

# CYBER CRIME

## THE ANATOMY OF THE HACK



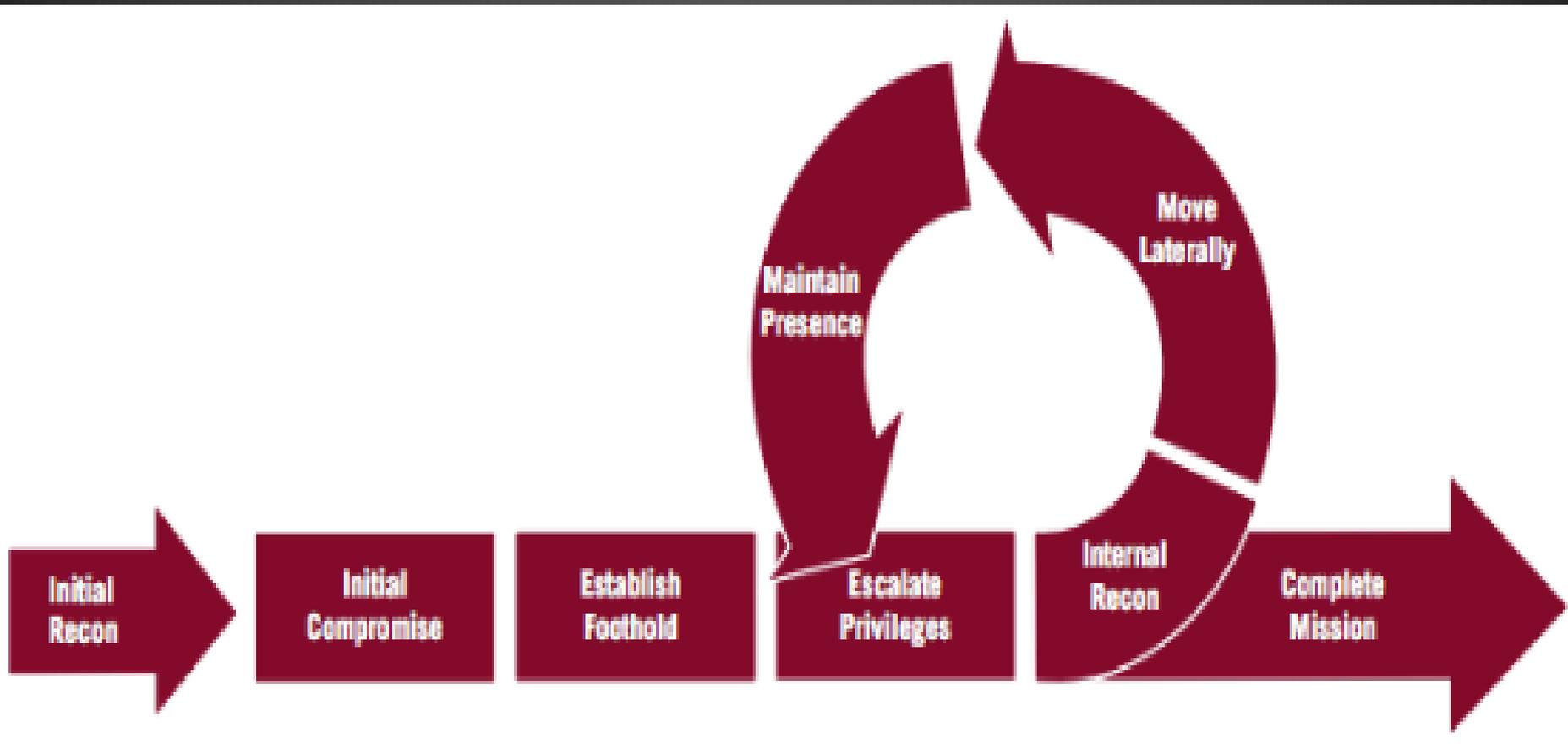
# ME

- ⊗ Aaron Sparling
- ⊗ Portland Police Bureau Criminal Intelligence Unit
- ⊗ TFO United States Secret Service ECTF (Seattle)
- ⊗ Cyber Investigator (OSINT)
- ⊗ Computer Forensic Examiner
- ⊗ Interests: Network Intrusions, Malware and Memory Forensics, Penetration Testing, OSINT.
- ⊗ **What I am NOT “Spelling Bee Champion”**

# OBJECTIVES

- ① Know the Profile of a Network Breach (Target, Home Depot)
- ② Cybercrime (ecosystem)and Organization
- ③ Safe Internet Practices
- ④ Understand Key Terms and Concepts

# CYBERCRIME MODEL



# Types of Computers

- PC or Personal Computer (Desktop Workstation)
- Laptop/Netbook/Chromebook (Mobile/Portable)
- Server (Companies, Government, Education, Commerce)
- Micro Controllers (Small form Factor ex: Raspberry PI)
- Mobile Devices (IOS, Android, Windows, Linux)

# THE COMPUTER





# THE INTERNET



# Internet or WWW

- Established in the 1960's by US Military as a fail safe form of communication.
- Early stage mostly used by Government and Large Universities (Distributive Processing)
- Grew exponentially in the 1990's
- Now covers entire globe and has numerous economies built on it infrastructure (Ecommerce, Gold Farming, Bitcoins)
- Wireless technologies Connect people via WIFI and Broadband Communications

# Networks

- A Network is more than one computer connected and able to communicate with one another following set protocols.
- Many Different Types of networks
  - Large = Government    Small = Home
- Public (The WEB)
- Private (PPB Intranet)
- Dark Net or Deep Net (TOR, P2P, VPN Services)

# DEEP WEB

## DARK NET

- Hidden Services
- Financial Services
- Commercial Services
- Hosting Services
- BLOGS
- Forums / Boards / IRC
- Email / Messaging
- IRC Command and Control Servers (BOTS/Malware)

# DARK NET

## Underbelly of the Internet

Drugs 8,984

Cannabis 2,191  
 Dissociatives 106  
 Ecstasy 912  
 Intoxicants 34  
 Opioids 299  
 Other 36  
 Precursors 60  
 Prescription 2,847  
 Psychedelics 877  
 Stimulants 943  
 Tobacco 228

Apparel 568

Art 59

Biotic materials 1

Books 1,197

Collectibles 38

Computer equipment 109

Custom Orders 53

Digital goods 837

Drug paraphernalia 459

Electronics 160

Erotica 715

Fireworks 7

Food 11

Forgeries 124

Hardware 49

Home & Garden 23

Jewelry 79

Lab Supplies 24

Lotteries & games 146

Medical 15

[Click here for an important security announcement](#)



7 GRAMS OF MEDICAL  
 CHERRY PI  
 B0.9466



Primobolan (LA Pharma), 30  
 tabs x 25mg  
 B0.1883



300 x Ritalin 10 mg  
 B8.4756



(1) 25I-NBOMe - 1100ug/ea  
 - Blotter  
 B0.0417



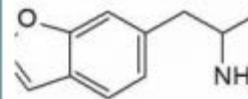
Modafinil 200mg - 300 Pills  
 B2.8871



Special 5x 50 (250) Pills  
 EPHEDRINE HCL Packets  
 B4.0187



1 gram PURE RAW  
 COLUMBIAN COCAINE - HQ  
 B1.6015



500mg of 3-MMC ultra pure  
 Pentedrone Crystalz  
 B0.3030



Masteron 10ml 100mg/ml -  
 Arrival Guaranteed



Pineapple Haze \*1.5 Gram  
 Listing\*



<Quality~MDMA!!! 1 Gram  
 1000mg



3 Ounces (84g) AAA  
 Organic Buds—Pick a Strain

From the forum

- Silk Road movie night nominations!
- Ask a drug expert physician about drugs and health
- Winning the war on drugs
- New display currencies
- Try Tails for a more secure OS
- Who's your favorite?
- Acknowledging Heroes

# PORTLAND

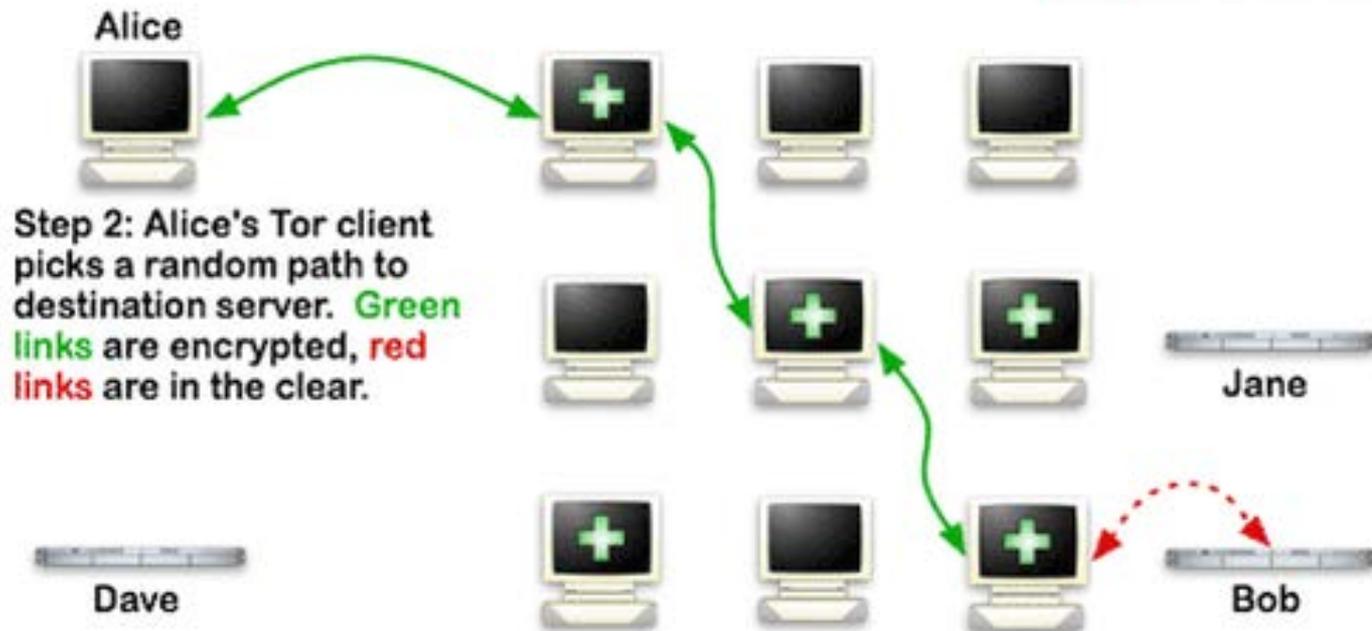
## **4 from Portland area linked to online meth ring, indicted on federal charges**

An indictment filed in U.S. District Court in Portland alleges Jason W. Hagen, 39, of Ridgefield, Wash; Chelsea L. Reder, 23, of Ridgefield, Wash; Richard E. Webster, 45, of Aloha; and Donald R. Bechen, 39, of Aloha, used black market website Silk Road to sell more than 17 pounds of meth between August 2012 and August 2013 in exchange for virtual currency Bitcoin, which can be exchanged for cash.

# HOW DOES IT WORK

## TOR Network

### How Tor Works: 2



# EXAMPLES OF CYBERCRIME

- Steal valuable information (financial)
- Embarrassment (personal Email or Photos)
- HACKTIVISM
- Destroy your Identity (financial and personal)
- Plant evidence on your system by using OR turning your machine into a BOT
- Use your System as DDOS platform or a BOT

# CYBER CRIME

	<b>NUISANCE</b>	<b>DATA THEFT</b>	<b>CYBER CRIME</b>	<b>HACKTIVISM</b>	<b>NETWORK ATTACK</b>
<b>Objective</b>	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
<b>Example</b>	Botnets & Spam	Intellectual Property Theft	Credit Card Theft	Website Defacements	Destroy Critical Infrastructure
<b>Targeted</b>	<b>X</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Character</b>	Automated	Persistent	Opportunistic	Conspicuous	Conflict Driven

# Anatomy of the Breach

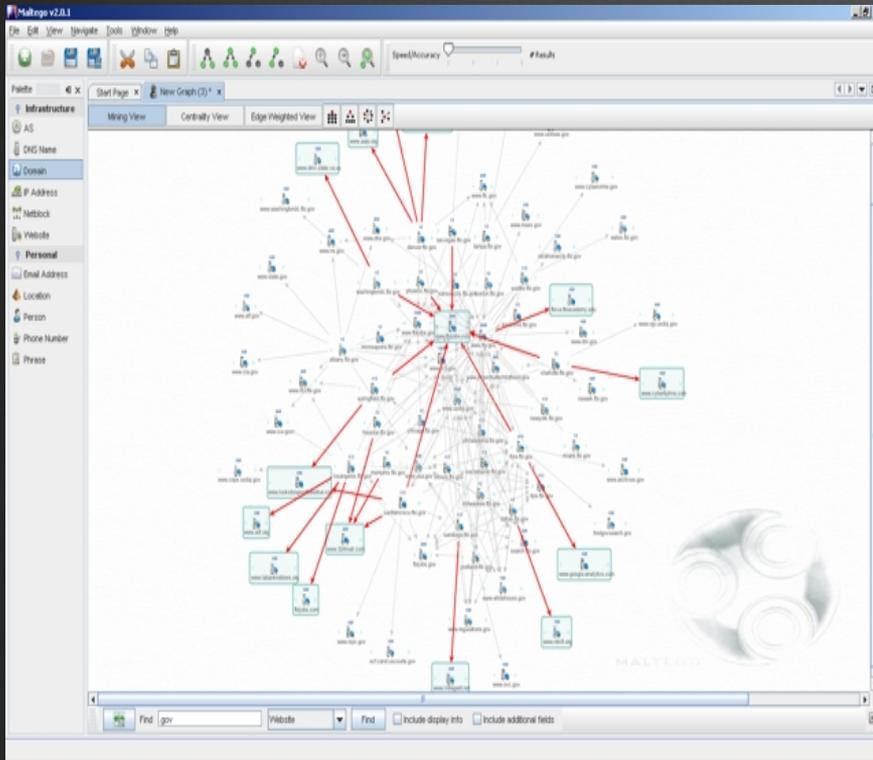


# RECONNAISSANCE

- OSINT (Open Source Intelligence)
  - Google-Fu (web based search engines/Bing, Yandex, ect)
  - Facebook, Twitter, LinkedIn,
  - OSINT Tools (Maletgo, Creepy, Spokeo, Casefile, ect.)
- Recon (Passive and Physical)
  - War Driving/ War Flying
  - Scan and Identify AP's (Open/Crypto Protected)
- Social Engineering Attacks
  - Persuasion, dumpster diving, **phishing attacks**,

# OSINT

Facebook, Twitter, LinkedIn,  
OSINT Tools (Maletgo, Creepy, Spokeo, Casefile,



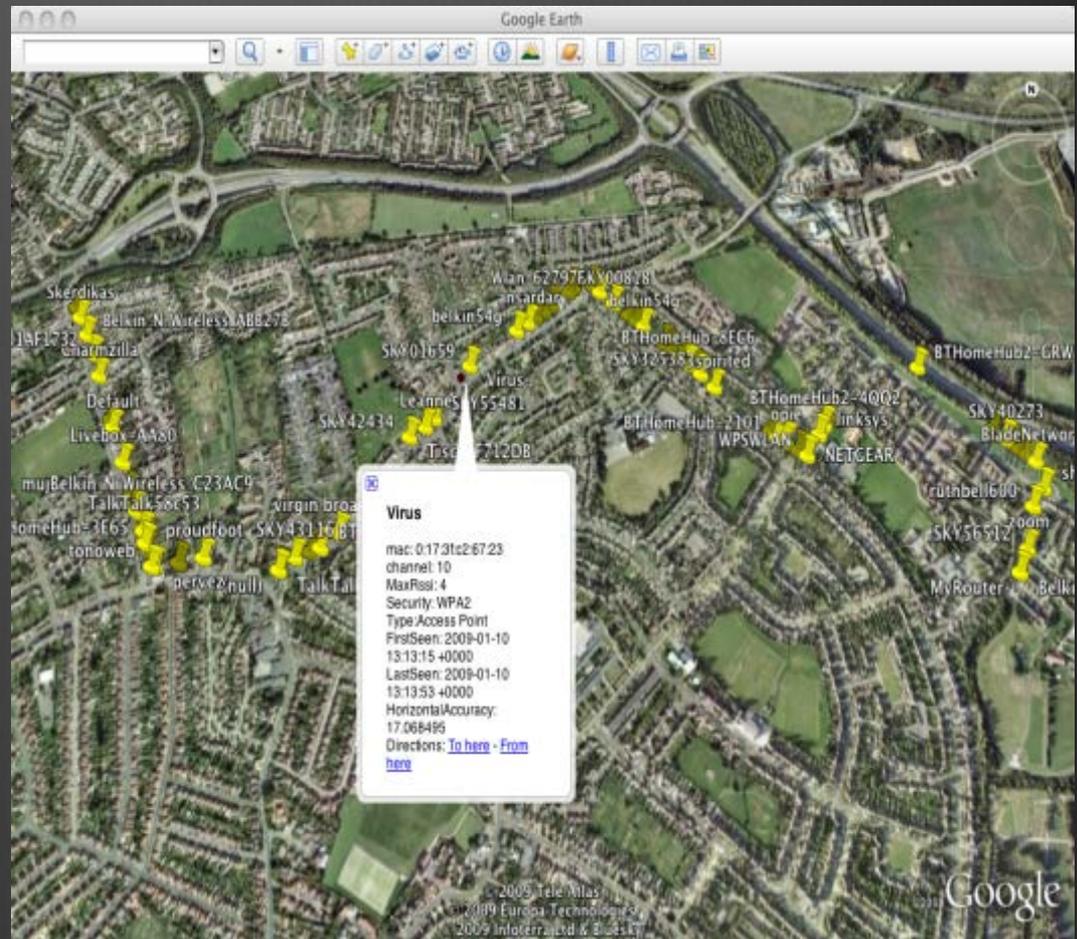
The screenshot shows the Cree.py location creeper interface. It features a table of coordinates and a map view. The table lists latitude, longitude, and time for various locations. The map view shows a satellite image of Uppsala, Sweden, with a red pin indicating a specific location. The map includes a scale bar (200m / 300yd) and coordinates (N 59° 51' 50.3", E 017° 38' 26.1").

Latitude	Longitude	Time
59.858393	17.637691	2010-08-30 23:25:08
59.858393	17.637691	2010-08-30 23:25:00
59.858393	17.637691	2010-08-30 23:24:43
59.858393	17.637691	2010-08-30 23:24:34
59.858393	17.637691	2010-08-30 23:24:26
59.858393	17.637691	2010-08-30 23:24:15
59.858393	17.637691	2010-08-30 23:23:59
59.858393	17.637691	2010-08-30 23:23:52
59.858393	17.637691	2010-08-30 23:23:46
59.858393	17.637691	2010-08-30 23:23:39
59.858393	17.637691	2010-08-30 23:23:26
59.858393	17.637691	2010-08-30 23:23:19
59.858393	17.637691	2010-08-30 23:23:12
59.858393	17.637691	2010-08-30 23:23:04
59.858393	17.637691	2010-08-30 23:22:57
59.858393	17.637691	2010-08-30 23:22:48
59.858393	17.637691	2010-08-30 23:22:38
59.858393	17.637691	2010-08-30 23:22:31
59.858393	17.637691	2010-08-30 23:22:21
59.858393	17.637691	2010-08-30 23:22:11

Photo from flickr  
Title : Uppsala domkyrka  
<http://www.flickr.com/photos/43529418@N06/4943217596>

# RECON

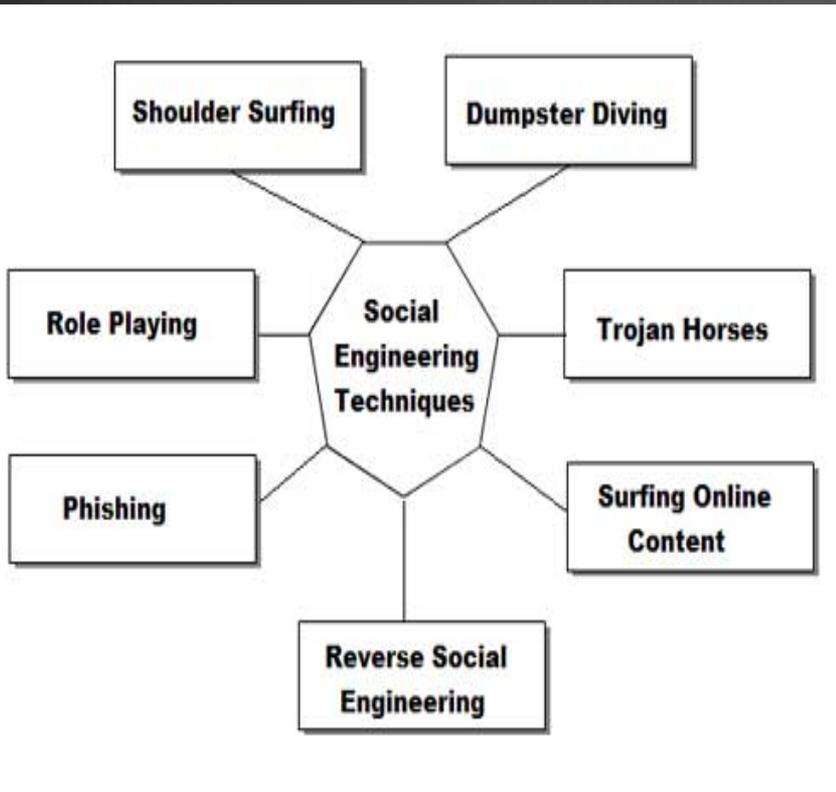
## Scan and Identify AP's (Open/Crypto Protected)



# War Driving/ War Flying Scan and Identify AP's (open/Crypto Protected)



# SOCIAL ENGINEERING



**SOCIAL ENGINEERING  
SPECIALIST**

*Because there is no patch  
for human stupidity*

# SOCIAL ENGINEERING PHISHING ATTACKS

- Use Social Profiling to gain detailed personal information  
(From the OSINT phase)
- Create FAKE websites which match the OSINT profile
- Send email with legitimate looking link to website
- Victim clicks the link directing them to a fake website
- Attacker either executes malicious code or records victims credentials

# CRYPTOLOCKER

- Computer is infected by clicking an email link (UPS, Fed-EX, or other tracking number type link which looks legit) **Social Engineering Attack**
- Malicious code finds all data files and wraps them in RSA 2048 bit encryption algorithm(private key stored on CC Server)
- Displays a Big red screen with instructions and count down timer, you pay or files are encrypted permanently
- 12,000 computers were infected in 1 week in United States, threatening 1 million mark in UK
- Last month Massachusetts PD paid 2 Bitcoins (\$750)
- Bitcoin 12/24/13 trading at \$667.00

The officers paid CryptoLocker's ransom. Police Lt. Gregory Ryan told press that his department shelled out around \$750 for two Bitcoin on November 10 - even then admitting his department had no idea what Bitcoin is, or how the malware functioned.

# Cryptolocker



Private key will be destroyed on  
**10/27/2013**  
1:22 AM

Time left  
**43 : 39 : 17**

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

MoneyPak (USA only)

Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

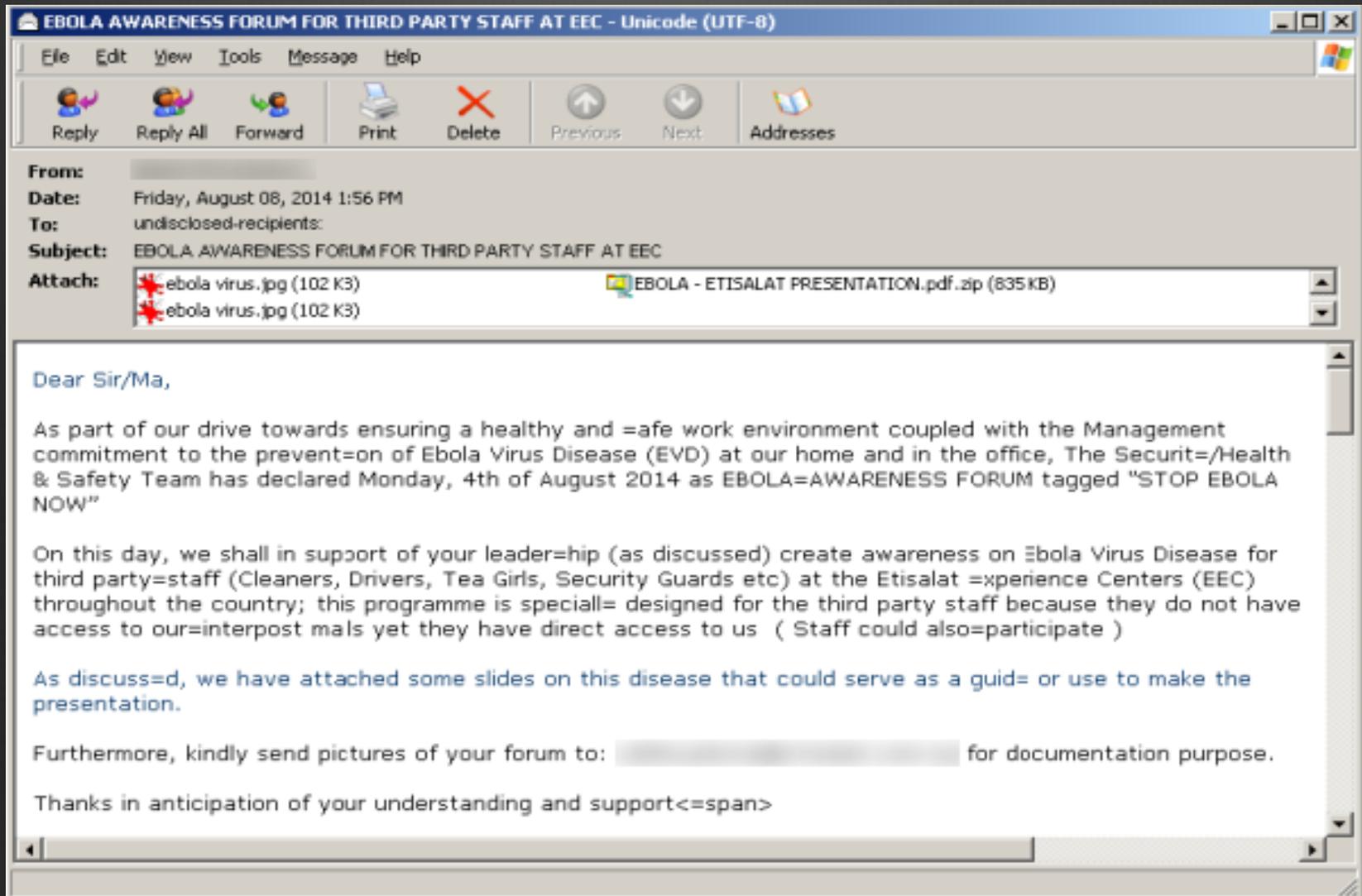
You have to send **2 BTC** to Bitcoin address

**1BrpkUXAoWf3SnFVwc2SKWQ37KrKjr2tus** and specify the Transaction ID on the next page, which will be verified and confirmed.

[Home Page](#)

[Getting started with Bitcoin](#)

# EBOLA MALWARE



**From:** [Redacted]

**Date:** Friday, August 08, 2014 1:56 PM

**To:** undisclosed-recipients:

**Subject:** EBOLA AWARENESS FORUM FOR THIRD PARTY STAFF AT EEC

**Attach:**  ebola virus.jpg (102 K3)  EBOLA - ETISALAT PRESENTATION.pdf.zip (835 KB)  ebola virus.jpg (102 K3)

Dear Sir/Ma,

As part of our drive towards ensuring a healthy and safe work environment coupled with the Management commitment to the prevention of Ebola Virus Disease (EVD) at our home and in the office, The Security/Health & Safety Team has declared Monday, 4th of August 2014 as EBOLA-AWARENESS FORUM tagged "STOP EBOLA NOW"

On this day, we shall in support of your leadership (as discussed) create awareness on Ebola Virus Disease for third party staff (Cleaners, Drivers, Tea Girls, Security Guards etc) at the Etisalat Experience Centers (EEC) throughout the country; this programme is specially designed for the third party staff because they do not have access to our interpost mails yet they have direct access to us ( Staff could also participate )

As discussed, we have attached some slides on this disease that could serve as a guide or use to make the presentation.

Furthermore, kindly send pictures of your forum to: [Redacted] for documentation purpose.

Thanks in anticipation of your understanding and support

# THE MALWARE

Interestingly, the executed Trojan is not the final payload. The malware is also crafted to inject **W32.Spyrat** into the victim's Web browser and allows attackers to perform the following actions:

- Log key strokes
- Record from the Web cam
- Capture screenshots
- Create processes
- Open Web pages
- Enumerate files and folders
- Delete files and folders
- Download and upload files
- Gather details on installed applications, the computer, and OS
- Uninstall itself

# ACCESS THE NETWORK

- Direct Tap (Ethernet/Cat5)
- Drop Box Method
- Cracking WIFI (WEP, WPA/WPA2)
- M.I.M. Attack (Man in the Middle)

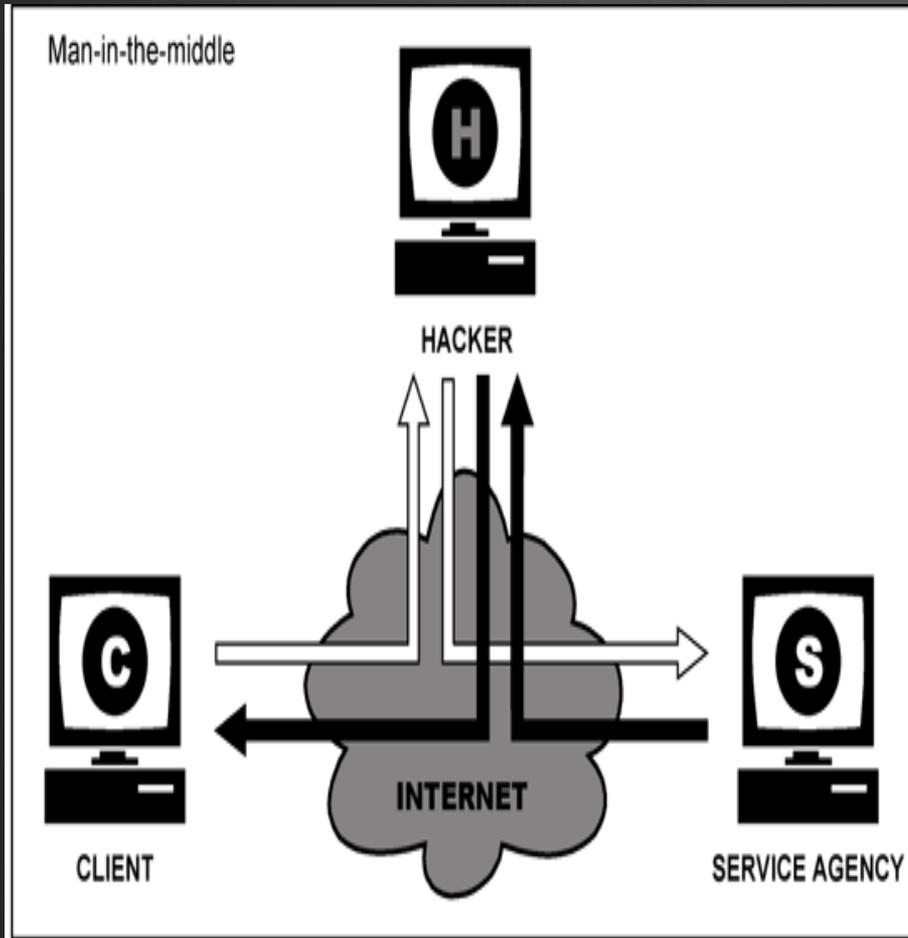


# PORTABLE PENTESTING TOOLS



# M.I.M.

## Man In The Middle Attack



# SCANNING

- Port Scanning-**Find Open Port**-Run Exploit
  - **\*\*PORTS.... WHAT ARE THEY\*\***
- Wireshark – Packet captures
  - Captures plain text information across the network
  - Grab password hashes
  - Study the network...better understand what is normal vs abnormal activity

# EXPLOITATION

- Malware
- Spyware
- Key loggers
- Access Camera and Microphone
- Pivot other machines or the network
- BOTS/BOTNETS
- Ransomware (Cryptolocker) \*\*New kid on the block\*\*

# MAINTAIN ACCESS

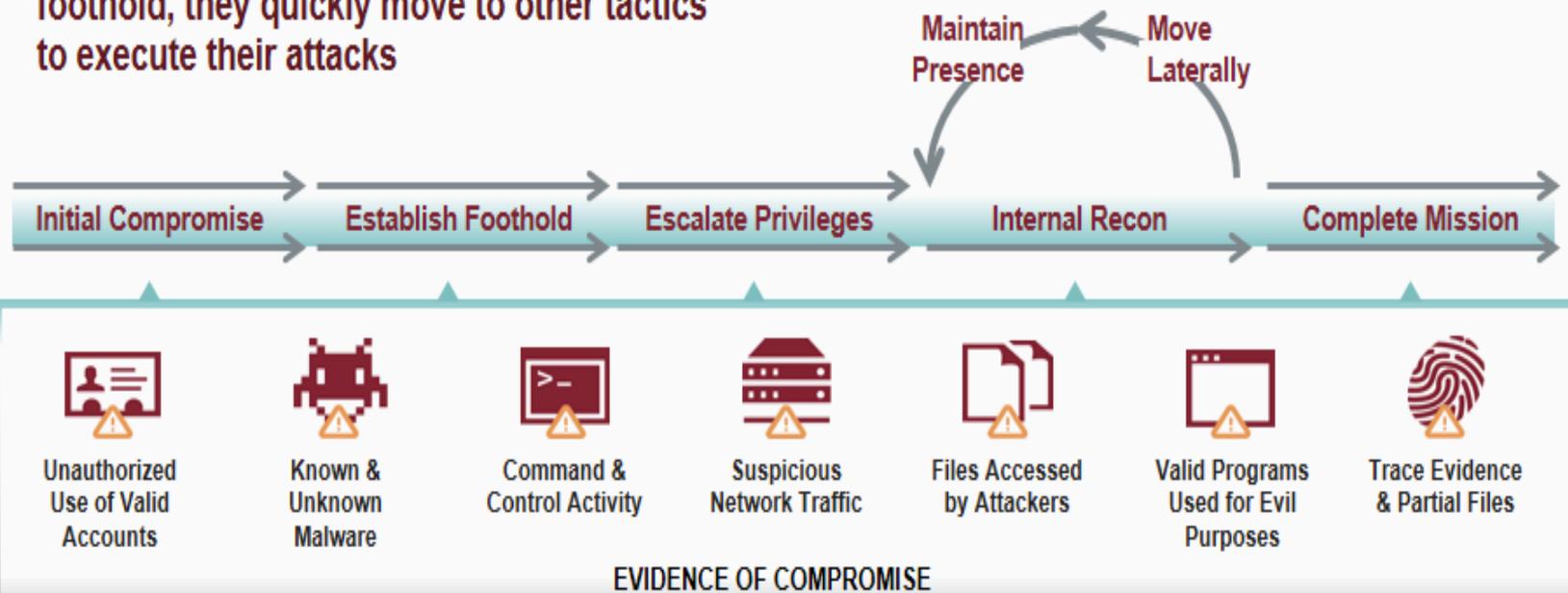
- ROOT Kits (RAT)
- Root or Administrator Privileges
- Change settings (open or close ports)
- Erase your tracks and logfiles

# EXFILTRATE DATA

- Remotely phone home (Activate RAT)
- Encrypted Text File via Email Script
- IRC Channel via SSH to CC Server

# BREACH LIFE CYCLE

While attackers use malware to gain an initial foothold, they quickly move to other tactics to execute their attacks

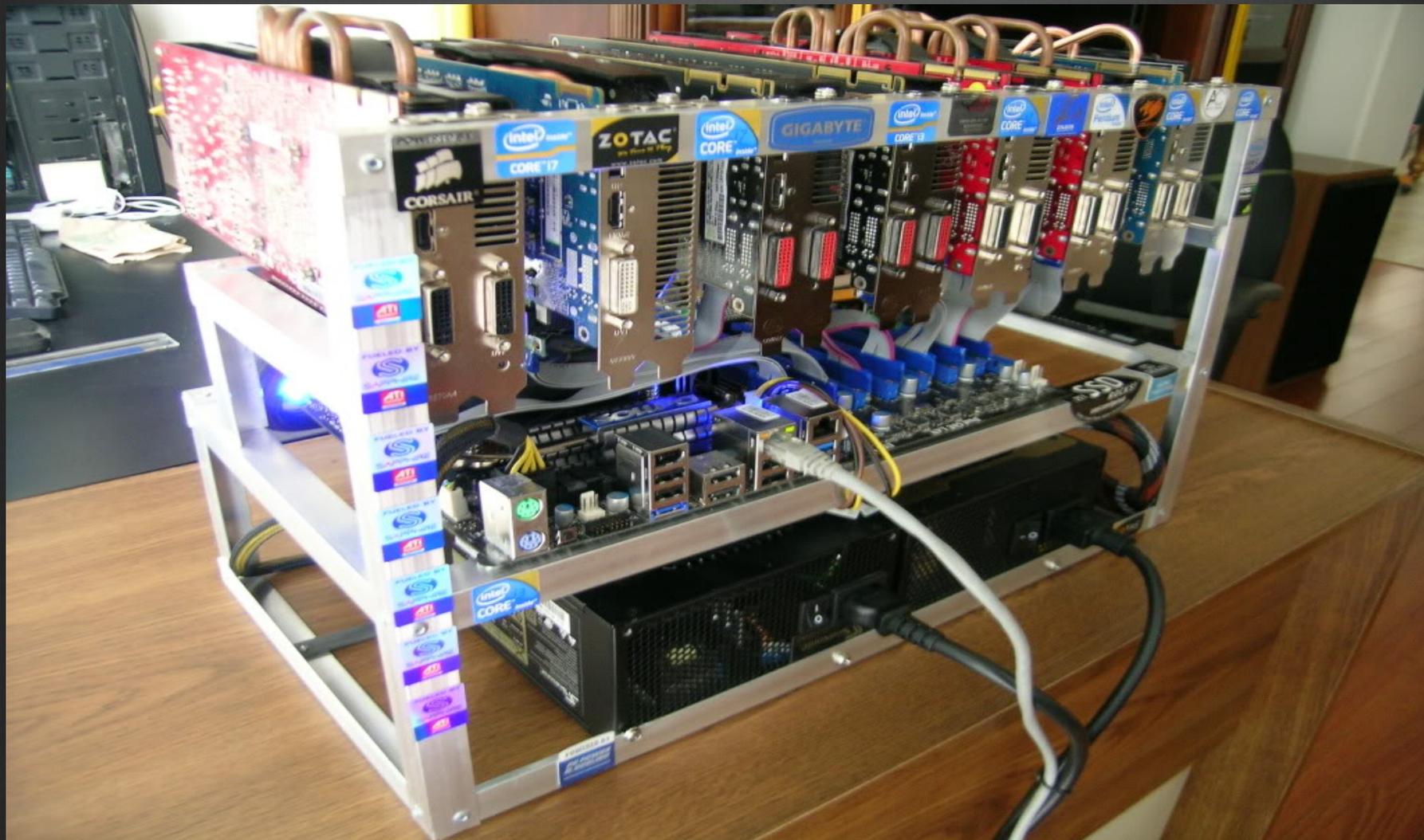


*Of all of the compromised machines Mandiant identified in the last year, only 54% had malware on them.*

# PASSWORD CRACKING

- Once the password hashes are retrieved they have to be cracked (LinkedIn 6.5 million)
- Passwords are stored as a HASH (one way function)
  - Example (Password! = 0040f2abc2cff0c8f59883b99ae9fab6)
- Collect all the stored HASH's to a text file
- Export text file to Hacker system
- Use a specialized GPU hacking system Multiple GPU cards

# GPU Hacking



# HOME BUILT GPU MACHINE

- Economical \$ 3,000 Machine
- 11 days for 8 character password
- Using Hashcat.ocl or similar (27/55 character length)
- Expand the system as resources grow
- Easy to make upgrades as technology improves
- Local Distribution (circle of trust)

# PUBLIC CLOUD COMPUTING

- Amazon / Peer 1 / Penguin Computing
- 23 hours for a 8 character password = 3,000\$
- Fast and easy
- Can handle large amounts of data at one time
- NO circle of trust (find a way to mask transaction)

# Low Tech Credit Card Theft

- Skimming
  - Small (pocket sized) device
  - Reads cards and stores number
- Usually waiters in restaurants
  - Recruited by higher-level criminal/organization
  - Card is out of view
  - No indication to cardholder that number has been stolen
- Waiter returns skimmer to handler
  - Paid \$10-\$20 per swipe

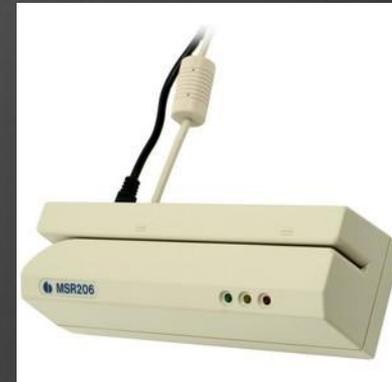
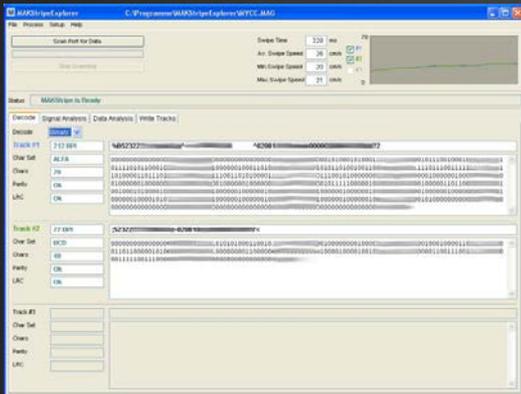
# Skimming

Skimmed number gets  
uploaded to a computer



"Box"

Magnetic stripe-writing  
software



"Machine"

Magnetic stripe writer

Illegally re-encoded  
card, aka, "swipe"

# LARGE DATA BREACH



# HOW DOES IT WORK

## Target Breach

- Compromise the Networks Point of Sales System (Server)
- Install the Malware – which executes as designed (date, time, duration, storage, exfiltration)
  - (harvest CC track data)
- CC track data is written to an encrypted text file
- Malware calls back home to Command Control server and emails the text file containing the CC track data back to the Cybercriminals
- CC numbers are broken off into batches and sold on CC hosting sites (Darknet)

# EXAMPLE OF A CREDIT CARD HOSTNG SITE TARGET NUMBERS

Bin	Card	Debit/Credit	Mark	Expired	Track 1	Code	Country	Bank	Base	Price
677522	 MAESTRO	DEBIT	N/A	09/15	Yes	226	 Turkey, CA, LOS ANGELES, 90024	N/A	Barbarossa 	67.5\$
677393	 MAESTRO	DEBIT	N/A	12/16	Yes	201	 Portugal, DC, WASHINGTON, 20010	N/A	Barbarossa 	67.5\$
677261	 MAESTRO	DEBIT	N/A	12/13	Yes	206	 Croatia, IL, CHICAGO, 60659	N/A	Barbarossa 	39.375\$
676992	 MAESTRO	DEBIT	N/A	12/15	Yes	221	 Macedonia, CA, BALDWIN PARK, 91706	N/A	Barbarossa 	67.5\$
676992	 MAESTRO	DEBIT	N/A	04/14	Yes	221	 Macedonia, TX, KATY, 77494	N/A	Barbarossa 	67.5\$
676969	 MAESTRO	DEBIT	N/A	06/14	Yes	221	 Greece, IL, ARLINGTON HEIGHTS, 60004	N/A	Barbarossa 	67.5\$
676938	 MAESTRO	DEBIT	N/A	04/14	Yes	226	 Portugal, FL, ORLANDO, 32828	N/A	Barbarossa 	67.5\$
676846	 MAESTRO	DEBIT	N/A	12/13	Yes	226	 Poland, IL, ALGONQUIN, 60102	N/A	Barbarossa 	23.625\$
676828	 MAESTRO	DEBIT	N/A	07/17	Yes	221	 Lithuania, FL, TAMPA, 33636	N/A	Barbarossa 	67.5\$

# Then What?

- Good
  - Buy merchandise and fund your lifestyle
- Better
  - Buy gift cards, then use the gift cards to fund your lifestyle
- Best
  - Buy gift cards, use them to buy merchandise, return the merchandise for cash, then use the cash to fund your lifestyle

- Local Criminals purchase a batch of CC numbers \$10-\$50 a number on the Dark Net or CC hosting sites
- Local Criminals encode the number to a forged CC or VISA type gift card
- Local Criminals then use the cloned cards to make purchases of high value merchandise which they then return for cash/credit or sale on Ebay or Craigslist
- In Portland we are averaging 1 out of state group about every 7-10 days \*One group has racked up 900K in 180 days.
- TARGET = 40 million CC/Debit numbers in 19 days. Estimated cost to target is currently 3 Billion Dollars

# How do Criminals Use Stolen Numbers?

- Get money!
  - High-value merchandise (fence)
  - Airline tickets for human smuggling
  - High-liquidity merchandise
    - Gift cards
    - Printer ink
    - Razor blades
    - Cigarettes
  - Exploit a merchant with a loose return policy

# Return Fraud

- Buy something expensive
- Return it
- Get cash
  - Gift card
  - Credit the value to a debit card

# THE HARDWARE



# THE PRODUCT



# BITCOIN



# WHAT IS IT?

- ⊗ Decentralized Peer to Peer Cryptographic Currency
- ⊗ Introduced in 2009 by Satoshi Nakamoto (Unknown). **OPEN SOURCE CODE**. Believed to have 1 million coins (\$371,255,000.00)
- ⊗ Self Stabilizing Economy (auto-adjust to inflation = mining rate)
- ⊗ All Payments are Public, **Traceable**, and Permanently Stored in the Public Ledger
- ⊗ 21 Million coins in total (year 2140)
- ⊗ 1 block created every 10 minutes (25 coins)

- ⊗ Offers Anonymity for Transactions when coupled with TOR
- ⊗ Bitcoin address is only used to show where stored and or sent in regards to traceability and transparency.
- ⊗ Bitcoin miners are part of the ecosystem they approve transactions
- ⊗ Requires use of a Bitcoin wallet to store and conduct transactions (software application /Computer or Mobile)
- ⊗ Wallet offers: Encrypted, Non-Encrypted and Offline transactions. **\*\*Paper Wallet\*\***
- ⊗ Use of Digital Signatures: Private and Public Key Encryption scheme
- ⊗ Private key creates the transaction
- ⊗ Public key verifies (checks) the transaction

- ⊗ Public Key is also the send to address
- ⊗ Generate a transaction message with private key, network nodes use the Public Key to verify that you are the originator of the transaction
- ⊗ Once a transaction is used it can't be re-used. NO double spending
- ⊗ Block chains prevent fraud...Transaction is broken into blocks and the network nodes solve these blocks, each chain has a hash that point to the next block in the chain
- ⊗ Uses ECDSA (Elliptic Curve Digital Signature Algorithm)

# BITCOIN MINING



# MINING

- ⊗ Computer (node) is given a complex algorithm to solve which creates a 64 digit number
- ⊗ Rewarded with New Block Solve (25 Bitcoins) \* every 4 years block chain reward is cut in half
- ⊗ Solve rate = 1 block every 10 minutes
- ⊗ Difficulty of algorithm is propionate to rate of solve
- ⊗ Miners help approve transactions within the network
- ⊗ Pool mining (GPU intensive)

# WHAT CAN YOU DO?

- Lock down your network (make sure it is closed and hidden)
- Use WPA2
- Use passphrase vs. password
- Scan you network to make sure no unauthorized devices are on it.
- Scan network for open ports...CLOSE them!
- Run a good firewall and virus software
- Use encryption (partial or full disk)

# Continued

- Back up or better yet store all important data on External drive and ENCRYPYT it
- Do a clean re-install
- Convenience vs. Security (Auto detect)
  - IOS/Android Mobile devices
- Educate your family and implement good security practices
  - Decrease your Digital Footprint
- Travel (safe practices)
  - Airport WIFI/Hotel WIFI/Coffee Shops WIFI/ ect.
  - Low hanging fruit

# THE LAB



# FORENSIC WORKSTATIONS



# DUPLICATION/WIPING



# SECURE EVIDENCE ROOM



ANY  
QUESTIONS  
?