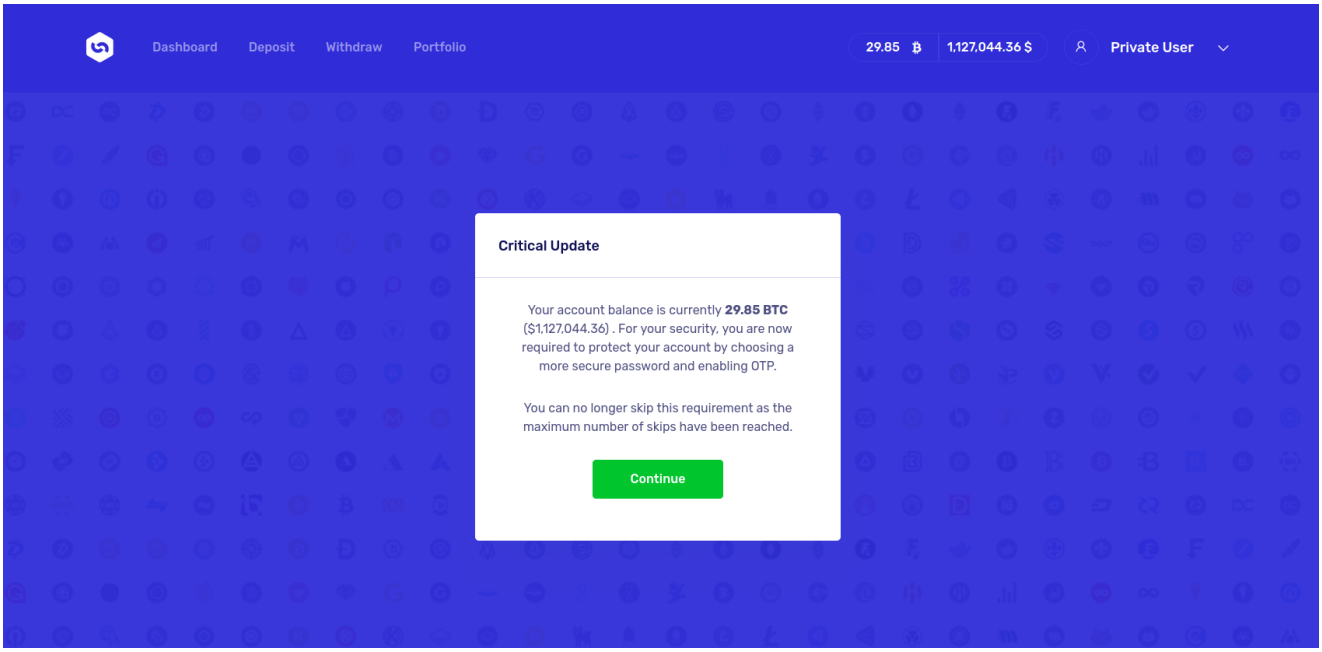

Figure 2. Change password and enable multi-factor authentication prompt.

This step may be intended to provide a false sense of security to the victim as they could see it as a sign of legitimacy given the emphasis on protecting the account via multi-factor authentication, which is considered a security best practice.

Once the victim follows through with this step, being guided to take over the account, they receive an automated call to the phone number they provided, giving the one-time password (OTP) to enable the additional account security. The OTP codes are sent from one of two numbers: +44 2045 383250 (UK number) or +1 (201) 379 6348 (US number).

After inputting the OTP, the website confirms the account has been secured as seen in Figure 3.

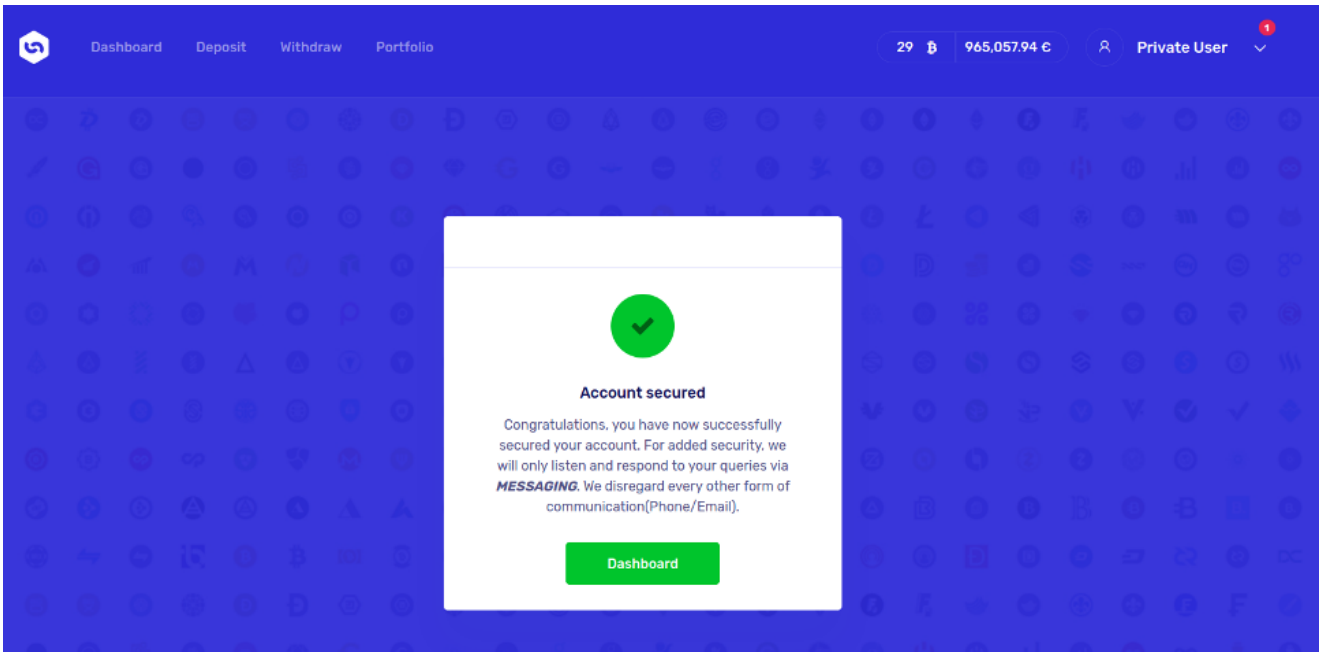

Figure 3. Confirmation of account security after the victim has changed the password and established multi-factor authentication via phone.

To provide even more reassurance to the victim, the account secured confirmation notes that the only way to get in touch with the platform support service is via the internal messaging system through the now secured account. Great! Whoever was the owner of the account prior to the victim now has no control over it. The victim can now go ahead and try to empty those 28.85 BTC into their wallet.

Step 2 – Inside the Platform

Navigating around the account, a victim can find a couple of messages from the alleged "previous owner" of the account, Figures 4 through 6.

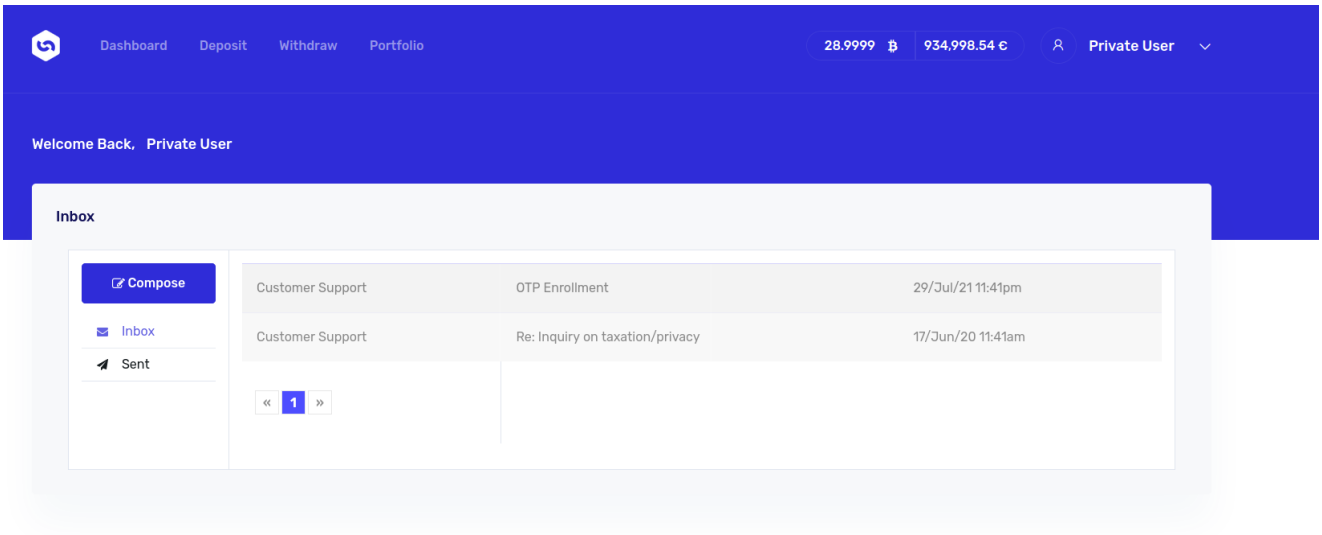

Figure 4.

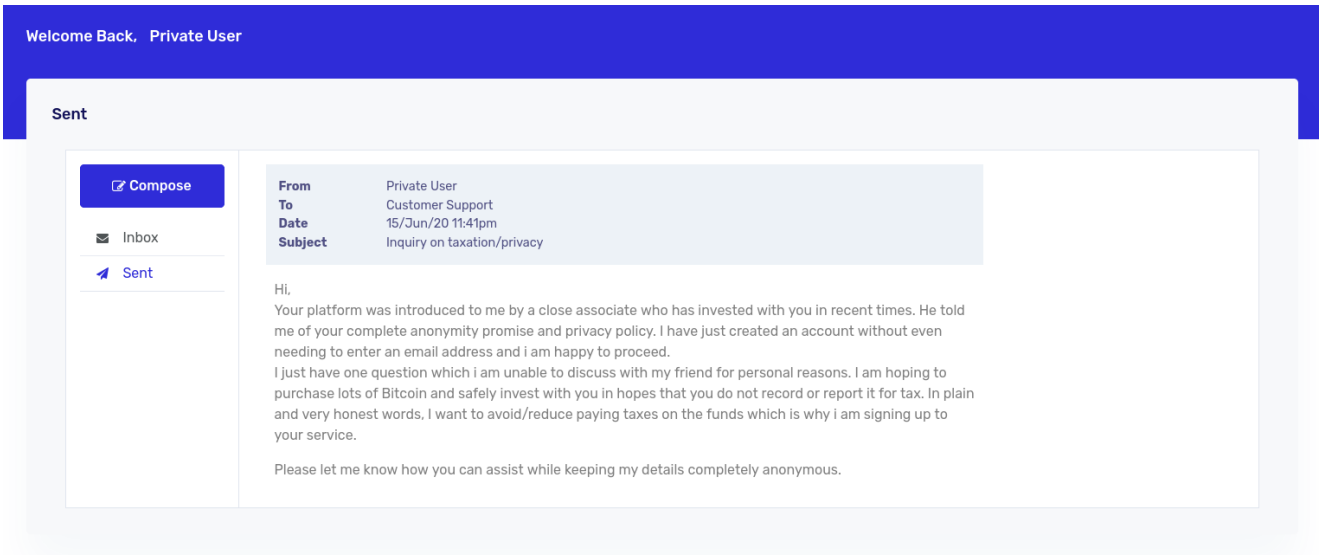

Figure 5.

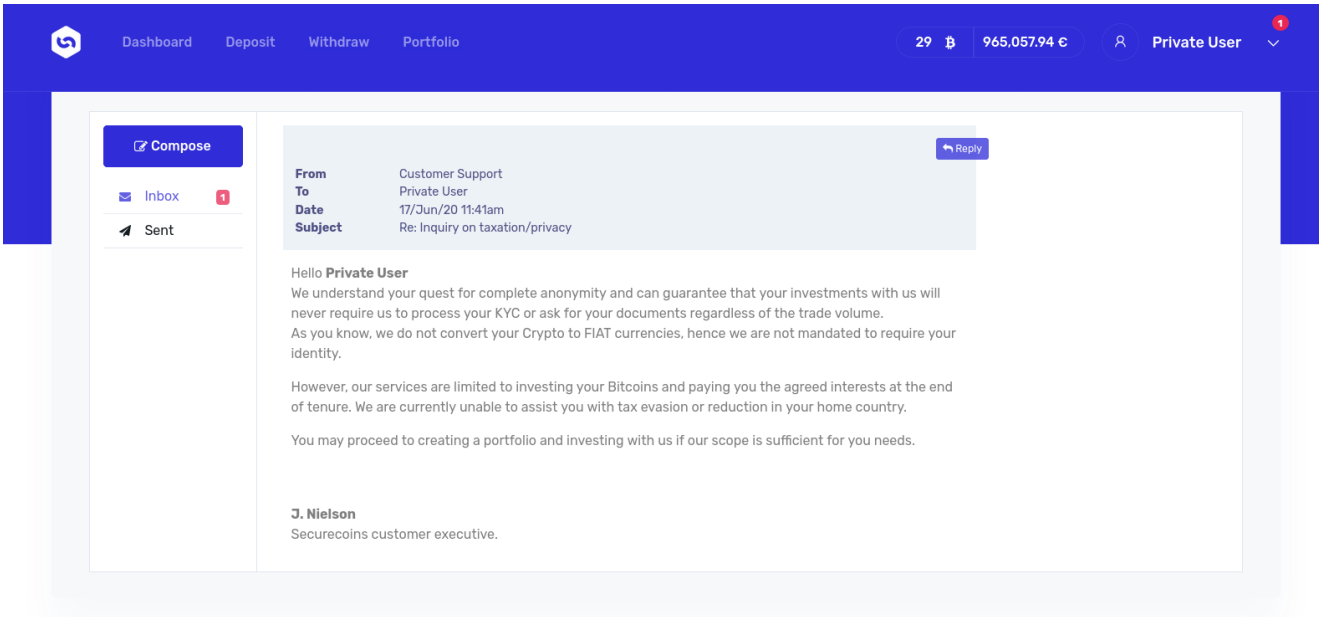

Figure 6.

The information provided in the messages indicates that this platform is completely anonymous, making it the perfect place to take some BTC from. The user account area shows there is no need to enter any name or address. The victim is only allowed to enter a phone number and an optional email address. The page also notes the last time the victim logged in and mentions that the IP address is never stored, putting a technically savvy victim even more at ease.

Step 3 – Withdrawing the Funds

As depicted in Figure 7, the account shows some BTC has been deposited and withdrawn in the past, making it appear as if the account is functional. Navigating to the “Withdraw” entry in the menu, a victim can try to transfer some funds out of the platform; however, the platform

states that the first transfer out of any portfolio must be 0.0001 BTC (about $4.75 USD as of 26 August 2021) to ensure everything works as expected from both sender/receiver ends.

As the victim proceeds and submits a transfer request, the transfer appears in the queue. After roughly 40 minutes, the transfer option appears to work! The victim starts to receive confirmations of the transfer along with the amount appearing in their personal wallet. The platform also appears to be updated in real time (Figure 7).

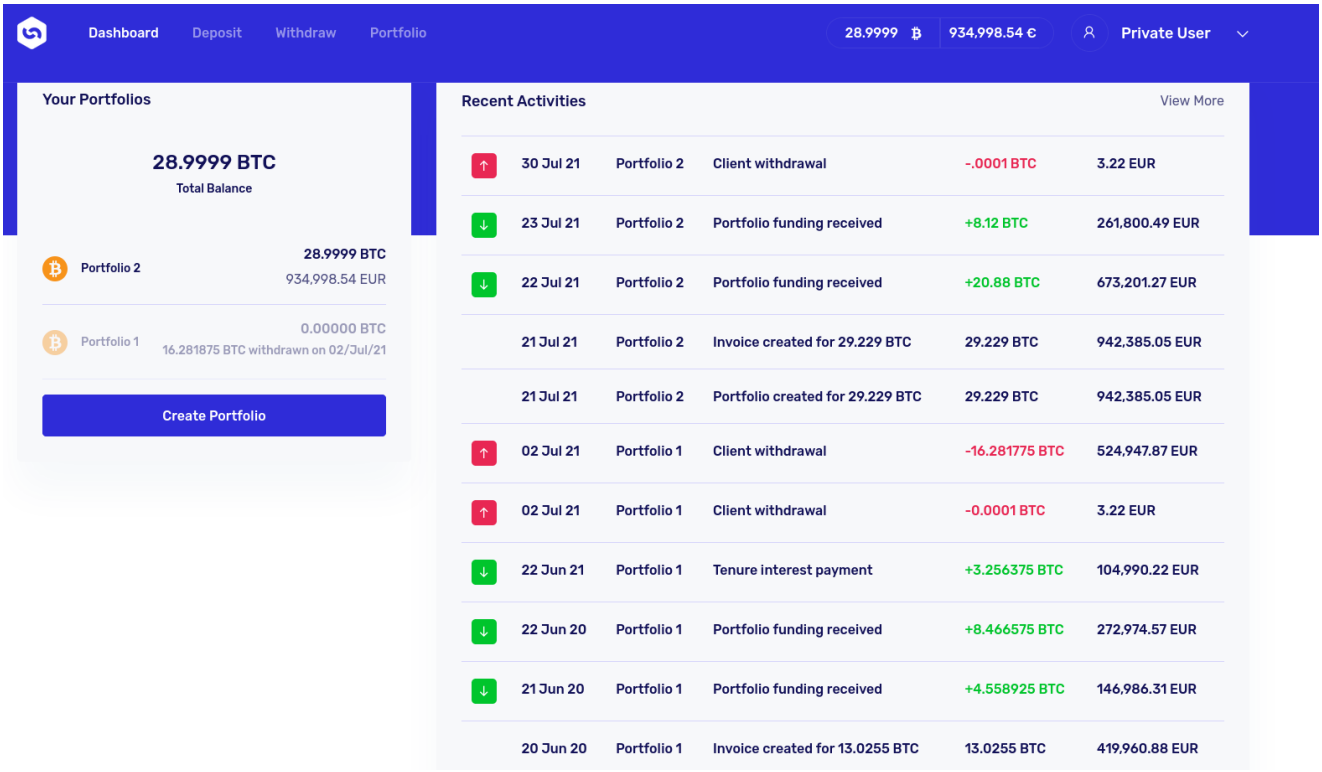

Figure 7.

Unfortunately for the victim, when they try to take out the rest of the BTC they hit a wall (Figure 8).

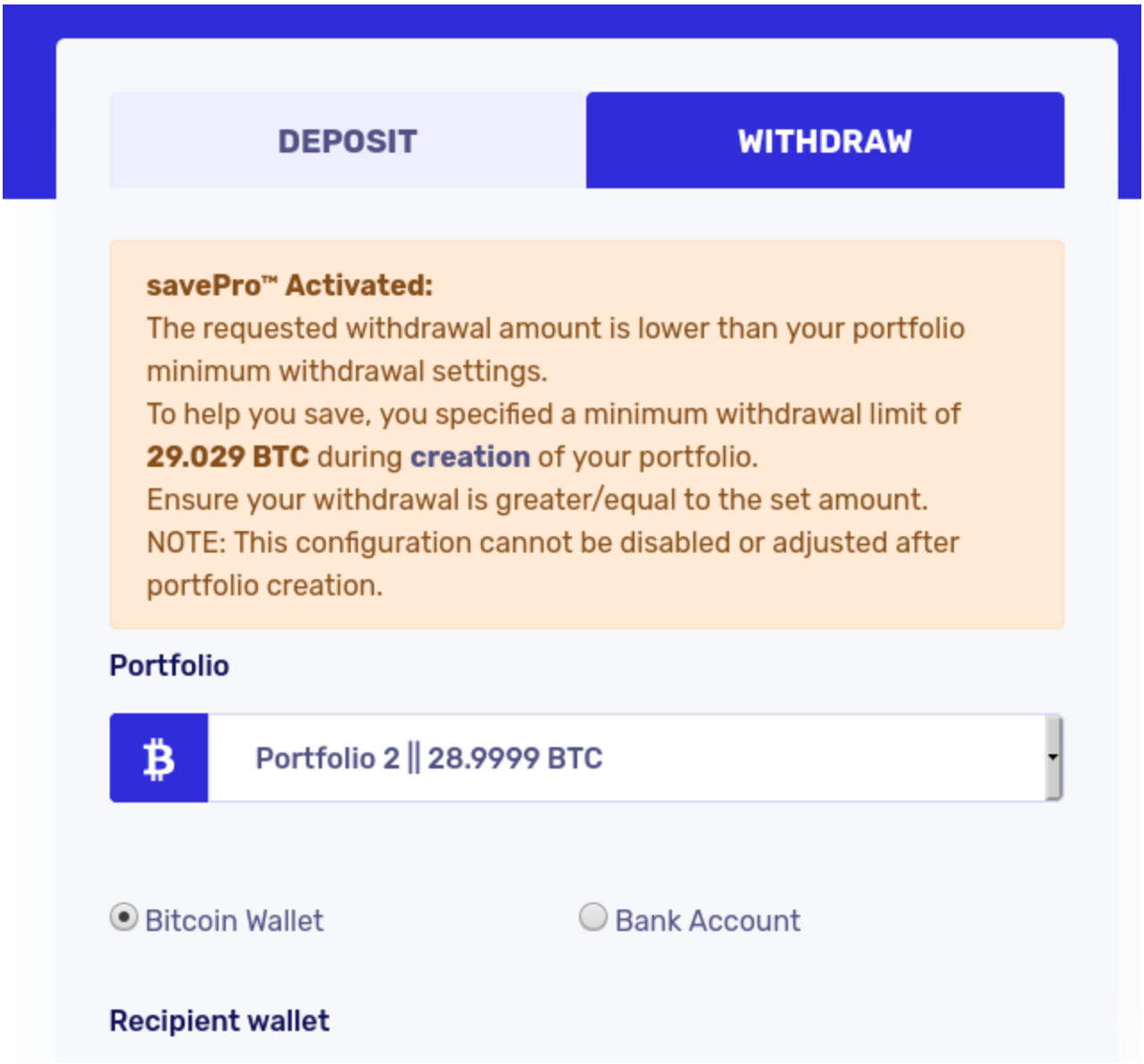

Figure 8. Notification that there is a monetary minimum for withdrawal from the account.

It is at this time that the platform informs the victim that, to help them save money, the account owner specified a minimum withdrawal amount of 29.029 BTC at the time the account was created. Thus, the victim cannot withdraw anything less than that amount. The victim will now likely conclude the only way to get those 28.9999 BTC is by transferring enough BTC to the platform (anything greater than 0.0291 BTC) to reach a balance of at least 29.029 BTC, as specified. At that point, the victim will be able to empty the whole account, right?

Wrong! While Proofpoint researchers were unable to verify, we assess with high confidence that the final transfer would not work, leaving the victim's wallet 0.029 BTC lighter. That amount is almost insignificant compared to the alleged account balance; however, it still represents about $1400 USD (as of 26 August 2021).

Additional Platform Functionality

The Bitcoin platform also has a Portfolio section that appears functional and shows previous portfolio activity. If a victim were to try to create a portfolio, they would be required to wire at least 0.25 BTC or the equivalent in fiat currency via the “Deposit” section of the site. Proofpoint researchers only tested the cryptocurrency transfer option, which the platform provided a new BTC address for the transfer of funds and generated a new “invoice” that appeared in the dashboard as awaiting payment. While Proofpoint researchers did not follow through with transferring any cryptocurrency to the platform, we expect that it would have been a successful transaction.

There is also an option to convert BTC to fiat and to wire that amount to a victim’s chosen bank account. To do so, the victim would have to create a new beneficiary, providing their full name, country, and address required, and add that individual’s SWIFT and IBAN number for payment. Interestingly, this option appears to be fully functioning with the platform employing a properly implemented IBAN parsing. Proofpoint researchers first tried entering random letters and numbers as IBAN and SWIFT, but that did not work until we provided a real SWIFT/IBAN pair.

An Ever-Evolving Platform

The platform appears to be under active development. The threat actors in August 2021 added an additional step to force prospective victims to pay money upfront before being able to log in and access the account. After changing the log in password and setting up multi-factor authentication, the victim must agree to a yearly fee of 0.0005 BTC, as seen in Figure 9.

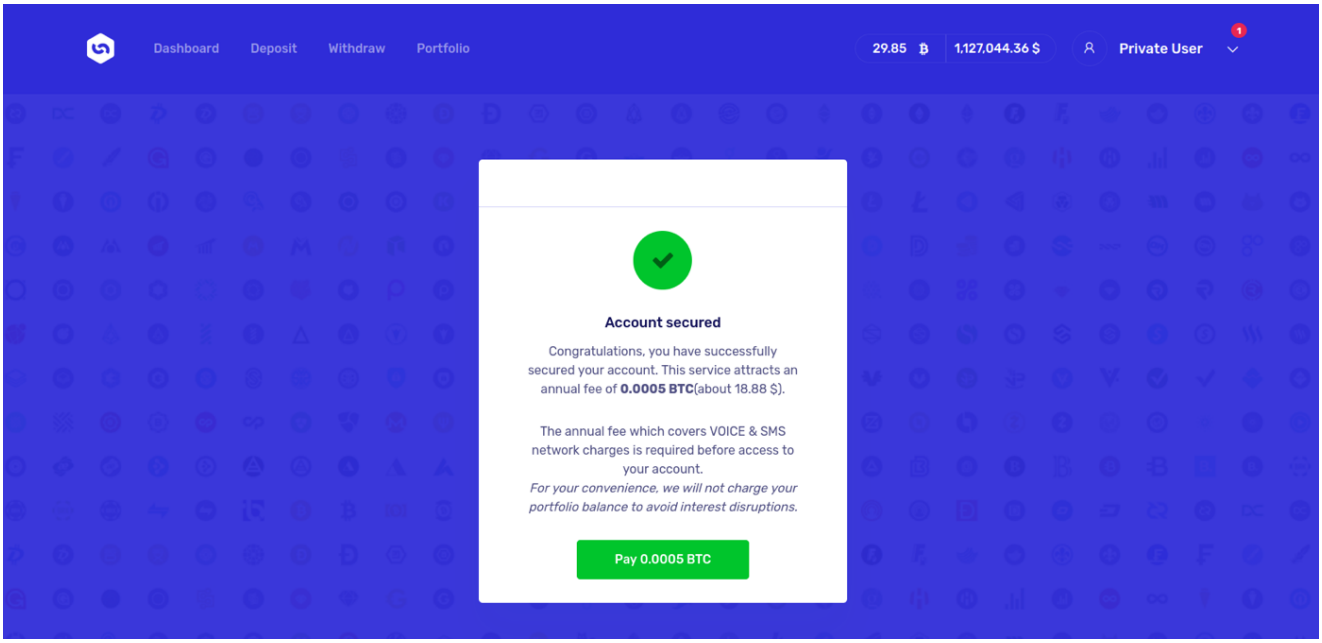

Figure 9.

Proofpoint researchers assess that this change will reduce the chances of this scheme continuing to be successful because the intended victim is not given the chance to engage with the platform and buy in to its legitimate-appearing features. Accounts whose password and phone number have been changed prior to August 5, 2021, however, are still able to login and use the platform without being requested this additional fee.

Conclusion

Using the incentive of monetary gain is always a timely and effective method of tempting potential victims into engaging in elaborate Advance Fee Fraud schemes. The reliance on robust interaction by the potential victim, in this instance, may serve as a disincentive but also enables the threat actor to bypass some automated threat detection services. Proofpoint researchers expect the threat actor to continue with this activity and to evolve their tactics in future campaigns with an eye on increasing their rate of success.

Indicators of Compromise

Indicator	Description
quetta@pec[.]org[.]pk	Email sender
marketing@thetenders[.]com	Email sender
info@kenmascs[.]com	Email sender
info@coin45[.]com	Email sender
info@securecoins[.]net	Email sender
inquiry@rosaritoindustries[.]com	Email sender
coin45@mail[.]com	Email sender
crypto@adminsupport[.]com	Email sender
cryptoadmin@adminsupport[.]com	Email sender
cryptoadmin@supportsystem[.]com	Email sender

admin1@coin45[.]com	Email sender
bitcoinfunds@mail[.]com	Email sender
bitcoinadmin@supportsystem[.]com	Email sender
coin1@efeasy[.]cloud	Email sender
coin2@efeasy[.]cloud	Email sender
coins4@efeasy[.]cloud	Email sender
coins5@efeasy[.]cloud	Email sender
coins6@efeasy[.]cloud	Email sender
coins7@efeasy[.]cloud	Email sender
adm@onlinemsc[.]xyz	Email sender
coins45@onet[.]eu	Email sender
adm1@efeasy[.]cloud	Email sender
ho@almasroor[.]com	Email sender
y.kirimura@nihonplant[.]jp	Email sender
m-iwasaki@wtw[.]co[.]jp	Email sender
sales@mphgroup[.]uk	Email sender
adm@caretis[.]gr	Email sender
info@mail[.]com	Email sender

015-0000@mfchmao[.]ru	Email sender
0786306834loans@gmail[.]com	Email sender
210231@itapemirimcorp[.]com[.]br	Email sender
Bitcoin@adminsupport[.]com	Email sender
Chabanova.O@mfua[.]ru	Email sender
John.Conkle@tempursealy[.]com	Email sender
a.bellantuono@aslfg[.]it	Email sender
a.petelin@sct[.]ru	Email sender
account@densen[.]dk	Email sender
admin@nanoptika[.]ru	Email sender
alessandra.lara@grupocanopus[.]com[.]br	Email sender
althuis@huissier-justice[.]fr	Email sender
aoperry925@gmail[.]com	Email sender
asapreps1.uce.report@gmail[.]com	Email sender
barclays.payout@gmail[.]com	Email sender
bitcoin@adminsupport[.]com	Email sender
bitcoin@support[.]com	Email sender
chernichenko_av@krsk[.]irgups[.]ru	Email sender

cs1.nissan.snp@grupocanopus[.]com[.]br	Email sender
danny.trom@ehess[.]fr	Email sender
davide@barbanoarredamenti[.]it	Email sender
dimvagia@otenet[.]gr	Email sender
e.skalova@mercedes-kanavto[.]ru	Email sender
eloglogs@palletsolutions[.]ca	Email sender
eshayko@guit[.]omskportal[.]ru	Email sender
fabio.dattanasio@tbsit[.]com	Email sender
faithkingsley@vivaldi[.]net	Email sender
galiullin.r@mercedes-kanavto[.]ru	Email sender
george@sunrisehouse[.]com	Email sender
info@ig-conseil[.]com	Email sender
k.iwakabe@nde[.]co[.]jp	Email sender
kst91178@gmail[.]com	Email sender
mamedova.nn@ocsial[.]com	Email sender
no-reply@kgsha[.]ru	Email sender
no-reply@mail[.]com	Email sender
no-reply@oaed[.]gr	Email sender

noreply@marketleader[.]com	Email sender
noreply@techradarportal[.]se	Email sender
o.dorodniaia@sct[.]ru	Email sender
ottt33754@gmail[.]com	Email sender
oyu.kocheva@vtc-service[.]ru	Email sender
philip.stephenson@oracle[.]com	Email sender
pope@mail[.]com	Email sender
regina@urosa[.]com	Email sender
rosaj@remax-alliance-houston-tx[.]com	Email sender
rosangelab@hc[.]ufu[.]br	Email sender
sergio.abreu@scml[.]pt	Email sender
smtpfox-ucvhy@crismedina[.]com[.]br	Email sender
yangjiang@cmagency[.]com[.]cn	Email sender
bc1qtrle8939dcu39hqfh0jt0y25d4wxqvt60f7pj8	Platform’s Bitcoin sending address
1ApdtuAoGvDi8BLK9CaZFSw8Ku9go6Mwdb	Platform’s Bitcoin sending address
securecoins[.]net	Campaign landing page
coins45[.]com	Campaign landing page
coinmace[.]net	Campaign landing page

coinomac[.]com	Campaign landing page
fortcoin[.]net	Campaign landing page

Subscribe to the Proofpoint Blog