Fake $50 bill – BelkaCTF 2024

Un incidente apparentemente banale e insignificante: un cassiere di un negozio all'angolo riceve una banconota falsa da 50 dollari e la denuncia alla polizia. L'obiettivo è smascherare una gang ben organizzata coinvolta in reati di contraffazione di valuta.

Apple ID e identità

Obiettivo: trovare l'ID Apple associato allo smartphone e il nome completo del proprietario.

Service...	User Name	Created Date/Time
iCloud	billthemegakill@icloud.com	04/04/2024 05:11:56.782
IDMS	billthemegakill@icloud.com	04/04/2024 05:11:52.040
IMAPMail	billthemegakill@icloud.com	04/04/2024 05:12:15.612
iTunes Store	billthemegakill@icloud.com	04/04/2024 05:12:25.550
Messages	billthemegakill@icloud.com	04/04/2024 05:11:56.704
Apple ID	billthemegakill@icloud.com	04/04/2024 05:11:52.203

Figura 1 - User Accounts

L'ID Apple è **`billthemegakill@icloud.com`.**

Cercando poi la mail all'interno dei contatti del telefono si trova l'identità del proprietario ed utilizzatore del telefono:

First Name	**William**
Last Name	**Phorger**
Email(s)	**billthemegakill@icloud.com**
Created Date/Time	**05/04/2024 22:07:44.000**
Last Modified Date/Time	**05/04/2024 22:07:44.000**
Artifact type	**Apple Contacts - iOS**
Item ID	**671**

Figura 2 - Identità owner smartphone

Il nome completo del proprietario del telefono è **William Phorger.**

Account Telegram

Obiettivo: trovare gli account con i quali il proprietario ha discusso di argomenti illegali.

Per risolvere questa challenge è necessario leggere le conversazioni di Telegram e, una volta individuato l'utente interlocutore, controllare il suo username salvato nell'apposito database: `private\var\mobile\Containers\Shared\AppGroup\A667456A-6F8F-48C7-A8CF-37EFCC6BD644\telegram-data\account-11254559246638807 4\postbox\db\db_sqlite`.
Gli username di interesse sono: `@locknload771`, `@diddyflowers`, `@Sm00thOperat0r`, `@JesusStreeton1999`.

Abitazione

Obiettivo: capire dove vive William.

Dall'analisi degli screenshot effettuati sullo smartphone ne è emerso uno dell'applicazione `Reminder`, nel quale si nota il seguente frammento:

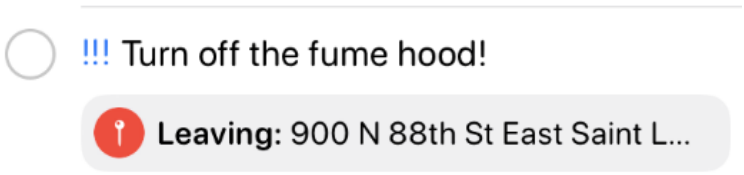

Figura 3 - Frammento dello screenshot app Reminder

Il messaggio del Reminder dice "Spegnere la cappa aspirante!". Cercando su Maps, l'indirizzo risulta essere `900 N 88th St, East St Louis, IL 62203, Stati Uniti`. Poi però sono state rinvenute le posizioni presenti nella cache dell'applicazione Uber e una di queste presente l'etichetta "*home*":

Tag	Address	Name	Latitude	Longitude
home	Nottingham Ave, 7402, Saint-Louis, MO, 63119	Nottingham Ave, 7402	38.5899458	-90.3253251

Figura 4 - Abitazione del proprietario del telefono

Si conclude che l'abitazione del proprietario del telefono sia a **`Nottingham Ave, 7402, Saint-Louis, MO, 63119.`**

Username PC

Obiettivo: trovare lo username dell'utente del computer

Analizzando i `SID` dal registro `SAM` o gli artefatti relativi agli `User Account` è possibile affermare che l'utente del computer abbia **`@phorger`** come username.

User Name	Security Identifier
WDAGUtilityAccount	504
phorger	S-1-5-21-1548112901-4150280657-3748420248-1000
Guest	501
DefaultAccount	503
Administrator	500

Figura 5 - User Account

Stipendio

Obiettivo: trovare lo stipendio di aprile.

È stata rinvenuta una conversazione Telegram con utente `the.boss`, nella quale è presente un messaggio nel quale si parla di un'applicazione di messaggistica non *parsata* dal programma utilizzato per l'analisi:

Chat ID	**7108672404**
Title	**the.boss**
Last Sender	**the.boss**
Last Sender Id	**7108672404**
Last Message Date/Time	**04/04/2024 02:26:53.000**
Last Message	**Hey William, got us a new chat on Element for the big brain moves. It's all hush, all tech. Hit up that invite I sent. Let's get to schemin'.**
Account ID	**112545592466388074**
Artifact type	**Telegram Chats - iOS**

Figura 6 - Chat in cui si parla di Element

`Element` è un'applicazione di messaggistica sicura, open source e decentralizzata, costruita sul protocollo Matrix, che offre messaggistica istantanea crittografata end-to-end, chiamate vocali/video, condivisione file e chat di gruppo, permettendo agli utenti di scegliere il proprio server per avere pieno controllo sui dati.

Dall'analisi del computer è emersa una notifica nella quale si fa riferimento allo stipendio di aprile, che risulta essere di `7012USD`. Si riporta di seguito:

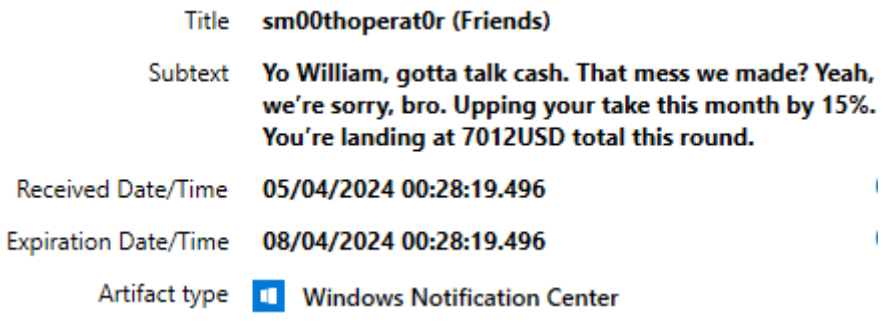

Figura 7 - Notifica con stipendio

Successo di marzo

Obiettivo: capire dove si è trovata la gang per festeggiare insieme il successo ottenuto a marzo.

Nella chat di gruppo su Telegram del 19/03/2024 l'utente `the.boss` chiede di festeggiare in un bar in centro:

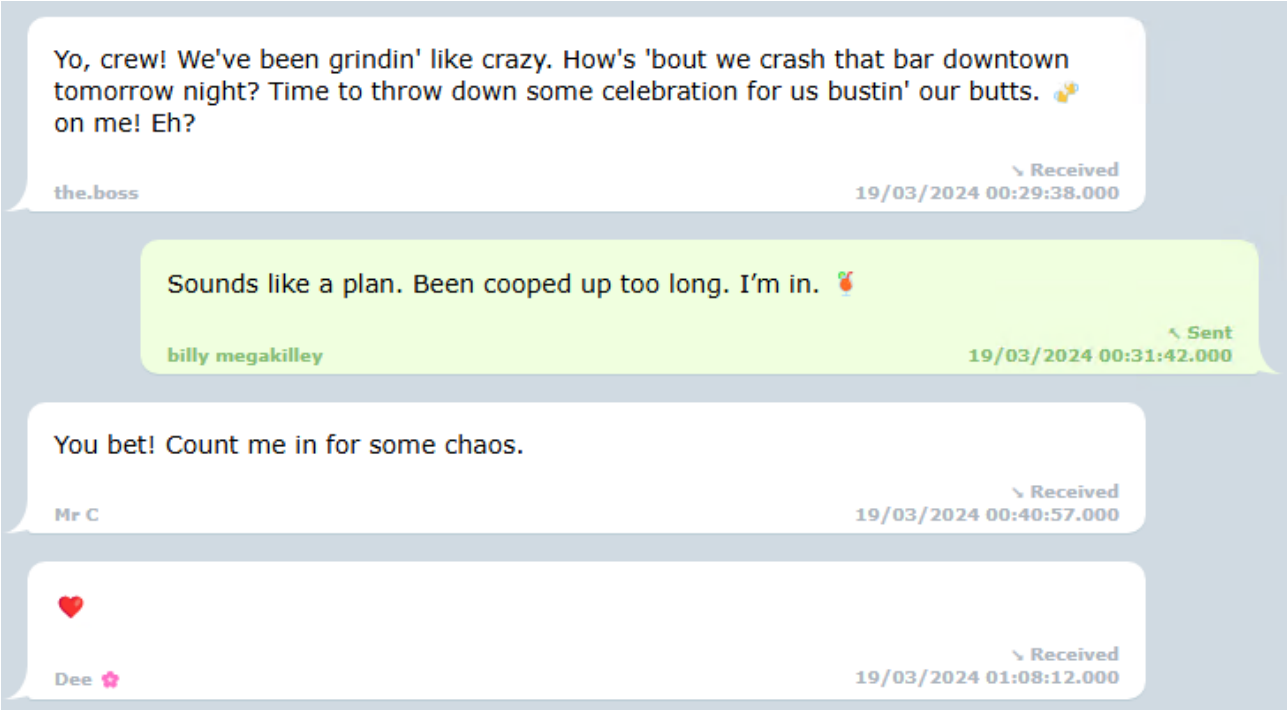

Figura 8 - Festeggiamenti al bar in centro

Ora è chiaro che debbano festeggiare il 20/03/2024. È stata quindi analizzata la timeline degli eventi susseguitesi sul telefono, mediante software open-source iLEAPP. In quella giornata sono stati registrati diversi eventi dell'applicazione `Splitwise`, per la divisione delle spese. Si riporta l'evento significativo:


```
{"Created Timestamp": "2024-03-20 04:13:52+00:00", "Updated Timestamp": "2024-03-20 08:44:52+00:00", "Payer": "Billy (halase1999@darkse.com)", "Expense Description": "Get-together at Cunetto", "Cost": "948.0", "Currency": "USD", "Category": "General", "Group Name": "Elite club", "Expense ID": "3015931189", "Expense GUID": "E58BC9DA-07B3-4D4E-BE4A-5FB4F679977E"}
```


Figura 9 - Splitwise Expenses

Per capire se Elite Group comprendesse i membri di interesse si è proceduto ad analizzare il database di Splitwise dove in effetti è presente la seguente entry:

2024-03-15 17:17:41+00:00	2024-03-19 15:44:16+00:00	Elite club	Billy (halase1999@darkse.com); babe (lavolam239@cmheia.com); SMH (xosane5653@azduan.com); Locky (gobic88442@darkse.com); m0m (vofivi5179@dovesilo.com); Jesus (wiyokak642@cmheia.com);	62605846	Home

Figura 10 - Elite Group

Cercando "*Cunetto USA*" su Maps esce un solo risultato `Cunetto House of Pasta` al `5453 Magnolia Ave, St. Louis, MO 63139, Stati Uniti`.

Encrypted container

Obiettivo: percorso completo del "contenitore crittografato".

Dall'analisi delle conversazioni di Telegram si riporta questo messaggio inviato dal bot denominato `Baker Bot`, il quale evidenzia un errore alla linea 98 del codice Python:

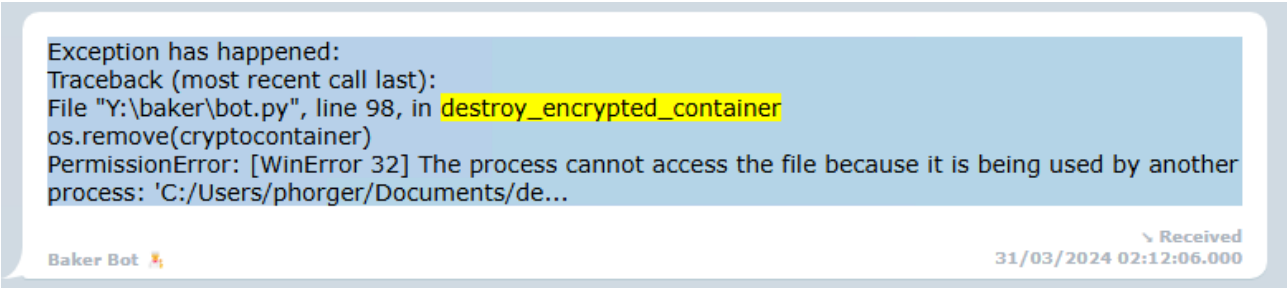

Figura 11 - linea 98 del codice bot.py

Nel messaggio è presente solo una parte del percorso, dunque si procede andando ad analizzare il file system del computer, nel quale effettivamente in `Users\phorger\Documents` si trova un disco virtuale in formato `vhdx`. Il percorso completo del file, dunque, è `Users\phorger\Documents\desktop.ini:vault.vhdx`.

Acquisto

Obiettivo: trovare l'articolo di lusso nel quale il proprietario del telefono ha messo il denaro.

Dall'analisi della cronologia browser si evidenzia la presenza di ricerche effettuate dall'utente sul tema:

Search Term	URL	Search Engine	Artifact
what to spend a lot of money on	https://duckduckgo.com/?va=i&t=hf&q=what+to+...	DuckDuckGo	Safari History
what to spend a lot of money on	https://duckduckgo.com/?va=i&t=hf&q=what+to+...	DuckDuckGo	Safari History
what to spend a lot of money on	https://duckduckgo.com/?va=i&t=hf&q=what+to+...	DuckDuckGo	WebKit Browser Web History (Carved)
what to spend a lot of money on	https://duckduckgo.com/?va=i&t=hf&q=what+to+...	DuckDuckGo	Safari History
what to spend a lot of money on	https://duckduckgo.com/?va=i&t=hf&q=what+to+...	DuckDuckGo	Safari History
what to spend a lot of money on	https://duckduckgo.com/?va=i&t=hf&q=what+to+...	DuckDuckGo	Safari Suspended State Tabs
what to spend a lot of money on	https://duckduckgo.com/?va=i&t=hf&q=what+to+...	DuckDuckGo	WebKit Browser Web History (Carved)

Figura 12 - Ricerche web

Le ricerche solo datate al 06/02/2024. Nella stessa giornata viene visitata anche la pagina "*How to spend your money for maximum happiness*"[1]. La ricerca sembra non portare a nulla.

Si è dunque tentato di aprire il disco virtuale rinvenuto nella challenge precedente. Nelle note è stata rinvenuta una chiave Bitlocker che potrebbe aprire il disco virtuale:

Title	**BitLocker recovery**
Folder	**On My iPhone / Notes**
Created Date/Time	**11/11/2023 04:52:08.238**
Last Modified Date/Time	**11/11/2023 04:54:14.301**
Body	**BitLocker recovery** **Identifier:** **929983CA-5012-49E9-A194-4550C08C6127** **Recovery key:** **590238-514580-359986-088242-029766-319495-4** **10509-636911**

Figura 13 - Bitloker Recovery Key

[1] https://www.popsci.com/story/science/how-to-spend-money-happiness

È stato dunque esportato dalla copia forense e poi montato il vhdx rinvenuto, mediante un tool denominato Arsenal Image Mounter:

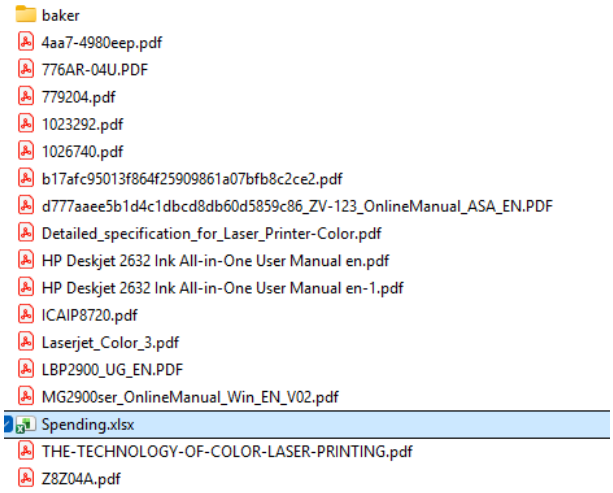

Figura 14 - Contenuto del Vault

Si ritiene di particolare interesse il file `Spending.xlsx`, il quale viene aperto:

When	What	How much
2024-02-05	Groceries	$50
2024-02-07	Dinner at Bella Italia Restaurant	$30
2024-02-09	Gasoline	$40
2024-02-10	Movie tickets for "The Batman"	$25
2024-02-12	Adidas Originals Hoodie from H&M	$100
2024-02-14	Bouquet of Roses from Rose Blossom Florist	$80
2024-02-16	Home utilities (electricity bill)	$150
2024-02-18	MacBook Pro M1 from Apple Store	$2000
2024-02-20	Gold's Gym Membership	$60
2024-02-22	Venti Caramel Macchiato at Starbucks	$10
2024-02-24	Dinner with friends at Smith & Wollensky	$70
2024-02-26	"1984" by George Orwell from Barnes & Noble	$20
2024-02-28	Car maintenance (oil change)	$120
2024-03-01	Haircut by David at Snip & Clip	$35
2024-03-03	Household supplies (cleaning items)	$45
2024-03-05	Sushi lunch at Sushi Palace	$15
2024-03-07	Verizon Wireless phone bill	$80
2024-03-09	Round-trip flight tickets to Paris	$1458
2024-03-11	Spotify Premium subscription	$12
2024-03-13	Dinner date at The Capital Grille	$90
2024-03-15	Apple AirPods Pro for friend's birthday	$269
2024-03-16	Sony 65" OLED TV from Best Buy	$1400
2024-03-17	Rolex Submariner Date ref 126619LB	$30500
2024-03-19	Airbnb	$636
2024-03-23	Laari Adda	$357

Figura 15 - Contenuto di Spending.xlsx

L'acquisto con il valore più alto è un **`Rolex Submariner Date ref 126619LB`**.

Concerto

Obiettivo: capire a quale concerto il proprietario del telefono aveva intenzione di assistere insieme alla sua ragazza a maggio.

Nella chat con Drew, il giorno 24/12/2023 viene citata una vacanza da fare a maggio come luna di miele, ma non sono comparsi altri dati all'interno della conversazione.

È stata analizzata la cache dei browser utilizzati da William, mettendo un filtro con la keyword "telegram" (visto che la conversazione è avvenuta su quella piattaforma di messaggistica), ed è stata rinvenuta un'immagine di interesse:

Figura 16 - Concerto di maggio

Dunque, il concerto al quale a maggio sarebbero dovuti andare William e Drew era quello di **`Eric Clapton, Accor Arena, Paris.`**

Modello stampa bollette

Obiettivo: trovare il nome della persona che ha progettato il modello di stampa per le banconote.

Nel `Volt` è presente un file in formato `psd` che risulta essere un template per le banconote che contiene la seguente riga:

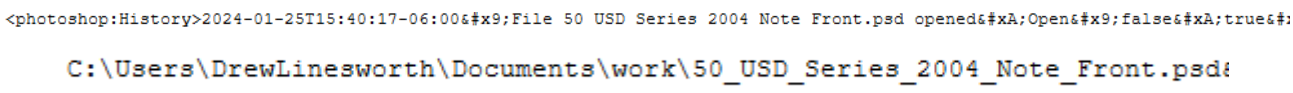

Figura 17 – Drew Linesworth

Si ritiene dunque che Drew Linesworth sia l'artefice dei template delle banconote. A conferma di ciò, nella conversazione Telegram tra William e Drew più volte si fa riferimento al fatto che lei sia esperta di design: "`Your design truly brought it to life`."

Laboratorio

Obiettivo: trovare il laboratorio dove hanno stampato le banconote.

In questo caso, potrebbe tornare utile il Reminder della cappa aspirante, precedentemente riportato:

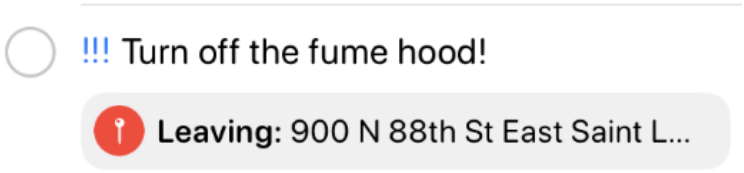

Figura 18 – Reminder

Come precedentemente riportato, il luogo si trova a `900 N 88th St, East St Louis, IL`.

Figura 19 - Laboratorio per stampare denaro

Lotto di stampa

Obiettivo: trovare il momento preciso in cui è stato completato il lotto di stampa più grande.

Si riporta di seguito la conversazione con il bot di Telegram:

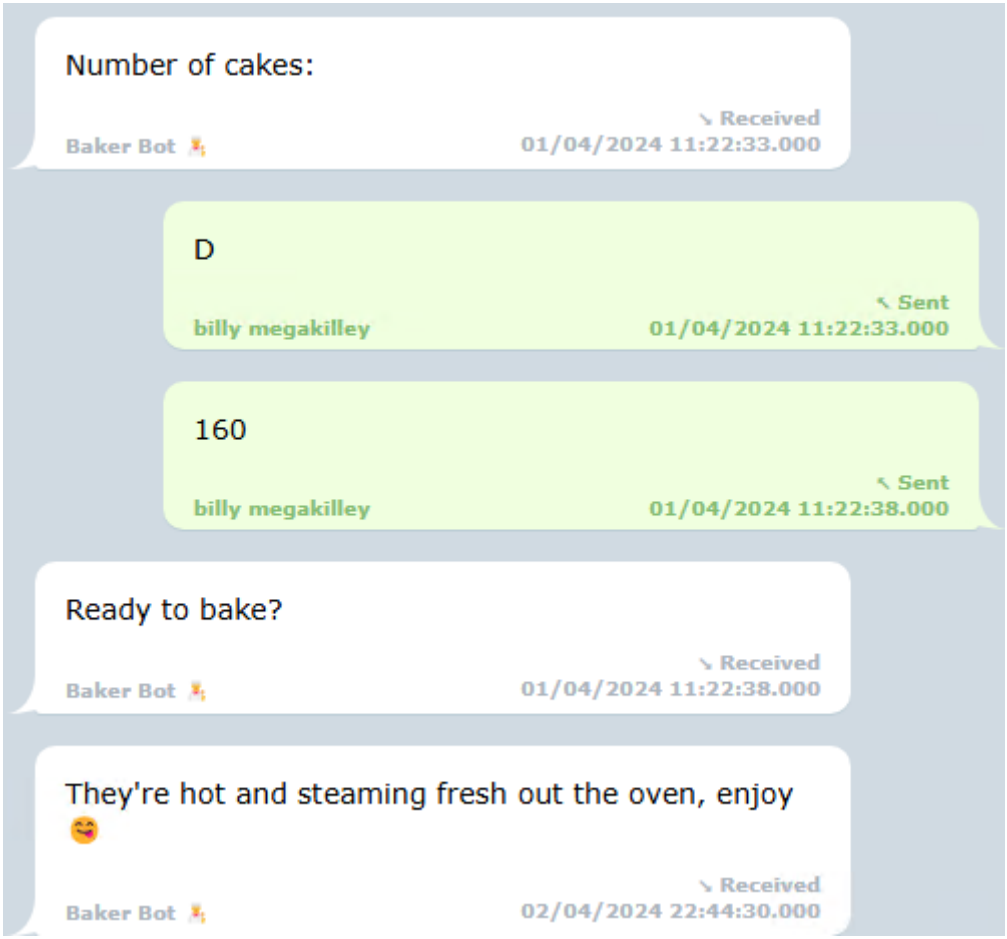

Figura 20 - 160 pezzi

Il momento preciso è il giorno **02/04/2024** alle ore **22:44:30.**

Modello stampante

Obiettivo: trovare il modello della stampante con la quale viene stampato il denaro.

Dall'analisi delle connessioni USB effettuate sul computer è stata immediatamente trovata la stampante di interesse: **`HP LaserJet Professional M1132 MFP.`**

ATM bancomat

Obiettivo: capire a qualche bancomat, Phorger ha testato le banconote recentemente.

Si riporta uno stralcio della chat di gruppo su Telegram:

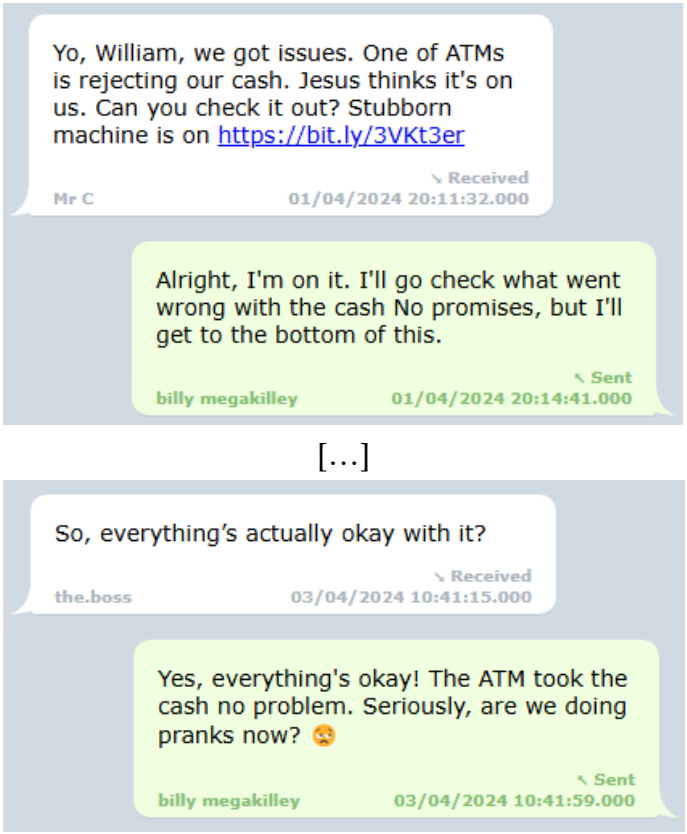

Figura 21 - ATM da controllare

Dalla Figura precedente è possibile affermare che Phorger sia andato a controllare lo sportello il 03/04/2024. A conferma di tale affermazione è presente una ricerca sul browser effettuata proprio in questa giornata:

Search Term	Search Date/Time	Artifact type
locked myself in atm booth	03/04/2024 07:27:51.044	iOS Safari Recent Search Terms

Figura 22 - Chiuso nella cabina bancomat

Facendo un filtro su quella giornata si evidenzia la presenza una connessione ad un Wi-Fi pubblico:

Network Name (SSID)	MAC Address	Last Joined Date/Time
UCPLPublicWireless	36:56:EE:50:83:97	03/04/2024 07:26:18.000

Figura 23 - Connessione Wi-Fi

È stato dunque utilizzato il tool https://wigle.net/ per trovare la posizione esatta del Wi-Fi, il quale risulta essere della `University City Public Library`.

Figura 24 - Localizzazione Wi-Fi

Cercando sportelli ATM bancomat nelle vicinanze su Google Maps si trova **`Regions Bank ATM on Delmar Blvd`**.

Leaked

Obiettivo: trovare chi ha fatto trapelare informazioni sui dati tecnici del validatore di banconote.

Il frammento di conversazione che potrebbe essere di interesse è il seguente:

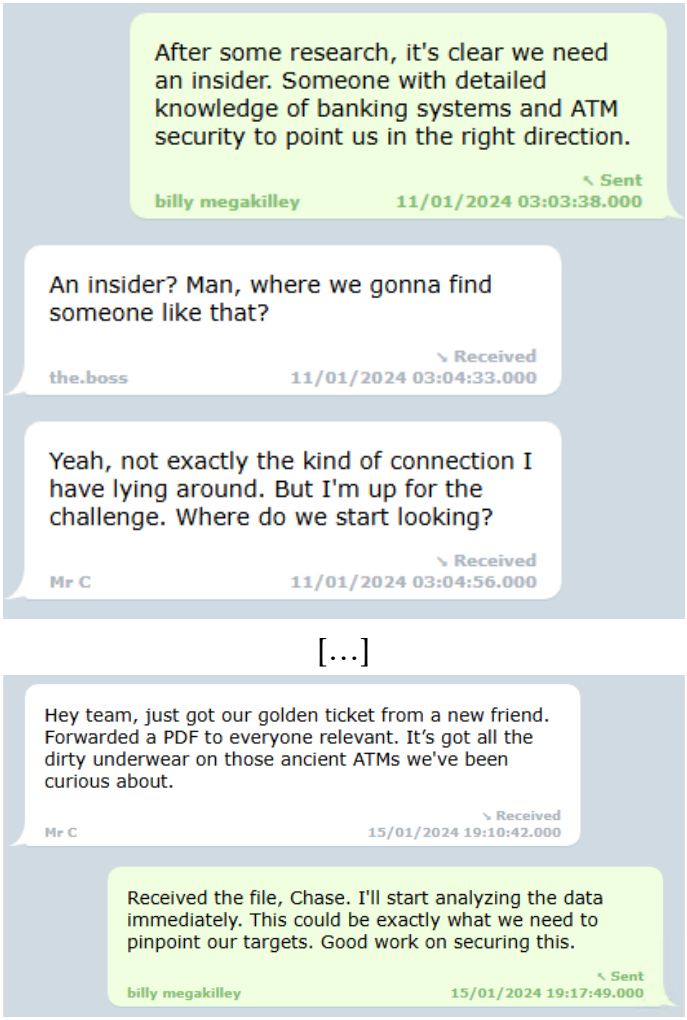

Figura 25 - Frammento della chat di gruppo Telegram

Nella conversazione di fa riferimento ad un file PDF inviato a tutti e cifrato. In effetti cercando un file PDF alla data del 15/01/2024 si trova un file cifrato: **`xpdfimport_err.pdf`**. L'autore del file risulta essere visibile, ma il file non sembra essere stato inviato . Inoltre, la data di creazione del file nel file system risale al **20/08/2015**.

Per trovare il documento PDF è stato fatto *carving* sul Volt di Phorger, mediante tool XWays Forensics. Dal carving è emerso un file denominato "**`B500 ATM Technical Documentation.pdf`**".

Original File Name	Original MFT Modified Date/Time - UTC+00:00 (dd/MM/yyyy)	Original Created Date/Time - UTC+00:00 (dd/MM/yyyy)	Original Modified Date/Time - UTC+00:00 (dd/MM/yyyy)	Original Accessed Date/Time - UTC+00:00 (dd/MM/yyyy)
Filter	Filter	Filter	Filter	Filter
B500 ATM Technical Documentation.pdf	15/01/2024 13:13:26.457	15/01/2024 13:13:20.301	01/08/2023 12:12:32.135	15/01/2024 13:13:20.317

Figura 26 - File di interesse

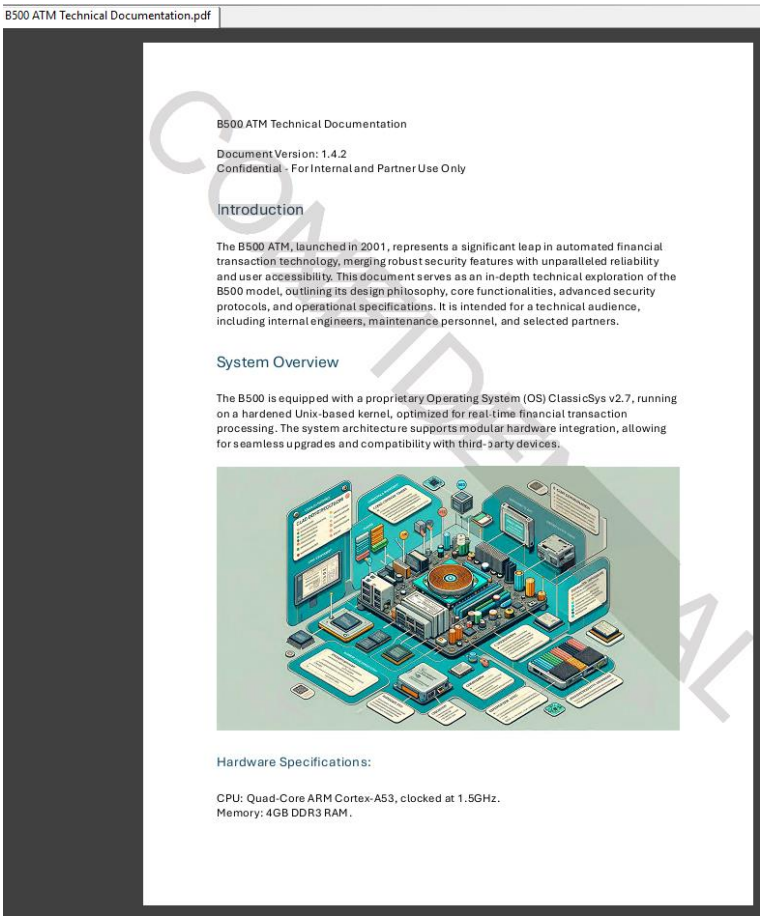

Figura 27 - Anteprima del file

Analizzando la firma (`signature`) del file è possibile affermare il l'autore è **Kenneth Leek**.

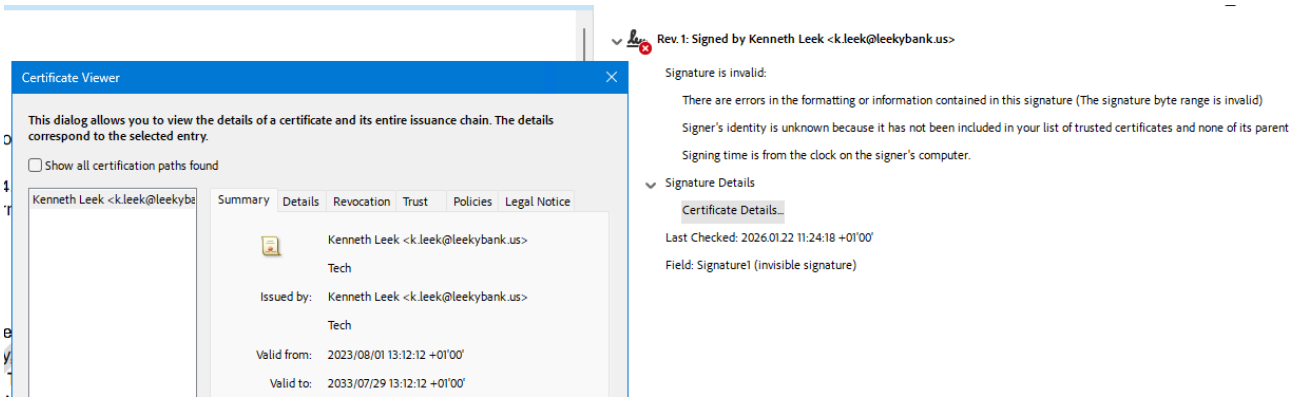

Figura 28 - Signature del file

Istituto bancario

Obiettivo: identificare l'istituto bancario con il quale la gang aveva rapporti.

Nella chat di gruppo `the.boss` afferma il 1° marzo di aver aperto un conto bancario e poi `Mr C` inizia a comunicare utilizzando messaggi esadecimali cifrati. Scorrendo all'inizio della conversazione con Phorger, si evidenzia come Mc C gli dice che le app di messaggistica non sono sicure e afferma di avergli inviato una Shortcut per cifrare messaggi:

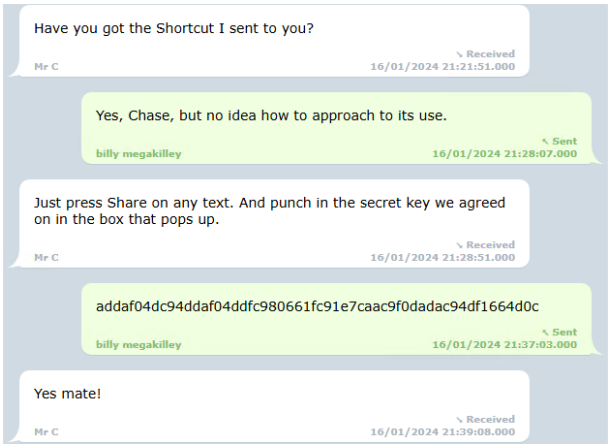

Figura 29 - frammento di conversazione di interesse

In effetti, un semplice convertitore da HEX a testo non funziona con questi messaggi. È stata effettuata la categorizzazione delle immagini e sono state trovate le Shortcut di cifratura e decifratura dei messaggi.

Figura 30 – Shortcut

Tra gli snapshot del dispositivo ne emerge uno contenente i seguenti dati:


```
"Background Style": "UIBackgroundStyleDefault",
"Bundle ID": "com.apple.shortcuts",
"Content Type": "1",
"Creation Date": "2024-04-04 05:18:57.261481",
"Expiration Date": "",
"File Location": "1",
"Fullscreen": "True",
"Group ID": "com.apple.shortcuts - {DEFAULT GROUP}",
"Identifier": "A8D83876-167E-4683-8EB7-570EE9EE95DA",
"Image Opaque": "True",
"Image Scale": "2.0",
"Interface Orientation": "1",
"Last Used Date": "2024-01-16 17:08:14.524852",
"Launch Interface Identifier": "__from_UILaunchStoryboardName__",
"Name": "",
"Reference Size": "{375, 667}",
"Relative Path": "A8D83876-167E-4683-8EB7-570EE9EE95DA@2x.ktx",
"Required OS Version": "",
"Snapshot Group": "com.apple.shortcuts - {DEFAULT GROUP}",
"Snapshot Index": "1"
```


Figura 31 - App Snspshot

Cercando quel Path relativo all'interno della copia forense dello smartphone viene effettivamente trovata la Shortcut di interesse:

Application...	Image	File Name	File...	Created Date/Ti...
com.apple.shortcuts		A8D83876-167E-4683-8EB7-570EE9EE95DA@2x.ktx	.ktx	21/01/2026 10:58:58.117
		\BelkaCTF_6_CASE240405_D201AP\private\var\mobile\Containers\Data\Application\D5B11F5D-8111-4F46-80AE-F50D6447F5EB\Library\SplashBoard\Snapshots\com.apple.shortcuts - {DEFAULT GROUP}\A8D83876-167E-4683-8EB7-570EE9EE95DA@2x.ktx		

Figura 32 - Shortcut di interesse

Navigand nel file system proprio nella cartella `Data/Application/D5B11F5D-8111-4F46-80AE-F50D6447F5EB\tmp`, si trova un file "`CFNetworkDownload_MHW6ip.tmp`", contenente un codice che effettivamente serve per decodificare un messaggio cifrato in esadecimale **usando una cifratura basata su una chiave**:

```
string = var key="￼";
var hexEncodedText="￼";
var sum = 0;
for (let i = 0; i < key.length; i++) {
   sum += key.charCodeAt(i);
}
a = sum % 137;
a = 2*a + 1;
b = sum % 89 + 1
let decodedText = '';
let modInverseA = 0;
for (let i = 0; i < 256; i++) {
   if ((a * i) % 256 === 1) {
      modInverseA = i;
      break;
   }
}
let encodedText = '';
for (let i = 0; i < hexEncodedText.length; i += 2) {
   let charCode = parseInt(hexEncodedText.substr(i, 2), 16);
   encodedText += String.fromCharCode(charCode);
}
for (let i = 0; i < encodedText.length; i++) {
   var tt = encodedText.charCodeAt(i) - b;
   if (tt < 0){
      tt+=256;
   }
   let charCode = (modInverseA * tt) % 256;
   decodedText += String.fromCharCode(charCode);
}
document.body.textContent = encodeURIComponent(decodedText);
```

Figura 33 - Codice di decifratura

Il codice di cifratura è stato invece invenuto all'interno del database delle Shortcut.

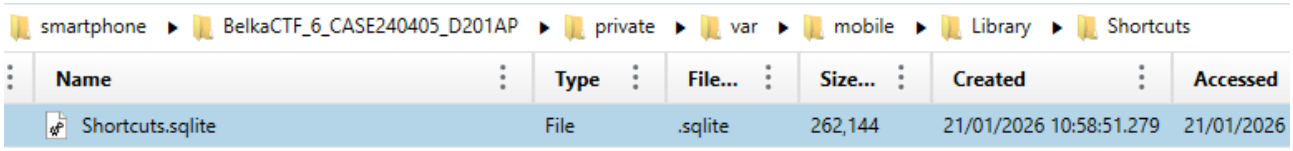

Figura 34 - Database Shortcut

Per decifrare i messaggi scambiati tra i due interlocutori è però necessaria anche la chiave di cifratura, della quale è possibile fare *brute-force*, scrivendo questo codice in Python.

```
import sys
import re

def decrypt(s, a, b):
    res = ""
    for ch in s:
        res += chr(((ord(ch) - b) * a) % 256)
    return res

if len(sys.argv) < 2:
    print(f"USAGE: {sys.argv[0]} <ciphertext> [a b]")
    sys.exit(1)

s = bytes.fromhex(sys.argv[1]).decode('latin1')  # Decodifica da hex

if len(sys.argv) > 3:
    print(decrypt(s, int(sys.argv[2]), int(sys.argv[3])) + "\n")
else:
    for a in range(0, 127):
        a = a * 2 + 1
        for b in range(1, 90):
            res = decrypt(s, a, b)
            if re.match(r'^[\x0a\x20-\x7e]*$', res):
                print(f"{a}\t{b}\t{res}\n")
```

Figura 35 - Codice brute-force in Py

Decifrando i massaggi inviati e ricevuti è possibile affermare che lo SWIFT Code della banca è **`CRVBPA2P`**.

Estratto conto

Obiettivo: trovare l'intero estratto conto bancario di Phorger, contenente tutte le sue transazioni offshore.

Cercando il termine “Bank” tra le foto (sulle quali è stato fatto OCR) emerge un’immagine di interesse:

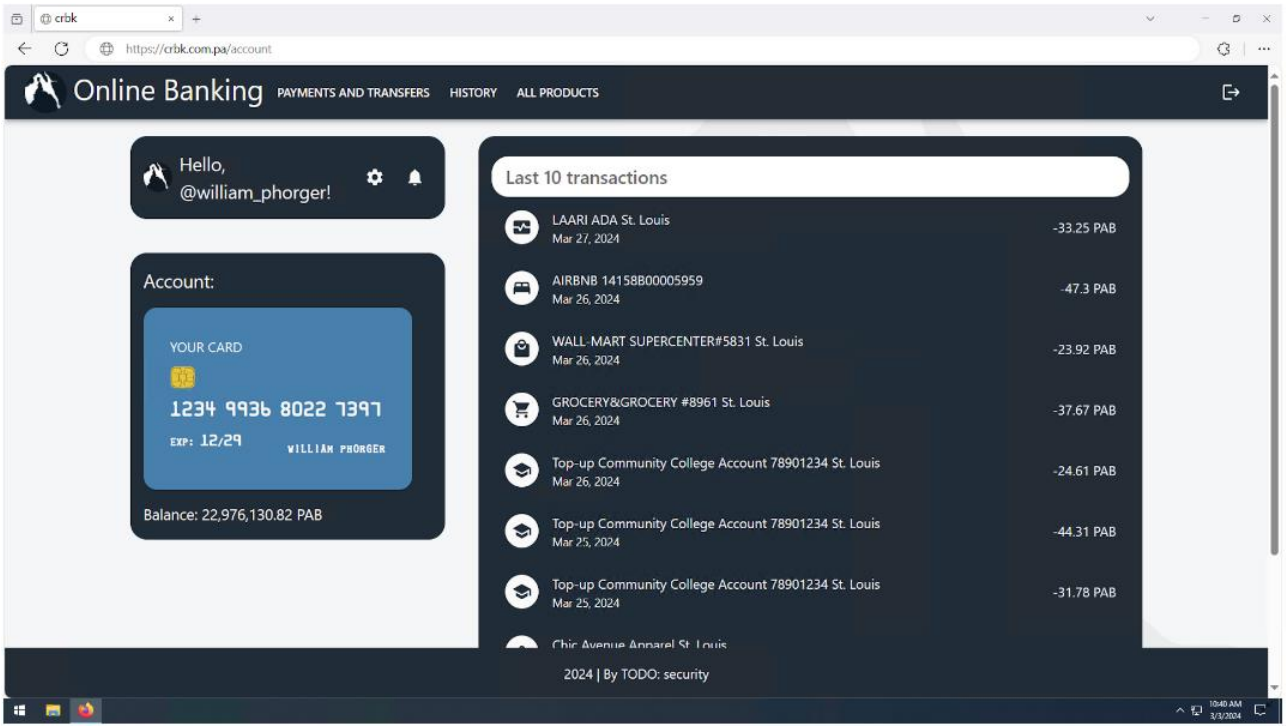

Figura 36 - Immagini di possibile interesse - Bank

Navigando su *crbk.org* è evidente come il login sia composto da username "william_phorger" e password, che però è possibile recuperare.

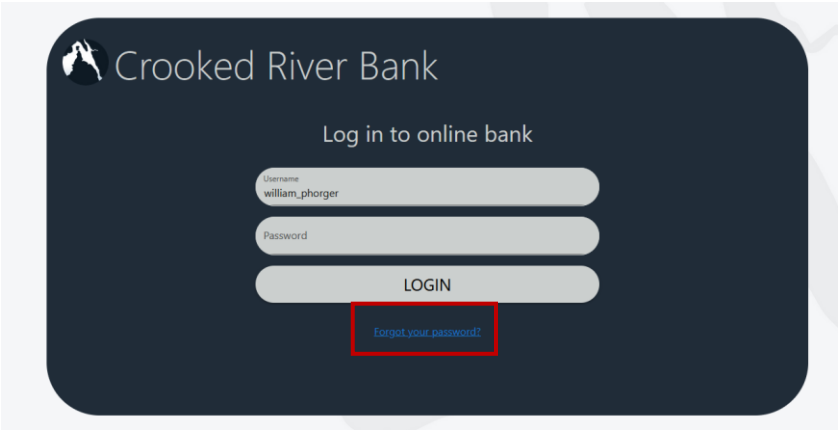

Figura 37 - crbk.org

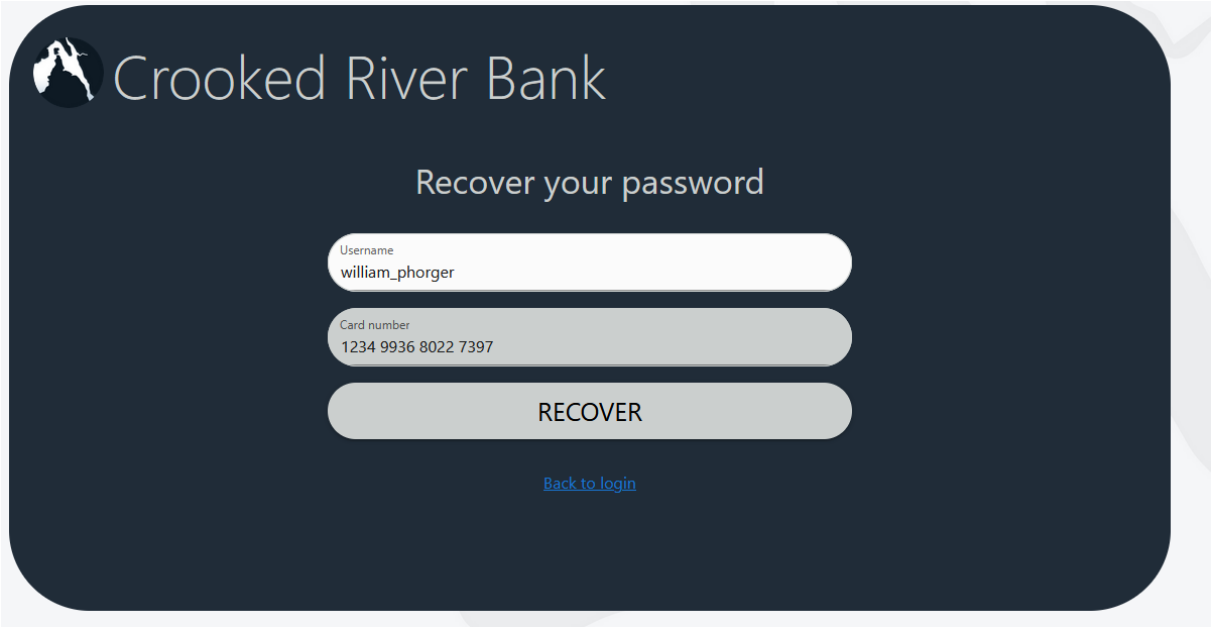

Figura 38 - Recupero password

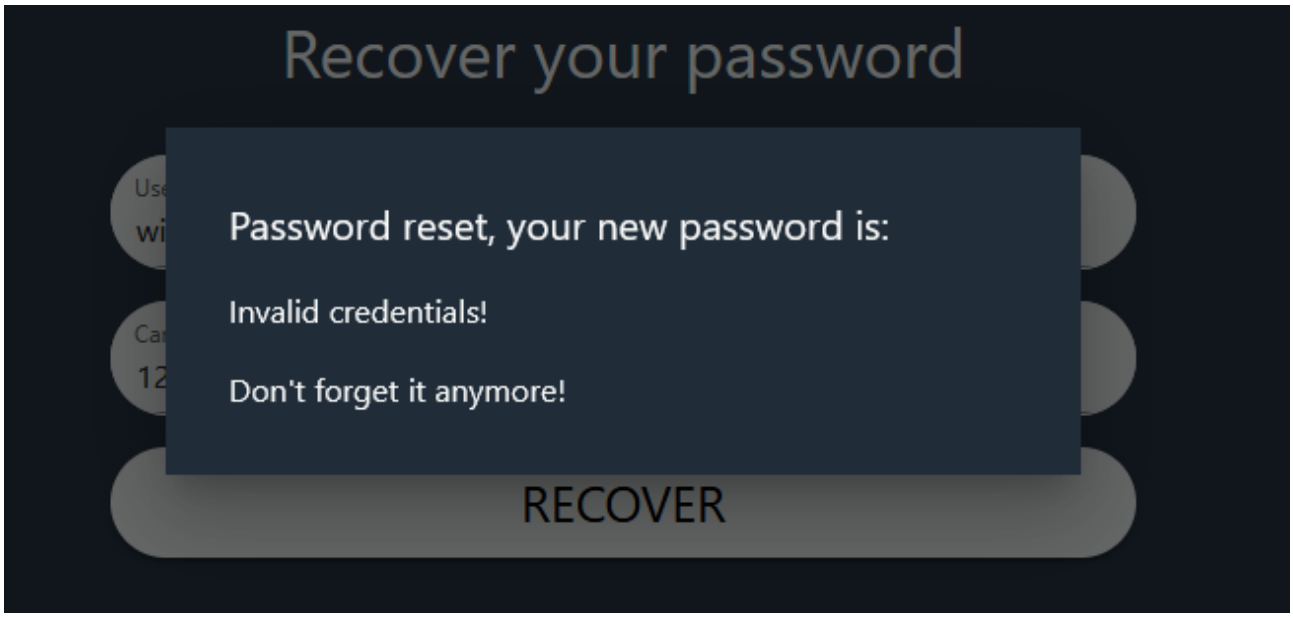

Figura 39 - Password trovata

Per scaricare le informazioni di interesse è però necessario avere il codice di 2FA. Sono stati dunque analizzati gli screenshot ed è stato rinvenuto il seguente QR:

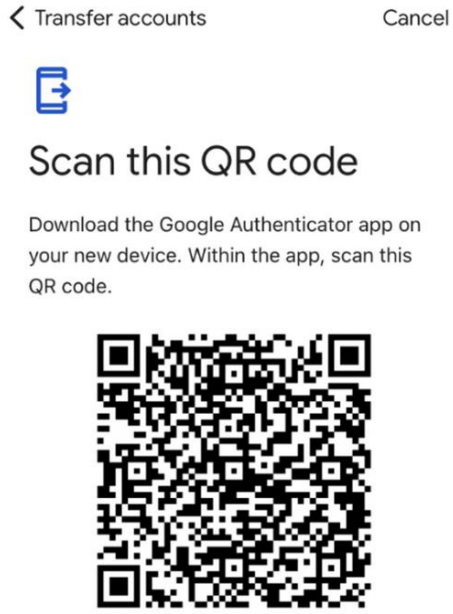

Figura 40 - QR Google Authentication

In effetti, tra gli screenshot cancellati è presente un QR con il quale è possibile registrare sul proprio cellulare la doppia autenticazione dell'account di William. Un'altra opzione è quella di usare un tool per la decodifica, come *https://github.com/dim13/otpauth* e ricevere in chiaro il codice a 6 cifre necessario.

Una volta ottenute tutte le credenziali di accesso, la banca restituisce un CSV con tutti i dati richiesti:

[…]

2024",GROCERY&GROCERY #8961 St. Louis Clothing,-1249.4,"Mar 06, 2024",S tyle Haven Boutique St. Louis Utilities,-38.6,"Mar 07, 2024",SHELL*C16410* PETRO Utiliti es,-98.36,"Mar 07, 2024",SHELL*C16410* PETRO Restaurant,-70.03,"Mar 08, 2024",U BER*1337 EATS Utilities,-41.26,"Mar 08, 2024",SHELL*C16410* PETRO Transportation,-52.49, "Mar 08, 2024",UBER*441* MISSOURI Entertainment,-96.66,"Mar 08, 2024",FACEBK VM QNIRW2 650-853-5853 Shopping,-10.45,"Mar 09, 2024",WALMART SUPERCENTER#5831 St. Louis Tr ansportation,-64.29,"Mar 09, 2024",UBER*441* MISSOURI Rent,-1796.47,"Mar 09, 2024&qu ot;,AIRBNB 14158B00005959 Groceries,-16.36,"Mar 09, 2024",GROCERY&GROCERY #8961 St. L ouis Groceries,-11.01,"Mar 09, 2024",GROCERY&GROCERY #8961 St. Louis Top-up,4671.54, "Mar 09, 2024",Top-up from Maximilian Senntens Utilities,-117.87,"Mar 10, 2024" ,SHELL*C16410* PETRO Groceries,-99.91,"Mar 11, 2024",GROCERY&GROCERY #8961 St. Louis Education,-30.65,"Mar 11, 2024",Top-up Community College Account 78901234 St. Louis Heal thcare,-514.59,"Mar 11, 2024",LAARI ADA St. Louis Healthcare,-236.47,"Mar 11, 2024&q uot;,LAARI ADA St. Louis Healthcare,-813.86,"Mar 11, 2024",LAARI ADA St. Louis Groceries ,-19.9,"Mar 12, 2024",GROCERY&GROCERY #8961 St. Louis Transportation,-31.02,"Mar 12, 2024",UBER*441* MISSOURI Transportation,-111.88,"Mar 13, 2024",UBER*441* MISSOU RI Restaurant,-95.38,"Mar 14, 2024",UBER*1337 EATS Clothing,-438.63,"Mar 14, 2024&q uot;,Fashionista Emporium St. Louis Transportation,-38.1,"Mar 14, 2024",UBER*441* MISSOUR I Shopping,-39.82,"Mar 14, 2024",WALMART SUPERCENTER#5831 St. Louis Transportation,-30.8 8,"Mar 14, 2024",UBER*441* MISSOURI Restaurant,-215.97,"Mar 15, 2024",UBER*1337 EATS Entertainment,-70.48,"Mar 16, 2024",FACEBK VMQNIRW2 650-853-5853 Entertainment,-24 .5,"Mar 16, 2024",FACEBK VMQNIRW2 650-853-5853 Restaurant,-45.1,"Mar 16, 2024", UBER*1337 EATS Rent,-563.17,"Mar 16, 2024",AIRBNB 14158B00005959 Restaurant,-127.27,&quo t;Mar 17, 2024",UBER*1337 EATS Education,-974.59,"Mar 17, 2024",Top-up Community Col lege Account 78901234 St. Louis Top-up,3040.88,"Mar 17, 2024",Top-up from Maximilian Senn tens Education,-217.08,"Mar 18, 2024",Top-up Community College Account 78901234 St. Louis Utilities,-120.73,"Mar 18, 2024",SHELL*C16410* PETRO Restaurant,-57.68,"Mar 18, 20 24",UBER*1337 EATS Transportation,-29.81,"Mar 19, 2024",UBER*441* MISSOURI Rent,-63 6.02,"Mar 19, 2024",AIRBNB 14158B00005959 Entertainment,-99.07,"Mar 19, 2024",F ACEBK VMQNIRW2 650-853-5853 Restaurant,-123.63,"Mar 19, 2024",UBER*1337 EATS Shopping,-2 9.02,"Mar 20, 2024",WALMART SUPERCENTER#5831 St. Louis Rent,-2021.94,"Mar 20, 2024&q uot;,AIRBNB 14158B00005959 Education,-869.29,"Mar 21, 2024",Top-up Community College Acco unt 78901234 St. Louis Transportation,-616.82,"Mar 21, 2024",UBER*441* MISSOURI Clothing ,-144.31,"Mar 21, 2024",Trendsetters Closet St. Louis Clothing,-511.82,"Mar 21, 2024 ",Glamour Galore Boutique St. Louis Entertainment,-54.43,"Mar 22, 2024",FACEBK VMQNI RW2 650-853-5853 Clothing,-986.85,"Mar 22, 2024",Glamour Galore Boutique St. Louis Top-u p,5796.08,"Mar 22, 2024",Top-up from Maximilian Senntens Healthcare,-357.81,"Mar 23, 2024",LAARI ADA St. Louis Shopping,-28.08,"Mar 23, 2024",WALMART SUPERCENTER#5831 S t. Louis Education,-40.28,"Mar 24, 2024",Top-up Community College Account 78901234 St. Lo uis Groceries,-41.31,"Mar 24, 2024",GROCERY&GROCERY #8961 St. Louis Clothing,-2200.4 9,"Mar 25, 2024",Chic Avenue Apparel St. Louis Education,-31.78,"Mar 25, 2024", Top-up Community College Account 78901234 St. Louis Education,-44.31,"Mar 25, 2024",Top-u p Community College Account 78901234 St. Louis Education,-24.61,"Mar 26, 2024",Top-up Com munity College Account 78901234 St. Louis Groceries,-37.67,"Mar

[…]

Figura 41 - Estratto conto e movimenti di Will

aCropalypse bag

Nella challange precedente era presente un bag molto interessante. Lo spiego qui sotto.

La vulnerabilità, indicata con CVE-2023-21036, consente di **recuperare le informazioni sensibili** che gli utenti hanno eliminato dagli screenshot PNG. Si tratta quindi di un grave problema di privacy, soprattutto se le immagini vengono condivise online o tramite servizi di messaggistica.

Chris Blume, ingegnere del software che ha lavorato per il PNG Working Group, ha scoperto lo stesso bug in *Snipping Tool*. In pratica, sovrascrivendo il file a quello originario, viene **conservata la parte finale.**