WBASNY

The Women's Bar Association of the State of New York

presents

Convention 2021
Continuing Legal Education Series

Trends in Cybercrime

May 21, 2021
10:15 am - 11:15 am

Presenter: Elizabeth Roper, Esq.

TRENDS IN CYBERCRIME

ADA Elizabeth Roper

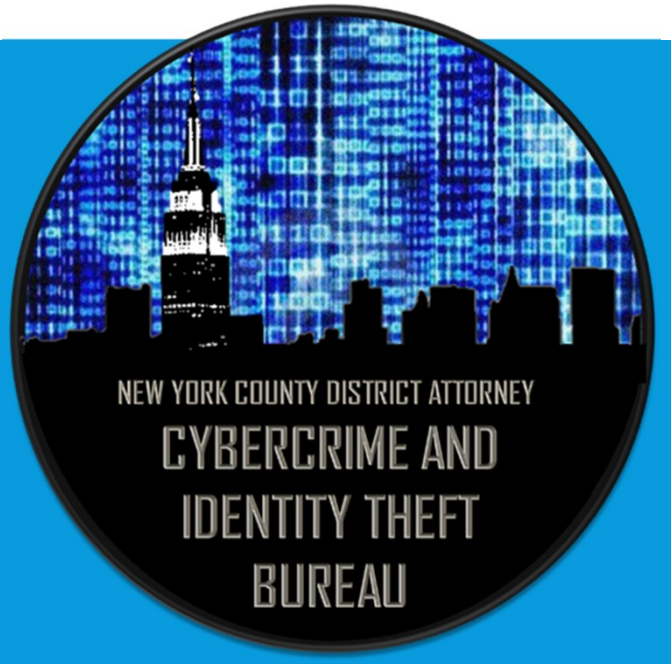
Chief, Cybercrime and Identity Theft Bureau

New York County District Attorney's Office

CYBERCRIME & IDENTITY THEFT BUREAU

- Personnel:
  - Dedicated Assistant District Attorneys
  - Cybercrime Analysts
  - Sworn Investigators
  - Embedded NYPD Detectives
  - High Technology Analysis Unit ("HTAU")
  - Cyber Intelligence Unit ("CIU")

- Investigates and prosecutes:
  - Computer hacking and cyber intrusions
  - Cyber enabled fraud
  - Money laundering
  - Check and credit card fraud rings
  - Child sexual abuse material (CSAM)



CURRENT TRENDS IN CYBERCRIME

- Phishing
  - Business Email Compromise Fraud
- Account Takeovers
  - SIM Swaps
- Ransomware

DA NY

CYBER-ATTACKS

COVID-19 blamed for 238% surge in cyberattacks against banks

Disarray caused by the pandemic has become a breeding ground for financially-motivated attacks.

- 80% of financial institutions surveyed by VMWare reported increase in cyber-attacks in last year.
- 64% of financial institutions reported increased business email compromise attacks
- 25% of financial institutions reported destructive attacks (vs. attacks that seek financial gain).
- Ransomware attacks against financial institutions has increased 9x in 2020 1Q.

PHISHING

- The fraudulent attempt to obtain sensitive information or funds by disguising oneself as a trustworthy entity in an electronic communication:
    - Usernames/Passwords
    - Credit Card Information
    - Money
- Phishing scams range in sophistication from shotgun approach to highly targeted (spear phishing/BECs).
- Not confined to email: text messages, robocalls, mail.

PHISHING

Greetings to you my friend,

I know this will come to you as a surprise because you do not know me.
I am John Alison I work in Central Bank of Nigeria, packaging and courier department.

I got your contact among others from a search on the internet and I was inspired to seek your co-operation, I want you to help me clear this consignment that is already in theEurope which I shipped through our CBN accredited courier agent. The content of the package is $20,000,000.00 all in $100 bills, but the courier company does not know that the consignment contains money.

All I want you to do for me now is to give me your mailing address, your private phone and fax number, and I believe that at the end of the day you will have 50% and 50% will be for me. My identity must not be revealed to anybody.

If this arrangement is okay by you, you can call

Phone: +234 8028776685
Email:john_alison444@yahoo.com

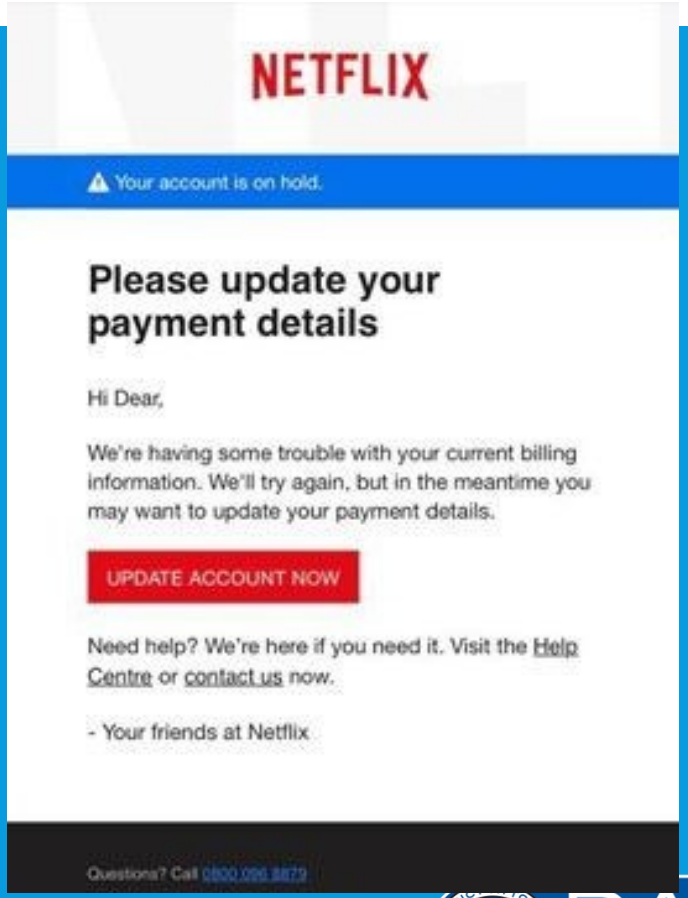
DISTRICT ATTORNEY NEW YORK COUNTY 1685 DA NY

PHISHING

- In 2020, phishing emails and text messages tend to induce recipients to trick an individual into clicking on a link and/or opening an attachment.

- Popular phishing tactics:

  - "We have noticed some suspicious activity on your account."
  - "We have noticed there's an issue with your payment information."
  - Include fake invoices.
  - Include links to make payments.



PHISHING

amazon

Your Amazon account has been locked

Dear customer,

We have locked your Amazon account because our service detected two unauthorized devices. Our service has protected your account from someone who has accessed your Amazon account from another devices and locations.

Before someone can change your account information or order some item with your credit / debit card bill. For your security, we have locked your Amazon account.

To continue using your account again, we advise you to update the infomation before 24 hours or your account will be Permanently locked.

How do I unlock my account?

You need to verify your Amazon account and complete the data information that has been printed on your account when you first registered.

Amazon service

Mon 3/25/2019 10:19 AM

Stripe <Stripe1111@patrica.hostpilot.com>

Stripe : deposit will not be made to your bank account

7:27

Text Message
Today 5:56 PM

Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: e3fmr.info/onAyXsVfomA

DISTRICT ATTORNEY NEW YORK COUNTY 1685 DA NY

PHISHING/BEC 2019 STATISTICS

- 88% of companies reported experiencing spear phishing campaigns.
- 38% of untrained users fail phishing tests.
- 1/3rd of all data breaches involve phishing.
- The average data breach costs $3.5 million.

BUSINESS EMAIL COMPROMISE

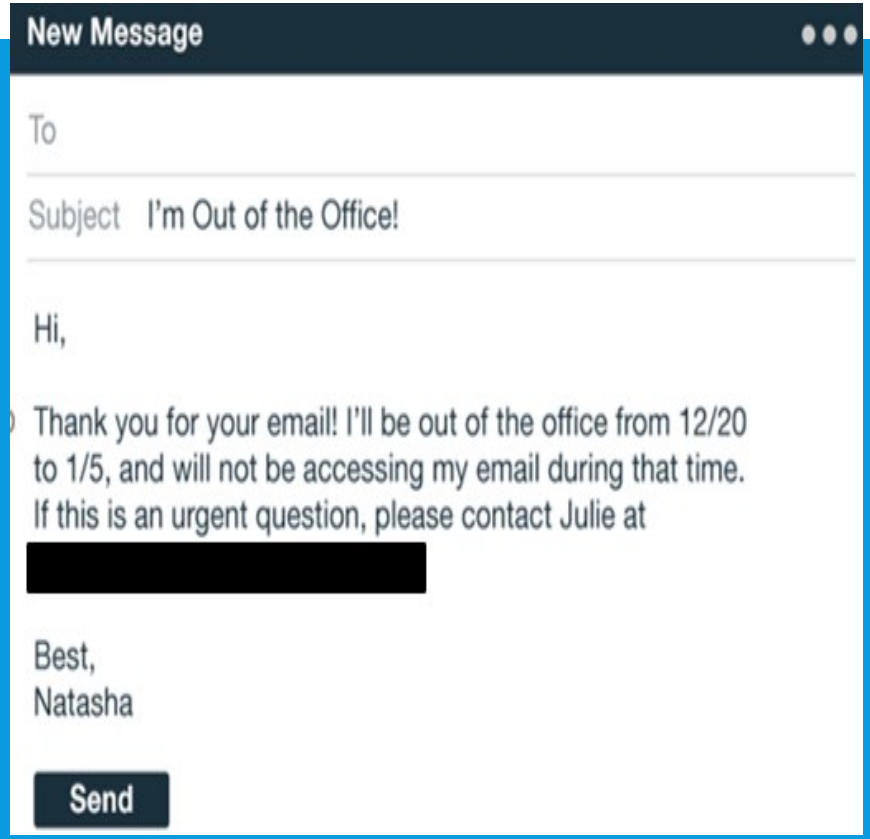
- IC3 received 467,361 complaints (that's about 1,300/day) for about $3.5 billion in losses.
- Phishing/BECs were a fraction of the total complaints (apprx. 24,000 complaints) yet amounted to more than $1.7 billion in losses ($75k/complaint)

BUSINESS EMAIL COMPROMISES

- Directed emails sent for the purpose of tricking the recipient out of money.
- Two main forms:
  - "Spear-phishing" is the targeted sending of emails to employees responsible for, or have control over, money transfers.
  - Breach of email account leading to interception.
- The success (and failure) of ALL of these campaigns turns on the people who receive the emails.

BUSINESS EMAIL COMPROMISES: SPEAR PHISHING

- Emails frequently occur when the executive is out of the office
  - Can be determined by a phone call to the executive or by an automatic “out-of-office” email reply
- Transaction is often marked or treated as “confidential” or “urgent” by the sender.



BUSINESS EMAIL COMPROMISES: SPEAR PHISHING

- Employee who is responsible for money transfers receives a seemingly legitimate email instructing a transfer of funds.
- "Sender" of the transfer-request email is often a high level executive within the company.
- The impersonation can take hours, days, or even weeks.

BUSINESS EMAIL COMPROMISES: SPEAR PHISHING

On Mar 30, 2017, at 11:11 AM, Orson [redacted] <dvcote1300@gmail.com> wrote:

Deb ,

Can we get a wire transfer out before the cut off time?

Orson

Sent from my U.S. Cellular® Smartphone

On Thu, Mar 30, 2017 at 11:16 AM, Renwick [redacted] <renwick@[redacted]com> wrote:

Orson,

Did you intend to send the message below to Deb Velazquez or to another person named Deb?

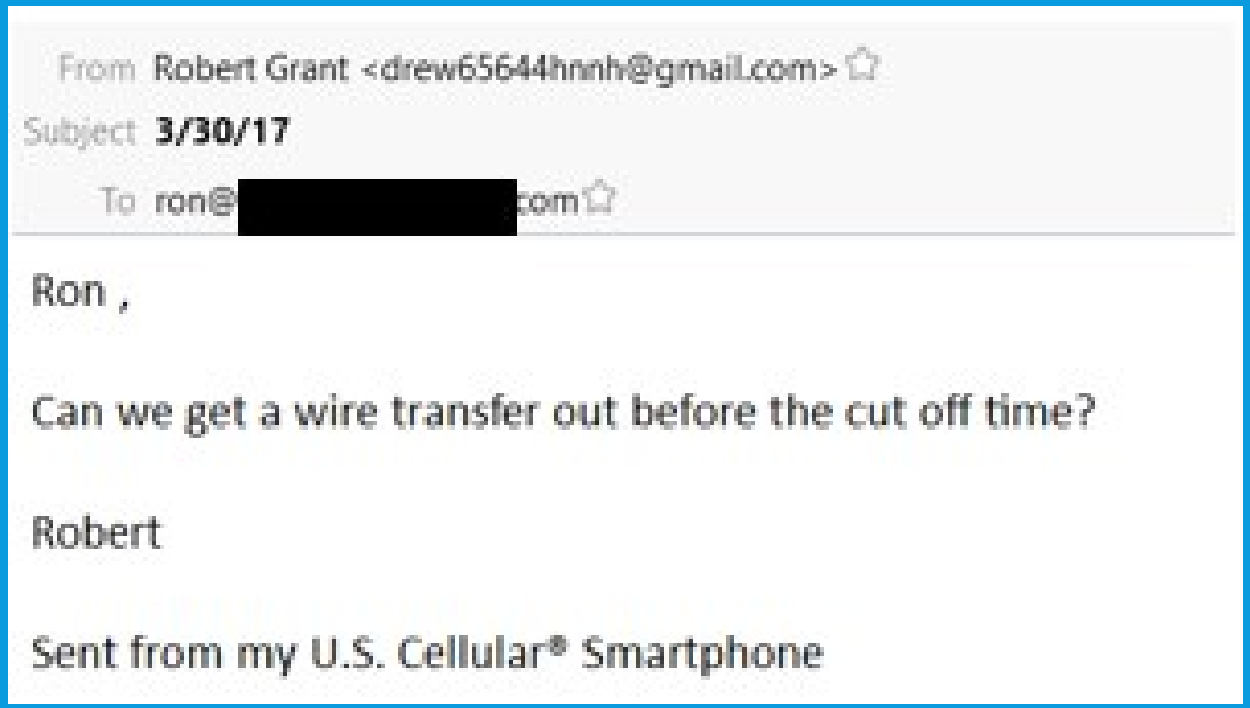
On Mar 30, 2017, at 11:19 AM, Orson [redacted] <dvcote1300@gmail.com> wrote:

I sent it to Deb Velazquez , Who will be able to process a wire transfer for me right now?

Orson

Sent from my U.S. Cellular® Smartphone

BUSINESS EMAIL COMPROMISES: SPEAR PHISHING



From Robert Grant <drew65644hnnh@gmail.com>

Subject **3/30/17**

To ron@[redacted]com

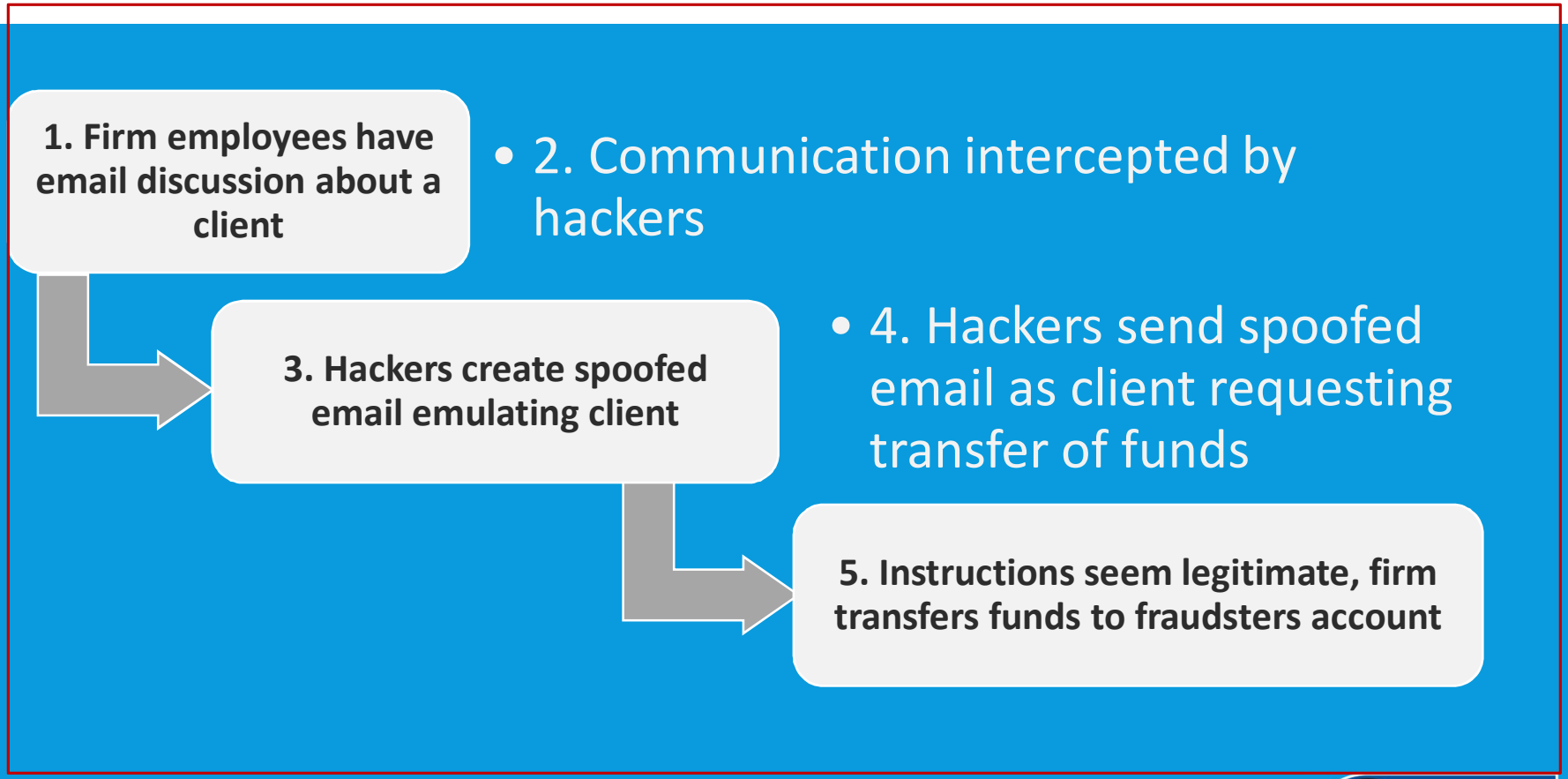
Ron ,

Can we get a wire transfer out before the cut off time?

Robert

Sent from my U.S. Cellular® Smartphone

BUSINESS EMAIL COMPROMISES: BREACHES



BUSINESS EMAIL COMPROMISES: BREACHES

From: "barbara colantuoni" <barbara.colantuoni@mmi.it>
Subject: R: Payment's schedule
Date: July 20, 2016 at 1:58:19 PM EDT
To: tiernan@[redacted]
Reply-To: "barbara colantuoni" <barbara.colantuoni65@gmail.com>

Sorry to bothering you again. I have just received a notice from out audit department that they started audit on our Unicredit bank account. There, payment should be made into our other bank details below.

BENEFICIARY NAME:	DUEMMEI SRL
BANK NAME:	BARCLAYS BANK PLC
ACCOUNT NUMBER:	[redacted]
SORT CODE:	20-25-19
IBAN:	GB66BARC20251960215759
SWIFT BIC CODE:	BARCGB22
BANK ADDRESS:	ROMFORD 3 , LEICESTER LE87 2BB. UK

Can you please relate this to your account department and advise on when possible payment will be made.

Looking forward to hearing from you soon as soon as payment is made.

Best Regards
Barbara Colantuoni
Accounting & Credit Control Dpt.

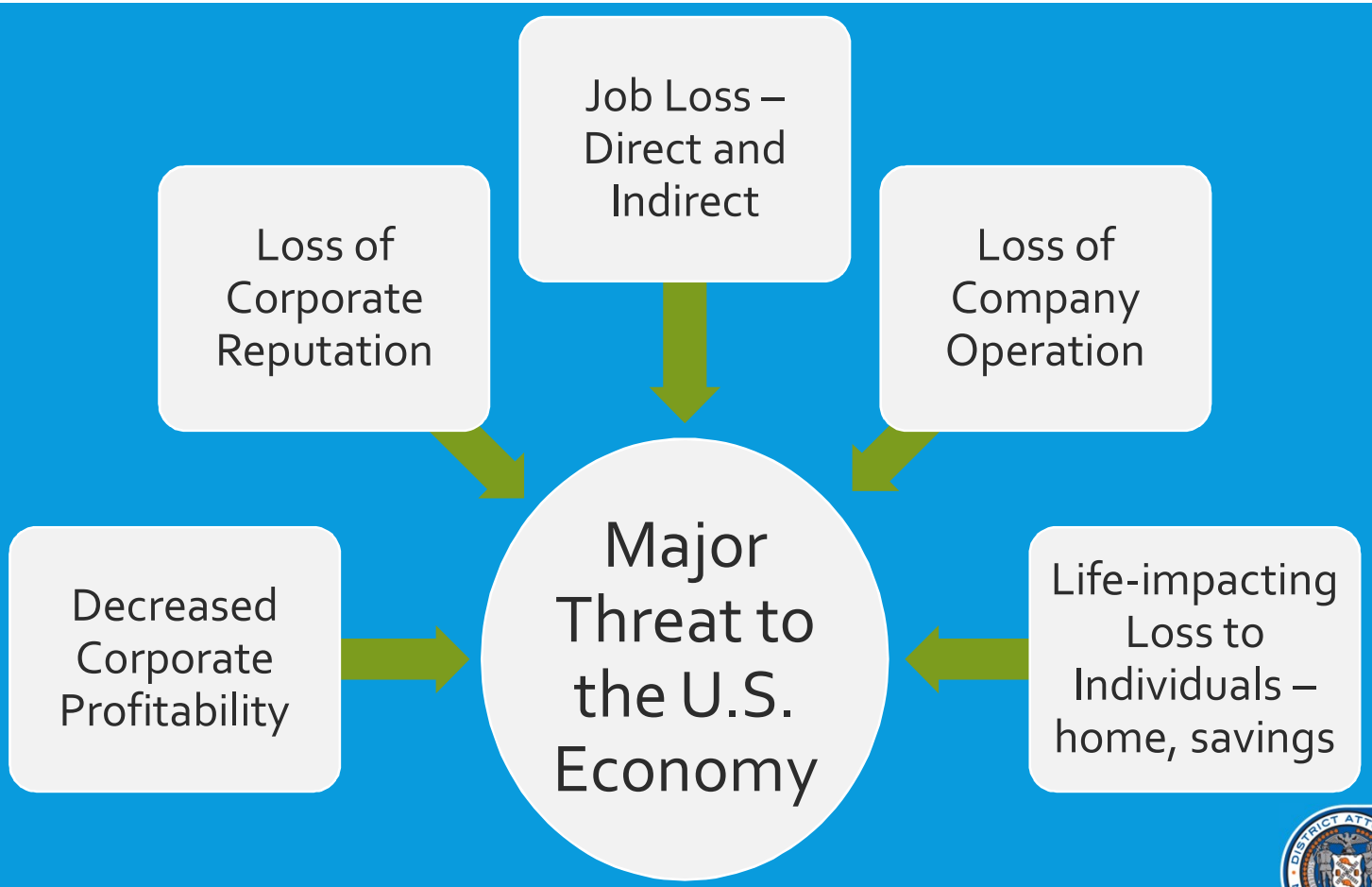
BUSINESS EMAIL COMPROMISES:
SPOOFING A NAME

Reverse Whois results for [redacted]@gmail.com

There are 13 domains that matched this search query.
These are listed below:

Domain Name	Creation Date	Registrar
7thwavelebs.com	2017-01-09	DOMAIN.COM, LLC
biocepit.com	2017-01-09	DOMAIN.COM, LLC
envyrnedical.com	2017-01-09	DOMAIN.COM, LLC
hospiceeastbay.org	2017-01-09	DOMAIN.COM, LLC
humanlongavity.com	2017-01-09	DOMAIN.COM, LLC
pacerunners.com	2017-02-11	DOMAIN.COM, LLC
postsky.org	2018-01-02	NETWORK SOLUTIONS, LLC
proteebio.com	2017-01-09	DOMAIN.COM, LLC
providiernmedical.com	2017-01-09	DOMAIN.COM, LLC
sgrnh.org	2017-01-09	DOMAIN.COM, LLC
spectrumrnedical.com	2017-01-09	DOMAIN.COM, LLC
vectre-corp.com	2017-01-09	DOMAIN.COM, LLC
vibrahaelthcare.com	2017-01-09	DOMAIN.COM, LLC

EFFECTS OF BECs



ADVANCED PAYLOAD
RANSOMWARE/MALWARE

- Emails sent by seemingly friendly contacts with attachments and/or links.

- Can lead to the installation of malware, that is then used to:
  - Give the bad actor access to the computer or network,
  - Allow the bad actor to use the computer to launce malicious attacks, and
  - Allow the bad actor to use the computer to perpetuate fraud campaigns.

ADVANCED PAYLOAD
RANSOMWARE/MALWARE

From: Andrew [redacted] <a[redacted]@gmail.com>
Date: January 30, 2018 at 1:28:30 PM EST
To: chris[redacted]@mac.com
Subject: Follow up
Reply-To: a[redacted]@comcast.net

Hi,

Hope you are doing great!

I just wanted to check if you received my previous email with the documents and got a chance to review them.

If you did not receive it here it is again. CLICK HERE TO VIEW DOCUMENTS and sign in to view the attachment.

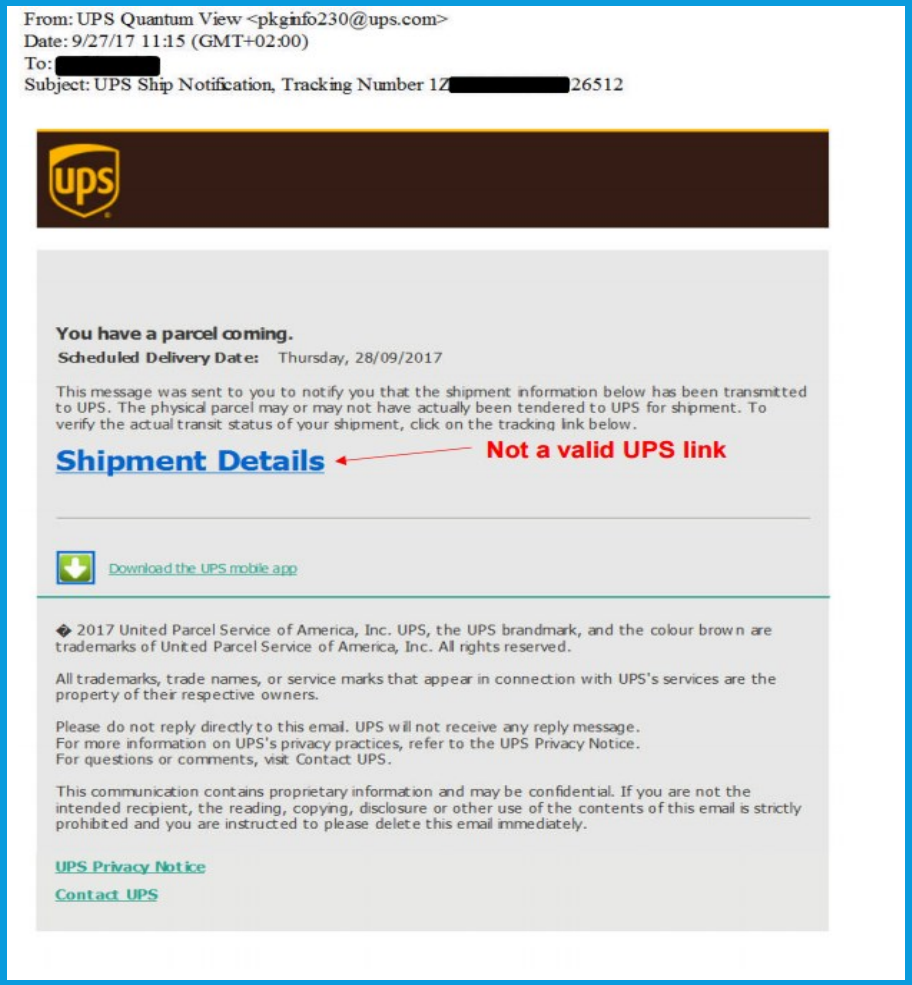
Hope it works.

Your response will be greatly appreciated.

Andrew

ADVANCED PAYLOAD

OBTAINING NETWORK ACCESS



From: UPS Quantum View <pkginfo230@ups.com>
Date: 9/27/17 11:15 (GMT+02:00)
To: [redacted]
Subject: UPS Ship Notification, Tracking Number 1Z[redacted]26512

You have a parcel coming.

Scheduled Delivery Date: Thursday, 28/09/2017

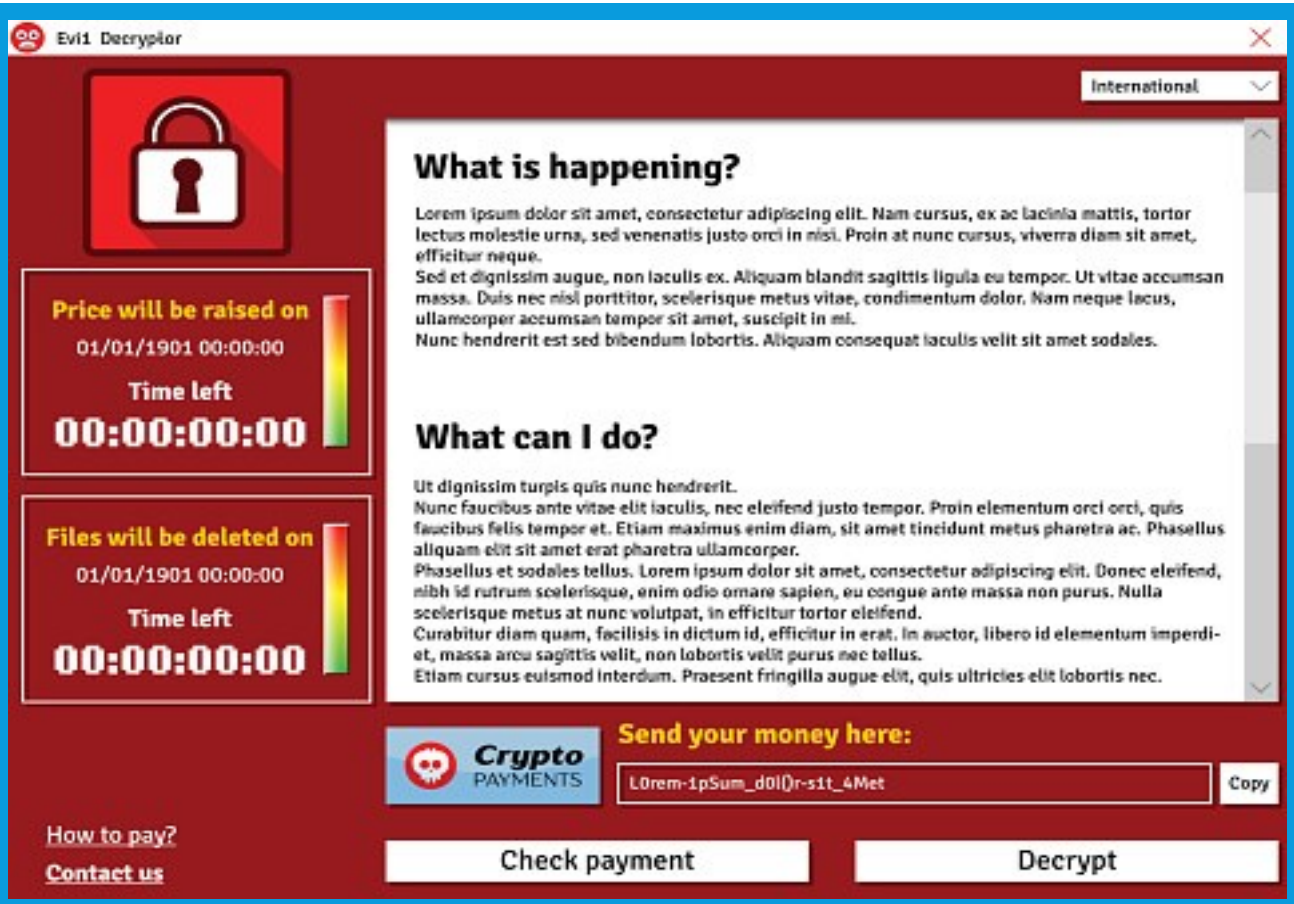
This message was sent to you to notify you that the shipment information below has been transmitted to UPS. The physical parcel may or may not have actually been tendered to UPS for shipment. To verify the actual transit status of your shipment, click on the tracking link below.

Shipment Details ← Not a valid UPS link

Download the UPS mobile app

Source; UPS

ADVANCED PAYLOAD
RANSOMWARE



ADVANCED PAYLOAD
RANSOMWARE

ADVANCED PAYLOAD
RANSOMWARE/MALWARE

- Average Initial Demand is $377,000
- Approximately $11.5 billion in damages in 2019
- Average cost of ransomware is $8.1 million
- Average days to recover: 287

ADVANCED PAYLOAD
RANSOMWARE/MALWARE

NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs

The shipping giant has suffered millions of dollars in damage due to the ransomware attack.

Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts

By IAN DUNCAN
THE BALTIMORE SUN | MAY 29, 2019 AT 7:45 PM

Ransomware is taking a toll on banks. Here's how they're fighting back

A recent rash of ransomware attacks on bank technology vendors — including Finastra, Diebold Nixdorf, Cognizant and Pitney Bowes — raises serious questions about why they're happening and what banks can do to protect themselves.

DA NY

ACCOUNT TAKEOVER: SIM SWAPPING FRAUD

Florida Teenager Is Charged as 'Mastermind' of Twitter Hack

The authorities arrested a 17-year-old who they said ran a scheme that targeted the accounts of celebrities, including former President Barack Obama and Elon Musk. Two others were also charged.

MOTHERBOARD
TECH BY VICE

The SIM Hijackers

The New York Times

Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too.

In August of last year, for example, hackers hijacked the Instagram account of Selena Gomez and posted nude photos of Justin Bieber. The first name on Gomez's account name was also changed to "Islah", identical to that used at the time by someone on OGUSERS who went by the username Islah. According to hackers in OGUSERS, the people claiming to be behind the Gomez hack said they did so by taking over the cell phone number associated with the singer-actress's Instagram account, which had 125 million followers when it was seized.

Europol, along with local police in Spain, Romania and Austria, arrested about two dozen alleged members of two criminal gangs that are accused of stealing millions in euros from bank accounts in several countries by using SIM swapping techniques to steal credentials and passwords.

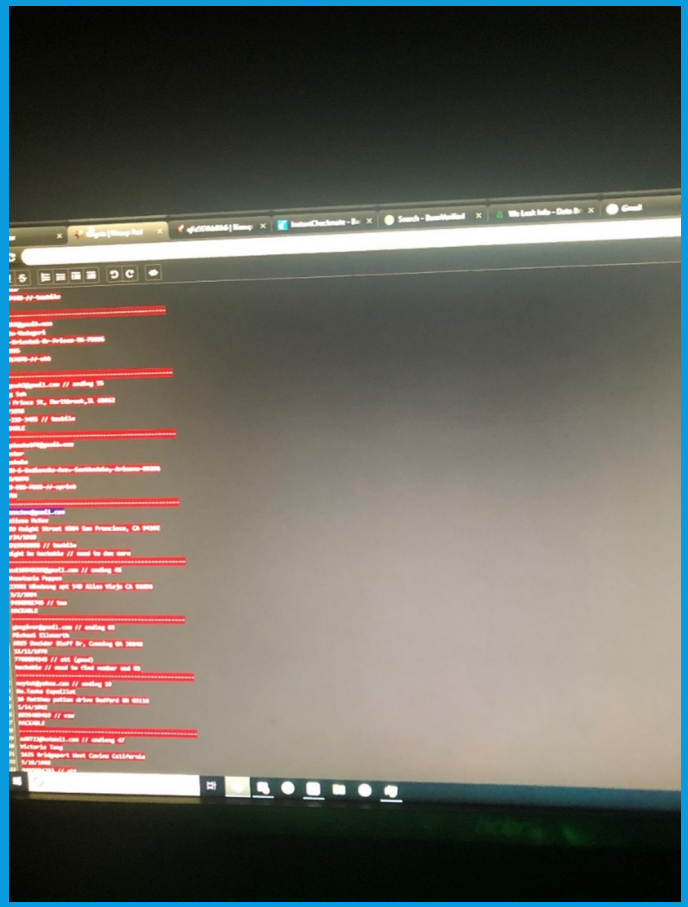
SIM swapping scams exploit the recent proliferation of SMS-based two-factor authentication. By intercepting text messages containing security codes, perpetrators are able to gain access to the victim's accounts.

DISTRICT ATTORNEY NEW YORK COUNTY 1635 DA NY

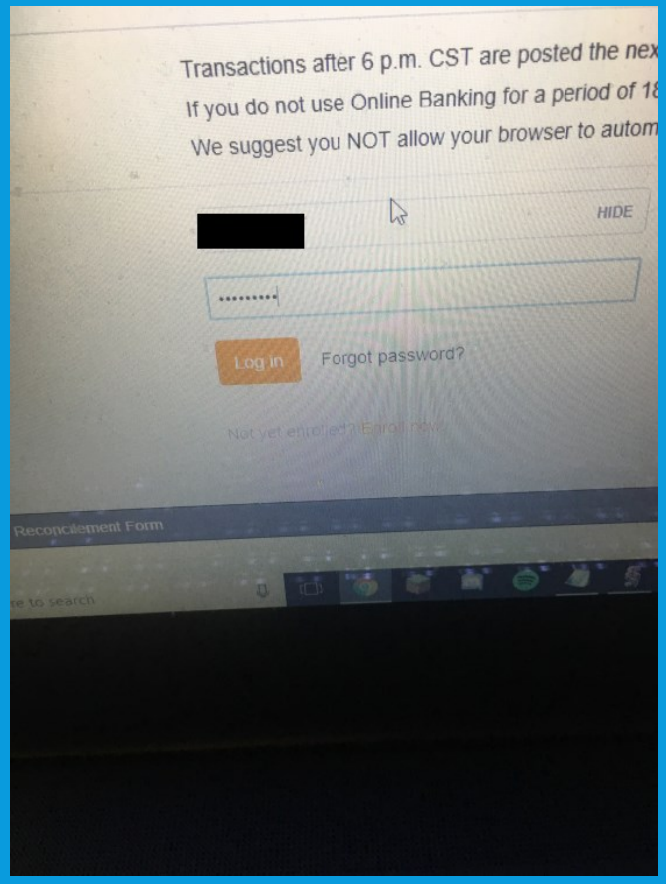
SIM SWAP SCHEME: OBTAIN CREDENTIALS FOR POTENTIAL VICTIMS

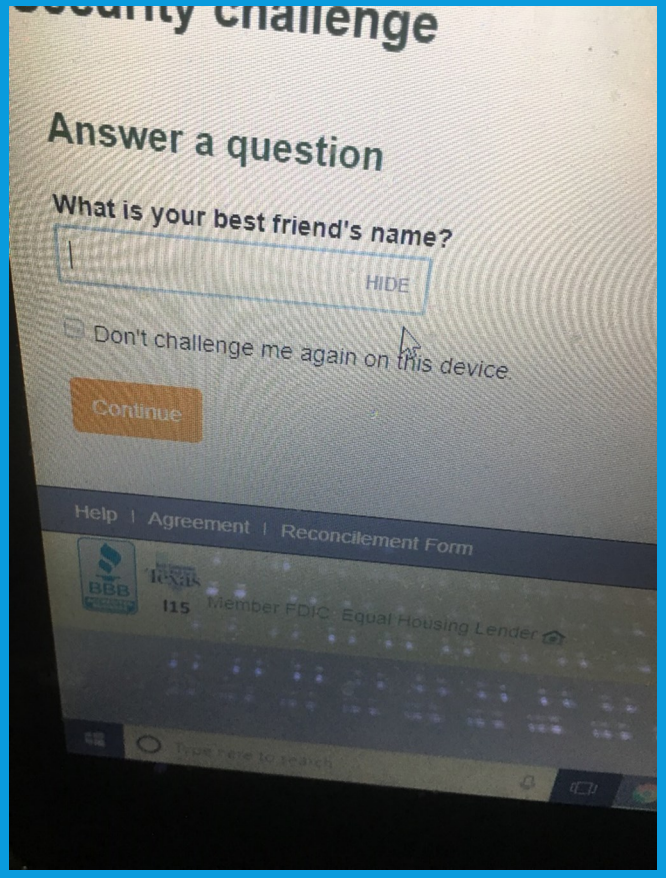
```
Hacker Shit!

Finished Targets:
---------------------------
Name: [redacted]
Phone: [redacted]3495
Emails:
[redacted]@gmail.com
---------------------------
Name: [redacted]
Phone: [redacted]0401
Pin: [redacted] att
Email:
[redacted]@gmail.com
---------------------------
Name: [redacted]
Phone: [redacted]4627 (T-Mobile)
Emails:
[redacted]@gmail.com
[redacted]@yahoo.com
---------------------------
Name: [redacted]
---------------------------
Name: [redacted]
Phone: [redacted]-4032
Pin: [redacted]
Emails:
[redacted]@gmail.com
---------------------------
Name: [redacted]
Phone: [redacted]-8373
Emails:
[redacted]gmail.com
---------------------------
Name: [redacted]
Phone: [redacted]1866
Pin: [redacted]
Emails:
[redacted]gmail.com
---------------------------
Name: [redacted]
Phone: [redacted]8605
Emails:
```

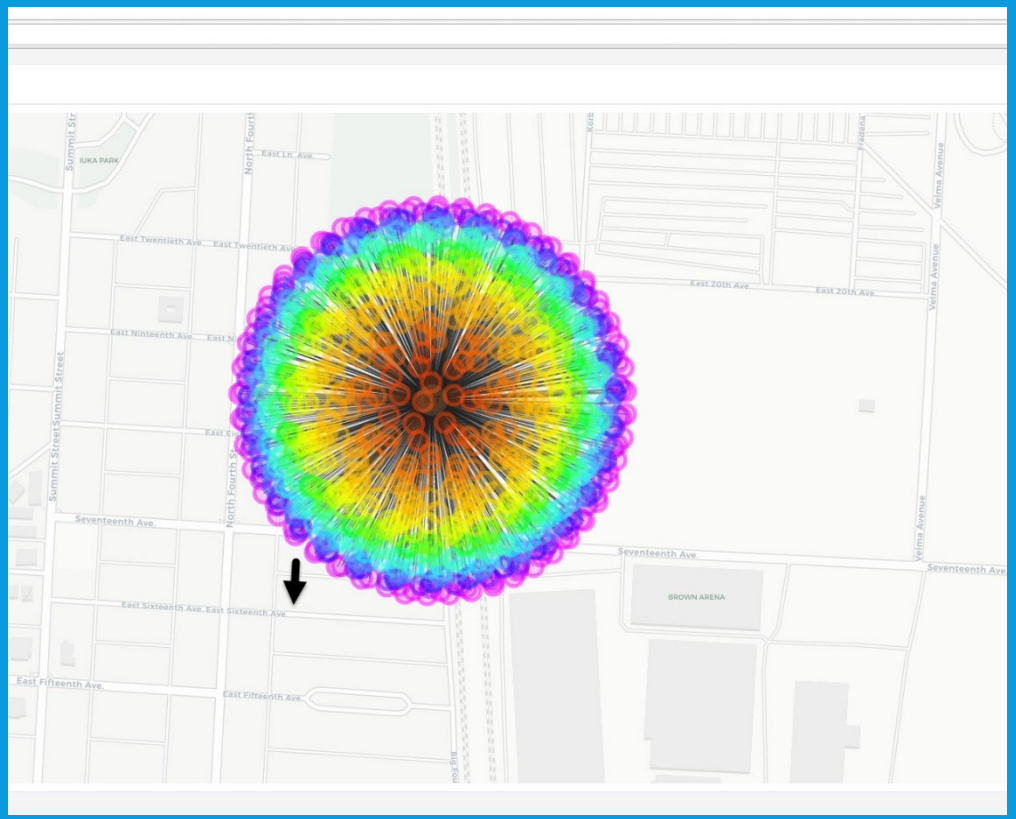


SIM SWAP SCHEME: CHANGE PASSWORDS TO LOCK VICTIMS OUT OF ACCOUNTS



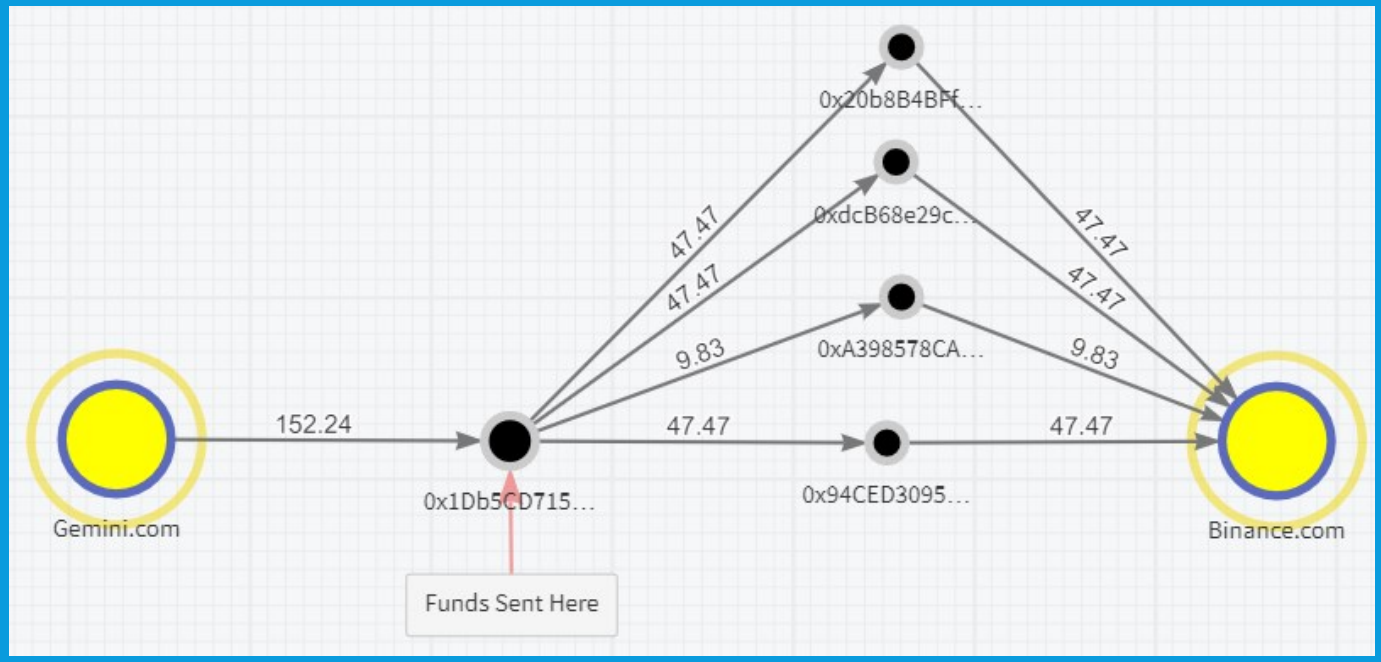


SIM SWAP FRAUD: INVESTIGATING THE CRIME



Cell site information from AT&T revealed one cell tower located in Columbus, Ohio, which handled the majority of communications from both suspected IMEIs.

SIM SWAP FRAUD: INVESTIGATING THE CRIME



Tracking the movement of the stolen cryptocurrency can be extremely difficult if the funds do not interact with a known exchange or merchant.

CALL US

Elizabeth Roper
Cybercrime & Identity Theft Bureau
vinocurj@dany.nyc.gov | (212) 335-9624