THURSDAY, MARCH 26TH ~ 4:40 PM TO 5:30 PM

FORENSIC AUDITING: A TOOL FOR FRAUD PREVENTION AND DETECTION

Ciro Cuono, CPA, Partner
Thomas DeMayo, Director of IT Audit and Consulting
O'Connor Davies, LLP

I. Increasing the Visibility of the Cyber Threat Landscape

II. Forensic Auditing Can Increase Awareness

- Risks to Protected Personal Information
- Assets
- Revenue
- Reputation

III. Gaining Insights Into the External and Internal Threat Factors That Perpetuate Cyber Fraud

IV. Utilizing Forensic Auditing as a Tool

- Understanding the Proper Defenses in Preventing and Detecting Fraud

Presented at:
New York State Government Finance Officer's Association Forum (Annual)

March 24-25 2015 Albany, NY.

O'CONNOR DAVIES

PKF

Cybercrime- A Clear and Present Danger

The Internal and External Threat

Ciro V. Cuono
Partner
CCuono@odpkf.com

Thomas J. DeMayo
Director
IT Audit and Consulting Services
TDeMayo@odpkf.com

O'CONNOR DAVIES

Objectives

- Increase visibility of the cyber threat landscape
- Increase awareness regarding the risk to protected personal information, assets, revenue, and reputation
- Gain insight into the internal and external threat actors that perpetrate cyber fraud
- Establish an understanding of the foundation for proper defenses in preventing and detecting cyber fraud

O'CONNOR DAVIES

Why Attack a Governmental Entity?

- Why Not?
- Governmental Entities have:
  - Bank accounts
  - Employee payroll
  - Employee personal information
  - Resident personal information
  - Perform EFT transactions
  - Credit card processing
  - Electronic health records

PKF

O'CONNOR DAVIES

Indisputable Cyber Truths

- Any governmental entity that is connected to the internet can become a victim
- Any governmental entity that uses software to manage their operations (business, home, car, etc.) can become a victim

O'CONNOR DAVIES

Indisputable Cyber Truths

- A governmental entity does not need to be a target to become a victim of "hacking"
  - Majority of attacks are opportunistic and not targeted
- What does this all mean?
  - **ANYONE** can become a victim of a cyber attack

O'CONNOR DAVIES

Cyber Fraud is Big Business

- Malware is specifically written to target your bank accounts
  - ZeuS
  - SpyEye
- Banking Malware is for sale on the web
  - Crime gangs are hiring rogue programmers to create new and modify existing malware to evade detection from anti virus software

PKF

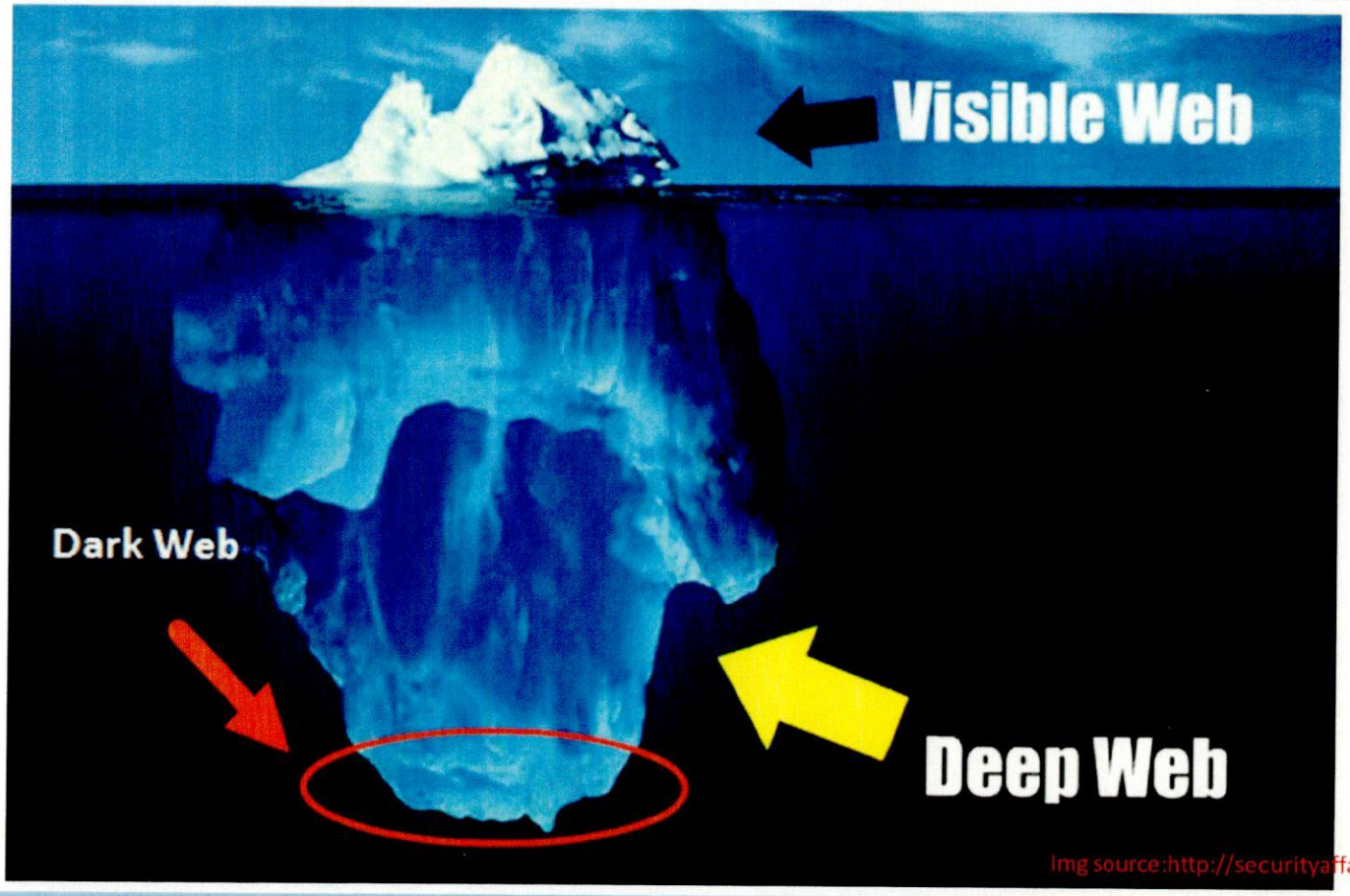
O'CONNOR DAVIES

Cyber Fraud is Big Business

- The cyber underground has developed a business model of providing turnkey cyber crime solutions hosted by criminal organizations
  - Malware as a Service ("MaaS")
  - Fraud as a Service ("FaaS")
  - Attacks as a Service ("AaaS")

O'CONNOR DAVIES

Cyber Fraud is Big Business



Img source:http://securityaffairs.co/

O'CONNOR DAVIES

Cyber Fraud is Big Business

Simon

Posted 02 July 2013 - 12:10 PM

Posts: 6
Number: 12591

Selling EU and US bank accounts that include:

- Online banking user name
- Online banking password
- Any data needed for secret questions or authentication
- The victim's IP and SOCKS proxy on the victim's device

Img Source - Trusteer

Не сервис, продажи разовые, пишете в ПМ какая нужна страна, скидываю что есть и почем.
Происхождение аккаунтов - работаю на человека по обработка его логов, оплата мне идет 50/50 аккаунтами.

К оплате принимаю Webmoney, PerfectMoney.

Если есть вопросы, предложения пишите в ПМ (предпочтительнее) или по icq [redacted]
Jabber по запросу.

O'CONNOR DAVIES

Cyber Fraud is Big Business

Johnny D. -
Junior Member

Johnny D. is offline

Join Date: Jan 2011

Posts: 4

Reputation: | +/-

Selling bank accounts packages:

- Bank account information + ATM card
- Online banking credentials
- Official documents (including passports)
- Price: 12,000 Ruble (~$360)

Also offering a cashout service for a 5% fee

Доставка осуществляется курьерской службой DHL или EMS, за счёт покупателя.

- Претензии по комплектации принимаются в течение суток после получения товара покупателем.
- Комплекты предназначаются для обналичивания ваших денег через банкомат, но не для хранения! За действия дропа, я несу ответственность, но за каждым уследить невозможно, соблюдайте правила, и все будет в порядке и со счетами и с нервами.

Мои контакты:

Изготовление и продажа банковских счетов с атм картами icq

Img Source
- Trusteer

O'CONNOR DAVIES

Cyber Fraud is Big Business

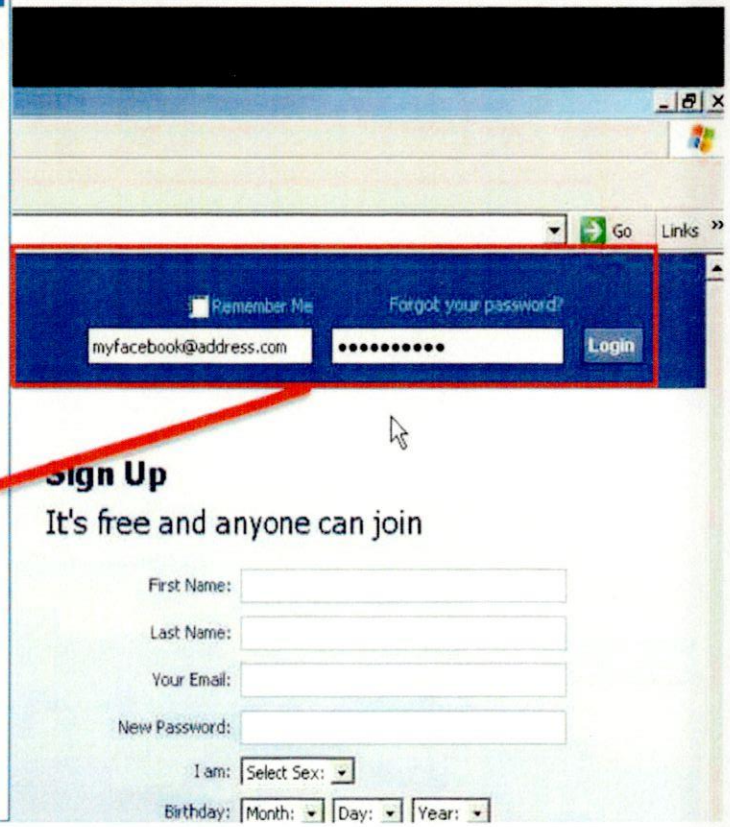
View report (HTTPS request, 424 bytes)

Bot ID:	vb4_014c5a43
Botnet:	plag
Version:	1.2.4.2
OS Version:	XP Professional SP 2, build 2600
OS Language:	1033
Local time:	07.10.2009 16:30:24
GMT:	-8:00
Session time:	06:39:34
Report time:	07.10.2009 23:30:28
Country:	--
IPv4:	192.168.1.83
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
Source:	https://login.facebook.com/login.php?login_attempt=1

```
https://login.facebook.com/login.php?login_attempt=1
Referer: http://www.facebook.com/
Keys: www.facebook.com
myfacebook@address.commyfacepass
Data:

charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%D0%94%2C%D0%84
locale=en_US
non_com_login=
email=myfacebook@address.com
pass=myfacepass
pass_placeholder=Password
charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%D0%94%2C%D0%84
lsd=TWISM
```

Zeus: Retrieved Form Data



Zeus: Retrieved Form Screenshot

PKF

O'CONNOR DAVIES

Cyber Fraud is Big Business

Search

Update companies

#	Name	Job	Company	Tax data	Pin	Transfer info	Use
1420		DIR OF SALES		YES	86885	**$3,599.19** to num	In Process
1421		SALES MANAGER		YES	11343	**$2,665.08** t	In Process
1422		TAXDIR - TAX DIRECTOR		YES	41122	**$4,293.20** to a8 amex	In Process
1423		TECHNICAL SUPPORT		YES	02933		used
1424		HR - HR ASSISTANT		YES			not used
1425		MARKETING COORDINATOR		YES	65533	**$2,113.17** to a8 amex donj8j xNUnjo0N2	In Process
1426		VPCOMINC - VICE PRES COMMUNICATIONS		YES	46782	**$2,204.82** to a8 amex	In Process
1427		ADMINISTRATIVE ASST		YES	88398	**$4,263.42** to a8 amex	In Process
1428		VP SALES		YES	47234	**$2,437.04** to a8 amex	In Process

Img Source Krebs on security

PKF

O'CONNOR DAVIES

Electronic Fund Transfer Fraud

- Electronic Fund Transfers ("EFT's") – The electronic exchange or transfer of money from one account to another

  Examples: Direct Deposit, Direct Debit, Electronic Bill Payment, Wire Transfers

- Can be classified as a Wire Transfer or Automatic Clearing House ("ACH") Transaction.

PKF

O'CONNOR DAVIES

Commercial vs Consumer EFT's

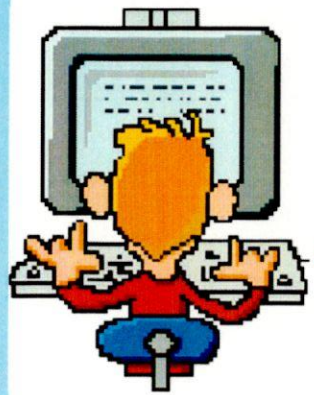
- Commercial and Consumer EFT's are protected differently under the law
  - Consumers are protected by the Electronic Funds Transfer Act
    - Consumers are allowed up to 60 Days to report fraudulent transactions
  - Commercial EFT's are regulated by the Uniform Commercial Code Article 4A
    - Businesses are allowed up to two days to report the fraudulent transaction depending if it was an ACH or Wire Transfer

PKF

O'CONNOR DAVIES

Banking Malware In Action

Initial Balance $5,000



Wire $500 to
Acct # 12345
Bank: ABC

Wire $2,000 to
Acct # 54321
Bank: XYZ

Wired $500 to
Acct # 12345
Bank: ABC
Balance: $4,500

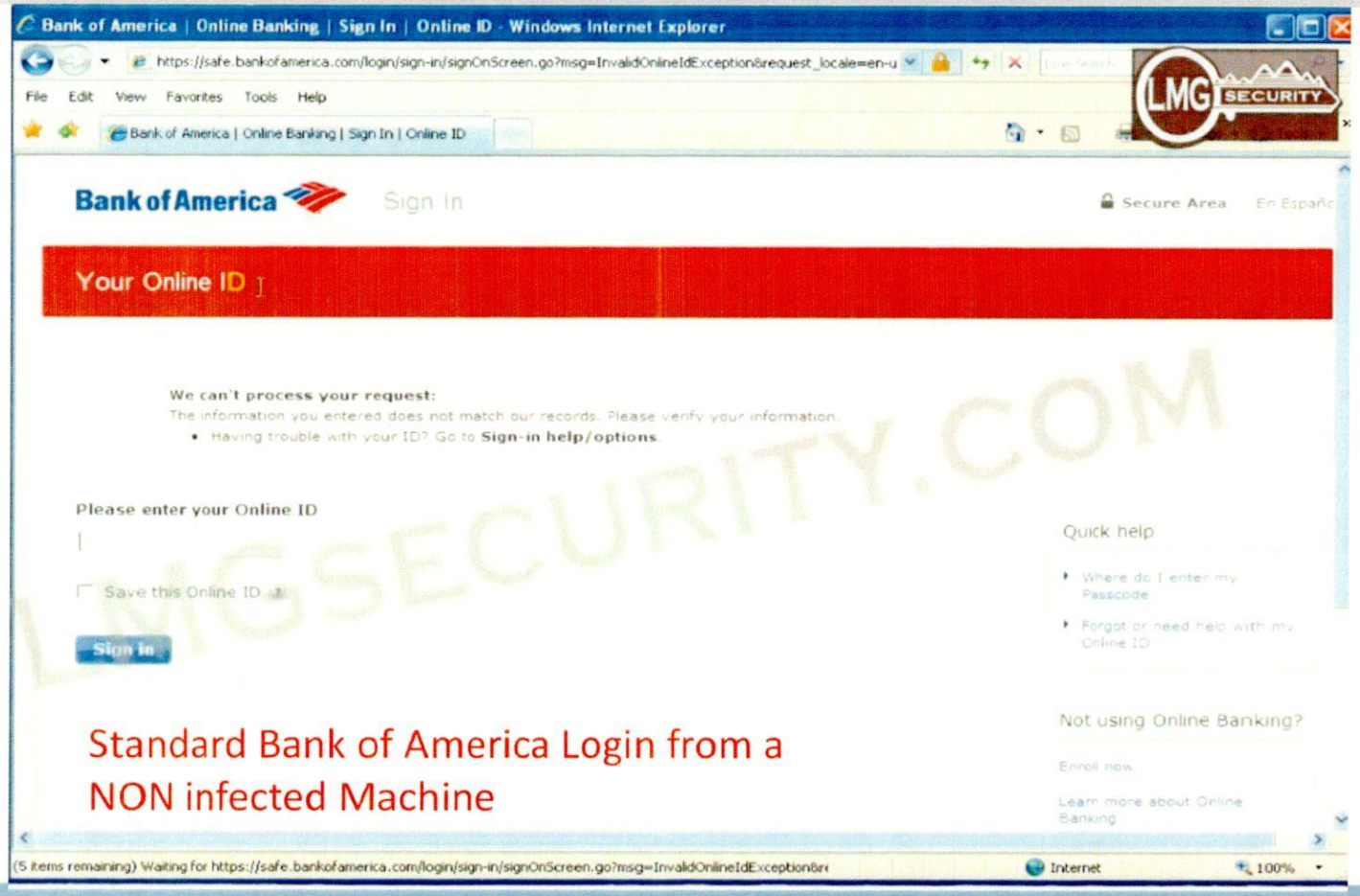
Wired $2,000 to
Acct # 54321
Bank: XYZ
Balance: $3,000

Final Balance $3,000

PKF

O'CONNOR DAVIES

Banking Malware In Action



Standard Bank of America Login from a NON infected Machine

PKF

O'CONNOR DAVIES

Banking Malware In Action (cont…)

Bank of America | Online Banking | Authorization - Windows Internet Explorer

https://safe.bankofamerica.com/login/sign-in/signOnScreen.go?msg=InvalidOnlineIdException&request_locale=en-u

File Edit View Favorites Tools Help

Bank of America | Online Banking | Authorization

Bank of America Sign In Secure Area En Españ

Confirm your identity

We can't process your request:
The information you entered does not match our records. Please verify your information.
- Having trouble with your ID? Go to **Sign-in help/options**.

We do not recognize the computer you are using. Please confirm your identity from this unrecognized computer.

Location where your accounts were opened:

State: Select location

City:

ATM or Debit Card Information:

Card Number:

15 or 16 digits no dashes or spaces

Expiration Date :

Quick help

What do I need to know?

Done Internet 100%

Same page from an infected machine (Part 1)

PKF

O'CONNOR DAVIES

Banking Malware In Action (cont…)

Bank of America | Online Banking | Authorization - Windows Internet Explorer

https://safe.bankofamerica.com/login/sign-in/signOnScreen.go?msg=InvalidOnlineIdException&request_locale=en-u

File Edit View Favorites Tools Help

Bank of America | Online Banking | Authorization

ATM or Debit Card Information:

Card Number:

15 or 16 digits, no dashes or spaces

Expiration Date :

Security Code:

Personal Information:

Social Security Number:

Date Of Birth:

Driver's License Number:

Mother's Maiden Name:

Remember computer:

Do you want us to remember this computer, so you can avoid answering your personal information next time you sign in?

Yes

No

Continue

Done

Internet

100%

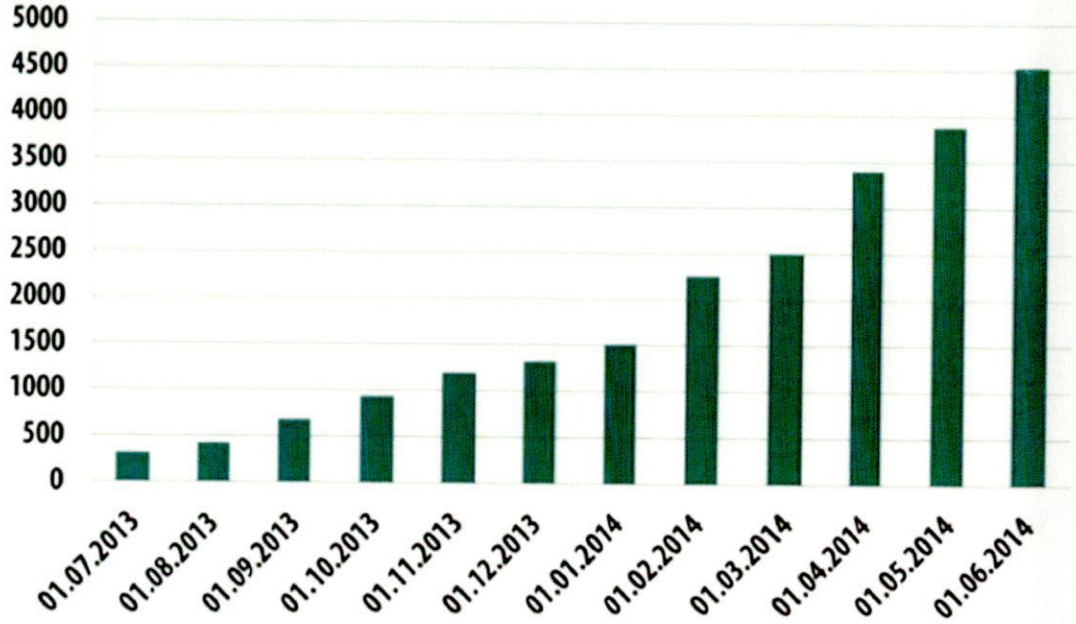
Page Scrolled Down on Infected Machine

PKF

O'CONNOR DAVIES

Mobile Device Malware - Why Worry?

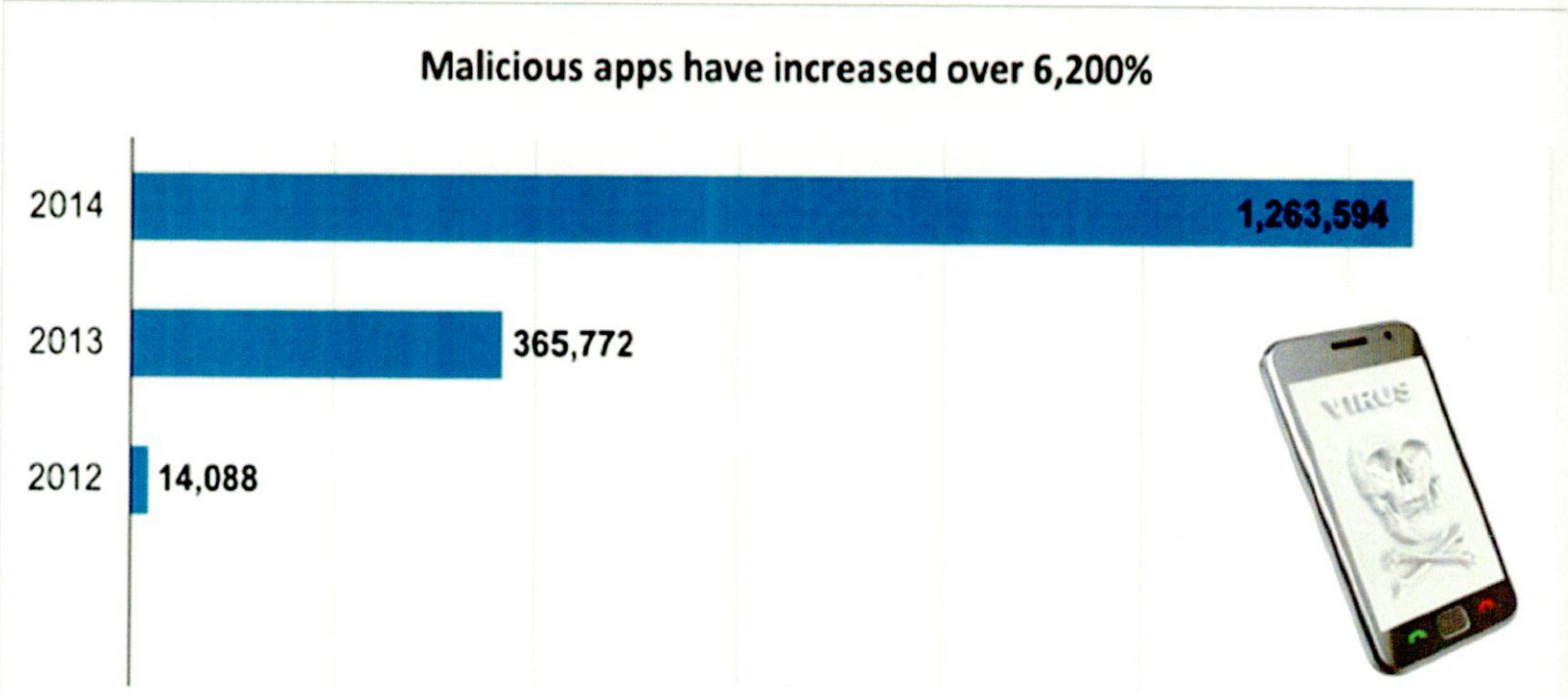
Mobile Malware grew 614% from March 2012 to March 2013



Number of mobile banking Trojans detected, Q2 2014

O'CONNOR DAVIES

Mobile Device Malware - Why Worry?



O'CONNOR DAVIES

Mobile Device Malware - Why Worry?

- What have the attacks accomplished?
  - Text messages intercepted and forwarded - specifically when banks send text messages with one-time codes to log in
  - Record phone calls - turn on microphone to record conversations
  - Track GPS location remotely
  - Send text messages to premium services increasing fees
  - Destroy the phone or components (Camera, Messaging, etc.)

O'CONNOR DAVIES

Mobile Device Malware - Why Worry?

Today's Threats

HijackRAT disguised as Google Service Framework combines various hijacking techniques to allow hijacker to:

- Steal and send SMS messages
- Steal contacts
- Initiate malicious app updates
- Scan for installed legitimate banking apps on the mobile device and replace them with fake utilities
- Attempt to disable mobile security software or antivirus installed on a compromised Android device

Source:Webroot

O'CONNOR DAVIES

Cyber Extortion – A Closer Look

- Entities are being held ransom at the risk of:
  - Releasing protected or personal data
    - Threats may be placed to expose employee SSNs or health information on file
  - Denial of service
    - Systems could be brought to a crawl or taken offline.

O'CONNOR DAVIES

Cyber Extortion – A Closer Look (con't)

- Entities are being held ransom at the risk of:
  - A ransomware variant placing child pornography on your system and threatening to alert the authorities

O'CONNOR DAVIES

Cyber Extortion – A Closer Look (con't)

Cryptolocker 2.0

Your personal files are encrypted

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files | << Back | Proceed to payment >>

O'CONNOR DAVIES

Verizon Data Breach Report - 2014

- Point of Sale Intrusions
- Web app attacks
- Insider misuse
- Physical theft/loss
- Miscellaneous errors
- Crimeware
- Card Skimmers
- Dos Attacks
- Cyber Espionage

OF THE INCIDENTS WE'VE SEEN OVER THE LAST 10 YEARS — AND 94% OF THE BREACHES IN 2013 — CAN BE DESCRIBED BY JUST NINE PATTERNS.

O'CONNOR DAVIES

The Insider Threat

- To have a holistic security program you must also consider the threat within
- Whenever an individual is given access to your environment, they pose a risk
- The individuals can be:
  - malicious and wish to perpetrate fraud or steal data; or
  - Insufficiently trained and monitored and cause data entry errors or introduce malware into the environment

O'CONNOR DAVIES

The Insider Threat

- Majority of financial fraud is still committed by the inside "trusted employee"
  - Data theft is predominately committed by external actors
- The "trusted employee" is in most cases leveraging the financial applications to commit and conceal the fraud

O'CONNOR DAVIES

How Do We Protect the Entity?

- Do not underestimate your cyber risk and fraud exposure – SIZE DOES NOT MATTER!
- Conduct a formal cyber security/IT risk assessment
- Do not assume that information security is an IT issue alone
  - IT Security is a business issue that requires the assistance of a technical solution

PKF

O'CONNOR DAVIES

How Do We Protect the Entity?

- Ensure you have a resource that can effectively communicate the identified risks in understandable and business related terms
  - In order to manage risk, you need to first understand it
- Establish or verify you have a strong IT security governance program
- Know your compliance obligations

PKF

O'CONNOR DAVIES

How Do We Protect the Entity?

- Provide routine security awareness training
  - Your employees are your biggest security investment and vulnerability
  - Phishing training is essential
- Perform due diligence on all third parties
  - Vendor management and monitoring is critical
  - Vendors are a means to delegate a task Responsibility will always remain with the Entity and cannot be delegated

PKF

O'CONNOR DAVIES

How Do We Protect the Entity?

- Have independent IT security evolutions/audits
  - IT is one of the highest risk areas in your Entity but also the least understood and controlled
  - Internal IT sometimes has difficulty seeing the "forest from the trees"
  - Security and Operations have different goals and skill sets
  - IT is often under resourced

PKF

O'CONNOR DAVIES

How Do We Protect the Entity?

- Use two-factor authentication when possible
  - If not possible, strong passwords are key
  - Train employees to use passphrases
    - "GoodLuckCrackingThisP@ssword!"
- Implement data loss prevention software
- Isolate key assets and data

PKF

O'CONNOR DAVIES

How Do We Protect the Entity?

- Ensure:
  - Users are provided the minimum privileges necessary
  - Incompatible roles are separated
    - If you cannot separate roles, provide independent reviews and reconciliations
  - Vendor patches are up-to-date and installed consistently and timely (Operating System and Third party Apps) (e.g., adobe, flash, java, etc.)
  - Antivirus is installed, active and up-to-date

PKF

O'CONNOR DAVIES

How Do We Protect the Entity?

- Ensure:
  - Network devices (routers, switches and firewalls) are configured correctly and securely using industry guidelines (e.g., Center for Internet Security)
  - Default vendor passwords are changed

PKF

O'CONNOR DAVIES

How Do We Protect the Entity?

- Ensure:
  - Effective monitoring and sufficient logging (operational and security)
    - A control is only as good as the control that exists to monitor it
    - All access to sensitive data and all sensitive transactions executed should be recorded and traceable to a person
  - A backup and disaster recovery strategy exists that meets the business requirements for acceptable downtime and data loss

PKF

O'CONNOR DAVIES

How Do We Protect the Entity?

- Ensure:
  - IT administrators are assigned separate credentials for management and non-management activities (browsing the web, e-mail, etc.)
- Have an incident response plan
  - It is a not a matter of if but when you will be breached

PKF

O'CONNOR DAVIES

How Do You Protect Your Entity?

- Mobile Device Protections:
  - Have a documented and defined mobile device policy
    - Critical if allowing employees to use their own device (BYOD)
  - Require phones be password protected
    - Enforce this via a system control and not the honor system

O'CONNOR DAVIES

How Do We Protect the Entity?

- EFT Fraud Protections:
  - Dedicate computers for online banking
  - Segregate EFT functions between initiator and approver
  - Establish ACH Debit Filters or Blocks
  - Dedicate clearing accounts using "just-in-time" deposits
  - Reconcile EFT Transactions daily
  - Establish restrictive dollar transfer limits

O'CONNOR DAVIES

How Do We Protect the Entity?

- EFT Fraud Protections:
  - Use multifactor authentication
  - Require additional "out-of-band" authorization or notifications of transfers (call back, text message, etc)
  - Establish ACH Debit Filters or Blocks
  - Dedicate clearing accounts using "just-in-time" deposits

PKF

O'CONNOR DAVIES

Questions?

Ciro V. Cuono,
Partner
CCuono@odpkf.com
914-421-5671

Thomas J. DeMayo,
Director, IT Audit and Consulting
TDeMayo@odpkf.com
646-449-6353

PKF