SIXGILL REPORT

Overstimulating

CARES Act Fraud On the Deep and Dark Web

April 30, 2020

Overstimulating: CARES Act Fraud On the Deep and Dark Web

Executive Summary

- In response to the economic impact of the COVID-19 pandemic, on March 27, 2020, the US Congress passed the CARES Act, an economic relief and stimulus package, providing over $2 trillion of funding to businesses and individuals. Naturally, we expected fraudsters would jump on the opportunity to make some cash.

- Keeping in mind that threat actors generally do not share their latest proven tactics, techniques, and procedures on open forums, we searched for direct indications of fraud. We found several examples of threat actors seeking to buy or sell stolen identity packages (*fullz*) with the explicit purpose of impersonating victims to take their stimulus money.

- We also searched for indirect indications of fraudulent activity. We discovered that mentions of ID-related terms (tax ID, paystub, Social Security number, and Form 1040) rose 90% from their March average to their peak on April 11, days before the initial payments were disbursed.

- Meanwhile, we could not find any indications that actors are impersonating businesses to defraud them of government loans, which, in our understanding, is a more sophisticated and risky endeavor. Nor did we find increased discourse about the largest US banks.

- We did find several compromised business and personal bank accounts posted for sale after the CARES Act was passed. We also identified 21 infected computers with accounts to freefilefillableforms.com (a site for non-filers to apply for stimulus money) being sold on a dark web market.

- In short, while we could find no definitive proof of widespread fraud, we found anecdotal indications combined with a significant increase of some of the ingredients necessary to commit it. Ultimately, the market for identity information on the dark web is established and robust. We assess, therefore, that it is natural for fraudsters to attempt using these fullz to illegally procure CARES Act money, and we recommend increased measures to safeguard accounts and identities.

Introduction

In response to a rapidly deteriorating economy impacted by the COVID-19 pandemic, on March 27, 2020, the US Congress passed the Coronavirus Aid, Relief, and Economic Security Act, also known as the CARES Act. The CARES Act was an unprecedented economic relief and stimulus package, providing over $2 trillion of government funding. This includes aid to businesses, in the form of loans and tax relief, and to individuals, including $1,200 to qualifying individuals, extended unemployment benefits, and assistance for students and retirees.

Most of the actors active on the dark web are opportunistic, seeking low-effort schemes where money is most available. With so much money being distributed by the government in so little time, we would expect widespread attempts of fraudulent activities.

Threat actors can attempt to take money before or after relief payment. That is, through impersonating an individual or business to receive money directly from the government, or through attempting to take funds from those that have already received it.

METHODOLOGY

From the outset, we understood that it would be difficult to find many direct implications of fraud on the deep and dark web. Simply put, threat actors generally do not share their latest proven tactics, techniques, and procedures on open forums; doing so would possibly compromise their lucrative schemes and possibly expose them in the process.

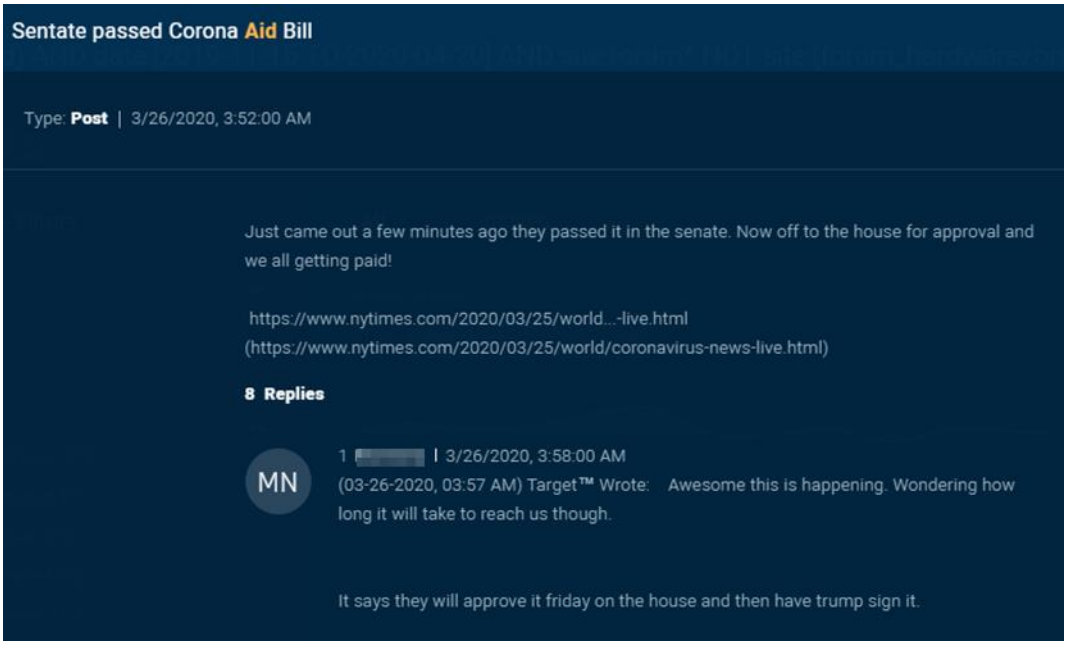
Rather, we chose to look for indirect implications of fraud. This includes:

- General discussions about the CARES Act
- Interest in or intention of fraud
- Components necessary in impersonating individuals (ex- SSNs)
- Components necessary in impersonating businesses
- Bank account compromise

General Discourse

Dark web actors closely follow general news and developments, and the CARES Act was no exception. Just minutes after the Senate passed the bill, there was already chatter about it:

Figure 1: A post on a dark web forum notifying of the passage of the CARES Act



Indeed, Sixgill has noted a considerable number of posts in which actors have expressed personal financial difficulty, such as loss of employment or investment, due to the economic impact of the virus. Therefore, it is no surprise that in the days before and after the bill's passage, mentions of *stimulus*, *bailout*, and *CARES Act* were high, peaking on at 317 posts in forums on March 26, when the bill was passed.

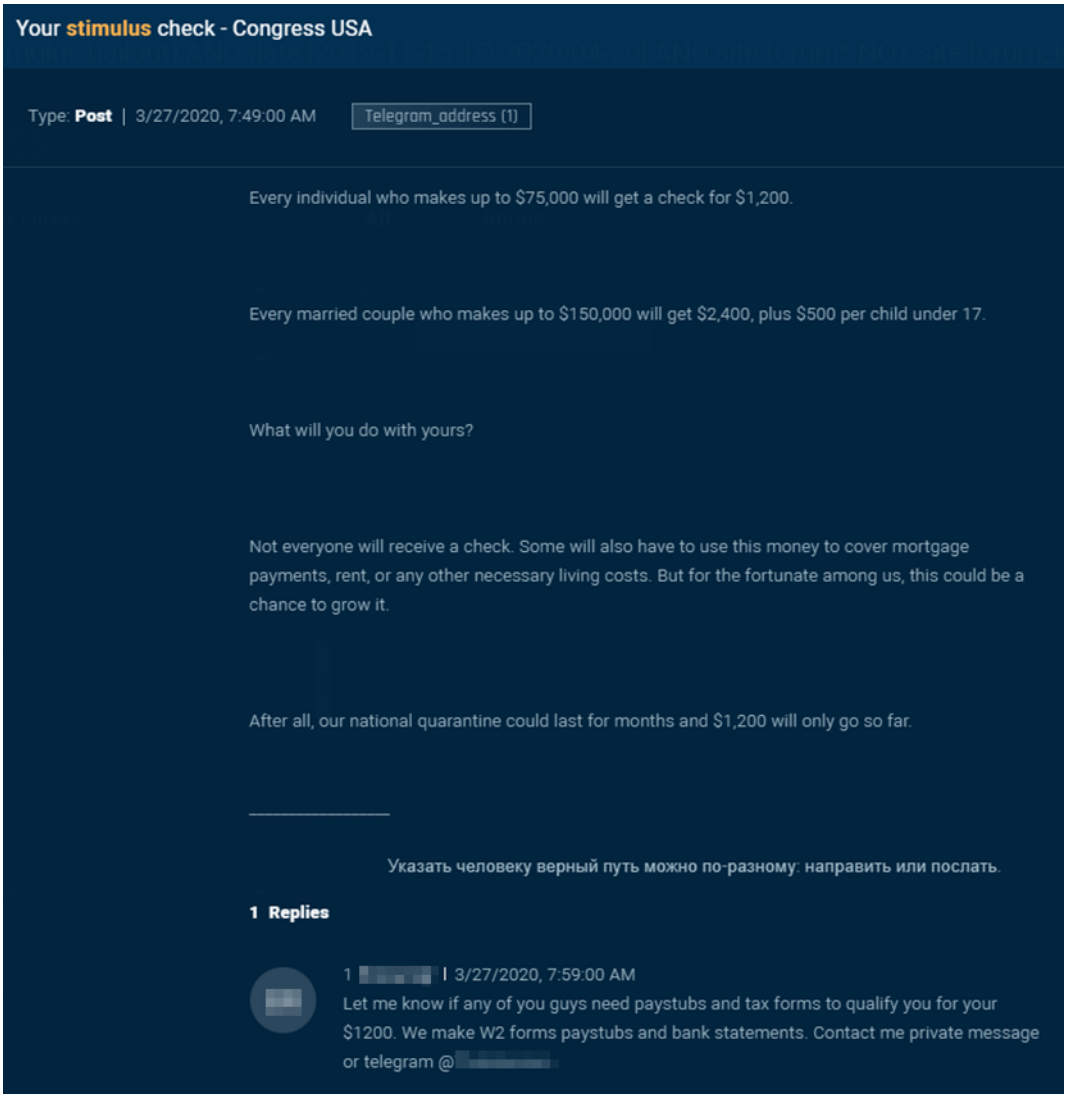
Figure 2: Dark web discourse about stimulus, peaking when the CARES Act was passed

Interest and Intent

Occasionally, threat actors reveal interest and intentions to commit cybercrime. Sometimes directly and sometimes through an offhand remark, these statements can reflect much broader activities that are taking place. To these ends, Sixgill discovered a variety of direct indications of explicit interest/intent in assisting or committing fraudulent activities surrounding the CARES Act.

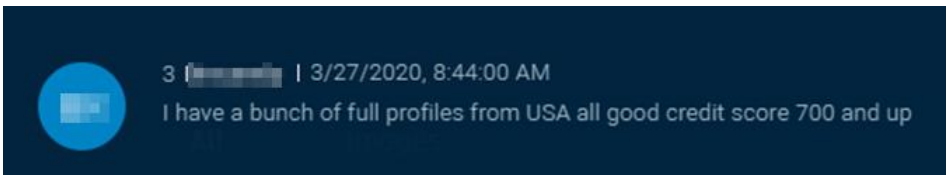
In response to a post on a dark web forum announcing the passage of the CARES Act, an actor wrote: *"Let me know if any of you guys need paystubs and tax forms to qualify you for your $1200. We make W2 forms paystubs and bank statements."*

Figure 3: A news item about the stimulus package, with a response from an actor offering W-2 forms, paystubs, and bank statements needed to perpetrate fraud



On that day, this same actor was engaged in a marketing blitz for his wares, writing on another post that he has "*a bunch of full profiles from USA all good credit score*." Clearly, he sees the stimulus package as a prime opportunity to sell forged and stolen identity information.

Figure 4: Another post from the previously actor, offering US profiles with high credit scores



Meanwhile, even more brazenly, an actor wrote a post recommending using *fullz* (dark web slang for an individual's identity package, including name, Social Security number, date of birth, account numbers, etc.) to claim stimulus checks:

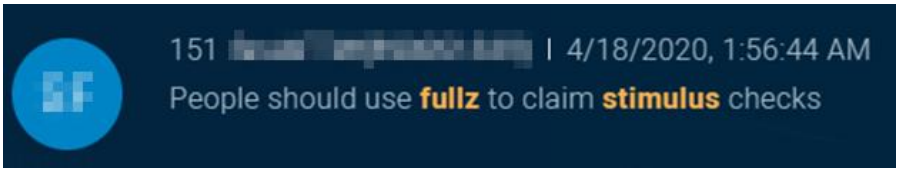


Figure 5: A suggestion to use *fullz* to claim stimulus checks

Similarly, an actor wrote in the beginners section of a forum that he was searching for fullz, "*since people are getting stimulus*." Three other actors responded that they are searching for the same items, and a fourth recommends that they create a phishing page impersonating the IRS.

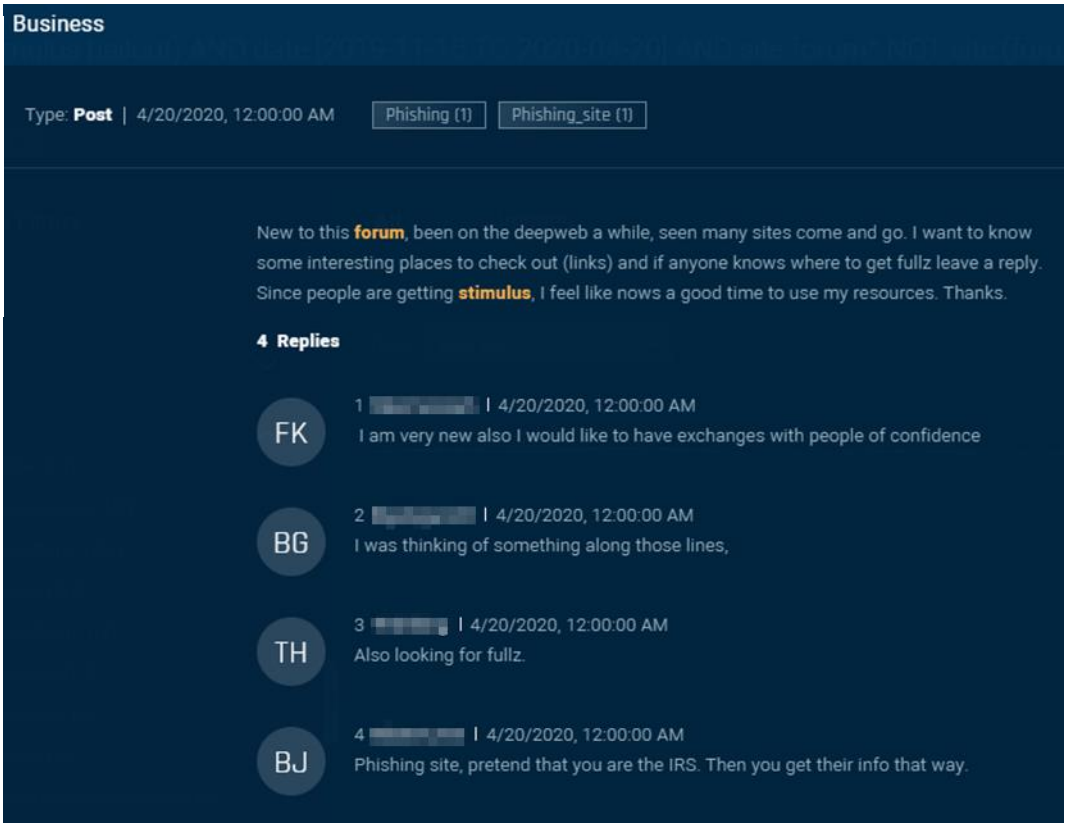


Figure 6: A discussion between several actors searching for fullz in order to steal stimulus money

We also found this rather aggressive statement from an actor warning that he is coming for your $1,200:

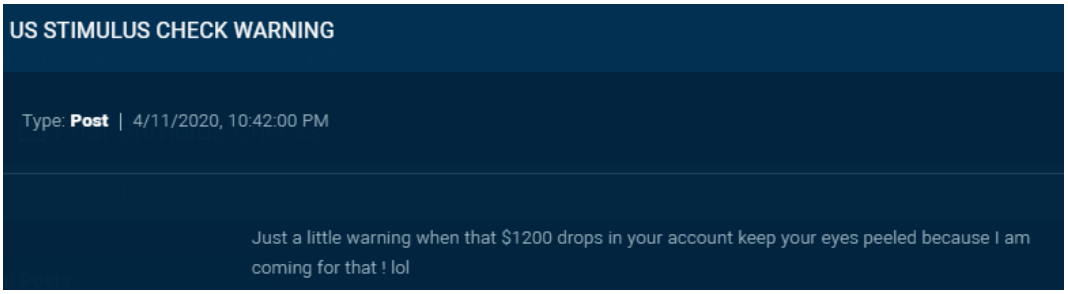


Figure 7: A threat actor warns that he is "Coming for that [$1,200]."

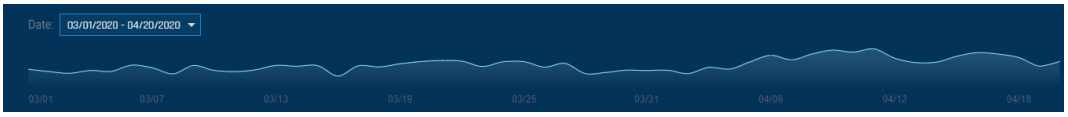
Ultimately, we believe that these posts, while anecdotal, offer a glimpse of much greater activity taking place below the surface.

Components to impersonate individuals

For an attacker to impersonate an individual in order to redirect a stimulus deposit to the attacker's bank account or address, they require sensitive information, which include a social security number, previous year's tax returns, address, and date of birth. Fortunately for threat actors, the dark web is already saturated with fullz identity packages. Dark web actors buy and sell fullz on a daily basis, using them for all sorts of schemes.

However, we noted rise in fullz and identity related items that began soon after the CARES Act was passed:

Figure 8: Mentions of ID-related information rose over 90% after the passing of the CARES Act

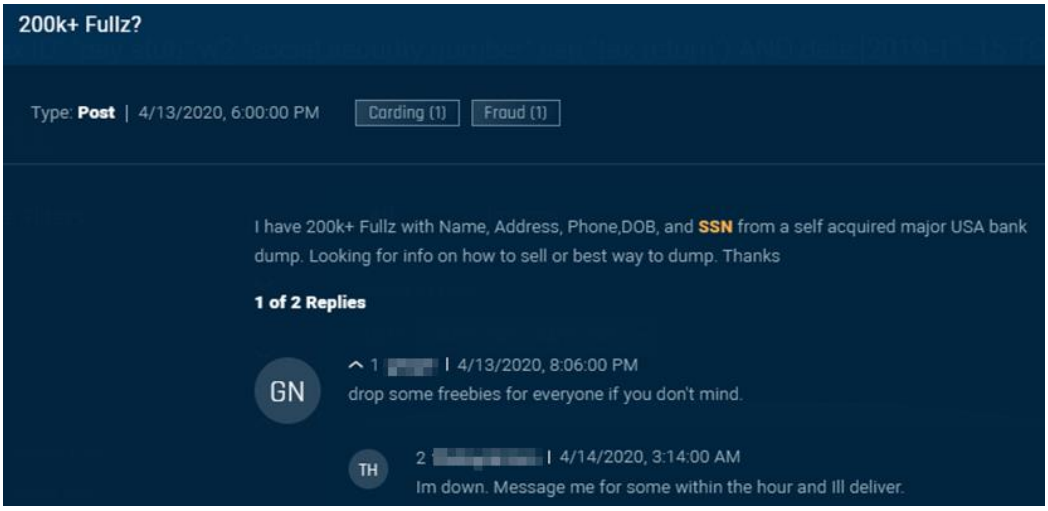


In numbers, mentions of terms such as *tax ID*, *paystub*, *Social Security number*, and *Form 1040* averaged at 925/day in March. They began to rise in early April in parallel to the stimulus law being passed; In April 5-18, they averaged at 1,444/day, peaking at 1,765 on April 11, a 90% rise from the March average, two days before the initial payments were first disbursed.

While this does not necessarily indicate widespread stimulus fraud, we find it highly suggestive that average mentions of components necessary to impersonating individuals nearly doubled while the stimulus was being deployed.

Certainly, there is no shortage of compromised identity information available for those seeking to exploit it. The following posts are examples of actors seeking to buy or to sell US fullz between when the CARES Act was passed until the first payments were deposited. This includes posts from sellers:

Figure 9: 200,000 fullz from a major US bank for sale



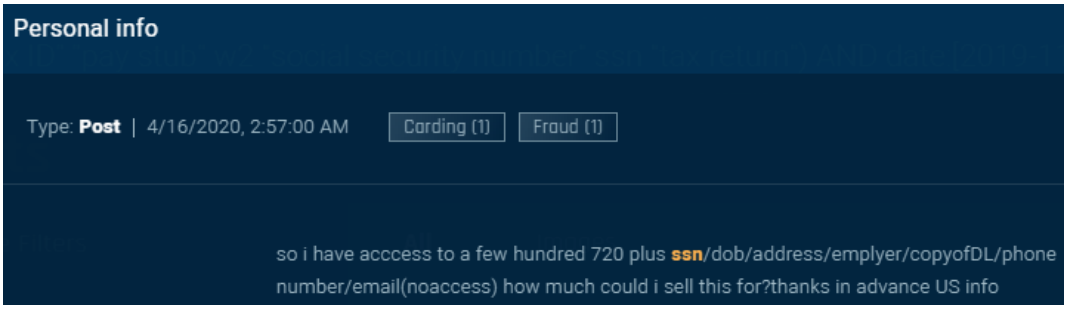


Figure 10: 720 US fullz for sale

There are also posts from aspiring buyers looking for specific items:

Figure 11: Actor seeking fullz

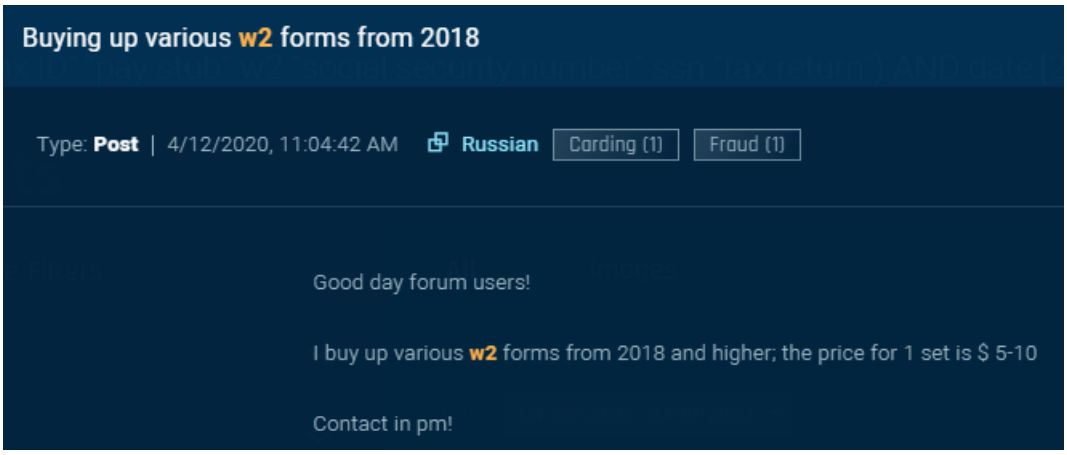


Figure 12: Actor seeking W-2 forms (possibly for resale

These posts were just a few examples of the robust supply and demand for identity information on the dark web. Any one of them, along with the thousands of others, could have been part of a transaction for the sake of fraudulent attempts to seize stimulus money.

NON-FILERS

In order to disburse payments to individuals that did not file taxes, the IRS and Intuit created a website called *Free File Fillable Forms* (www.freefilefillableforms.com) for individuals to enter their salary and payment information.

Security researchers have already noted the relatively weak identification required by this site to verify applicants.[1] To add to these concerns, Sixgill

[1] https://krebsonsecurity.com/2020/04/new-irs-site-could-make-it-easy-for-thieves-to-intercept-some-stimulus-payments/

identified (through April 30) 21 infected computers with accounts to www.freefilefillableforms.com that were being sold on a popular underground market that sells access to compromised systems. Possibly, attackers could purchase access to these compromised machines and change the users' filing information to their own bank accounts without the users knowing.

Components to impersonate businesses

In addition to providing direct assistance to individuals, the CARES Act offers four main programs to assist businesses:[2]

- **Paycheck Protection Program**: loan forgiveness for retaining employees
- **EIDL (Economic Injury Disaster Loan) Advance**: up to $10,000 of economic relief to businesses
- **SBA Express Bridge Loans**: access up to $25,000
- **SBA Debt Relief**: Financial reprieve to small businesses

Applications for these programs and loans are directed to the US Small Business Administration (SBA), and, when approved, money is disbursed to the business through a direct deposit into the business's account in an accredited financial institution.

Unlike the individual relief payments, in which an attacker simply needs to divert payment to a different bank account or redirect a check, it is presumably far more difficult for an attacker to abuse these programs. Here, an attacker would theoretically need to use a stolen identity of an official with signature authority to open a bank account in that business's name, and then submit an application to the SBA requesting payment to that account.

The process described above is far more complicated than garden variety identity theft, and also, with a $1 million penalty, it is far more risky. Therefore, unsurprisingly, we found considerably fewer mentions of any of these programs and loans on the dark web, with all discussions being informational in nature. Furthermore, we were also unable to find any discussions between threat actors on Taxpayer Identification Numbers (TIN), registering/impersonating a business, nor registering a business bank account.

[2] https://www.sba.gov/funding-programs/loans/coronavirus-relief-options

It is our assessment, therefore, that it is relatively unlikely that the typical dark web actor will seek to defraud businesses through falsely identifying as them. However, more advanced groups may still attempt to do so. Meanwhile, any attacker hungering to steal government money from businesses can still use more simple methods, such as social engineering and account takeover.

Bank account compromise

Another tactic that threat actors may use to secure stimulus cash is to simply take over bank accounts of those that have already received the money.

We searched for posts whose titles contain the name of any of the top-10 US banks and *account* or *login*[3]:

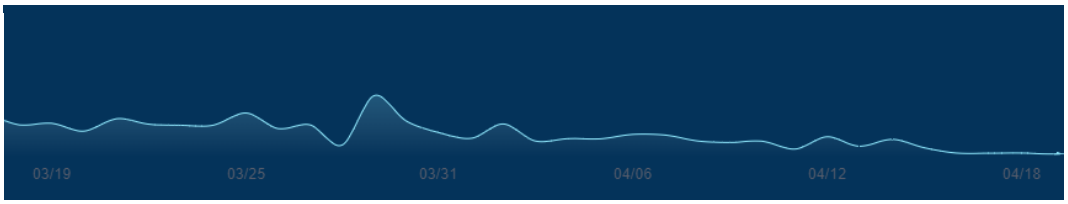


Figure 13: Discourse about banks does not correlate with the stimulus

From March 1-25, there were 169 average daily mentions. It quickly spiked to 586 on March 28, a day after the law was passed, however, it dropped from there, averaging at only 116 per day in April.

Accordingly, it does not seem like there is any correlation between the stimulus and availability of compromised bank accounts. Perhaps those that have taken over accounts withdraw the funds themselves. Perhaps actors attempting to take over bank accounts were already operating at full capacity, so they cannot scale up their attempted takeovers, even despite a possible surge in demand for these accounts. And lastly, perhaps the stimulus money does not actually create a surge in demand, since ultimately, businesses have a much lower overall balance than they did before the crisis began.

Having said this, we did find examples of bank accounts that we can verify as compromised *after* the CARES Act was passed. The following screenshots show compromised bank accounts from Chase for Business, SunTrust, and Wells Fargo for sale. These listings include references to the "Paycheck Protection Program" of the CARES Act, indicating that they were recently

[3] title:((chase "bank of america" boa "wells fargo" citibank citi "US bank" pnc "capital one" TD "BB&T" suntrust visa mastercard discover) AND (account* log*)) AND date:[2019-12-31 TO 2020-04-20] NOT site:(telegram paste* twitter)

compromised, and that attackers have found ways to potentially siphon government funds from businesses.

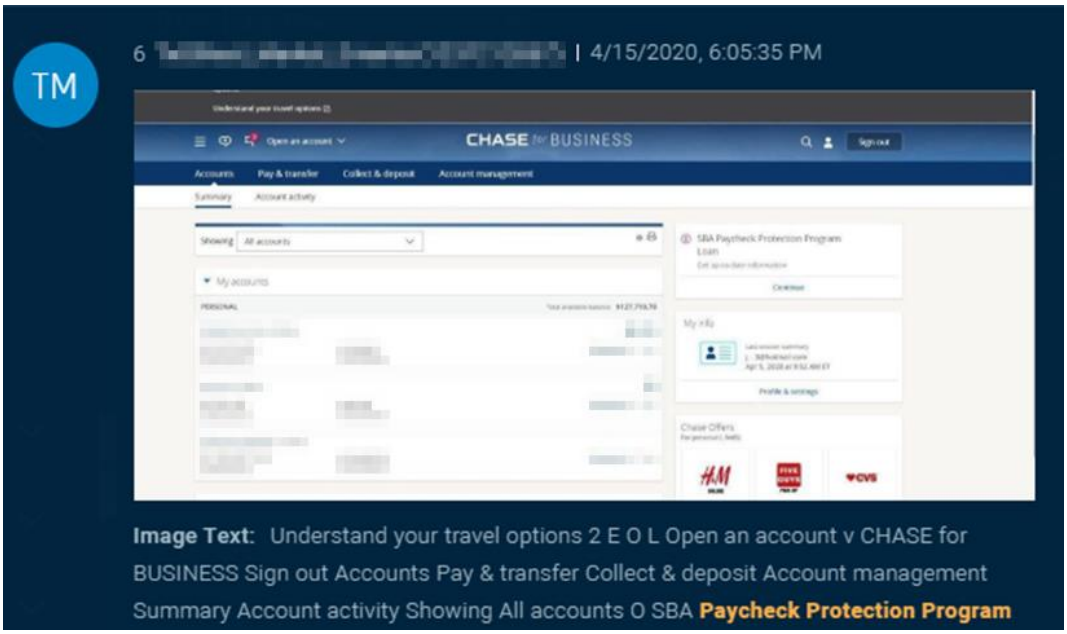


Figure 14: A compromised Chase for Business account mentioning the Paycheck Protection Program

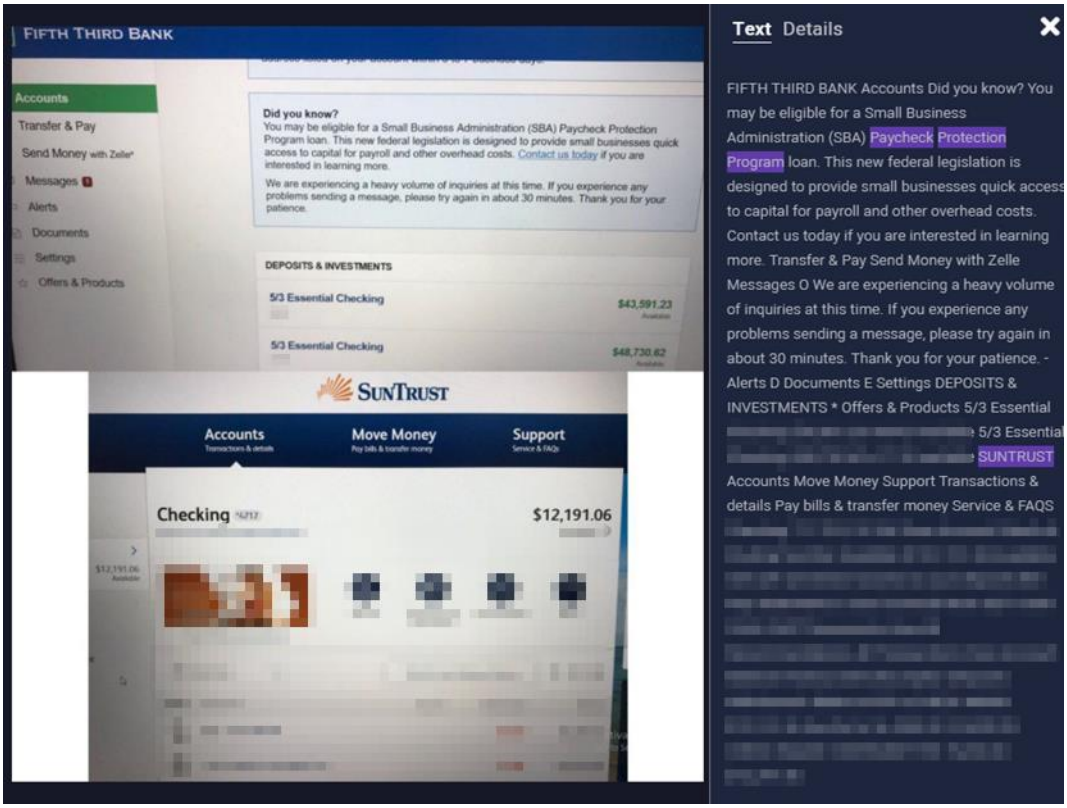
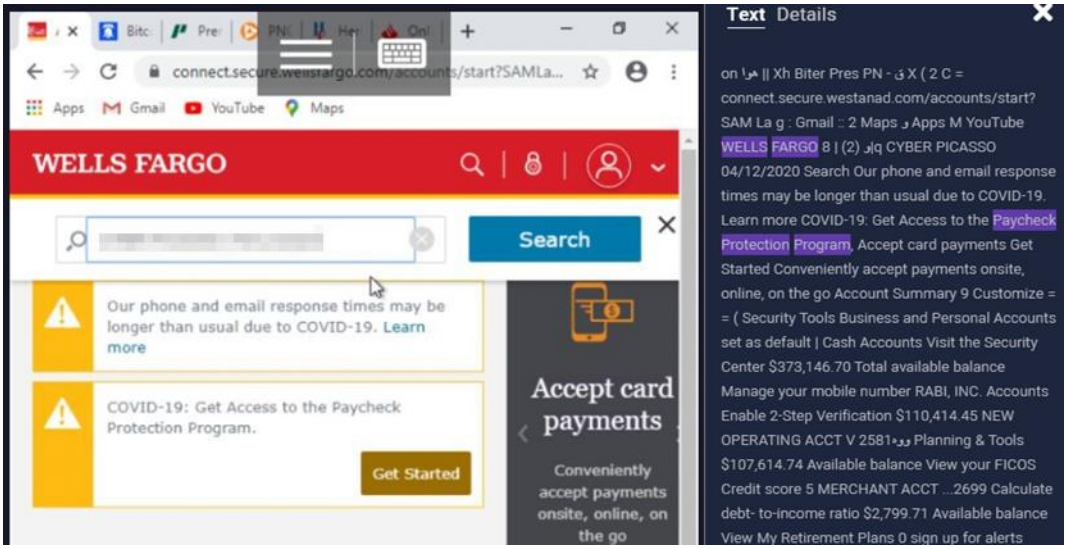


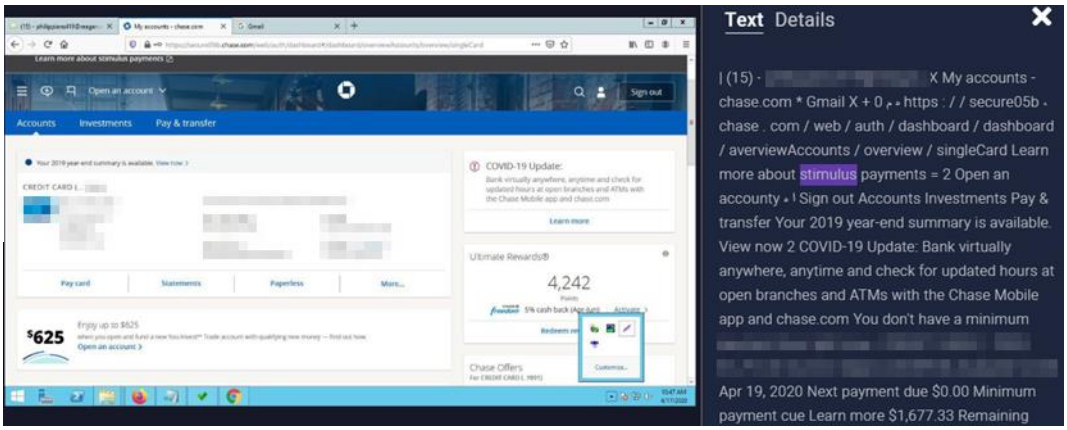
Figure 15: A compromised SunTrust account mentioning the Paycheck Protection Program

Figure 16: A compromised Wells Fargo account mentioning the Paycheck Protection Program



Similarly, we detected some personal accounts that were compromised after the stimulus payments were announced, such as the Chase account below:

Figure 17: A compromised Chase account mentioning the stimulus payment



It is unclear how these accounts were taken over. However, malware/keyloggers, password cracking, and social engineering are all likely vectors used by actors to compromise accounts of stimulus recipients.

Conclusion

Without a doubt, threat actors are seeking ways to illegally profit from the largest-ever government stimulus package. The sheer haste in which the bill was assembled and in which the money was disbursed, amidst a broader climate of fear and uncertainty, makes fraud almost inevitable. The real questions are "How?" and "To what extent?"

Threat actors generally refrain from overtly sharing details of their schemes. Even so, this report has found several examples highlighting that threat actors are indeed aware of the stimulus, and that they are looking for ways to fraudulently procure money. We also found examples of compromised computers and bank accounts, allowing purchasers to siphon stimulus money that was already disbursed.

While we could find no definitive proof of widespread fraud, we found a significant increase in April of some of the ingredients necessary to commit it—stolen identity information, which can be used to impersonate a victim.

Ultimately, the market for identity information on the dark web is established and robust. There is plenty to satiate the appetites of aspiring stimulus fraudsters. We assess, therefore, that it is natural for them to attempt using these fullz to illegally procure CARES Act money, and we recommend that individuals and organizations (that have not yet done so) increase preventative and detective measures to safeguard their accounts and identities.