Amid Boom in Phishing, Fraudsters Target Customers of Small and Mid-sized Banks

geminiadvisory.io/amid-phishing-boom-fraudsters-target-small-and-mid-sized-banks/

August 11, 2021

Key Findings

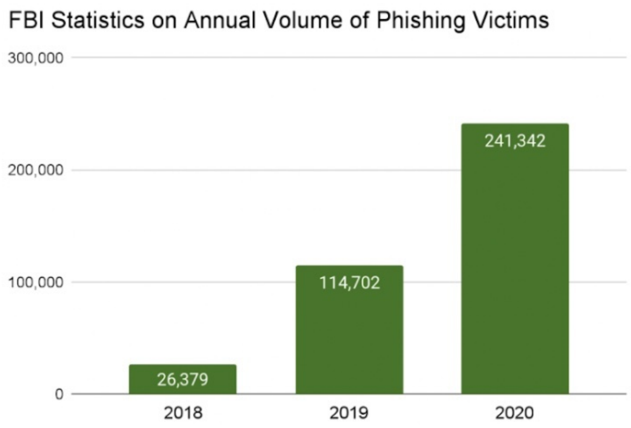
- Phishing attacks sharply increased in 2020 with the FBI reporting a 110% increase in phishing victims. Gemini Advisory identified a 72% increase in the volume of dark web forum posts referencing phishing and a 101% increase in the volume of compromised US payment cards with a high likelihood of being phished that were posted to the dark web.
- Dark web actors are increasingly advertising bank-specific phishing pages and associated services that target customers of small and mid-sized financial institutions. This marks an expansion from established methods of creating generalized phishing sites or phishing sites for major companies with large customer bases.
- Fraudsters leverage "useless" compromised payment card data and personally identifiable information (PII) and "bank leads" to harvest victims' email addresses, phone numbers, and financial institutions for the purpose of creating target lists.
- While small and mid-sized financial institutions, as well as their customers, are less accustomed to targeted phishing campaigns, the well-established best practices for protecting against phishing attacks serve as their best mitigation strategies.

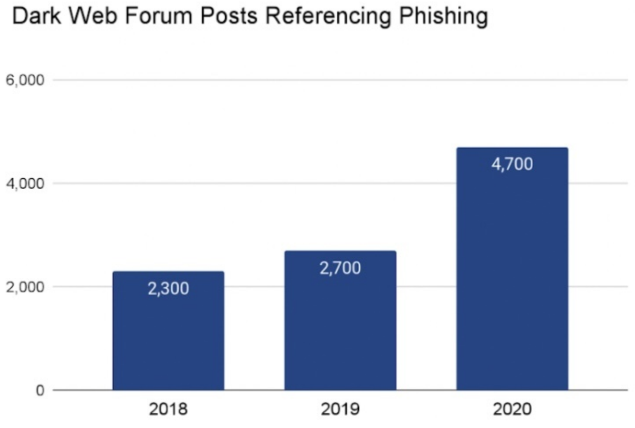
Background

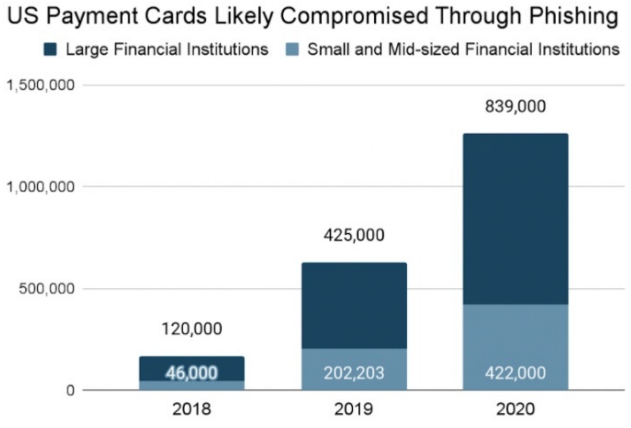
Payment card and bank account phishing—a method in which fraudsters trick victims into unwittingly providing payment card data, login credentials, or personally identifiable information (PII)—has always been a popular criminal scheme. However, many indicators show that phishing attacks rose sharply in 2020. From 2019 to 2020:

- The FBI reported a 110% increase in phishing victims
- Gemini identified a 72% increase in the volume of dark web forum posts referencing phishing
- Gemini identified a 101% increase in the volume of compromised US payment cards with a high likelihood of being phished that were posted for sale on the dark web

As Recorded Future's Insikt Group has reported, the boom in phishing in 2020 has been facilitated by the proliferation of phishing-as-a-service (PhaaS). PhaaS—which includes customized phishing pages, "outsourced" spam phishing campaigns, and other web traffic schemes—makes it easier for less technically sophisticated fraudsters to engage in phishing, thereby increasing the pool of attackers. Furthermore, COVID-19 restrictions forced many fraudsters to look for criminal profits outside of well-established methods of exposing in-person transactions, known as Card Present (CP) transactions. Phishing, made easier through PhaaS, has offered fraudsters a way to seek new sources of profits by using fake sites to compromise payment card data, PII, login credentials, and bank account information.







Historically, the most common method of phishing has been “mass” phishing. With this method, fraudsters hope to draw victims to their “bait” (a phishing page for a massive company or financial institution, or simply an enticing offer like discounted medications) by phishing in a “large pond” (sending out spam emails to “random” recipients or creating phishing ads through Google or Facebook). The idea is simple: most potential victims will not take the bait, but the pond is big enough and the bait is “generalized” enough that even a small percentage is enough to turn a profit.

For this reason, fraudsters have largely avoided using small and mid-sized financial institutions as bait in this analogy. Throw a phishing page for a small regional bank into that large pond and the already small percentage of victims becomes so small that it is not worth the time or effort for most fraudsters.

However, analysis of phished records posted to the dark web, and the chatter occurring on dark web forums, shows that the game has changed. In the past year, fraudsters have increasingly found ways to shrink the pond and make sure the fish in the pond are customers of small and mid-sized financial institutions. As a result, fraudsters are now creating phishing pages for specific small and mid-sized financial institutions, identifying their customers, and targeting them with phishing attacks. Unfortunately, both the institutions themselves and their customers may be unprepared for the rising threat, rendering them soft targets in the eyes of fraudsters.

Fraudsters Turn Their Phish Eyes to Small and Mid-sized Financial Institutions

Since January 2018, the volume of phished records posted to the dark web has steadily increased, with metrics for small and mid-sized US financial institutions dovetailing the metrics for large US financial institutions. This is expected as the majority of phishing sites are generalized and non-bank specific, suggesting a broadly proportional distribution of exposed cards per the size of each financial institution.

Importantly, the volume of phished records from small and mid-sized financial institutions increased at a higher rate—14 more percentage points—than records from large financial institutions when comparing the past 18 months to the preceding 18-month period.

Against this backdrop of rising phishing attacks, Gemini Advisory has also witnessed the steady emergence of dark web actors advertising phishing sites and services for “semi-targeted” phishing attacks against customers of small and mid-sized institutions. Correspondingly, actors are increasingly seeking and selling data that can be used to create target lists of these institutions’ customers. These semi-targeted phishing attacks use aspects of both mass phishing and spear phishing—which are personalized phishing attacks against individuals—to launch phishing campaigns that specifically target customers of small and mid-sized financial institutions.

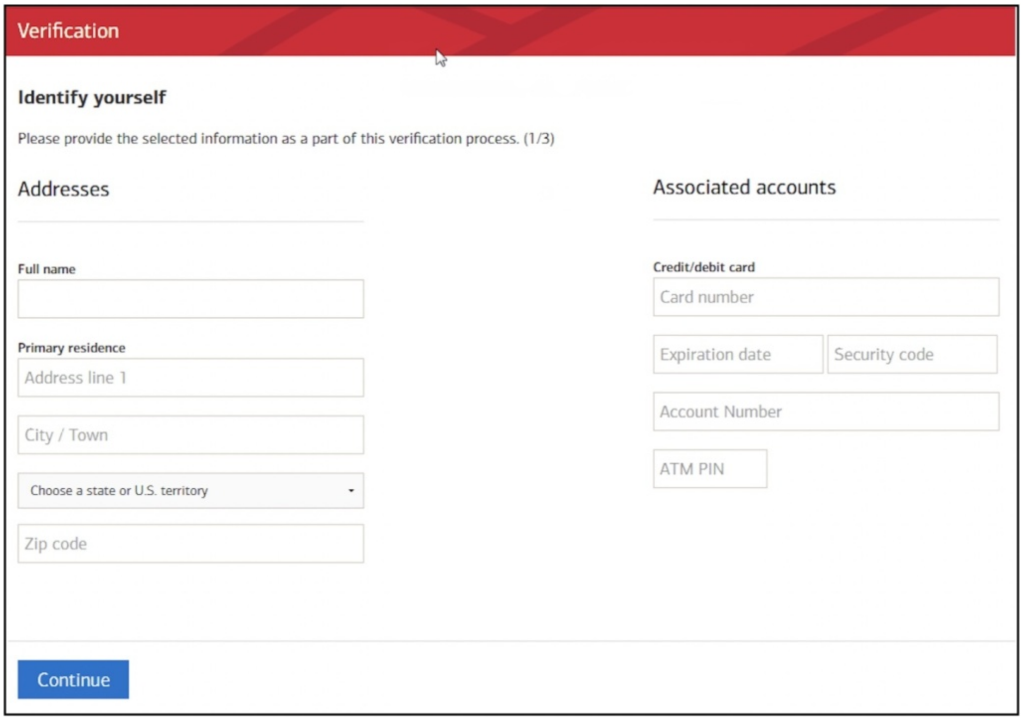
Why Small and Mid-sized Financial Institutions Make Bad Bait for Mass Phishing

In the context of bank and card fraud phishing, mass phishing relies on two methods of delivering the “bait”, which refers to the phishing page that captures victims’ data:

The large-scale distribution of generalized spam emails that contain links to a phishing page

Although mass phishing is the most common type of phishing attack, it is not cost-effective, and the life cycle of a mass phishing campaign is very short. The key aspect of mass phishing is that the bait are typically:

- Widely-used companies, such as Amazon or Netflix, for phishing payment card data and PII
- Major financial institutions with the largest customer bases for phishing online bank account login credentials, payment card data, and PII
- Attractive offers, such as investment opportunities, cryptocurrency information, or pharmacology deals
- “Scary” threats, such as urgent requests for tax information



Verification

Identify yourself

Please provide the selected information as a part of this verification process. (1/3)

Addresses

Full name

Primary residence

Address line 1

City / Town

Choose a state or U.S. territory

Zip code

Associated accounts

Credit/debit card

Card number

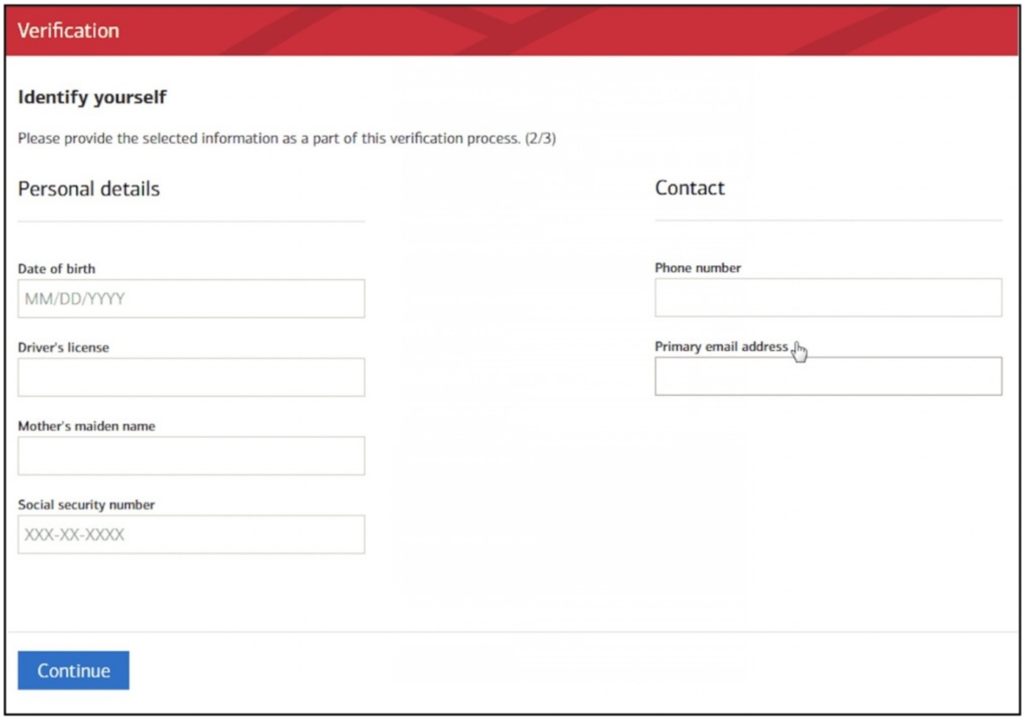
Expiration date

Security code

Account Number

ATM PIN

Continue


Verification

Identify yourself

Please provide the selected information as a part of this verification process. (2/3)

Personal details

Date of birth: MM/DD/YYYY

Driver's license

Mother's maiden name

Social security number: XXX-XX-XXXX

Contact

Phone number

Primary email address

Images 1-2: A phishing page for a large financial institution that was posted for sale by the dark web actor “iHack”. Fraudsters use ID verification pages to trick victims into providing payment card data and PII.

If the fraudsters deliver the phishing bait through spam emails, they typically purchase or freely download one of the many spam email databases on offer on dark web forums. The idea is that the mimicked company is so large, they will likely still have a high number of customers in their distribution list.

If fraudsters use Google or Facebook ads to deliver the bait, they create an ad and may select some criteria—such as region, age, or gender—to narrow the audience by choosing specific interests. Actors on dark web forums frequently advertise their services to create tailored ads designed to drive traffic to bank phishing sites, and other actors regularly create posts seeking these services.

Although using Google and Facebook ads to drive visitors to phishing sites is typically reserved for more typical mass phishing campaigns, fraudsters can leverage these ads for small and mid-sized financial institutions. For these smaller institutions, the success rates of ad-driven phishing campaigns would typically be lower than phishing emails to identified bank clients; however, fraudsters could increase their odds by phishing for a small regional bank and setting their ads to focus on individuals residing in the area of the regional bank.

Despite the fact that mass phishing is better suited to phishing at large financial institutions and companies, these larger organizations have greatly improved their capacity to detect and disrupt phishing attacks against their customers. To counter spam emails, large financial institutions and email providers have partnered to implement systems like DMARC that block phishing emails before they arrive in potential victims' inboxes. At the same time, threat intelligence companies now offer services designed to proactively identify typosquatted domains used as phishing sites.

Notably, large organizations' capacity to leverage these tools to mitigate phishing attacks is one of the major contributing factors that has driven fraudsters to devise new phishing techniques for targeting comparatively less protected small and mid-sized financial institutions.

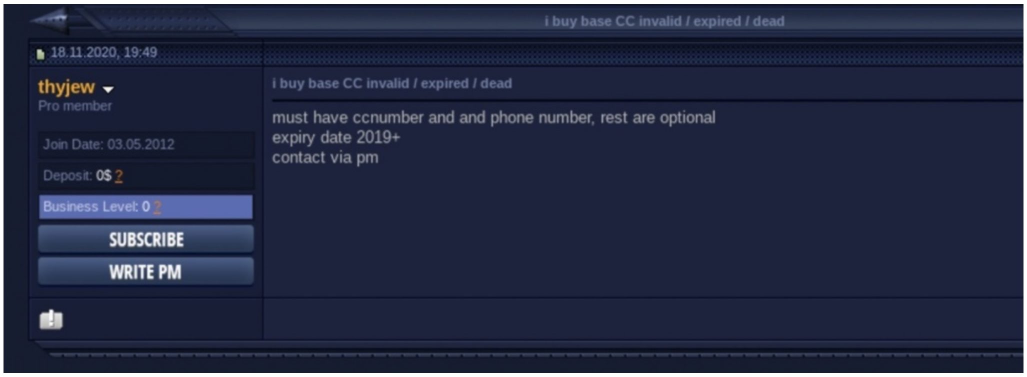
How Fraudsters Find Phishing Victims for Small and Mid-sized Financial Institutions

For fraudsters to target customers of small and mid-sized financial institutions, they need to know who the customers are. While customer databases containing email addresses are easily accessible for large companies on the dark web, they rarely exist for banks. Conversely for major banks, fraudsters are happy to roll the dice with mass phishing, safe in the knowledge that those banks' customer bases are large enough for an acceptable success rate.

To get around this issue, fraudsters have begun devising new methods of converting compromised personal data with a low price on dark web forums into target lists for small and mid-sized financial institutions. From there, they launch semi-targeted and spear phishing attacks to achieve higher rates of success from smaller, "stocked" ponds of potential victims.

Method 1: Leveraging "Useless" Compromised Data to Find Victims

One of the main methods involves leveraging compromised payment card records and bank logs that are no longer valuable to most cybercriminals for conventional fraud schemes, and then harvesting from them their victims' contact information and the financial institution. Bank logs are files that contain victims' login credentials, cookies, PII, and other information that were stolen by cybercriminals through a variety of means, including phishing, keyloggers, or various malware.



i buy base CC invalid / expired / dead

18.11.2020, 19:49

thyjew
Pro member

Join Date: 03.05.2012

Deposit: 0$?

Business Level: 0 ?

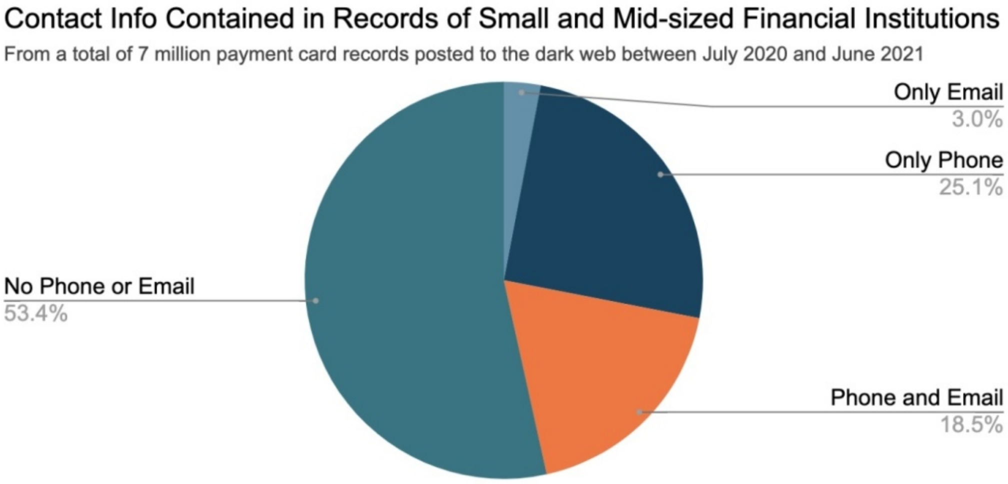
i buy base CC invalid / expired / dead

must have ccnumber and and phone number, rest are optional
expiry date 2019+
contact via pm

Image 3: On November 18, 2020, the actor “thyjew” on a top-tier dark web forum sought to purchase invalid, expired, or “dead” compromised payment card records that contained the victim’s phone number. The actor could leverage this information for phone call spear phishing or SMS-based semi-targeted phishing.

These records and bank logs are most valuable when they can be monetized through fraudulent transactions, account takeovers, or other cashout schemes. But once a payment card expires, or a bank reissues a card due to fraudulent activity, or a bank re-secures a compromised online bank account, the records and bank logs lose almost all their value and become “useless”. As a result, these records and bank logs sell for pennies on the dark web and allow fraudsters to cheaply acquire and clean the data they need.

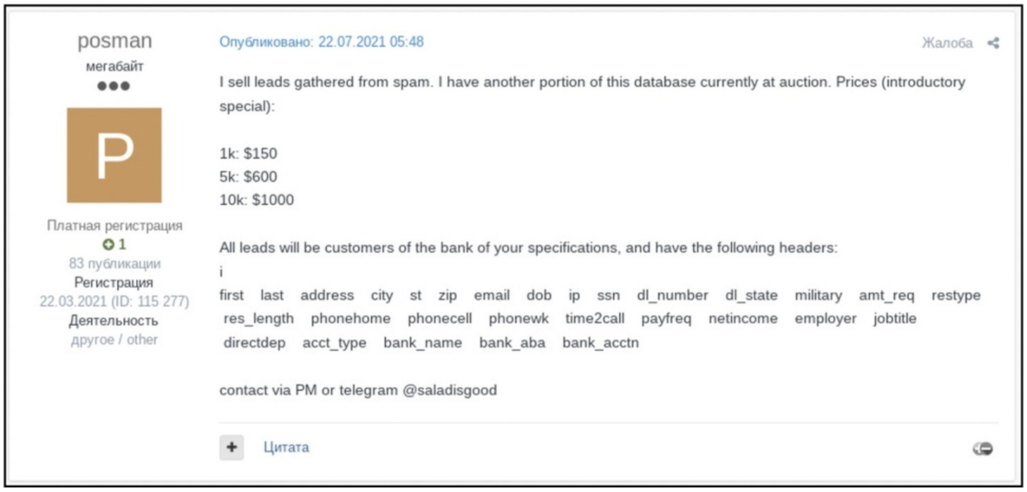
Whereas bank logs always contain information about the victim’s financial institution and overwhelmingly contain the victim’s email address or phone number, compromised payment card records typically contain contact info if the breached source collected that info during checkout. In the past year, 47% of the 7 million US payment card records from small and mid-sized financial institutions that were compromised during online transactions contained either the victim’s email address or phone number.



Compromised payment card records do not contain overtly explicit information about the victim’s financial institution, but fraudsters can use widely available “BIN checkers” or “BIN lists” to determine the financial institution of compromised payment card records. BIN checkers allow fraudsters to input the first 6 to 8 digits of the compromised card and receive the name of the financial institution that issued the card. BIN lists, which are lists of BINs and their corresponding financial institution, are frequently freely posted on dark web forums.

Method 2: Pivoting Off “Bank Leads”

The second method involves purchasing so-called “bank leads” from other cybercriminals. Typically, these cybercriminals acquired a victim’s contact information, their financial institution, and other associated PII, but did not acquire the more lucrative payment card data, account information, or login credentials. As a result, these bank leads are priced significantly cheaper than those with payment card data, account information, or login credentials. Bank leads typically come from mass phishing campaigns or the compromised databases of payment processors and marketing companies.



posman
мегабайт

Платная регистрация
1
83 публикации
Регистрация
22.03.2021 (ID: 115 277)
Деятельность
другое / other

Опубликовано: 22.07.2021 05:48

Жалоба

I sell leads gathered from spam. I have another portion of this database currently at auction. Prices (introductory special):

1k: $150
5k: $600
10k: $1000

All leads will be customers of the bank of your specifications, and have the following headers:
i
first last address city st zip email dob ip ssn dl_number dl_state military amt_req restype res_length phonehome phonecell phonewk time2call payfreq netincome employer jobtitle directdep acct_type bank_name bank_aba bank_acctn

contact via PM or telegram @saladisgood

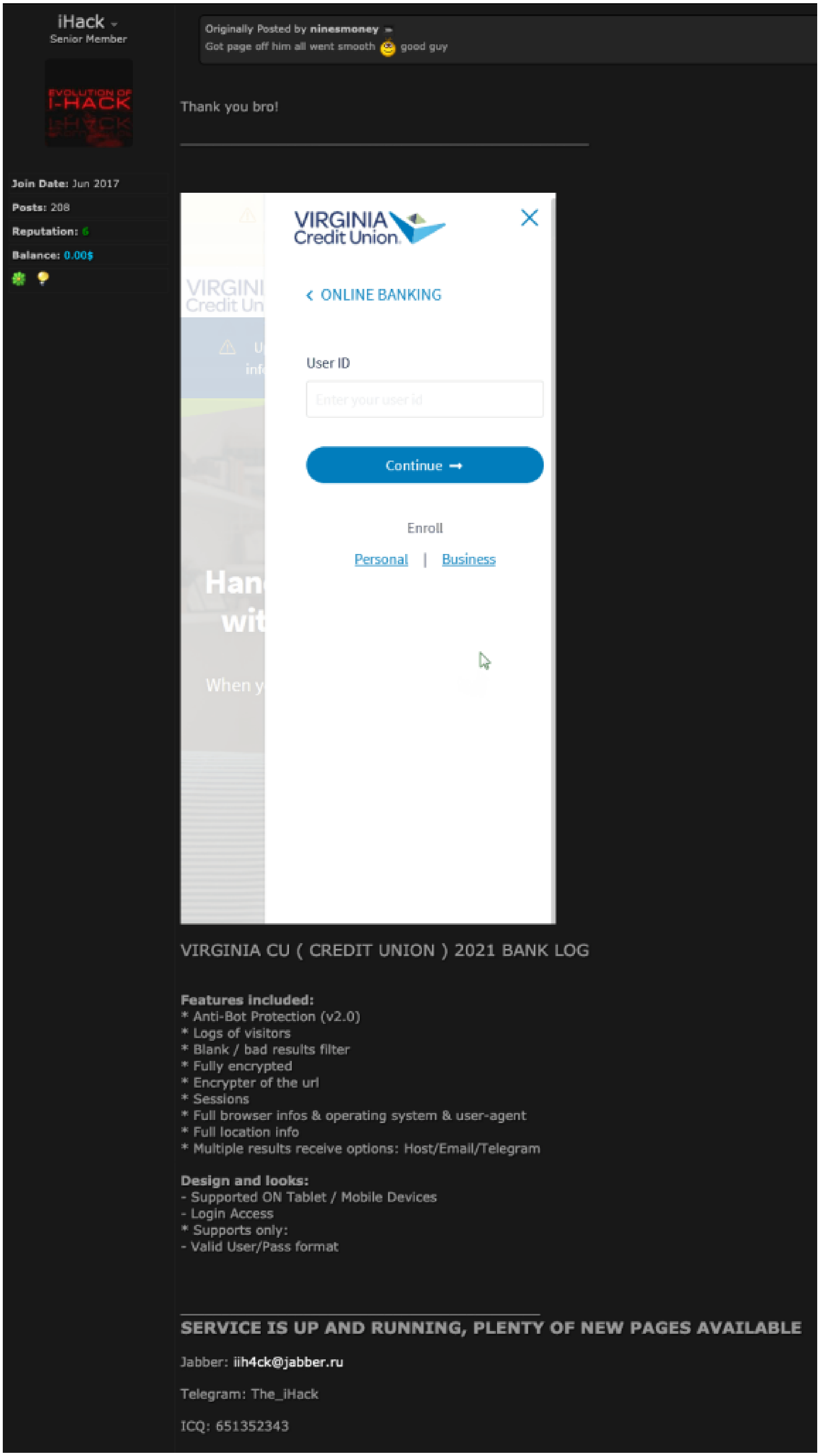
Image 4: On July 22, 2021, the actor “posman” on a top-tier dark web forum offered to sell bank leads that fraudsters could use for phishing campaigns targeting small and mid-sized financial institutions.

Semi-Targeted Phishing for Small and Mid-sized Financial Institutions

Once a fraudster has their list of victims for a small or mid-sized financial institution, they can attempt to lure them in through methods similar to mass phishing. With these methods, they create a fake phishing page for the bank that they are targeting. They then distribute phishing emails if they have collected customers’ email addresses or distribute phishing text messages if they collected phone numbers.

Importantly, although email providers have improved their spam filtering systems and end users have become more savvy to phishing threats, the rise of criminal software like Email Appender has given fraudsters new avenues to bypass these protections and increase their chances of success.

Additionally, while many fraudsters may not have the technical expertise to create viable, convincing phishing pages, threat actors on dark web forums regularly advertise their services to create customized phishing pages for any financial institution. These actors typically include examples of their fake sites, which may include large entities but frequently also include small and mid-sized financial institutions.



iHack
Senior Member

Join Date: Jun 2017

Posts: 208

Reputation: 6

Balance: 0.00$

> Originally Posted by **ninesmoney**
> Got page off him all went smooth 😎 good guy

Thank you bro!

VIRGINIA CU (CREDIT UNION) 2021 BANK LOG

Features Included:
* Anti-Bot Protection (v2.0)
* Logs of visitors
* Blank / bad results filter
* Fully encrypted
* Encrypter of the url
* Sessions
* Full browser infos & operating system & user-agent
* Full location info
* Multiple results receive options: Host/Email/Telegram

Design and looks:
- Supported ON Tablet / Mobile Devices
- Login Access
* Supports only:
- Valid User/Pass format

SERVICE IS UP AND RUNNING, PLENTY OF NEW PAGES AVAILABLE

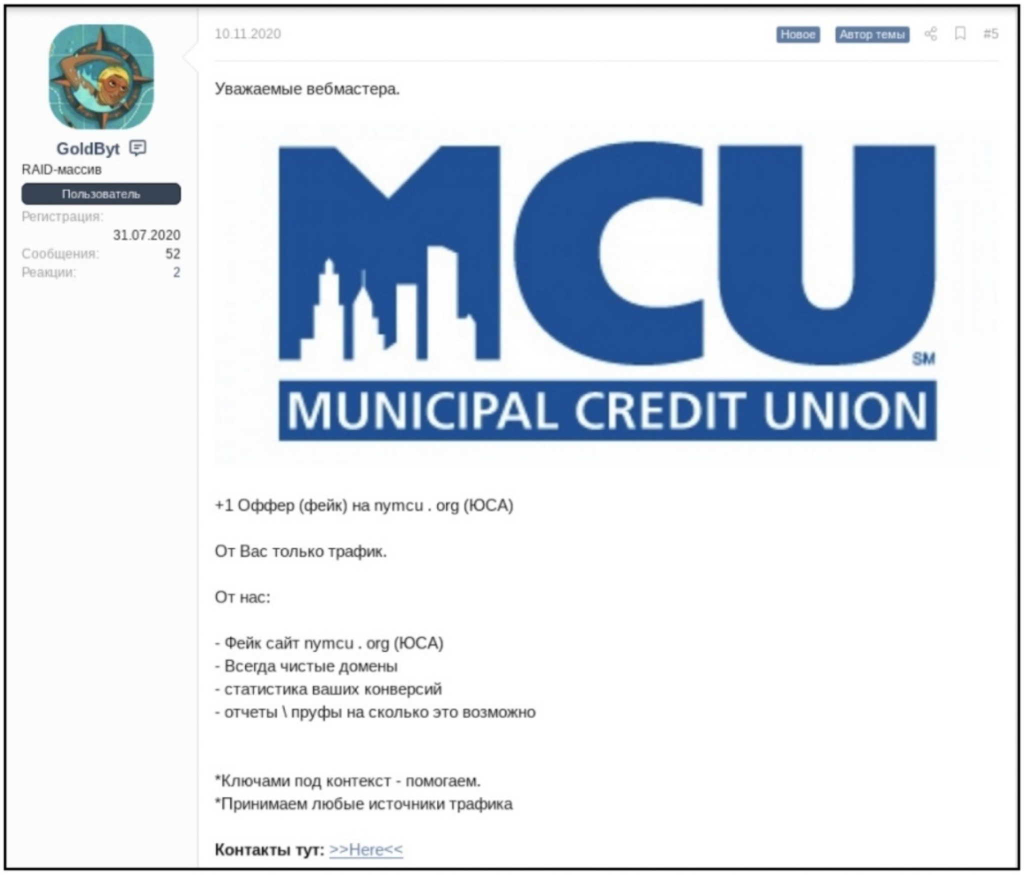
Jabber: iih4ck@jabber.ru

Telegram: The_iHack

ICQ: 651352343

Image 5: The actor “ninesmoney” thanks “iHack” for creating a customized phishing page of Virginia Credit Union for them. iHack regularly advertises their services creating phishing pages on a mid-tier dark web forum.

Furthermore, actors on dark web forums also advertise services to drive web traffic to phishing sites through either phishing emails or online ads. In practice, the combination of services for creating customized phishing pages and driving web traffic to the sites enables fraudsters with comparatively limited technical expertise or time to service out key functions.



GoldByt
RAID-массив
Регистрация: 31.07.2020
Сообщения: 52
Реакции: 2

10.11.2020

Уважаемые вебмастера.

+1 Оффер (фейк) на nymcu . org (ЮСА)

От Вас только трафик.

От нас:

- Фейк сайт nymcu . org (ЮСА)
- Всегда чистые домены
- статистика ваших конверсий
- отчеты \ пруфы на сколько это возможно

*Ключами под контекст - помогаем.
*Принимаем любые источники трафика

Контакты тут: >>Here<<

Image 6: The actor “GoldByt” on a mid-tier Russian language dark web forum seeks partners that can direct internet traffic to their phishing site for Municipal Credit Union.

Spear Phishing at Small and Mid-sized Financial Institutions

Alternatively, once the fraudster has their list of victims, they can attempt to lure in their victim with spear phishing techniques. Spear phishing refers to attacks targeting a single individual, or in some cases a small company, in which the attacker uses personal information to deceive the victim into believing the attacker is a trustworthy interlocutor. Spear phishing is typically conducted through phone calls or personalized emails and requires the fraudster to customize each attack to each victim. As a result, the fraudster must devote more time and resources to each attack.

As noted above, the data about victims that fraudsters collect must include either email addresses or phone numbers to be useful. If the data includes phone numbers, the fraudster could spoof their calling number in order to impersonate a victim's bank and then call the victim. The fraudster would attempt to manipulate the victim into divulging sensitive information over the phone by asking "typical" ID verification questions, such as date of birth and address, and then sneak in other questions, like Social Security number or login information. Alternatively, the fraudster could convince the victim to navigate to a phishing page—likely distributed by text message or email during the conversation—whereupon the victim would then input sensitive information.

Mitigation

While the techniques that fraudsters use to collect target lists for small and mid-sized financial institutions differ from those used for large banks and prominent companies, the best practices for mitigating the dangers are largely the same.

The key difference is that the historical lack of cybercriminal focus on creating phishing pages for small and mid-sized financial institutions may have led some of these financial institutions to underestimate the current threat that they face. As a result, there is now greater pressure on these financial institutions to ensure they have processes in place to monitor for phishing attacks mimicking their institution and that their customers are properly informed of the dangers.

For individuals with an account at a small or mid-sized financial institution, the best way to protect yourself is to take an extra second to make sure the person you're speaking with, or the site you're visiting, is truly who you believe them to be.

If you receive a call from a person claiming to be a bank representative:

> Ask them to provide you with an extension that can be used with a phone number listed on their website. If you are not provided with a phone number matching the bank's official listed numbers, call one of the bank's official numbers and inform them.

If you receive an email claiming to be from your bank:

- It is best to avoid clicking any links in the email. Instead, log in to your bank account directly from a browser to review any possible alerts. Alternatively, call your bank at a number listed on their website.
- Verify where the link will send you by hovering over it. If it shows a domain that does not exactly match the domain of your financial institution, do not click it.
- Double-check the sender's email address to verify that it is truly coming from a bank-affiliated email address. Search the sender's email address on a search engine to see if that email address has been previously reported as fraudulent. Alternatively, verify that the display name for the email's sender field has not been spoofed.

- Always practice extra caution if a bank requires you to provide extensive payment card data and PII to “verify” your identity when logging in. For non-bank sites, always confirm that the amount of PII you are providing matches the product or service you are purchasing.

Conclusion

The development of novel techniques to target customers of small and mid-sized financial institutions with phishing attacks has been facilitated by the emergence of various cybercriminal phishing services. Due to the ease with which fraudsters can order a custom-made phishing page and pay other actors to direct traffic to their site, the only barrier preventing fraudsters from ramping up the targeting of small and mid-sized financial institutions is the availability of victim data that contains their financial institution and an email address or phone number.

As more fraudsters find ways to extract victims’ information and begin to see the value in selling this data, the result will likely be a further rise in phishing attacks against customers of small and mid-sized financial institutions. As these types of attacks rely on deceiving the victim as opposed to lax security, the best strategy for individuals is to follow the well-established security practices for phishing. For small and mid-sized financial institutions themselves, the best strategy is to ensure they have processes in place to monitor for phishing attacks targeting their clients and to keep clients well-informed of the dangers.

Gemini Advisory Mission Statement

Gemini Advisory provides actionable fraud intelligence to the largest financial organizations in an effort to mitigate ever-growing cyber risks. Our proprietary software utilizes asymmetrical solutions in order to help identify and isolate assets targeted by fraudsters and online criminals in real-time.