United States District Court

for the
Western District of New York

United States of America

v. **Case No. 24-mj-1187**

Abdellah Belmili, a/k/a Dila Belmili, a/k/a SPOX

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief:

Between in or about March 2020 and in or about January 2023, the exact dates being unknown, in the Western District of New York, and elsewhere, the defendant, Abdellah Belmili, a/k/a Dila Belmili, a/k/a SPOX, did knowingly and willfully combine, conspire, and agree together and with others, known and unknown, to knowingly execute a scheme and artifice to defraud financial institutions and to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, financial institutions, by means of materially false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Section 1349.

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

JORDAN F. SLAVIK
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Affidavit submitted electronically by email in .pdf format.
Oath administered, and contents and signature attested
to me telephonically pursuant to me telephonically pursuant
to Federal Rule of Criminal Procedure 4.1
on: October __7__, 2024

HON. JEREMIAH J. McCARTHY
UNITED STATES MAGISTRATE JUDGE

City and State: Buffalo, New York

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, Jordan F. Slavik being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. Abdellah Belmili (hereinafter BELMILI), also known as "Dila Belmili" and by the online moniker "SPOX," is an Algerian national located outside the United States, including in Algeria, Ukraine, and various countries in Europe.

2. From at least in or about March 2020 through the present, BELMILI created, managed, and supported the operation of a number of nefarious online marketplaces, including www.market0day.com, www.spoxy.us, and the Telegram market "SpoxCoder Official Channel."[1] These marketplaces are dedicated to selling stolen access devices, such as bank account, credit card, and debit card information, as well as other tools for carrying out cybercrime and fraud. Since their inception, these marketplaces are believed to have generated at least $800,000 in profits and impacted at least 1600 victims in the United States and internationally.

3. As detailed below, I make this affidavit in support of a criminal complaint and arrest warrant charging BELMILI with a violation of Title 18, United States Code, Section 1349 (Conspiracy to Commit Bank Fraud).

---

[1] Telegram is an encrypted messaging platform.

AGENT BACKGROUND

4. I am a Special Agent with the Federal Bureau of Investigation and have been so employed since September 2019. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York, where I work on investigations relating to criminal and national security cyber intrusions. These investigations specifically focus on unlawful computer access, nefarious online marketplaces, phishing activity, and online sexual extortions. I have gained experience through training through numerous FBI, government, and private sector trainings and certifications such as: multiple certificates through the FBI's Advanced Cyber Training Program and cryptocurrency training curriculum; the Department of Homeland Security's Cybersecurity for Industrial Control Systems certificate; certificates from SANS on Cyber Security essentials, Hacking Tools, and Open Source Cyber Investigations; and certificates from Mandiant on the Cybersecurity Intelligence Cycle, as well as through everyday work related to these types of investigations. Through my work in cyber-related investigations, I am familiar with the fundamental operations of the internet, hardware, and software, and the communication protocols across each. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against the United States.

5. The facts of this affidavit come from my personal observations, my training and experience, my review of physical and documentary evidence, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about

this matter. The facts contained in this affidavit are based upon my personal involvement in this investigation and information provided to me by other law enforcement agents and private companies.

PROBABLE CAUSE

Background on the Market0Day Marketplace

6. In September 2020, FBI Buffalo became aware of the existence of the nefarious online marketplace www.market0day.com through reliable source reporting (CHS-1).[2] The administrator of the website was an unknown individual who utilized the moniker "SPOX." SPOX is a cyber actor who is known for creating "phishing kits" that have been used to compromise major U.S. financial institutions.[3] Between September and November 2020, SPOX advertised the marketplace and facilitated some of the customer support for the

[2] CHS-1 has been operating as an FBI source since early 2020 and has provided information to the FBI on a number of cyber threat actors, online nefarious marketplaces, and phishing kit developers. CHS-1 does not have a criminal history and I am not aware of any pending criminal matters involving CHS-1. CHS is private-security computer security expert. CHS-1 is being paid for their activity with the government. I assess these payments, along with a desire to protect the public from nefarious cyber-actors, serve as CHS-1's motivation for providing information to the government. The FBI believes CHS-1 to be both reliable and credible.

[3] "Phishing" refers to the practice of sending fraudulent emails or text messages that purport to be from legitimate companies in order to induce a person to reveal personal information, such as their password or credit card number. A "phishing kit" is a package of software—such as source code, images, and computer scripts—that allows a cybercriminal to launch a phishing attack. The kit allows the cybercriminal to generate a login page that looks identical to the legitimate company's login page but sends the stolen credentials directly to the cybercriminal.

marketplace on his personal Telegram channel @SpoxCoder. SPOX's Telegram listed the email spoxcoder@gmail.com as an additional way to contact him.

7. Part of the www.market0day.com website's organizational structure also included a directory folder named "Spox Files." The main product sold on the www.market0day.com marketplace was phishing kits that SPOX had created. Based on my training and experience, it is sometimes possible to identify the creator of a given phishing kit, as the creator places his name or moniker inside the code, to take credit for the code. In this case, Spox' phishing kit signatures typically included "Spox," the kit version, date, Spox' Telegram handle, and a short message encouraging users to go to *www.market0day.com* to purchase similar phishing kits. Based upon these factors, there is probable cause to believe that SPOX was the creator and administrator of *www.market0day.com*.

8. Based on my training and experience investigating cyber-crimes, specifically nefarious online marketplaces, cyber actors typically open marketplaces on the internet to facilitate the anonymous selling and purchasing of illicit goods and services. These websites operate similarly to Amazon or eBay, where vendors can sell goods and services to customers and conduct the transactions online. Unlike such legitimate websites, however, these websites are dedicated to the sale of illegally acquired online banking information, stolen credit card information, victim computer login information, malware tools, and other nefarious goods and services. The illegal nature of the goods and services for sale through these websites is readily apparent to any user visiting the sites as the marketplaces are openly advertised as such.

9. A means by which the *www.market0day.com* marketplace protects the anonymity of its users is by requiring that all transactions to be paid for through the use of "bitcoins." Bitcoin is a decentralized, peer-to-peer form of electronic currency that has no association with banks or governments. In order to acquire bitcoins initially, a user typically must purchase them from a bitcoin "exchanger." Bitcoin exchangers accept payments of currency in some conventional form and exchange the money for a corresponding amount of bitcoins based on a fluctuating exchange rate. Similarly, exchangers will exchange bitcoins for conventional currency. Once a user acquires bitcoins from an exchanger, the bitcoins are kept in a sometimes-anonymous "wallet" controlled by the user, designated by a seemingly random string of case-sensitive letters and numbers. The user can then use the bitcoins to conduct anonymous financial transactions by transferring bitcoins from his or her wallet to the wallet of another Bitcoin user. All bitcoin transactions are recorded on a public ledger known as the "Blockchain." This ledger only reflects the movement of funds between anonymous wallets and therefore cannot by itself be used to determine the identities of the persons involved in the transactions.

10. Open source research indicated that the www.market0day.com website was registered using GoDaddy. Based upon a review of records from GoDaddy provided in May 2024, FBI Buffalo identified that the www.market0day.com website had been registered in May 2019 with the name whose initials are "A.S."; a Cairo, Egypt address; and an Egyptian phone number. In May 2020, the website was renewed, this time using the name "Abdellah

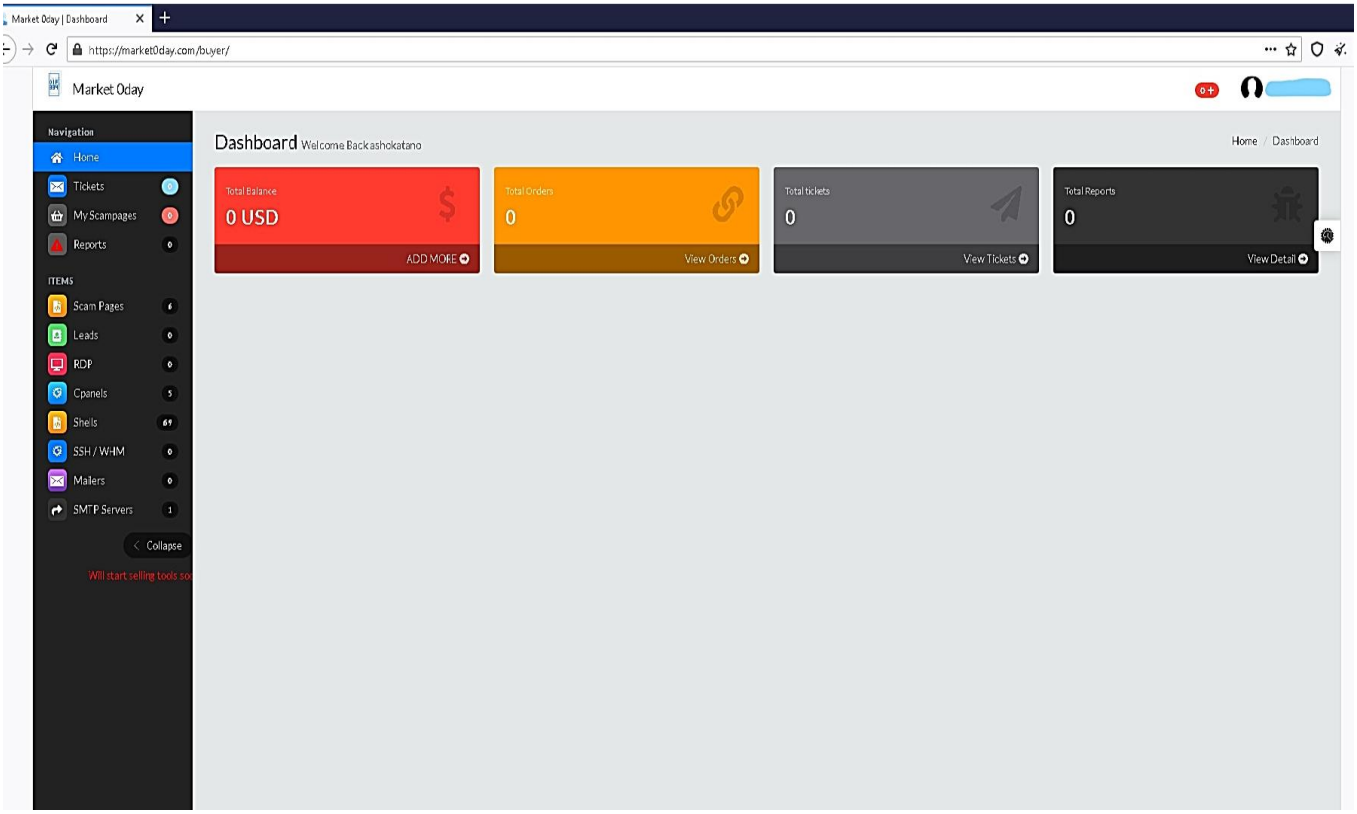
Belmili"; a Rue Bounit Ali, Mila, Algeria address; a +213667459490 phone number (BELMILI PHONE); and the spoxcoder@gmail.com email address.

Undercover Operation within the Western District of New York

11. In or around December 2020, FBI Buffalo initiated an undercover operation with the objective of targeting the *www.market0day.com* marketplace and the administrators of the marketplace. From a TOR browsing session and a covert computer, an FBI Undercover Employee ("UCE-1") who was physically located in the Western District of New York created a user account on market0day.[4]

12. On or about December 27, 2020, UCE-1 created a new user account for market0day and conducted a review of the products and services for sale on the marketplace. A screenshot of the homepage of market0day.com is shown below:

[4] "TOR" or the "TOR Network," also known as the "Onion Router," is a network of computers designed to facilitate anonymous browsing of the internet.



13. The review identified numerous items for sale, including phishing kits, Cpanels,[5] Shells,[6] and SMTP Mailers.[7] All of the items for sale appeared to cater to illegal activities. The marketplace also contained a customer portal in which he/she could access and download purchased phishing kits and other products. Before purchases could be made,

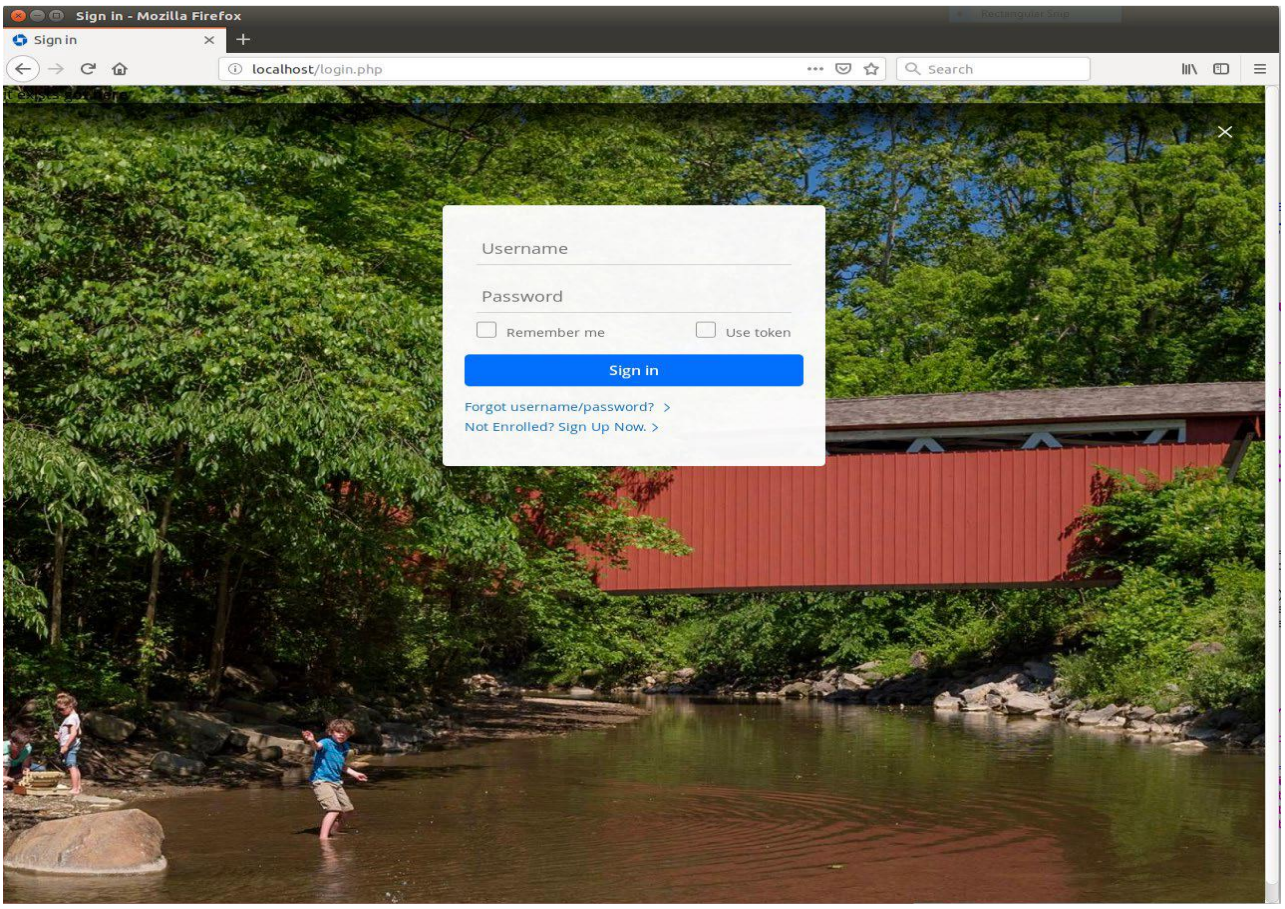
[5] Cpanel allows website owners to manage and publish on their websites. Compromised cpanel access would allow the purchaser to access and alter the compromised website.

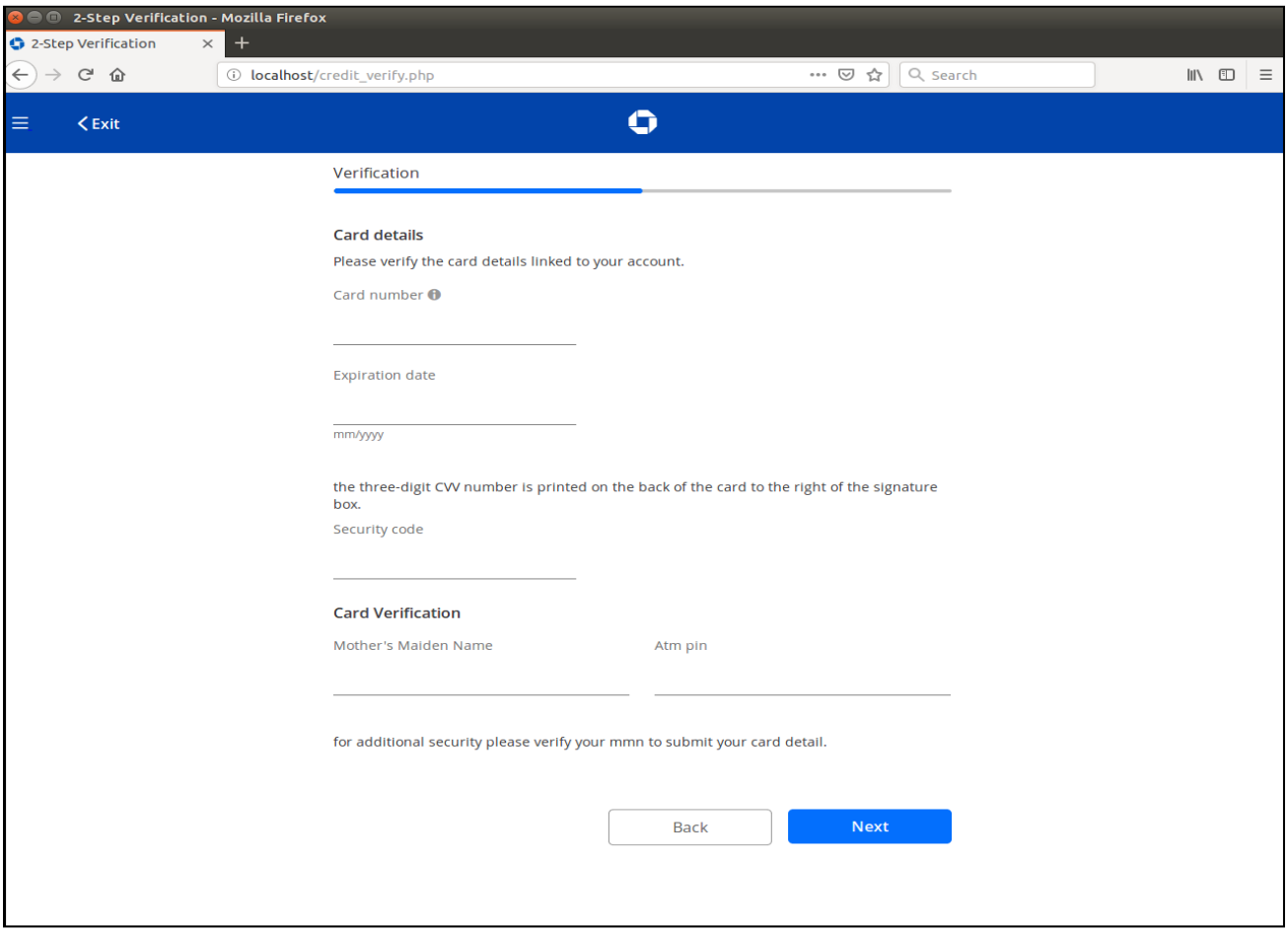
[6] Shell entries contain an IP Address and a URL, indicating a compromised machine on which the purchaser could execute commands.

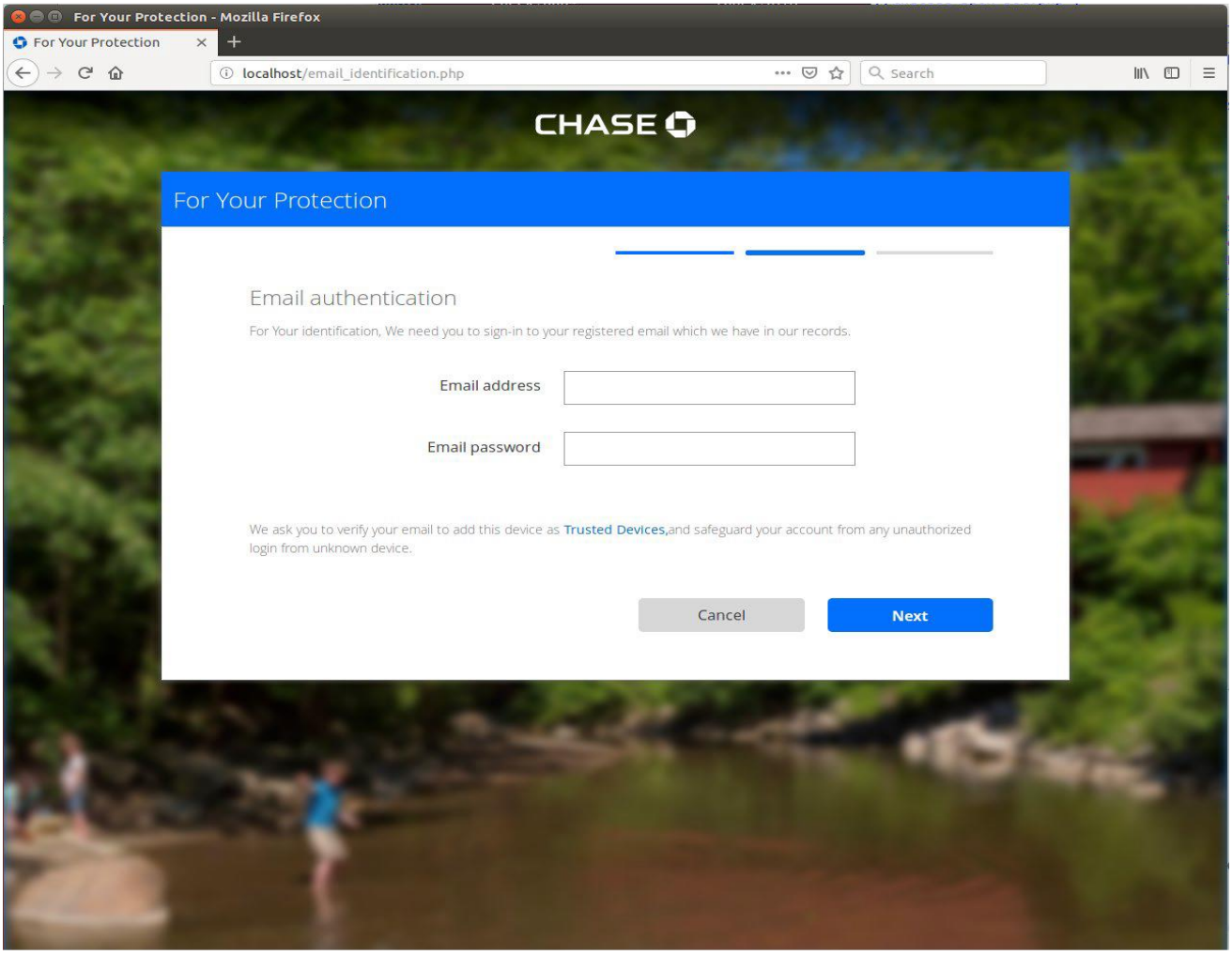
[7] Simple Mail Transfer Protocol (SMTP): sales typically include a mail server's IP Address, username (email), and password. This allows the purchaser to access the user's email messages.

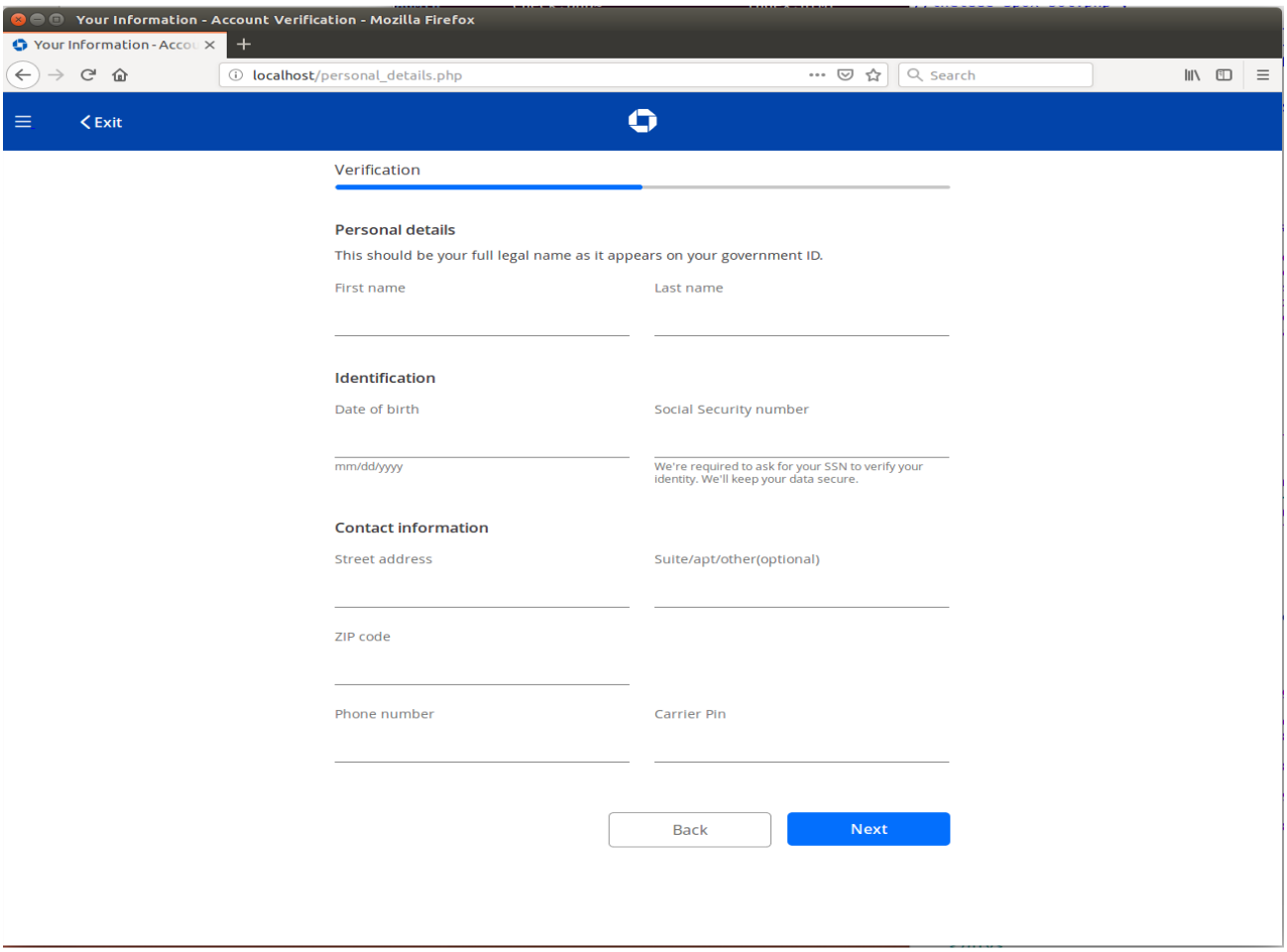
bitcoin had to be loaded onto a market0day wallet which could then be used for purchases on the marketplace. There was also a section of the website in which users could submit a support ticket to the marketplace administrator.

14. On or about December 27, 2020, UCE-1 purchased a JP Morgan Chase phishing kit from the market0day marketplace. Upon completing the purchase, the phishing kit became available to be downloaded and used by UCE-1. FBI Buffalo confirmed that the downloaded file contained a phishing kit. The phishing kit was not used or sent to anyone outside of the FBI. The FBI accessed the phishing kit in a controlled digital environment. The screenshots below show what a person would have seen if they received, for example, a phishing email that used the phishing kit. As seen in these photos, the phishing kit is designed to replicate a JP Morgan Chase website, such that victims would believe that they could enter their personal identifying information.


Sign in - Mozilla Firefox
Sign in
localhost/login.php
Search
Username
Password
Remember me
Use token
Sign in
Forgot username/password? >
Not Enrolled? Sign Up Now. >


2-Step Verification - Mozilla Firefox
2-Step Verification
localhost/credit_verify.php
Search
Exit
Verification
Card details
Please verify the card details linked to your account.
Card number
Expiration date
mm/yyyy
the three-digit CVV number is printed on the back of the card to the right of the signature box.
Security code
Card Verification
Mother's Maiden Name
Atm pin
for additional security please verify your mmn to submit your card detail.
Back
Next


For Your Protection - Mozilla Firefox
For Your Protection
localhost/email_identification.php
Search
CHASE
For Your Protection
Email authentication
For Your identification, We need you to sign-in to your registered email which we have in our records.
Email address
Email password
We ask you to verify your email to add this device as Trusted Devices,and safeguard your account from any unauthorized login from unknown device.
Cancel
Next



15. On or about December 29, 2020, UCE-1 purchased a OVH SAS Cpanel from the market0day marketplace. Despite completing the purchase, the cpanel was never sent to UCE-1. UCE-1 submitted a support ticket on market0day to inquire why he/she had not received the cpanel upon purchase but received no response.

16. On or about December 31, 2020, UCE-1 purchased an Indonesian SMTP from the market0day marketplace. Upon completing the purchase, the SMTP became available to

be downloaded and used by UCE-1. FBI Buffalo confirmed that the downloaded file contained SMTP credentials. The SMTP was not used or sent to anyone outside of the FBI.

Spoxy.us Marketplace

17. During December 2020, several individuals posted onto SPOX's Telegram channel @spoxcoder to complain that they had not received their purchases on market0day. In response to these complaints, SPOX replied that he was no longer administrating the market0day marketplace. Instead, on December 31, 2020, SPOX announced on his Telegram that he had opened up a new marketplace – *www.spoxy.us*. SPOX advertised this new marketplace as a "new store for bulk sms." Based upon my training and experience, in a cybercriminal context, "bulk sms" typically refers to the act of sending text messages to a large number of different recipients for the purpose of sending phishing or other fraudulent messages via text message.

18. In addition to advertising the new marketplace on his Telegram page, SPOX posted a message onto the www.market0day.com sign in page to encourage marketplace customers to come visit his new marketplace. SPOX also sent an email to every customer who had registered an account with market0day.com, again telling them to come visit the new spoxy.us marketplace. UCE-1 received this email. SPOX sent this email from an iCloud account spoxy.us@icloud.com and also listed the email spoxcoder@gmail.com.

19. On or about January 5, 2021, your affiant visited the www.spoxy.us marketplace. The structure and content of the marketplace was very similar to the

www.market0day.com marketplace. Specifically, the www.spoxy.us marketplace utilized the same website template, color scheme, fonts, and navigation panes as the www.market0day.com website.

20. Open source research indicated that the www.spoxy.us website was registered using GoDaddy. Based upon a review of records from GoDaddy provided in May 2024, FBI Buffalo identified that the www.spoxy.us website had been registered on November 20, 2020, using a name with the initials J.P.; a Texas phone number; an address in Bonham, Texas; the spoxcoder@gmail.com email; and a business name of "Spoxy inc." The FBI confirmed through record checks that the name and information used to purchase the spoxy.us website correspond with a 77-year-old victim residing in Texas at the given address.

Identification of Abdellah Belmili

21. In or around January 25, 2021, CHS-1 provided FBI Buffalo with copies of an additional 27 different phishing kits developed by SPOX during the previous year to target multiple U.S. companies. FBI Buffalo examined the coded files within these phishing kits to verify that the code had been created by SPOX. In approximately 25 of these phishing kits, the code included the name "Dila Belmili" in the signature, along with the "Spox" moniker. The appearance of BELMILI's name in these kit signatures only appeared in the earliest versions of the SPOX phishing kits, suggesting that BELMILI later removed his name for anonymity and instead just put "Spox" into the signature. Some of the phishing kits likewise

listed a contact Facebook profile page: www.facebook.com/hackeeeed. For example, screenshots of the code from one of BELMILI's Wells Fargo phishing kits are below:

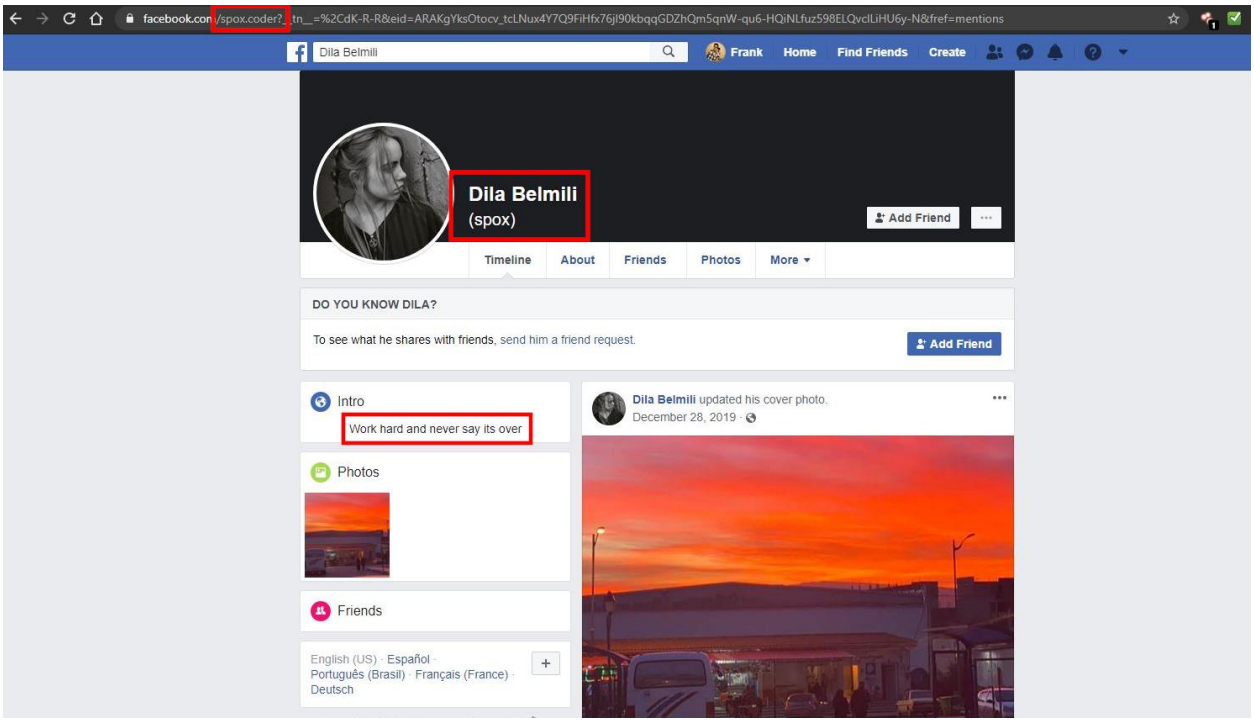
```
if ($fraud_score >= "".$max_fraud_score."") {
    exit(header("Location: https://utilify.me/hide-referrer/http://www.cpanel.com"));
}

if ($success == "false") {
    echo "<br><br><br><h3><center><h3 style='color:red'>YOUR API PROTECTION IS DEAD</h3> Please Contact Owner < Dila Belmili >
    }

if($isPhone || $isMobile) {

   $_SESSION['WELLS_SPOX'] = $WELLS_SESSION_SPOX;
   exit(header("Location: loginmobile?wells_id=".$key."&country=".$_SESSION['country']."&iso=".$_SESSION['countrycode'].""));
```

php.phishing.spox.wellsfargo - Notepad

File Edit Format View Help

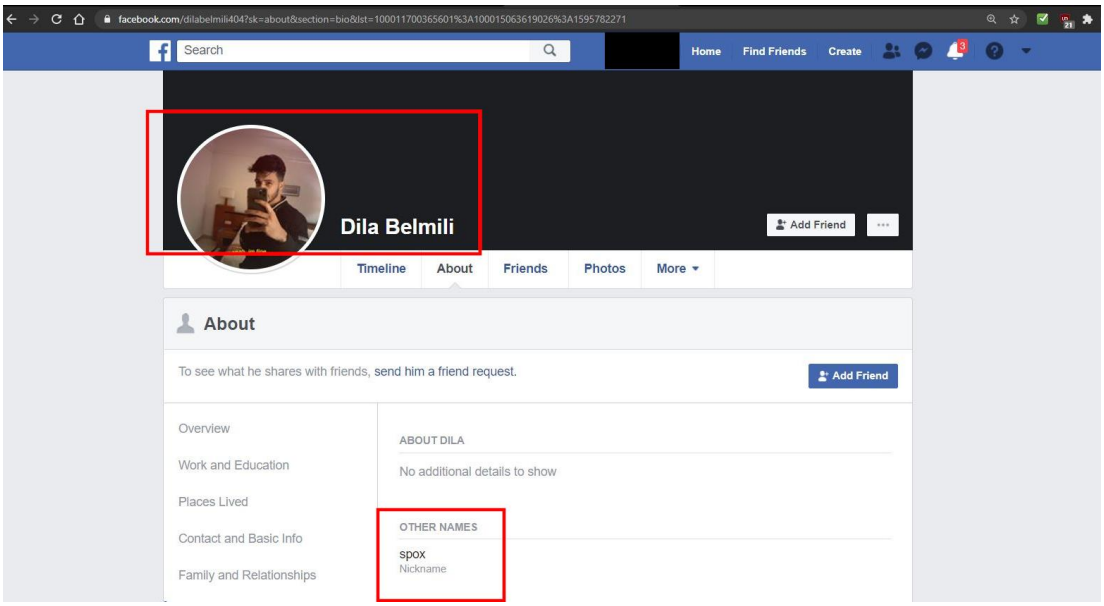
```
<?php
session_start();

/**
 * DO NOT SELL THIS SCRIPT !
 * DO NOT CHANGE COPYRIGHT !
 * Wells -
 * version 1.0
 * Https://facebook.com/hackeeeed.html
 * icq+teleg = @spoxcoder
 |
################################################
#$            C0d3d by Spox_dz               $#
#$   Recording doesn't  make you a Coder     $#
#$          Copyright 2019 Wells             $#
################################################

**/

include'Spox/config.php';
include'Spox/Anti/IP-BlackList.php';
include'Spox/Anti/Bot-Crawler.php';
include'Spox/Anti/Bot-Spox.php';
include'Spox/Functions/Fuck-you.php';
include'Spox/Anti/Dila_DZ.php';
@require "Spox/Anti/Crawler/src/CrawlerDetect.php";
```

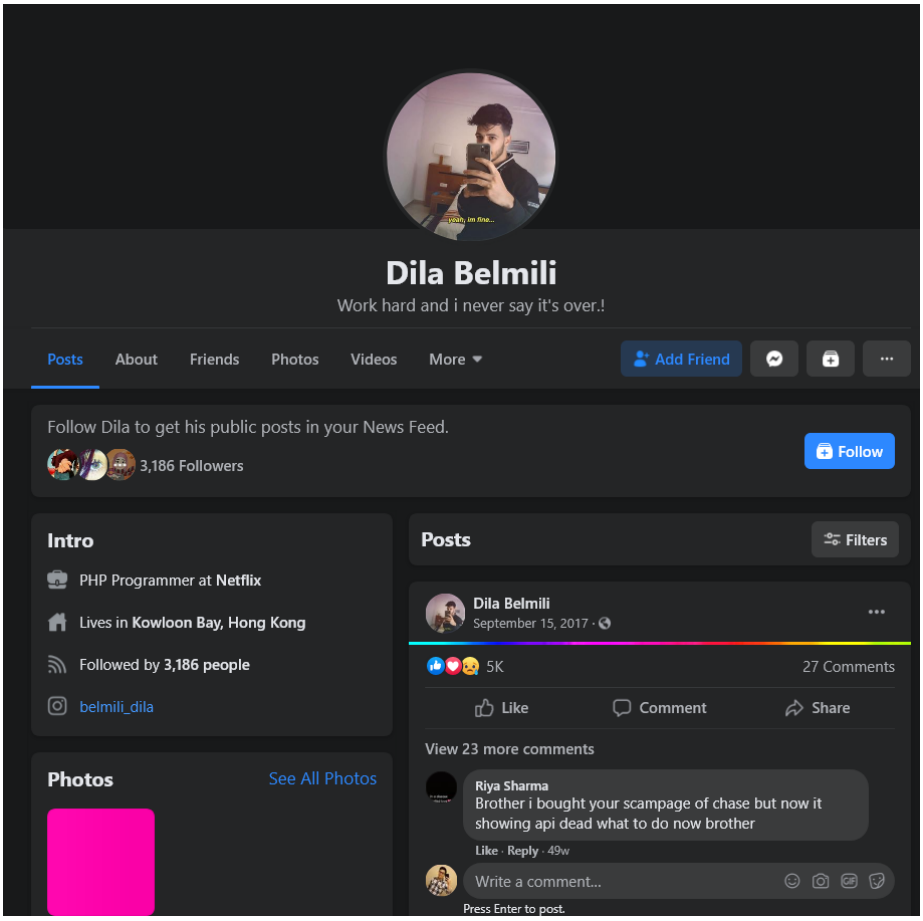
22. In January 2021, FBI Buffalo performed checks on "spoxcoder." Based upon these checks, FBI Buffalo identified screenshots of a Facebook account with username "spox_coder." This account had a display name of "Dila Belmili (spox)." The account likewise had the phrase "Work hard and never say its over" in its Intro section. A screenshot of the account is below:



23. In January 2021, FBI Buffalo performed checks on Dila Belmili. Based upon these checks, FBI Buffalo identified screenshots of a second Facebook account belonging to Dila Belmili, which had later been deleted. In these screenshots, Dila Belmili openly identified himself as Spox by listing "Spox" in the "Other Names" section of his Facebook profile page. Comments on his Facebook page also indicate that Belmili was Spox, as customers reached out to him concerning issues with phishing kits that they had purchased from him. Belmili's

Facebook page indicated that as of July 2019 he resided in Mila, Algeria. The account's status message read "Work hard and I never say it's over.!" Dila Belmili was likewise listed on the "About" page as one of the creators of the website getpaid-daily[.]com. Screenshots of the second Facebook account are below:


facebook.com/dilabelmili404?sk=about&section=bio&lst=100011700365601%3A100015063619026%3A1595782271
Search
Home
Find Friends
Create
Dila Belmili
Add Friend
Timeline
About
Friends
Photos
More
About
To see what he shares with friends, send him a friend request.
Add Friend
Overview
Work and Education
Places Lived
Contact and Basic Info
Family and Relationships
ABOUT DILA
No additional details to show
OTHER NAMES
spox
Nickname


Dila Belmili
Work hard and i never say it's over.!
Posts
About
Friends
Photos
Videos
More
Add Friend
Follow Dila to get his public posts in your News Feed.
3,186 Followers
Follow
Intro
PHP Programmer at Netflix
Lives in Kowloon Bay, Hong Kong
Followed by 3,186 people
belmili_dila
Photos
See All Photos
Posts
Filters
Dila Belmili
September 15, 2017
5K
27 Comments
Like
Comment
Share
View 23 more comments
Riya Sharma
Brother i bought your scampage of chase but now it showing api dead what to do now brother
Like · Reply · 49w
Write a comment...
Press Enter to post.

24. In January 2021, FBI Buffalo visited the getpaid-daily[.]com website. On the page, the website listed "Dila Belmili" as the individual responsible for website design. The name "Dila Belmili" contained a hyperlink which resolved to the "hackeeeed" Facebook account mentioned above as having appeared in one of the SPOX phishing kits.

25. FBI Buffalo open-source searches also indicate that one of the main personal email accounts of BELMILI was belmilidila159@gmail.com. A lookup on the website Domain BigData also linked BELMILI and this email account to the creation of numerous spoofed domains, *i.e.*, fraudulent websites that are designed to mimic legitimate websites. Domain BigData is a company that tracks the registration of new website domains on the internet. According to Domain BigData, BELMILI had registered dozens of domains, utilizing the email address belmilidila159@gmail.com. Included in these created domains were the websites support-blockchaine.com, which was created to impersonate the legitimate website support.blockchain.com; goodsfoods.com, made to impersonate goodfoods.com; seender.info, made to impersonate sender.info; and bestmake-up.info, made to impersonate bestmakeup.com. Based on my knowledge and experience, it is common for phishing kit actors to purchase spoofed domains that can be used to impersonate legitimate company websites in order to fool visitors into entering personal data. These spoofed domains often represent an important aspect of the phishing kit's infrastructure and can be utilized by a number of other scams. It is typically impossible to register for a domain without providing an email account.

BELMILI Email Accounts

26. In February 2021, FBI Buffalo served a search warrant onto Apple for records associated with the spoxy.us@icloud.com account. A review of these records showed that the account had been registered using phone number +213667459490 (BELMILI PHONE). The account also contained a screenshot of a Facebook post made by Facebook user "Abdellah Bel." A review of the emails on the spoxy.us@icloud.com account identified multiple emails being sent to and from the account pertaining to the administration of BELMILI's marketplaces, including emails regarding the purchase and operation of phishing kits. The account likewise contained the email sent by BELMILI to all of the www.market0day.com customers regarding the opening of the new www.spoxy.us website. This email was sent to approximately 913 email accounts, including UCE-1.

27. The spoxy.us@icloud account similarly sent emails to other accounts that appear to have also been controlled by BELMILI. The emails containing no subjects or contextual information. These included spoxcoder@gmail.com, spoxdz@yahoo.com, and dilabelmili@yandex.com.

28. The spoxy.us@icloud.com account also received an email pertaining to an in-app purchase that had been made from "Dila's iPhone."

29. In February 2021, FBI Buffalo served a search warrant onto Google for records associated with the spoxcoder@gmail.com and belmilidila159@gmail.com accounts. A review of the spoxcoder@gmail.com records showed that the account used dilabelmili@yandex.com and the BELMILI PHONE as recovery methods. The

spoxcoder@gmail.com account's Google Drive contained several documents named "Spox." The Google Drive also included an image of an Algerian Passport in the name "Abdellah Belmili."

30. The Google records likewise indicated that numerous additional accounts had also been created by BELMILI. For example, the BELMILI PHONE had been used to register spoxy.us@icloud.com, belmilidilaa123@gmail.com, spoxcoder@gmail.com, and marwabelmili9@gmail.com. Similarly, cookie linkage indicated that the same device that BELMILI had used to access spoxcoder@gmail.com had also been used to access other email accounts associated with BELMILI and SPOX, including abdellah.bel.contact@gmail.com, abdellah.belmili.ltd@gmail.com, dilabel124@gmail.com, marwabelmili9@gmail.com, spox0day@gmail.com, spoxcoder@gmail.com, and spoxhelton99@gmail.com.

31. A review of the email communications from the spoxcoder@gmail.com showed numerous connections between the account and BELMILI. For example, on December 16, 2020, Belmili received an email regarding an ongoing application for a Ukrainian Visa. The request included the BELMILI PHONE as well as BELMILI's photograph, date of birth, and passport number. This information matched BELMILI's passport identified above. Emails also indicated that BELMILI utilized the cryptocurrency exchange Binance. Emails found on the spoxcoder@gmail.com account demonstrated that BELMILI had registered accounts with various online services and companies using the name "Abdellah Belmili" and "Dila Belmili." Emails received by BELMILI also contained receipts for purchases made using the spoxcoder@gmail.com account. These included the purchase

of a 10 USD Google Play gift card, with a billing address sent to "Dila Belmili" at "Roue Bounit Ali, Mila 43004, Mila, Algeria," as well as a UV Pen sent to "Abdellah Belmili" sent to "Roue Bounit Ali, Mila 43004, Mila, Algeria." This second purchase also listed the BELMILI PHONE.

32. A review of the email communications from the spoxcoder@gmail.com showed numerous connections between the account and BELMILI's criminal activity. For example, between March 2020 and January 2021, BELMILI received approximately 1400 emails generated from active phishing kits, returning victims' personal identifying information (PII). This victim information corresponded with six different U.S. financial institutions, including American Express, Bank of America, Cash App, JP Morgan Chase, PayPal, and Wells Fargo.[8] Based upon the structure of these emails, there is probable cause to believe that the phishing kits providing the victim data were deployed by BELMILI. BELMILI also received approximately 3000 emails from between March 2020 and October 2020, largely from the account chase_spox@backdo0r.dz. These emails all had the same subject line: "#SPOX BACKD0OR HEY BITCH !." These emails included different URLs for scampages. Based upon FBI Buffalo's analysis of BELMILI's phishing kits provided by CHS-1, the FBI concluded that BELMILI built in a backdoor into some of his phishing kits that he sold to others. This allowed BELMILI to continue to access the phishing kits after

[8] The deposits of American Express, Bank of America, JP Morgan Chase, and Wells Fargo are all insured by the Federal Deposit Insurance Corporation.

they were hosted on various domains, essentially allowing him to see and steal the PII gathered by whomever was using his phishing kits. This backdoor access would not have been known by the customer.

33. In addition to these phishing emails, BELMILI's spoxcoder@gmail.com account also received numerous emails between July 2020 and January 2021 from customers of the www.market0day.com and www.spoxy.us marketplaces discussing their purchases. Email communications similarly showed BELMILI making purchases for various other domains, including spox-coder.space and spox-coder.xyz. These domains were purchased using the name Abdellah Belmili.

34. A review of the belmilidila159@gmail.com records showed that the account had been used to conduct research on various U.S. and U.K. financial institutions. These included Google image searches for information and logos of financial institutions that could be used in phishing kits. BELMILI likewise used this account to search for various hacking tools and methodologies. For example, some of BELMILI's search terms included: "fake address US, UK"; "fake name generator"; "how to hack blockchain private key"; "hack and spam"; "send spoofed email"; "hacking tutorials"; "cardable websites"; "fake visa card"; "credit card generator"; "anonymous email checker."

BELMILI's Financial Gains and Victimization

35. In March 2021, FBI Buffalo received record returns from Binance pertaining to the Binance account used by BELMILI associated with the spoxcoder@gmail.com account

described above. The Binance account had also been identified through the tracing of the bitcoin payments that had been used by UCE-1 to make purchases from www.market0day.com. The money from these purchases was all ultimately sent to the Binance account. A review of the Binance return records identified a passport that had been uploaded by BELMILI as part of Binance's Know Your Customer identification verification requirements. The uploaded passport was the same passport found on the spoxcoder@gmail.com account. Moreover, there were two phones that had been paired with the Binance account. These were named "Dila's iPhone" (uploaded in January 2020) and "Abdellah's iPhone (uploaded in January 2021).

36. In March 2024, FBI Buffalo received an updated record return from Binance. A review of these records identified updated information that BELMILI had provided to Binance. BELMILI's account included his full name, his date of birth, and the email abdellah.bel.contact@gmail.com. The account also listed multiple connected devices, including "Abdellah's iPhone," "Abdellah's Wifi," "Dila's iPhone," and "Dila's Wifi." BELMILI had likewise uploaded his Algerian driving license as a new form of identification. The license included BELMILI's full name, date of birth, and photograph.

37. The 2021 and 2024 record returns from Binance also identified the cryptocurrency transactions that had been conducted by BELMILI. In sum and substance, between January 2020 and January 2023, approximately $900,000 had been deposited into BELMILI's Binance account, including the money from the UCE-1 purchases. Of this money, approximately $41,000 was withdrawn as cash from ATMs, $118,000 was used by

BELMILI for purchases using Binance Pay, and approximately $760,000 was rerouted to other accounts or converted from bitcoin to other forms of cryptocurrency.

38. In November 2023, FBI Buffalo received information on BELMILI's previous phishing activities from private sector partners. This information included a compilation of the results of Spox phishing kits that had been exported to various Telegram pages. Based upon my training and experience, when a victim visits a phishing website and enters in his/her person information or credentials, the victim information is then usually sent somewhere to be retrieved by the cybercriminal who launched the phishing attack. As described above, BELMILI utilized the spoxcoder@gmail.com email account to retrieve some of his phishing exports. Other cybercriminals utilize Telegram so that the victim information is automatically sent to a Telegram page where it can be stored. By analyzing the code of phishing kits, law enforcement and private sector researchers are often able to determine which Telegram pages are being utilized to receive this victim data. As such, by reviewing these Telegram pages it is possible to estimate how many different people have been victimized by each specific Spox phishing kit. Overall, approximately 595 different Spox phishing kits were identified as having been created by BELMILI. Of these kits that exported to Telegram, approximately 1600 U.S. and international victims were identified. The email exports from the spoxcoder@gmail.com account suggest that at least an additional 4,000 U.S. victims were likewise impacted by BELMILI's kits throughout 2020.

CONCLUSION

39. I respectfully submit that this affidavit supports probable cause for a complaint charging BELMILI with violations of Title 18, United States Code, Sections 1349 (Conspiracy to Commit Bank Fraud). I also respectfully request that the proposed criminal complaint, this affidavit, and the arrest warrant be sealed and remain sealed to facilitate BELMILI's arrest.

Respectfully submitted,

Jordan F. Slavik
Special Agent
Federal Bureau of Investigation

Affidavit submitted electronically by email in .pdf format. Oath administered, and contents and signature attested to me telephonically pursuant to me telephonically pursuant to Federal Rule of Criminal Procedure 4.1 on: October _7th___, 2024.

HON. JEREMIAH J. McCARTHY
United States Magistrate Judge