Lizzie McGowan

Real Estate Deals: The New Frontier in Business Email Compromise

In and outside of the business world, traditional phishing emails have caused significant financial damage. However, there is a new kind of business email compromise gaining in popularity: "real-estate business email compromise." This phishing technique has caused $675 million in losses for its victims, and illustrates the unrelenting nature of cyber criminals in innovating fraudulent activity.

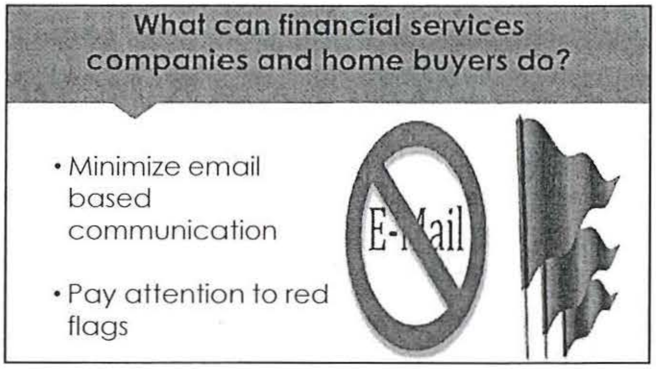
Real-estate business email compromise is an appealing and lucrative form of business email compromise because it involves large sums of money, specifically down payments for property. Unlike traditional business email compromise, this method does not involve the use of altered domain names, compromised links, or attached malware. Instead, it takes advantage of the relationship formed between the real-estate agent, the lending officer, the escrow agent, and the client.

Put simply, this is just an advanced form of wire fraud that uses enhanced phishing techniques designed to take over accounts to trick customers into sending their down- payments into the criminal's bank accounts. To do this, the fraudster will assume the identity of the title company representative or real-estate agent conducting the sale. To make the emails as convincing as possible they spoof the email address of the escrow officer or agent and include as much relevant personal information to make it seem convincing. Next, they send an email to the buyer giving wire instructions to the fraudsters bank account instead of the title company's legitimate account. In cases where there has been an actual email account takeover, the hacker will patiently and inconspicuously monitor the progress of the transaction. When the time is right, they will enter the conversation and proceed with giving the client wiring instructions to send money to the criminals' accounts. Unfortunately, once the money is sent, it is impossible to get it back.

By nature, criminals are shrewd and convincing. Since homebuyers are optimistic and excited about the purchase of their new homes, they are easily manipulated and overlook red flags. Therefore, the best practices for employers and homebuyers are to avoid email-based communication or follow-up with a phone call. Additionally, a verbal code phrase should be established for voice and text communications that is only known between the two legitimate parties. But they need to remember that this phrase should *never* be emailed. Verification of all requests for a change in payment type and/ or account information should be communicated through at least two channels. An additional legitimate phone number from the real estate agent or lending officer that is not in the email should be provided to the customer. This should be done in conjunction with two-factor authentication (arranged early in the relationship) and not through email.

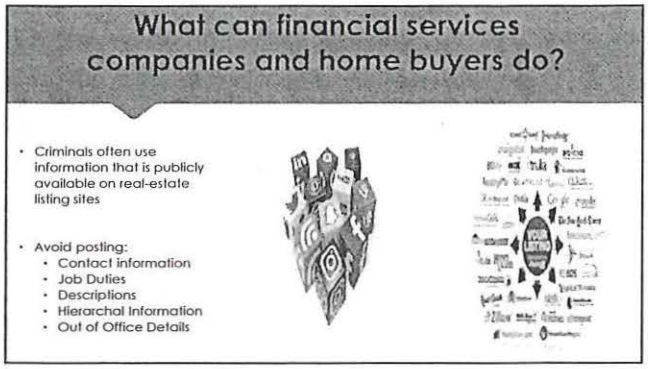
Employees should also keep all software updated. Mortgage professionals should stay abreast of constantly evolving phishing schemes to improve their company's cyber security measures. Homebuyers must also be educated as to how these schemes work so they can be on alert when asked to wire money.

If you discover a fraudulent transfer, immediately contact your local FBI office and report it to www.iC3.gov Notifying law enforcement helps gather intelligence and enables law enforcement to disrupt future scams.



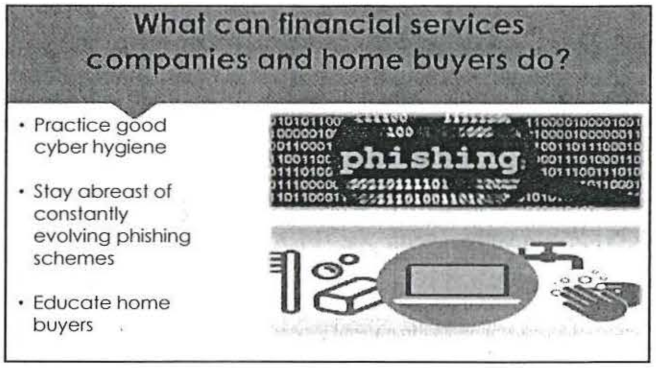
What can financial services companies and home buyers do?

- Minimize email based communication
- Pay attention to red flags



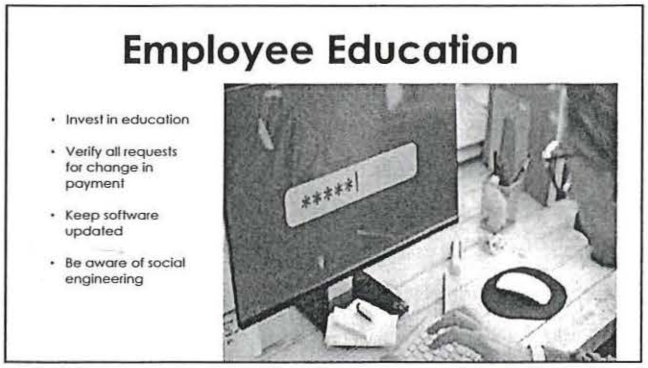
What can financial services companies and home buyers do?

- Criminals often use information that is publicly available on real-estate listing sites
- Avoid posting:
  - Contact information
  - Job Duties
  - Descriptions
  - Hierarchal Information
  - Out of Office Details



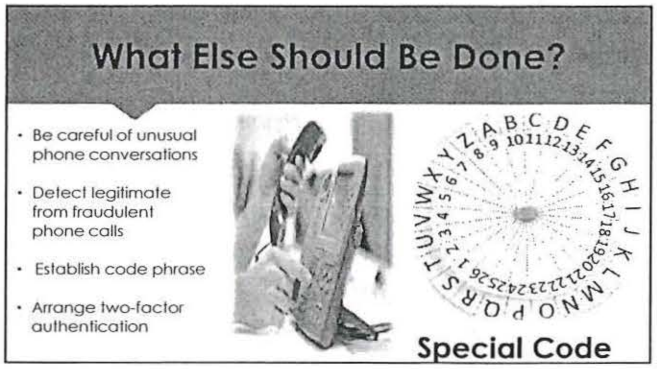
What can financial services companies and home buyers do?

- Practice good cyber hygiene
- Stay abreast of constantly evolving phishing schemes
- Educate home buyers



Employee Education

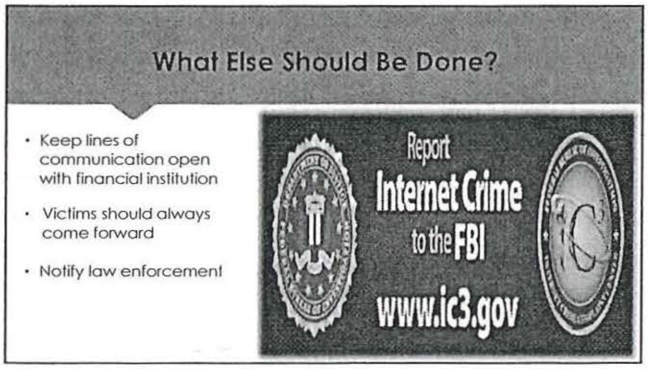
- Invest in education
- Verify all requests for change in payment
- Keep software updated
- Be aware of social engineering



What Else Should Be Done?

- Be careful of unusual phone conversations
- Detect legitimate from fraudulent phone calls
- Establish code phrase
- Arrange two-factor authentication

Special Code



What Else Should Be Done?

- Keep lines of communication open with financial institution
- Victims should always come forward
- Notify law enforcement

Conner Freeman, CFCS

Operation Ababil: The Iranian Cyber-attacks Against the United States

What is Distributed Denial of Service (DDoS)?

- **Type of cyber-attack in which a criminal attempts to overload a network or system to prevent it from its normal or intended operations**
    - DDoS overwhelms available bandwidth, CPU, and RAM capacity
    - Causes reduction in operating speeds and crashes
- **The attack is facilitated through multiple computers and directed at a single target**
    - Difficult to stop traffic coming from diverse origins

How is DDoS done?

- **DDoS attacks are done in three stages**
    - **Recruiting**
        - Commandeering remote control of computers and servers via malware
            - A compromised network is called a *botnet*
    - **Propagation**
        - Using worms to spread the attack code among the compromised computers
        - Essentially, this code is telling the botnet when, where, and how it will attack
    - **Attack**
        - Sending requests, queries, etc. from across the botnet to a single victim

What Happened in the Operation Ababil Case?

- **The United States financial sector suffered a seven-month DDoS attack from an actor in Iran**
    - The attack was claimed by hacktivist group Qassam Cyber Fighters
    - Disrupted and crashed websites of nine large US banks
- **US Intelligence community has attributed the attack to the state of Iran, using Qassam as a front**

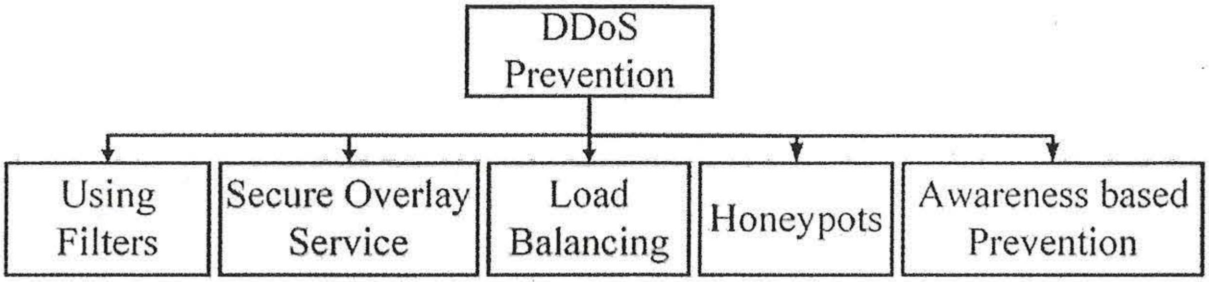
How does DDoS threaten the financial sector?

- **DDoS attacks are growing in sophistication, and being used in conjunction with other cyber and financial crimes**
    - **Encrypted DDoS** – Sending encrypted requests demands more network capacity
    - **DDoS with Ransomware** – Using the threat of DDoS as incentive to pay a ransom
    - **DDoS as a diversion** – Using DDoS as a diversion of resources/attention in order to facilitate a more threating attack
    - **Fintech evolution** – As more of the US financial sector moves online, the ability to access those networks becomes more critical

How can we protect ourselves?

- **Prevention procedures**
    - **Filtering** – Filtering traffic based on IP address and metadata
    - **Security overlays** – Distributed firewalls that allow only trusted traffic
    - **Honeypots** – Less secures networks to attract DDoS attacks from functional network
    - **Load balancing systems** – Distribution of workload across multiple network channels
    - **Awareness** - Proper policy and procedures to respond to DDoS, with a culture of awareness

Prevention



DDoS Prevention

Using Filters

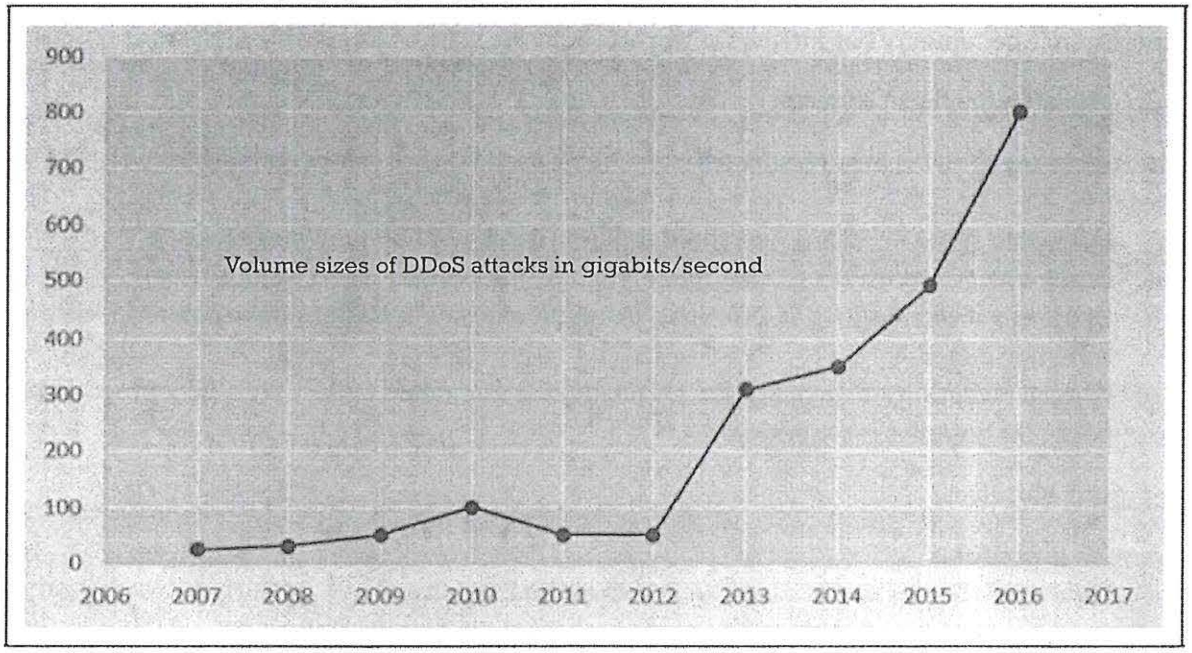
Secure Overlay Service

Load Balancing

Honeypots

Awareness based Prevention

EVOLUTION OF DDOS ATTACKS



This Photo by Unknown Author is licensed under CC BY-NC-ND

Mark A. Leon-Guerrero Jr.

Mobile Payments Fraud

What are mobile payments?

- **Mobile payments refer to any sort of transaction that occurs through the use of a mobile device.** Some examples include:
  - Paying with your phone at the register (Apple Pay, Android Pay,etc.)
  - Using a mobile application to pay for a transaction (Uber, Starbucks, etc.)
  - Online shopping (Amazon, eBay, etc.)

What is mobile payments fraud?

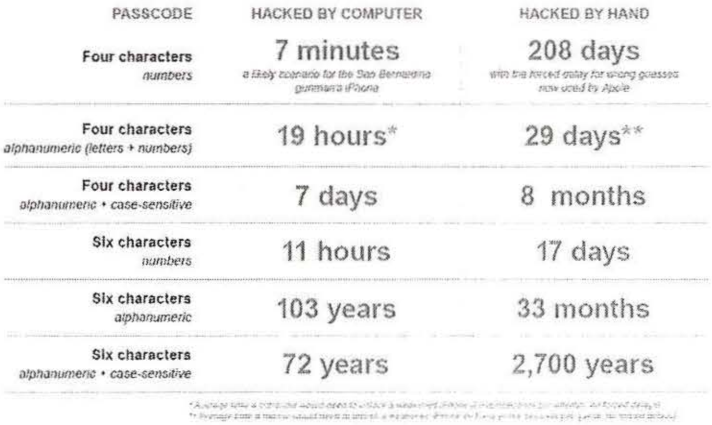
- **Mobile payment fraud refers to "any false or illegal transaction that can happen on the internet or through your mobile phone"[1]**. Common examples include:
  - Card-not-present transactions (card number used online)
  - Spoofed card number (skimmed number, card added to a mobile wallet that is not yours, etc.)

How does it happen?

- Fraud can occur in a number of ways. Some examples include:
  - Credit card numbers are bought or stolen on the dark web
  - Lost/stolen mobile devices
  - Insufficient security measures (on devices themselves or at the point of sale)

How can you better protect yourself against fraud?

- Steps to take:
  - Secure your mobile device to protect it in the event that the device is lost or stolen. **The best type of security is a combination of an alphanumeric password and biometrics (if available).**



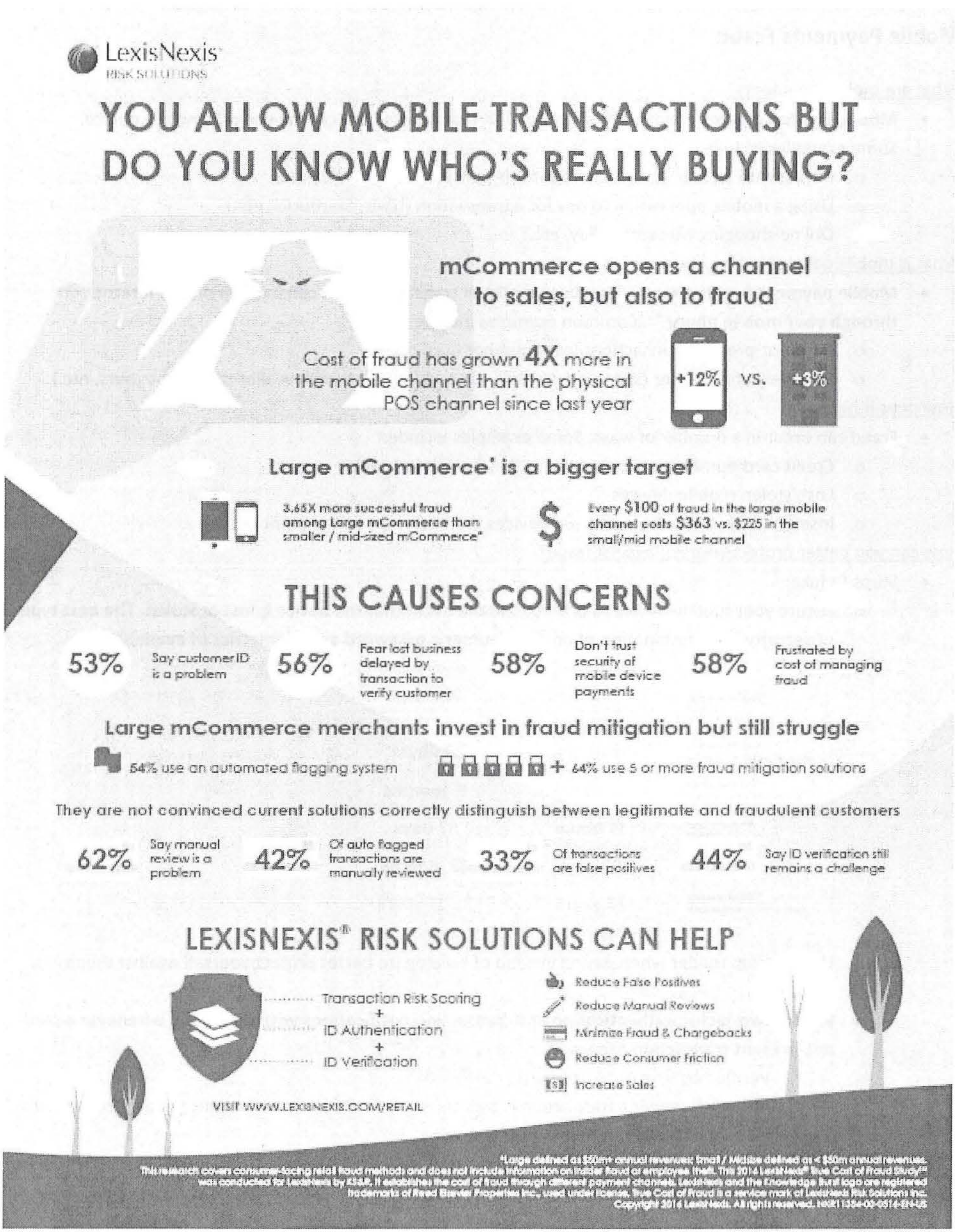
PASSCODE	HACKED BY COMPUTER	HACKED BY HAND
Four characters *numbers*	7 minutes *a likely scenario for the San Bernardino gunman's iPhone*	208 days *with the forced delay for wrong guesses now used by Apple*
Four characters *alphanumeric (letters + numbers)*	19 hours*	29 days**
Four characters *alphanumeric + case-sensitive*	7 days	8 months
Six characters *numbers*	11 hours	17 days
Six characters *alphanumeric*	103 years	33 months
Six characters *alphanumeric + case-sensitive*	72 years	2,700 years

* [illegible]
** [illegible]

  - Use the chip reader when paying instead of swiping (to better protect yourself against skimming devices)
  - **Enable two-factor authentication and transaction notifications with your bank whenever a card-not-present transaction occurs**
    - Verified by Visa or Mastercard SecureCode
    - Alerts whenever a transaction is over a certain limit, card-not-present transactions, used at locations that are not typical for you, etc.)

[1] https://securionpay.com/blog/what-is-a-payment-fraud/

Mark A. Leon-Guerrero Jr.



LexisNexis
RISK SOLUTIONS

YOU ALLOW MOBILE TRANSACTIONS BUT DO YOU KNOW WHO'S REALLY BUYING?

mCommerce opens a channel to sales, but also to fraud

Cost of fraud has grown 4X more in the mobile channel than the physical POS channel since last year

+12% VS. +3%

Large mCommerce* is a bigger target

3.65X more successful fraud among Large mCommerce than smaller / mid-sized mCommerce*

Every $100 of fraud in the large mobile channel costs $363 vs. $225 in the small/mid mobile channel

THIS CAUSES CONCERNS

53% Say customer ID is a problem

56% Fear lost business delayed by transaction to verify customer

58% Don't trust security of mobile device payments

58% Frustrated by cost of managing fraud

Large mCommerce merchants invest in fraud mitigation but still struggle

54% use an automated flagging system

+ 64% use 5 or more fraud mitigation solutions

They are not convinced current solutions correctly distinguish between legitimate and fraudulent customers

62% Say manual review is a problem

42% Of auto flagged transactions are manually reviewed

33% Of transactions are false positives

44% Say ID verification still remains a challenge

LEXISNEXIS® RISK SOLUTIONS CAN HELP

Transaction Risk Scoring
+
ID Authentication
+
ID Verification

Reduce False Positives

Reduce Manual Reviews

Minimize Fraud & Chargebacks

Reduce Consumer Friction

Increase Sales

VISIT WWW.LEXISNEXIS.COM/RETAIL

*Large defined as $50m+ annual revenues; Small / Midsize defined as < $50m annual revenues. This research covers consumer-facing retail fraud methods and does not include information on insider fraud or employee theft. This 2014 LexisNexis® True Cost of Fraud Study℠ was conducted for LexisNexis by KS&R. It establishes the cost of fraud through different payment channels. LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. True Cost of Fraud is a service mark of LexisNexis Risk Solutions Inc.

Copyright 2014 LexisNexis. All rights reserved. NXR11354-02-0514-EN-US

Monica Methe

APT = Advanced Persistent Threat: A cyber group that is an uninvited intruder in a system with sophisticated tools, techniques and procedures. It has a clear purpose and objective, which is usually to exfiltrate data. In the case of APT 38, they are after money.

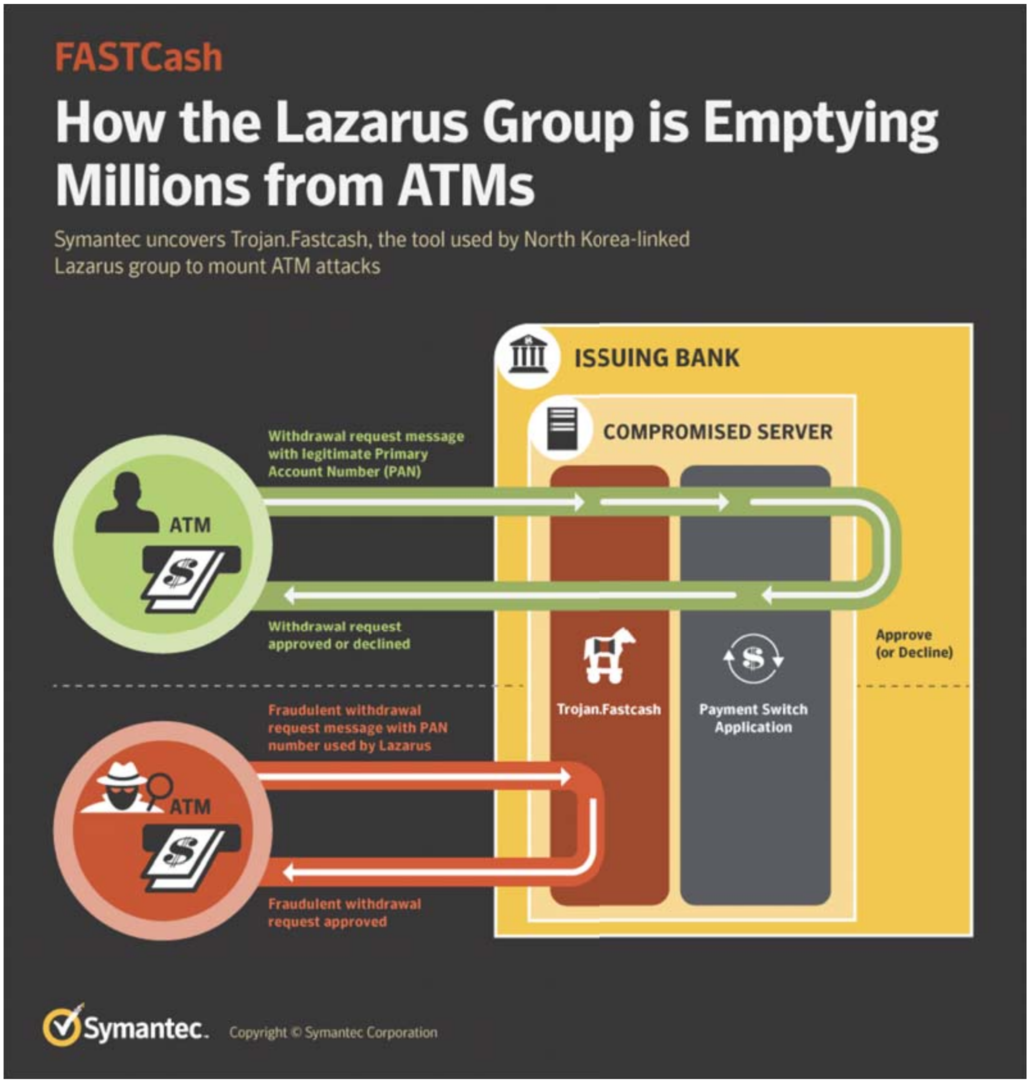
- APT38 is most likely a North Korean cyber criminal group (some refer to them as the Lazarus Group or Hidden Cobra)
    - ➢ At least 5 cryptocurrency exchanges have been attacked -> estimated $571 million was stolen
- North Korea is most likely responsible for FASTCash attacks (see image on back)
- APT38 pulls off cyber bank heists
    - ✧ Vietnam TP Bank (December 2015)
    - ✧ Bangladesh Central Bank (February 2016)
    - ✧ Far Eastern International Bank in Taiwan (October 2017)
    - ✧ Bancomext (January 2018)
    - ✧ Banco de Chile (May 2018)
- Since 2013, North Korea continues to build its nuclear program, which has resulted in 6 United Nations Security Council Resolutions imposing financial and trade sanctions (timeline available on the back)

APT38 bank Heist Characteristics:
APT38 researches its victims very thoroughly, is very well timed in their execution of the heist, and very good at wiping their footprints – they are very good at cleaning up after the heist.

APT38 Cyber Bank Heist Phases (as identified by FireEye’s report)

1. Initial Information Gathering via Social Engineering
    - ✓ Often LinkedIn invites are sent
    - ✓ Personnel and organizational structure – who has access to what – is mapped out
2. Initial Compromise by Watering Holes
    - ✓ Compromised websites (watering holes) infect preconfigured IP addresses with malware
    - ✓ In February 2017, Polish banks confirmed their systems were infected by malware, most likely from accessing the Polish Financial Supervision Authority (Komisja Nadzoru Finansowego – KNF) website, which had been turned into a watering hole
    - ✓ Similar code was also discovered on the National Banking and Stock Commission of Mexico
3. Reconnaissance on the Victim’s Internal System
    - ✓ Spyware contracted from watering holes helps gather further information, and map out the victim’s system-scape
    - ✓ Evade anti-virus programs. Response time is very quick. When they are detected, they “patch up” detected malware, and redeploy into the victim’s system
    - ✓ FireEye has observed that APT38 stays in a victim’s system on average of 155 days, longest being 678 days (almost two years)
4. Reconnaissance on the SWIFT Servers
    - ✓ APT38 deploys active and passive backdoors, as well as install port monitoring tools such as MAPMAKER on the SWIFT system
    - ✓ Continue to gather intelligence while evading detection
5. Strike! And Transfer Funds
    - ✓ Malware such as DYEPACK a “SWIFT transaction-hijiacking framework” are used to enable fraudulent transactions
    - ✓ Funds are transferred out into other banks in other countries with lax money laundering regulations (e.g. Philippines, Sri Lanka)
6. Destroy Evidence
    - ✓ Wiperware such as BOOTWRECK destroys files and logs
    - ✓ Ransomware and other malware that misdirects and distracts investigators, buys time for the digital footprint to be destroyed

Who will they strike next?



FASTCash

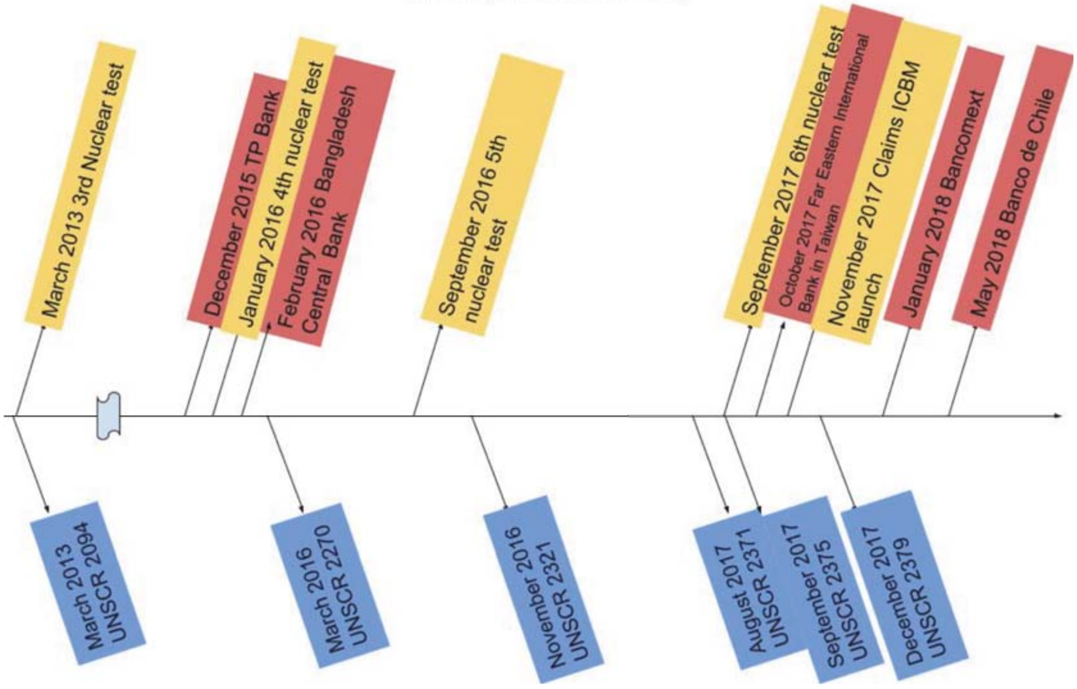
How the Lazarus Group is Emptying Millions from ATMs

Symantec uncovers Trojan.Fastcash, the tool used by North Korea-linked Lazarus group to mount ATM attacks

ISSUING BANK
COMPROMISED SERVER
Withdrawal request message with legitimate Primary Account Number (PAN)
ATM
Withdrawal request approved or declined
Approve (or Decline)
Trojan.Fastcash
Payment Switch Application
Fraudulent withdrawal request message with PAN number used by Lazarus
ATM
Fraudulent withdrawal request approved
Symantec.

Copyright © Symantec Corporation

North Korea Cyberheist & Nuclear Program Activities
with United Nations Security Council Resolutions
Timeline (March 2013-Present)



March 2013 3rd Nuclear test
December 2015 TP Bank
January 2016 4th nuclear test
February 2016 Bangladesh Central Bank
September 2016 5th nuclear test
September 2017 6th nuclear test
October 2017 Far Eastern International Bank in Taiwan
November 2017 Claims ICBM launch
January 2018 Bancomext
May 2018 Banco de Chile
March 2013 UNSCR 2094
March 2016 UNSCR 2270
November 2016 UNSCR 2321
August 2017 UNSCR 2371
September 2017 UNSCR 2375
December 2017 UNSCR 2379