

Online Security: What You Need To Know

JUNE 2017

KEN PALLA, DIRECTOR

ENTERPRISE INFORMATION SECURITY

MUFG UNION BANK, N.A.

Agenda

Key Online Security Trends	3
How Malware Gets on the PC	11
How Malware Gets on the Mobile Device	16
Malware Attack Vectors	17
Business Email Compromise (BEC)	18
Threats are Moving to Organization Platforms	29
How to Prevent Attacks	32
What to Do If You are A Victim of Online Fraud	33
Additional Thoughts from Cybersecurity Experts	35
Appendix	38

Key Online Security Trends

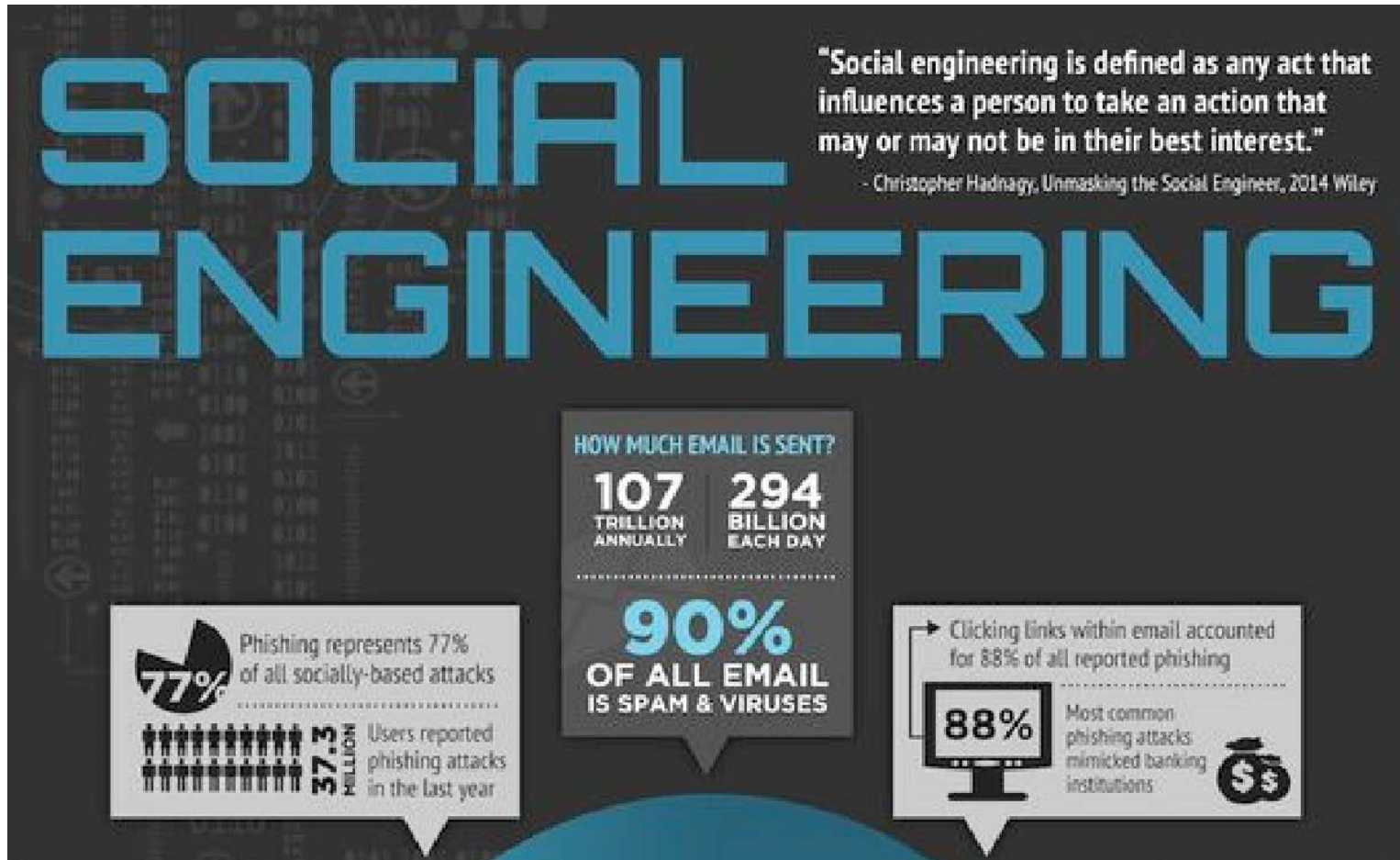
Social Engineering More Dangerous Than Malware

- With every attack we see a social engineering component
 - Malware on customers PCs allows their bank credentials to be compromised
 - Customers see pop-up windows requesting contact information.
 - Shortly afterwards, customer receives call from the “bank”.
 - Bogus email from CEO to Finance Manager requesting wire be sent to support “new acquisition” being handled by outside law firm.
 - Romance scams and job opportunities morph into bogus remote check deposit scams.



Key Online Security Trends

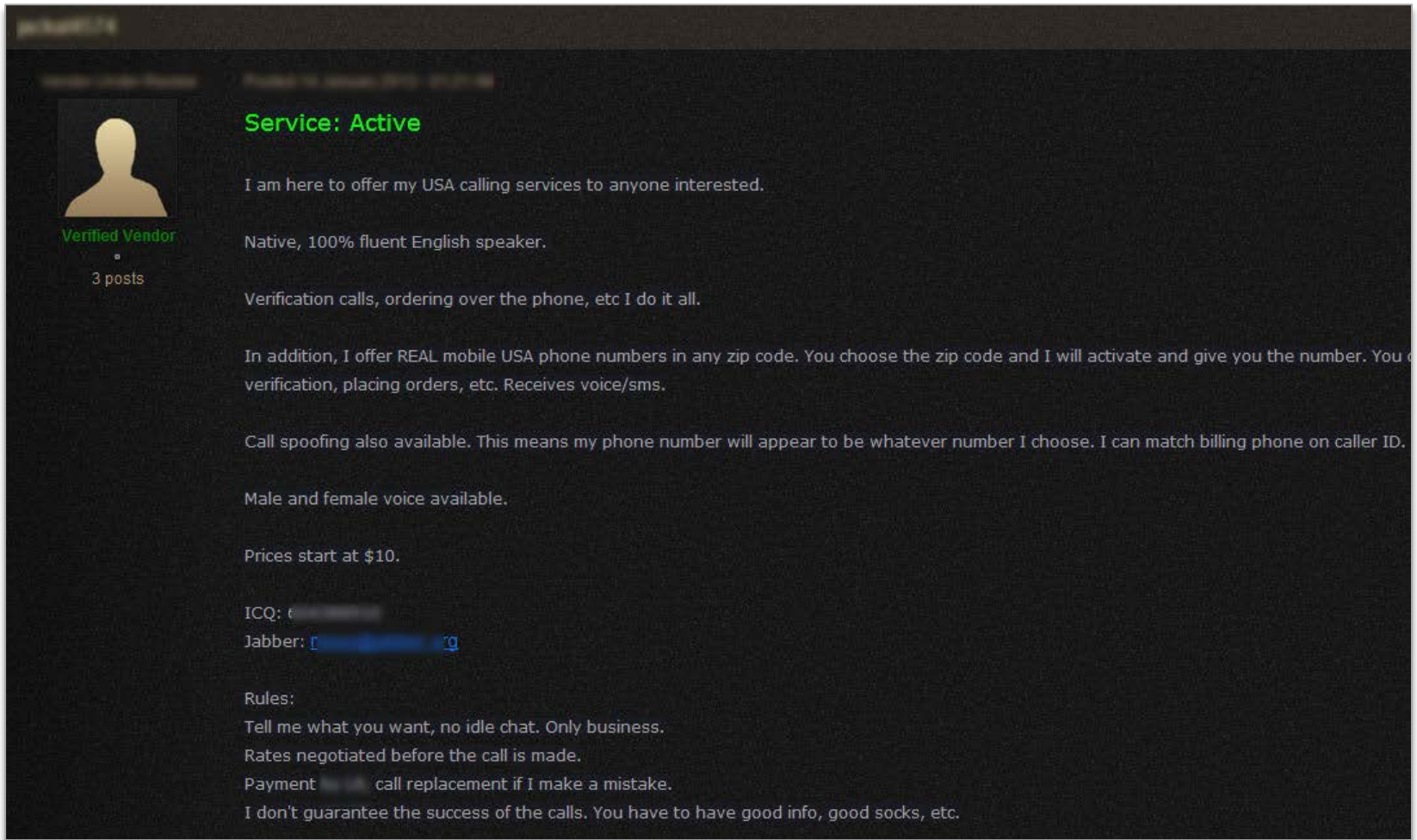
Social Engineering Facts



Source: Fox-IT

Key Online Security Trends

What Phone Number do You Want?



Service: Active

I am here to offer my USA calling services to anyone interested.

Native, 100% fluent English speaker.

Verification calls, ordering over the phone, etc I do it all.

In addition, I offer REAL mobile USA phone numbers in any zip code. You choose the zip code and I will activate and give you the number. You can verify the number, placing orders, etc. Receives voice/sms.

Call spoofing also available. This means my phone number will appear to be whatever number I choose. I can match billing phone on caller ID.

Male and female voice available.

Prices start at \$10.

ICQ: [REDACTED]

Jabber: [REDACTED]

Rules:

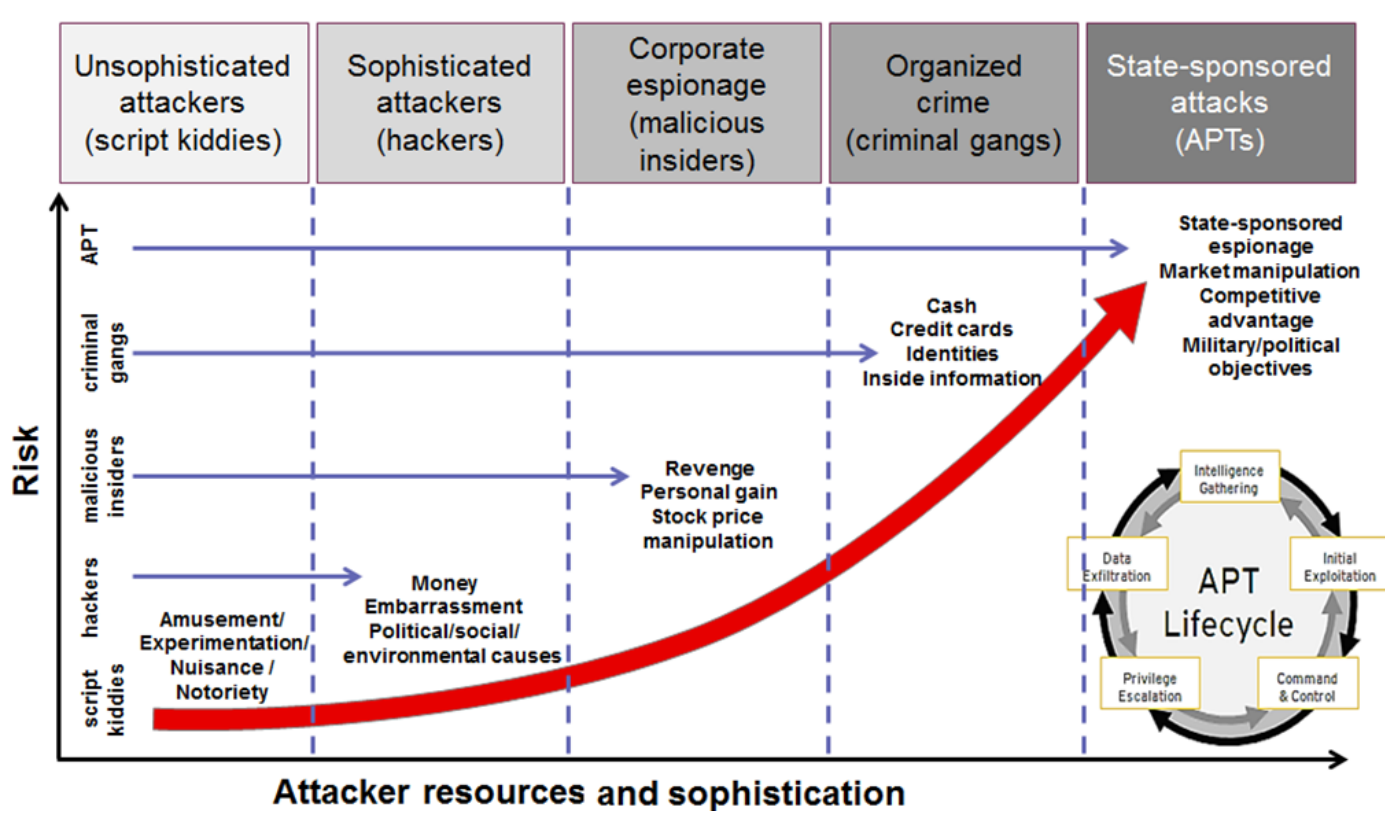
- Tell me what you want, no idle chat. Only business.
- Rates negotiated before the call is made.
- Payment [REDACTED] call replacement if I make a mistake.
- I don't guarantee the success of the calls. You have to have good info, good socks, etc.

Source: RSA

Key Online Security Trends

State-Sponsored Actors

- Nation State actors sharing with financial fraudsters
- Quality of malware becoming more sophisticated

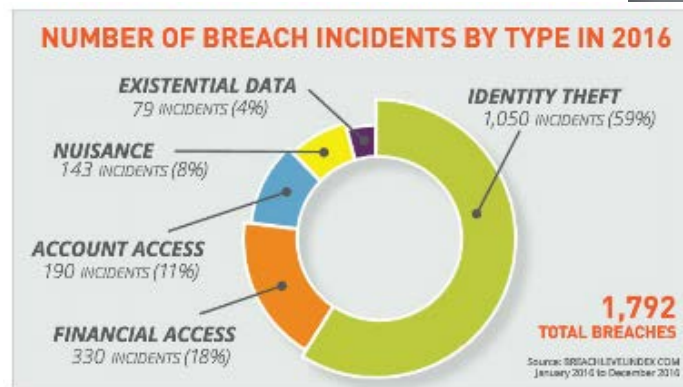
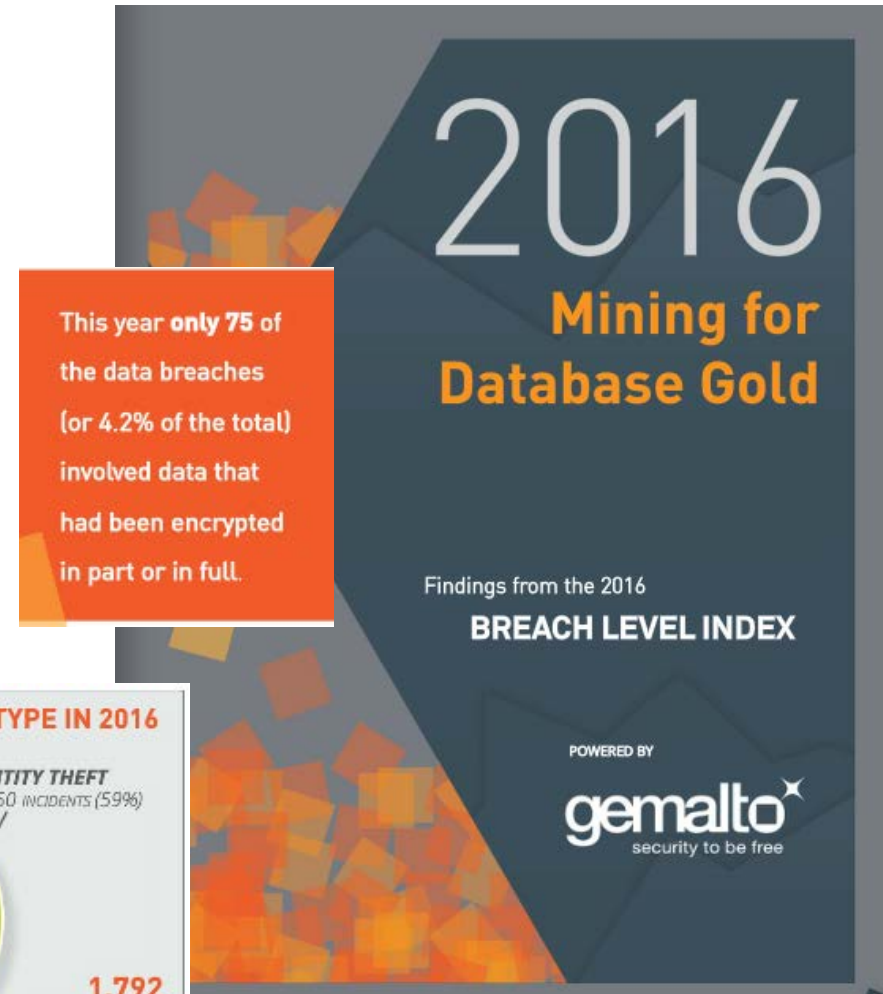


Key Online Security Trends

Data Breaches

Key Points:

- **1.4 billion data records compromised in 2016**
- Government accounted for 15 percent of all data breaches in 2016



Key Online Security Trends

Ransomware

- Ransomware moves from consumers to business
- Difficult to not pay, with all files encrypted



Action Steps:

Locally, on the PC

- Have two backups of your data – on an external hard drive and in the cloud – Dropbox, Google Drive, etc.
- Make sure your operating system and software is up to date, including the latest security updates
- Turn off macros in the Microsoft Office suite – Word, Excel, PowerPoint, etc.

Online behavior

- Never open spam emails or emails from unknown senders
- Never download attachments from spam emails or suspicious emails
- Never click links in spam emails or suspicious emails

Some red flags

- Message is addressed generically, “Dear Customer”
- Incomplete or missing contact information

Key Online Security Trends

Examples of Ransomware

Hospital Paralyzed by Hackers

A cyberattack in Los Angeles has left doctors locked out of patient records for more than a week. Unless the medical facility pays a ransom, it's unclear that they'll get that information back



University of Calgary Pays Ransom

Canadian School Shells Out \$15,700 to Ransomware Attackers |

Jeremy Kirk ([jeremy_kirk](#)) • June 10, 2016



Key Online Security Trends

Data Destruction

- 2010: The Stuxnet attack against Iranian industrial control systems involved the exploitation of four zero-day vulnerabilities
- Used to launch attack to sabotage centrifuges of Iranian nuclear plan
- 2012: Shamoon malware destroyed data on 30,000 computers in Saudi Arabia.
- 2015 and 2016: Destructive attack against Ukraine energy companies
- 2017: Shamoon returns to Saudi Arabia

With Nation States interested in destabilizing the Western world, these could become more common against less secure companies and organizations.

How Malware Gets on Your PC

Malware Payload Delivery Evolving



Examples of Payload Delivery

- Email phishing/spear phishing
- Bogus Google search results
- Drive-by web sites
- Malvertising

PHISHING VOLUMES (RSA AFCC)



Source: RSA

Where everybody knows your name...

- Stolen logon credential often contain email address as user ID.
(tom.wilson@cityofstars.org)
- This makes it easy to craft phishing/spear phishing emails to government employees:
 - Dear Tom, your recent expense report was rejected due to serious violation of expense policy. [Click here](#) for details. Or download attached Word document for new HR policy (loaded with malware).

New airline phishing campaign is so real...

- Email-based phishing campaigns is targeting airline consumers.
- For the airline phishing attack, attackers are successful over 90 percent of the time in getting employees to open airline impersonation emails.

Anti-Phishing Training

Is This Email Legitimate?

To: samantha@mail.com
From: Bank of North America
Subject: Great Service is Just a Click Away!

Attachments:

Bank of North America

Dear Samantha,

We are excited to announce the launch of our new Customer Service portal, the BoNA Support Center. This will give you easy access to account management tools, special incentives, and BoNA Rewards.

You can access this secure portal from any page on our website.

We hope you will enjoy this new customer experience.

James Connor, Customer Service Manager
Bank of North America
[800-555-1234](tel:800-555-1234)

Sender details
You can't tell if an email is legitimate just from the sender. Scammers can put anything they want in an email, including the sender information, in order to make it look more official.

To: samantha@mail.com
From: Bank of North America
Subject: Great Service is Just a Click Away!

Attachments:

Bank of North America

Dear Samantha,

We are excited to announce the launch of our new Customer Service portal, the BoNA Support Center. This will give you easy access to account management tools, special incentives, and BoNA Rewards.

You can access this secure portal from any page on our website, <https://www.bona.com>

We hope you will enjoy this new customer experience, and we thank you for your loyalty.

James Connor, Customer Service Manager
Bank of North America
[800-555-1234](tel:800-555-1234)

Links
Safe, legitimate links can be verified through experience or an online search. It pays to study links carefully, and only click those you know to be safe.

With Phishing so common and successful, you need to train your employees to detect bogus emails.



How Malware Gets On The Mobile Device

- Charging your phone on an infected PC
- Drive by ads on mobile
- Downloading apps from third party stores
 - Many look and act like the real app, but are loaded with malware
- SMS (text) Phishing (Smishing)
 - Receive text message with link (click link and malware downloaded)



Hi Karen just got this as a text and thought you would like to see it.

A Payment of £748.96 has been issued by HMRC for an overpayment of tax in 2015. Please complete form <http://bit.ly/2bRPN4r> to process.

GOV.UK

Malware Attack Vectors – PC

Bank Malware Fakes Bank Site

- Customer logs in and enters online credentials, including token
- Fraudster does transaction behind the scenes
- Fraudster tells customer there is a logon problem
- Will ask for second user to log in
- May have pop up asking for user name and phone number
- Fraudster will call pretending to be bank (social engineering) “apologize” for problems



Ransomware

- Customer's files get encrypted
- Customer required to pay in bitcoin to get files unlocked
- After payment, files may or may not be decrypted

Malware Attack Vectors – Mobile

- Overlay
- Smishing
- Forward SMS text messages and calls (without user being aware)
- Taking over the mobile device (full permissions)
- Remote Access
- Exfiltration of contact lists, photos, etc..
- Auto recording and picture taking

Business Email Compromise (BEC)

Business Email Compromise (BEC)

Definition

Business Email Compromise (BEC) targets organizations working with foreign suppliers or companies that regularly perform wire transfer payments.

Compromises legitimate business email accounts to trick people into placing payments.

Usually involves wire transfers and sometimes checks.

Source: Federal Bureau of Investigation, Internet Crime Complaint Center (IC3) press release "Business Email Compromise, August 27, 2015, alert number I-082715a-PSA.

Business Email Compromise (BEC)

Main Types of BEC Scams

Business employee receives an email from what appears to be the CEO or CFO of the company

Business receives an email from what appears to be a supplier or vendor

Business Email Compromise (BEC)

Hallmarks of the BEC Scam

Spoofed emails look legitimate and are well-written

Often the sender's email domain is slightly different
(j.smith@light.com)

Or the sender's domain is completely different
(j.smith@gmail.com)

Recipients are usually employees who handle wire transfers

Convey a sense of urgency

Demand recipient keep the payment a secret

"Code to admin expenses" or "urgent wire transfer"

Dollar amount is normal for the business to keep suspicion low

Fraudulent emails often are sent when the spoofed "requester" is not available

BEC: Impact to Organizations

BEC – Impact to Organizations

Impact of the BEC Scam: 10/01/2013 – 05/01/2017

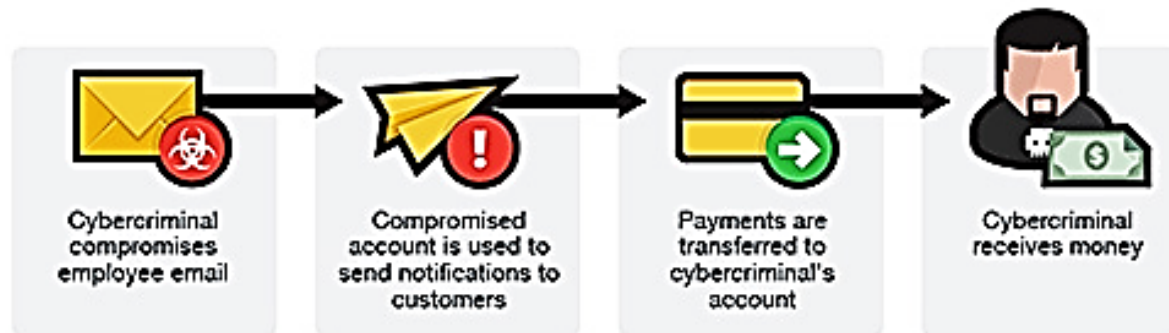


The single largest BEC loss so far was over **\$100 million.**

May 04, 2017

Alert Number
I-050417-PSA

**BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM**



Source: Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), and Fox News April 15, 2016

CEO Impersonation

Scenario

- The CFO received an email from the CEO requesting that a wire payment be sent. CEO stated she will not be available to take any calls.
- The CEO's email address looked correct in the "From" line. However, the CEO's email account had been hacked and the email header showed the return path as a completely different address.
- From: john.doe@corp.com
- Email Header Return Path: harry.smith@yahoo.com



Organization's Loss or Exposure

- **\$150,000**
- The client's bank identified this as suspicious and contacted the sender.
- Even after being educated on the scam by the bank, the employee who entered the wire refused to verify the wire with his CEO and requested the wire be released immediately.

CEO Impersonation

Scenario

- CFO received email from CEO asking to send a wire.
- CFO neither questioned the email, nor noticed that the email's domain was slightly different.
- Email domain change: john.doe@business.com vs. john.doe@busines.com



Organization's Loss or Exposure

- **\$67,000**
- Customer went into a banking office to create the wire.
- Wire was sent to a domestic bank.
- Customer notified his bank when he determined the wire request was fraudulent, and bank recovered funds.

CEO Impersonation

Scenario

- Employee received email from CEO stating there is a confidential acquisition coming up and a need to urgently send a wire.
- Email said not to disclose this information to anyone.
- CEO's email was spoofed and looked totally legitimate.



Organization's Loss or Exposure

- **\$4,500,000**
- The bank identified the wire as suspicious and contacted user and discussed BEC fraud.
- The user told the bank that he had verified the wire and asked the bank to release the wire.
- The user called back saying the instructions were from a fraudulent email.

Vendor Impersonation

Scenario

- Business normally sends checks to its vendor but the vendor (who was impersonated) requested a wire instead.
- The email was in the vendor's contact list but the email domain was different.
- Example: jane.smith@corp.com vs. jane.smith@gmail.com



Organization's Loss or Exposure

- **\$350,000**
- The customer's bank detected the transaction as suspicious and contacted the client to explain the BEC scam to the user.
- The user asked to hold the wire to verify it with the vendor.
- The user called back within an hour saying the instructions were from a fraudulent email.

Reminders

- Have a process to validate payments, regardless of channel
- Be aware of red flags and validate your suspicions when you think something is not quite right. We often hear disappointed customers saying “How come I didn’t see this?” or “I thought it was odd but I didn’t question it.”
- Banks can often help detect suspicious BEC wire transactions and alert clients.
- Please pay attention to your bank

Threats Are Moving to Organization Platforms

Just as we saw with Business Email Compromises...

- Customer financial applications are at risk
- Applications (e.g., SunGard, SAP) that create Wires and ACH (to be sent to banks via APIs) are being compromised at the customer site
- Security at customer site is typically less than bank online sites (tokens, anomaly detection, detection of malware, etc...)

2016: Homeland Security warns of hackers exploiting SAP security flaw

At least 36 organizations are affected by outdated or misconfigured software. |



Source: <https://www.us-cert.gov/ncas/alerts/TA16-132A>

What Happened to Bangladeshi Bank Could Happen to You

- \$81 million loss via SWIFT transaction
- Poor internal controls on platform that had no previous losses
- That attack vector can just as easily be applied to a larger organization to empty its accounts by commandeering the accounting system etc.
- It's the same skillset, just applied differently
- Fraudsters are able to mule away large amounts of money

How to Prevent Attacks

Malware

- Train your employees to not click on unknown emails (run training exercises)
- Use dedicated PC for financial transactions. No email or Internet searching on this PC.
- Implement true dual controls (separate users on separate devices) for ACH and wire transactions
- Have strong anti-virus software on PCs and mobile devices. Seriously consider bank offered anti-virus software.
- Keep your PC patched with all security updates (Adobe, Microsoft, etc...)

BEC

- Have financial expert review your Wire/ACH processing procedures
- Always do a verbal call back to requestor (even if person is traveling/on vacation)
- Never reply to original email asking for confirmation. It will just go to fraudster.

What to Do if You Are Attacked by Malware, BEC, Ransomware

If it is a financial transaction

- Contact your banker immediately.
 - Fast action may allow recovery of funds
 - Contact the FBI and Internet Crime Complaint Center (IC3)--www.ic3.gov

For ransomware

- Contact the FBI
- See information provided in attachment

What to Provide FBI in Case of Ransomware Attack

- Date of infection;
- Ransomware variant, as identified on the ransom page or by the encrypted file extension
- Victim company information - industry type, business size
- How the infection occurred - link in email, browsing the internet, etc..
- Requested ransom amount
- Attacker's bitcoin wallet address - often listed on the ransom page
- Ransom amount paid, if any
- Overall losses associated with a ransomware infection, including the ransom amount
- Victim impact statement.

File a report with the local FBI field office or via the website of the Internet Crime Complaint Center, or IC3 (www.ic3.gov).

Additional Thoughts From Cyber Experts

- Train your staff to be aware. .. 90% of all Malware compromises start from employees “clicking”
- The Russian Criminals started with Consumers. Now they have moved to Commercial Accounts.
- Nation-State style attacks are being used against Commercial entities
- Add monitoring and new authentication as you expand into new cash management services, especially as you do this on your accounting platforms

See more details in the Appendix

In Closing...

As we close today, it is worthwhile to remember what the U.S. Navy did in 2015. Due to the risk of attacks on navigational satellites, the Navy is equipping every U.S. ship with a sextant for backup navigation.

The U.S. Navy is reinstating the ancient art of celestial navigation to fight a very modern threat.



October 15, 2015

If the satellites stop working, do this.

Questions and Answers

The content of this presentation does not
reflect the views or opinions of MUFG
Union Bank

Appendix: Detailed Comments from Cyber Security Experts

- **Controls for expanded cash management services** – more business banking customers are utilizing automated billing and e-payment services to enhance their cash management operation. However, monitoring and new authentication services are a top of mind priority. New mobile centric solutions are becoming the preferred solution to improve experience and security for corporate customers.
- **Cyber assessment of customers** – more medium-sized business are leveraging services provided to large corporate customers – e-payment processing, direct deposit and digital payments. These services are allowing them be more nimble in their day-to-day operations. However, not all have the right level of internal cyber controls in place to safeguard their systems and employees which is putting them at significant higher risk. Banks will begin to perform monitoring if their customer's digital controls to asses credit worthiness, limits and services availability.
- **Don't trust e-mail**
- **Assume all your credentials are compromised**

Expert Comments

- It's no longer a Northern Europe & North America problem, Cybercrime has gone global... Examples of this are - Australia in 2016 had more attacks against per capita than any other country and it was not in the top 10 in 2015. Another example in Q4 in 2016 we saw the first POS (point of sale) BotNets in Asia...previously only the US had POS Botnet.
- Analytics of BotNets or you could say the maturity of the Criminal Business model... they are getting a greater level of ROI. It's clear that different Russian speaking criminal gangs are running analytics across the Bots, in some way it appears they are able align the PC data scraped by the Malware with outside data, examples of this we have seen Bots being moved from a Dyre based attack being used in Business Email Compromise (CEO Fraud). Another example is Dridex infection being moved (we have no clarity what the financial arrangement is to a gang who's chosen criminal expertise is to deploy APT Style attacks.
- The Russian criminals started with Consumers to Hijack Accounts (used ATM's to mule the stolen money) then they moved to Commercial accounts to hijack (used bogus companies to launder the money). So with analytics and targeting interesting Bots, we have seen criminals who only targeted online Banking customers from 2009 to 2015 now targeting "any" interesting companies such as Insurance, Health, Legal, Oil, Hospitality, Software to name a few. The Criminals also do not just steal money.. they will also scrape everything on the infected PC which is interesting.

Expert Comments

- Nation State style attacks are being used against Commercial entities with the biggest risks in the loss (theft) of money coming from Russia and North Korea (image attached of a South Korean Intel company of money stolen by North Korea in the past 12 months)
- So many of these attacks start with a spear phish mail - stress the importance of ensuring that they are doing their utmost to:
 - Catch the stuff at the gateway / desktop (spam filters, SPF, DMARK, etc., etc.)
 - Train their staff to be aware - don't count on them just instinctively being able to tell good from bad, especially if they don't know how bad can be (think mail from a contact you know, about a usual subject you discuss and a malicious attachment - this happens when the org that the other person works in was "popped" and the attackers are using that existing mail link to make you and your organization the next victim)
 - Have procedures for reporting and dealing with batches of strange mails, as well as procedures to prevent the BEC fraud
- An overhyped Marketing myth... "The Criminals are innovating and we are playing catchup..." - not really... three of the top 5 malwares deployed against financial institutions in 2016 were Zeus based.. if it works why change...
- Social engineering is still the preferred attack vector used to steal Money from Customers and in the case of Swift employees. Authentication is overcome by social engineering.
- Number one piece of advice – Train & Educate your staff... 90% of all Malware compromises start from employees "clicking" and still the number one favorite is the Microsoft Macro attack (Example: Criminals embed malware in a word file)