

Deloitte.

Computer Crime: A Growing Concern

Jean-François Legault
Sr Manager – Analytic & Forensic Technology

Audit . Tax . Consulting . Financial Advisory .

Factors of Influence



The Dissolving Perimeter

- Technology has dissolved the organization's security perimeter:
 - Remote access
 - Mobile devices
 - Wireless technology
 - Web applications
- The home PC has assumed the role of "secure" terminal for financial transactions:
 - Online banking
 - Electronic commerce

Ubiquity of VoIP

- Routing of voice conversations over an Internet Protocol based network
- Uses for VoIP
 - Toll bypass
 - Internet Telephony
 - PBX
- Provides many opportunities for fraudsters
 - Appear to be calling from a local number
 - Obtaining phone number for shell companies
 - Spoofing the called ID

Influence of Organized Crime

- Important player in the world of online crime
- Groups do not need to possess technical skills
 - Provide financial backing for online crime ventures
 - Technical aspects are outsourced to cybercriminals
- Currently estimated that 75-80% of malware is developed by or for organized crime
 - High profit margins and low sanctions
- Online crime is also used to finance the classic criminal enterprise

Emergence of Mobile Devices

- Integrated mobile devices have become the norm for executives in today's business world
- Integrate personal digital assistants, cellular phone as well as high-speed wireless Internet access using a variety of technologies
- Allows the user to access email, browse the web or access diverse mobile applications and information services
 - Many integrate digital storage features which range from simple file storage to MP3 players

Emergence of the Web 2.0

- Coined by O'Reilly Media in 2003
- Represents a perceived second generation of web-based communities and hosted services
- Social networking sites focus on connecting individuals through the building of a network of online contacts
- Sites have proven themselves very interesting to fraudsters since its members share quite a bit of information about themselves
 - Including educational background, professional history as well as their list of contacts

Paradigm Shift in Information Protection

Corporations/Government

Consumers/Clients



Blogs

Social Networks

Deloitte.

Corporate Fraud and Technology



Audit • Tax • Consulting • Financial Advisory.

Corporate Fraud and Technology

- Organizations rely on technology to conduct daily operations
- Data is stored in digital form to facilitate storage and analysis
- Fraud schemes have not changed, they are simply facilitated by technology

Data Manipulation

- Manipulating stored data or reports produced by an ERP system can easily conceal certain schemes:
 - Changing the invoice due date for short term skimming
 - Manipulating the direct deposit bank account for an employee who just left
 - Removing records from a report to hide manual adjustments
 - Changing sales associate information to obtain additional commissions

User Privileges

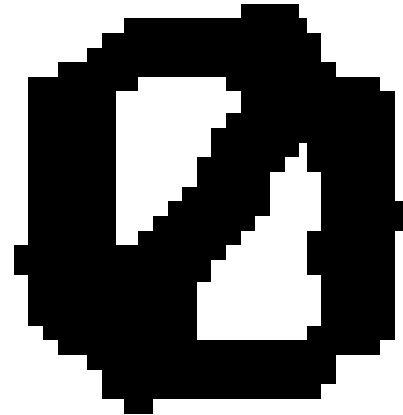
- Access control is the foundation for most IT security
- Fraudsters can exploit flaws in authentication schemes:
 - Least privilege not enforced
 - No segregation of duties
 - Weak passwords
- Can lead to:
 - Information disclosure
 - Approvals granted using compromised accounts

Document forgeries

- Fraudsters can easily forge and alter documents using inexpensive software and technology
 - Documents can be scanned and altered
 - Signatures can be scanned and used on other documents
 - Documents can be forged
- Much higher quality forgeries and alterations than what was previously seen
- Forged documents can be used in a wide number of schemes:
 - Producing fictitious receipts as part of an expenses scheme
 - Forged approvals

Document Forgeries

Ticket System
Generated Zero

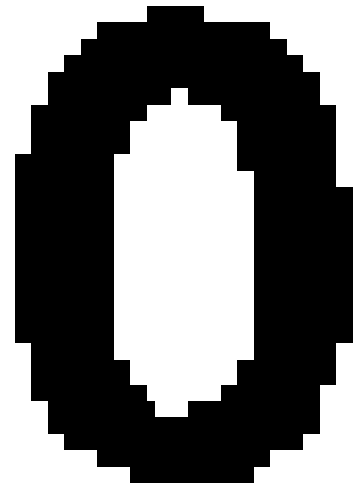


FOR: MR [REDACTED]

----- I T I N E R A R Y -----

*** AIR/RAIL/BUS ***
FROM TO CARRIER FLT/CL ST DATE DEPART ARRIVE MEALS BAG:
CALGARY REGINA AIR CANADA B508 M HK 10JULY 6:45A 8:00A 2PC
FOKKER F28
SEAT 06D
INA CANADIAN REG
CALGARY AIR CANADA B517 M HK 12. P 2PC
FOKKER F28
SEAT 03B
CANADIAN REG

Generated by
Expense Submitter



AIR CANADA TKT

CL 2

787.00

Shell Companies

- Fraudsters use shell companies that only appear to be real
- Information is falsified in order to fool the victim:
 - Corporate website
 - Corporate charter
 - Financial statements
 - Independent data
 - False financial institutions
- Technology can be used to facilitate all aspects of a shell company

Shell Companies

- Using Internet services, a shell company can be created in a matter of seconds
 - Corporate website/email: low cost domain registration and hosting
 - Fax: email to fax gateways
 - Phone: Internet telephony
 - Postal information: Remote mail scanning
- Allows fraudster to build a web of shell companies
- Payment for Internet services can be made using a compromised credit card

Theft of Trade Secrets

- Organizations invest time, money and energy into developing information, processes, techniques and other forms of trade secrets
- Often priceless and can make or break a company
- Most often stored in digital form on a variety of media

Theft of Trade Secrets

- Approximately 85% of IP theft is committed by insiders
- Employees have the most knowledge about trade secrets and have the means to access them
- Other insiders like contractors, temporary staff, utility/maintenance personnel may also have access to electronic storage
- Employees have precise intentions when they steal trade secrets:
 - Establish a new business
 - Hired by a competitor
 - Selling to the highest bidder

Theft of Trade Secrets

- Intangible assets like trade secrets are easily transportable
- Electronic Messaging can be used to redirect information outside the organizations: personal accounts, webmail or third party
- Ever increasing capacity of removable storage devices simplifies copying of information:
 - USB Thumbdrives
 - MP3 Players
 - Mobile devices (PDAs, cell phones, etc.)
- Less technology inclined resort to printing out documents stored on the network

Disclosure of Personally Identifiable Information

- IT staff has access to databases containing sensitive information
 - Databases can easily be queried by the IT staff in order to extract valuable personally identifiable information
- Call center agents have access to customer profiles which also contain valuable personally identifiable information
 - Agents can “surf” this information and collect profiles with the best credit ratings for identity thefts

Deloitte.

Evolutions in Online Fraud



Audit • Tax • Consulting • Financial Advisory.

A Look at Phishing

- Has become one of the most recognized online scams
- Uses social engineering to fraudulently acquire sensitive information
- Typically carried out over email
- Some statistics (APWG report, April 2007)
 - Number of unique phishing sites received in April: **55643**
 - Number of brands hijacked by phishing campaigns in April: **172**
 - Country hosting the most phishing websites in April: **United States**
 - Contain some form of target name in URL: **13.5 %**
 - No hostname just IP address: **6 %**

Exploiting Social Networks for Fun & Profit

- Phishers are increasingly targeting users of social networking sites
 - Capturing credentials via fake social networking site that resembles the one being spoofed
 - Using captured information or compromised accounts are to send advertising to friends and contacts
 - Attempting to gain access to the victim's email account using the captured credentials
 - Using the compromised email accounts to gain access to commercial sites and reselling access to these accounts
- An Indiana University study established that 72% of individuals who received messages spoofed to appear as they are coming from social networking "contacts" were fooled

Vishing (Take One)

- Media coverage of phishing has made potential victims skeptical of such attacks
- Fraudsters have resorted to providing a phone number instead of a URL
- VoIP is used to establish a hard to trace regional presence
- Certain scams reuse IVR system instructions to reduce victim skepticism

Vishing (Take Two)

- Fraudsters use VoIP and Caller-ID spoofing techniques to place calls which appear to come from legitimate companies
- Thinking the call is legitimate victims see no reason not to provide the requested information
- Fraudsters will go as far as to leave an alarming voicemail requesting the potential victim return their call

SMiShing

- Mobile devices have become ubiquitous in the corporate world and with younger crowds
- Fraudsters are leveraging these devices to commit another form of phishing
- Text messages (SMS) are used as the delivery medium
- Techniques and objectives vary:
 - Opt-out of mobile spam in order to deliver mobile malware
 - Attempt to collect personal information through various alarming messages

Pump & Dump

- False or misleading information is sent to “potential” investors in order to bait them into buying the targeted stock
- Scheme involves telemarketing and spam:
 - Telemarketing can now be done using VoIP as a cloaking method
 - Spamming now involves the use of images and PDFs to evade spam filters

Pump & Dump



Criminal Resources

▶ [Mrsam...@gmail.com](#) [View profile](#) [More options](#) Jul 3, 9:06 pm

HELLO

1) Manufacturing plastic cards ready for shopping
2) Record on white and color plastic.

1) Manufacturing plastic of bank quality is made on the newest equipment with use of own technologies.

I make following kinds of cards:
MasterCard
Visa
AMEX

I guarantee a correct bank microfont, with an excellent strip of the signature. Quality card 2800 dpi. The design of a card is identical to the bank original. Holograms on cards are IDENTICAL to the presents. The price 150 USD for 1 ready card. Cost is not included in cost of plastic dumps. Minimal order of 5 products of the given type.

2) Record on white and color plastic Record on white plastic - 30 USD. Record on color plastic - 80 USD. Cost of record does not include cost dumps. The minimal party of the order 10 pieces.

Payment: E-gold, WEbMoney.
Delivery is made through a conductor, or by mail. The price of delivery through a conductor 25 USD, by mail 40 USD. Sending Order immediately after reception of money.

Criminal Resources

=====

Dumps Are also Available

Europe(and the rest of the world) \$USD

Visa Classic / Mastercard Europe \$80

Visa Gold / Platinum / Business / Signature \$140

Visa Gold / Platinum / Business / Signature (Swiss, Spain, France, Italy, Turkey and more) \$150

Canada

Visa Classic \$20

Visa Gold / Platinum / Business / Business / Signature \$35

MasterCard Canada \$20

USA

Visa Classic \$15

Visa Gold / Platinum / Business / Business / Signature \$35

MasterCard USA \$15

Discover, American Express, JCB \$30

American Express + CID (Card Identification Digits) \$100

P.S

Prices are very negotiable, all depends from how much you buy :-)

If you're big customer, prices are VERY negotiable. Just contact me.

Minimal order 500\$. Payment methods: E-Gold,WebMoney.

ICQ: 400291609

THE EQUIPMENT!

Readers/Writers:

PR232 Portable Magnetic Card Reader \$350

MSR206 Card Writer/Reader/Encoder \$300

MSR 500M Portable Magnetic Card Reader \$300

Mini400 USB Portable Magnetic Credit Card Reader \$350

Embossers/Tipper:

EM2000A Plastic Card Embosser \$1200

EM2000B Plastic Card Embosser \$1800

TP-90 Tipper/Hot Stamper the improved model \$1000.00


Also we can sell skimmers for different bankomats, hologramms and programms and software available for sale

God Luck !!!

Criminal Resources

▸ Accounts from banks in EUROPE, dump+pin for sale! Outline · [Standard] · Linear+

[Track this topic](#) | [Email this topic](#) | [Print this topic](#)

scarlett	Today, 02:53 PM	Post #1
Unregistered	<p>Hello to everyone who interested in my information!</p> <p>I sale accounts from banks in EUROPE (and some times America) with information for transfer (tan, password, etc). It cost 10% of Balance.</p> <p>And i sale dumps + pin. Price:</p> <p>3-10 Dump+pin = 250\$ each 10-20 Dump+pin = 200\$ 20-100 Dump+pin = 100\$</p> <p>Minimum order 3 Dump+pin</p> <p>Also i have dumps, but no pins, i sell them for</p> <p>10-50 = 40\$ each 50-100 = 25\$</p> <p>Minimum order 10 Dump</p> <p>My contacts: icq 33-77-11-656 or scarletteng@gmail.com</p> <p>Contact me with any questions as well i will answer all your questions!</p> <p>Payment can be made by E-GOLD and Webmoney ONLY!</p>	
		QUOTE REPLY

Mortgage Fraud

- Mortgage fraud has become pervasive in the real estate industry
- Web sites designed to facilitate mortgage fraud:
 - “Rental” of well funded bank accounts
 - Hitching customers to strangers credit cards
 - Offering pay stubs from bogus companies
- Sites also offer tools to create false documents like pay stubs and financial statements

Mortgage Fraud

*IN THE REAL ESTATE BUSINESS? THEN YOU NEED THIS PROGRAM!
IF YOU CANT MAKE IT, AT LEAST YOU CAN FAKE IT!*

FINALLY, A COMPUTER PROGRAM THAT WILL CREATE PERSONALIZED PAYCHECK STUBS INSTANTLY! GO AHEAD AND "FAKE HOW MUCH YOU MAKE"



This computer program does it all! All you have to do is type in the name of employee, type in company name (and logo if desired), hourly salary and what state you live in (for precise tax computations) and the computer program does the rest! It is THAT EASY!!!

This template creates authentic looking pay stubs and is intended for entertainment purposes only!

Once payment is made, an email will be sent to you with the EASY TO USE computer program attached! Use this computer program not just once, but TIME AND TIME AGAIN!

I highly suggest you do not use logos from companies that are real on these stubs, I wouldn't use any company trademarks or copyrights either. Remember, these are intended for entertainment purposes only.

Social Networks

- Social networks have become the media darlings of the Web 2.0 but behind this hides many risks to individuals
- Members of these networks will build a profile which may include location, job, education as well as friends or business contacts
- It is also possible to join networks (cities and colleges), special interest groups as well as indicate events they will be participating in
- They can also post pictures and tag other members which are in the picture

The Risks of Social Networking

- Social networks can directly impact an organizations, its employees and clients:
 - Information disclosure
 - Image and reputation impacts
 - Information for targeted attacks
 - Impersonation and social engineering

Questions



Deloitte.

Crimeware



Audit • Tax • Consulting • Financial Advisory.

Malware for the criminal enterprise

- Organized crime is involved in the production of crimeware
 - Financing of crimeware development
 - Recruiting of highly skilled graduates
 - Crimeware for hire
- Open source development model
 - Multiple contributors, bug fixes, paid feature enhancements, module reuse
- Transition from wide scale attacks to targeted attacks:
 - More Trojans, less viruses and worms

Trojan Horse

- Perform malicious actions while appearing to perform a useful function
- Rely on social engineering rather than computer flaws as they cannot operate autonomously
- Used to facilitate the installation or injection of crimeware on the targeted system

Keystroke Loggers

- Crimeware designed to capture a victim's keystrokes
- Some will capture all keystrokes while others capture keystrokes based on specific criterias
- Delivered through Trojans, browser exploits, etc.

Botnets

- Botnets are networks of compromised systems under a single command and control infrastructure
- Infected using a variety of techniques such as worms, remote exploits affecting the operating system or the web browser as well as using malware dropping Trojans
- Command and control infrastructures have evolved to using resilient server infrastructures to prevent the botnet from being taken down when the server is located

Botnets

- Newer bots use proprietary protocols (like P2P) for command and control and will also use encryption protocols to protect the communication channels
- The size of botnets have scaled down over time
 - Stay below the radar of law enforcement and ISPs
 - Targeted botnets designed for various criminal activity
- No longer a question of how many bots are "owned", its about profit:
 - Spam delivery
 - Phishing infrastructure
 - Malware delivery

Capitalizing on Malware

- Malware (malicious software) is software designed to infiltrate or damage computer systems and other electronic devices
- Crimeware is a form of malware used to simplify or automate online criminal activities
 - Categories of crimeware are similar to malware
 - It is differentiated from malware based on the intended use
- Financially neutral malware have fewer variants than successful crimeware

Spear Phishing

- "Personalized" phishing campaigns
- Highly targeted towards specific groups of individuals:
 - Companies
 - Government
 - Organization/Agency
- Email appears to come from legitimate source in relation to the targeted group
- Social networking sites can be used to obtain targeting data
- Objective is to gain access to corporate resources:
 - Collect username/password
 - Trojan

Compromised Servers & Browser Exploits

- Exploiting security flaws in web browser has become a common occurrence for delivery of crimeware to a computer
- Cybercriminal delivers "infected" web page to unsuspecting users:
 - Compromise vulnerable web servers to host web pages
 - Pay webmasters to host the web pages
- Cybercriminal lures potential victims to site and injects crimeware using the malicious page:
 - Spear Phishing type attack
 - Ad servers, Social network profiles, etc.
 - Webmaster participation

Compromised Servers & Browser Exploits

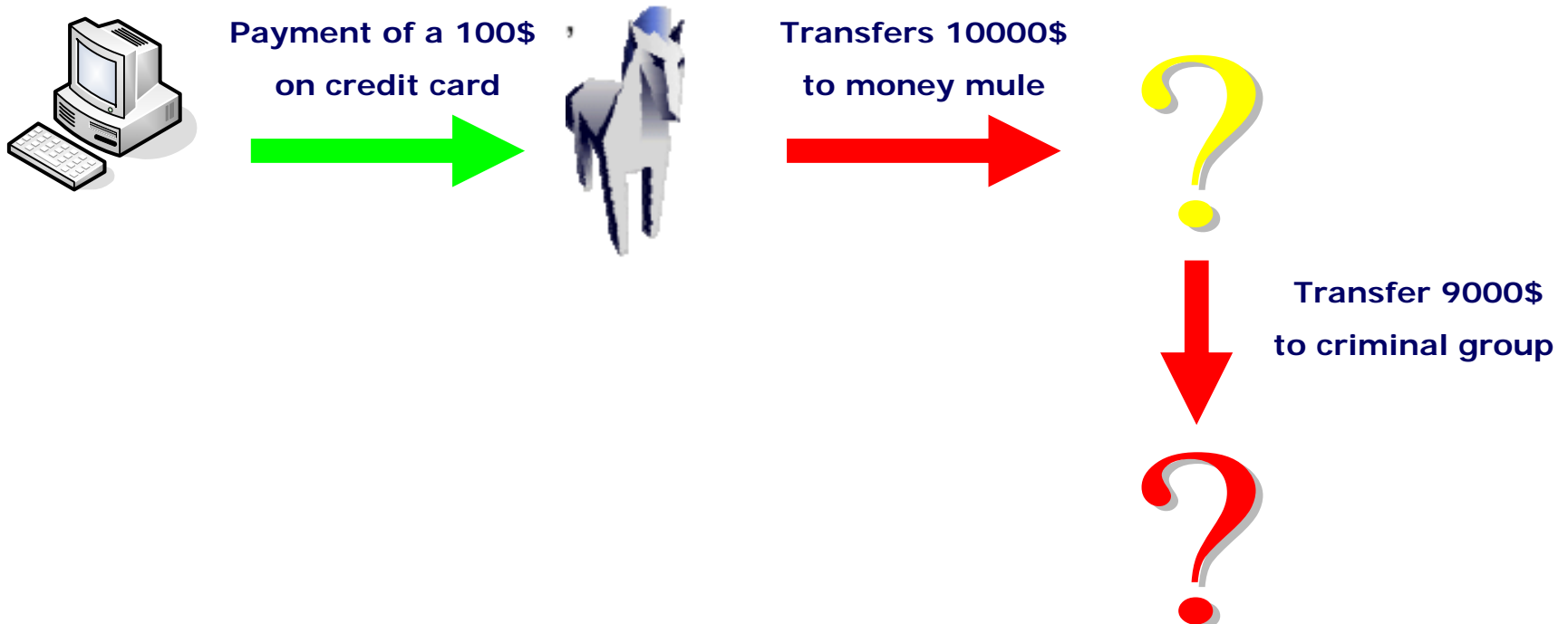
- Everyone is welcome to join the iframeCASH.biz partnership program
- Earn \$0.08 (\$80/1000 installs) and more for each unique iframe installs
- You only put the short one line iframe code on your page(s) and start to MAKE MONEY
- WITHOUT any Active-X console or any pop-ups...It means that you will not lose your unique visitors with our iframe!
- The best percentage of installs (10-40 % from the total traff or it's \$4-\$15 FOR 1000 UNIQUE VISITORS)
- DAILY updated soft
- We have 3 reliable servers with excellent speed
- Payments every Tuesday
- Real-time statistic of your work
- Payment via: Fethard, Webmoney, Wire Egold ; and Western Union (WU)
- More than 300 webmasters work with us
- Friendly support service
- Everybody who works with us is satisfied.

Inflating Stock Prices

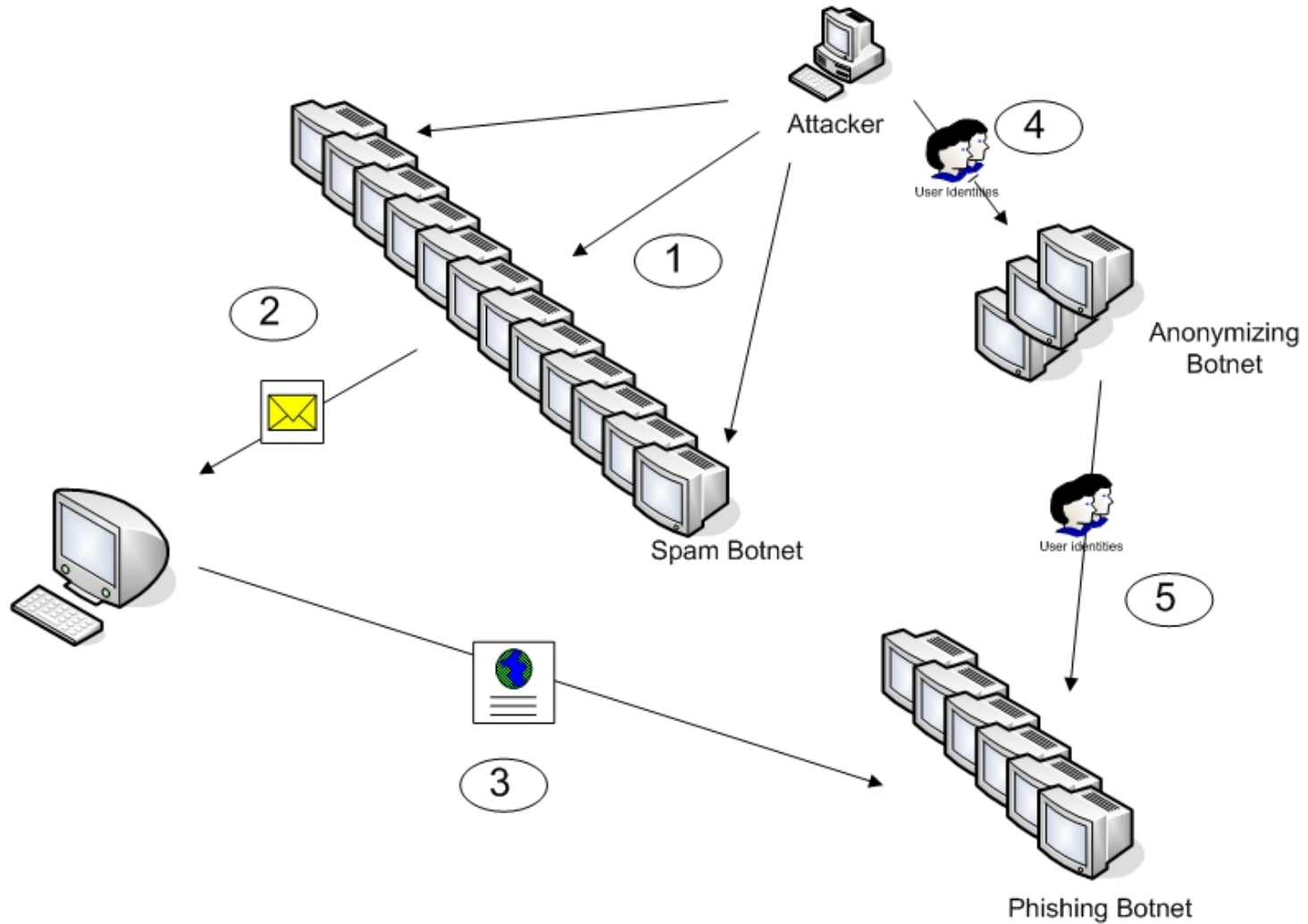
- Pump and dump scheme are common occurrences of the online fraud world
- Using keystroke loggers, criminals haven taken a different approach to inflate stock prices:
 - Keylogger captures credentials for online trading sites
 - Criminals sell off the content of the portfolio
 - Funds are used to purchase the targeted stock
 - Criminals sell off the stocks they purchased before the scam
 - Online investors are left with worthless stocks in a potentially flourishing portfolio

Man in the Browser

- Malicious software which inserts itself in the communication flow between the browser and the web application
- Allows fraudster to manipulate the transaction



Botnets for Phishing



Geopolitics and the World of Crimeware

- China:

- Responsible for 30% of malware distributed in the world
- Of this, 17% is designed to steal passwords from online gamers

- Brazil:

- Accounts for 14.2% of malware distributed in the world
- Majority are Trojans designed to steal information from online banking users

- Russia and Ukraine:

- Produce 7.5% of malware distributed in the world
- Mainly backdoors used to gain access to sensitive information

Proceeds of Crime



Virtual Money and Illicit Fund

- Digital currency systems have been linked to various facets on online crime, being the medium of choice for funds transfers relating to cybercrime
 - Payment for personal identifiable information
 - Payment for malware development/hosting
 - Payment of other illicit materials
 - Online money laundering
- Used as part of high yield investment programs like Ponzi and pyramid schemes as many make transactions irreversible

Virtual Money and Illicit Funds

- Digital currency operators are not banks:
 - No current requirement to perform "know your customer" background checks
- Many only require an email address to open an account
 - Other contact information is requested but rarely verified

Online Money Laundering

- Online criminals must transfer funds or high value goods acquired as part of online scams
- Need for money mules arises as criminals located in developing countries need to convert financial information obtained into usable funds and goods in their country of residence
- Money mules are recruited to act as “Financial agents” or “Money Transfer Agents”
 - Receive the funds and transfer them out using a money transfer service
 - Keep a percentage of the funds as payment for their services

Online Money Laundering



Dear Sirs,

Our Company [REDACTED] is a research-driven investment firm focused on de novo, seed and early stage investments in the physical and life sciences. Both big companies and private entities are among our customers.

We'd like to declare a recruitment for a new position – **regional assistant**.

In order to get this position you do not need to have any special education, training or experience. You will be required to have 1 or 2 free hours a day and b to have a bank account, to be used for the customers' needs. You should also be a confident internet user and have calculation skills.

While performing your duties on a position of a regional assistant, you will be supposed to deal with the 2-3 bank transactions from customers every week (2000-3000 euro each transaction), to make calculations concerning each remittance (to deduct 10% salary out of the total amount you have available, the expenses for traveling and charges for Western Union/Money Gram transfer, etc.) and to accomplish Western Union//Money Gram instant transfers for the company's regional branches.

The staff in our head office will be glad to assist you if you have any difficulties while performing your duties, especially in the beginning of our business cooperation. You will be provided with a professional advice anytime it should be necessary for you.

We are sure that in a short period of time you will start enjoying your new job and will be seeking for the opportunity of professional growth!

We are looking forward to handling business with you!

You may find more detailed information about the position at our website by visiting the following [hyperlink](#) or by forwarding an e-mail to the Chief Manager.

Yours faithfully

Josh Wolfe

The Head of personnel department

Laundering Proceeds of Crime

- The Internet presents a number of opportunities for laundering proceeds of crime:
 - Use of botnets to play in online casinos
 - Use of virtual currencies and virtual worlds
- These methods can only be successful if the criminal is able to convert his proceeds into a financial vehicle which can be used online (virtual currencies, credit cards, electronic fund transfers, etc.)

Sources

- MessageLabs Intelligence : 2006 Annual Security Report
- iC3 Internet Crime Report 2006
- Sophos Security Threat Report 2007
- McAfee Organized Crime and the Internet 2006
- 2006 ACFE Report to the Nation on Occupational Fraud & Abuse
- Anti-Phishing Working Group

Jean-François Legault

Sr Manager – Analytic & Forensic Technology

Deloitte & Touche LLP (Montreal, Canada)

jlegault@deloitte.ca

514-393-5417



Deloitte.

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 6,800 people in 51 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. The firm is dedicated to helping its clients and its people excel. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

© Deloitte & Touche LLP and affiliated entities.



Member of
Deloitte Touche Tohmatsu