RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HT-W09

When cyber criminals with good OPSEC attack

Liam O'Murchu

Director
Broadcom
@liam_omurchu

Ryan Macfarlane

Supervisory Special Agent
FBI, Cleveland Division

RSAConference2020

Bringing hackers to justice

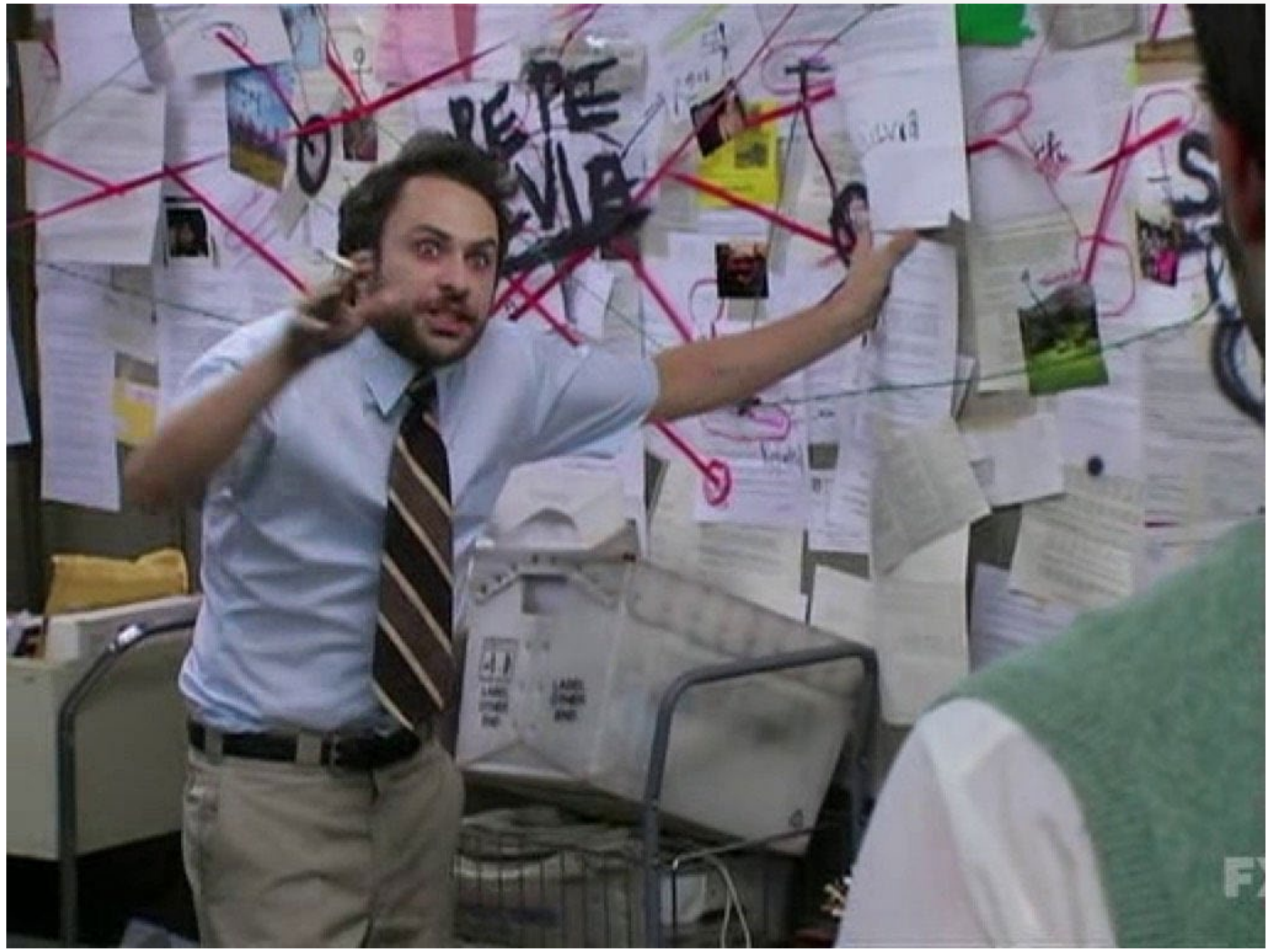
Apply What You Have Learned Today

- Identify key partners:
  - LE should find key researchers and establish collaboration with the help and support of your prosecution team
  - Private Sector should find an aggressive LE partner (domestic or foreign) to actually impact malicious actors
- Understand the process:
  - This doesn't happen overnight: We are really in the business of waiting for mistakes to make, put yourself in a position to see as much as possible
- Shape the future by doing the right thing thru collaboration:
  - These threats aren't going away, protection is important, but so is deterrence

RSAConference2020

OPSEC

Putting the jigsaw puzzle together



Some good rules

1. Don’t talk openly
2. Don’t operate from home
3. Encrypt everything
4. No logs
5. Create Personas
6. Don’t contaminate
7. Don’t trust
8. Be paranoid
9. Don’t talk to police
10. Don’t give people power over you

1. OTR, radio noise, no phone talk ✓
2. Stolen wifi, hacked routers, proxies, TOR ✓
3. SFTP, SSH, PGP, OTR, LUKS, Truecrypt,+ ✓
4. Logging disabled ✓
5. Hacker Handles ✓
6. Isolated hacking environment ✓
7. Built all tech themselves ✓
8. Triple encrypted drives, proxychaining ✓
9. A lot of pressure ✓
10. Limited inner circle ✓

The good news about hacker OPSEC

- Flips the power dynamic
- Hackers only need to be right once in an attack
- Hunters only need to be right once in an investigation

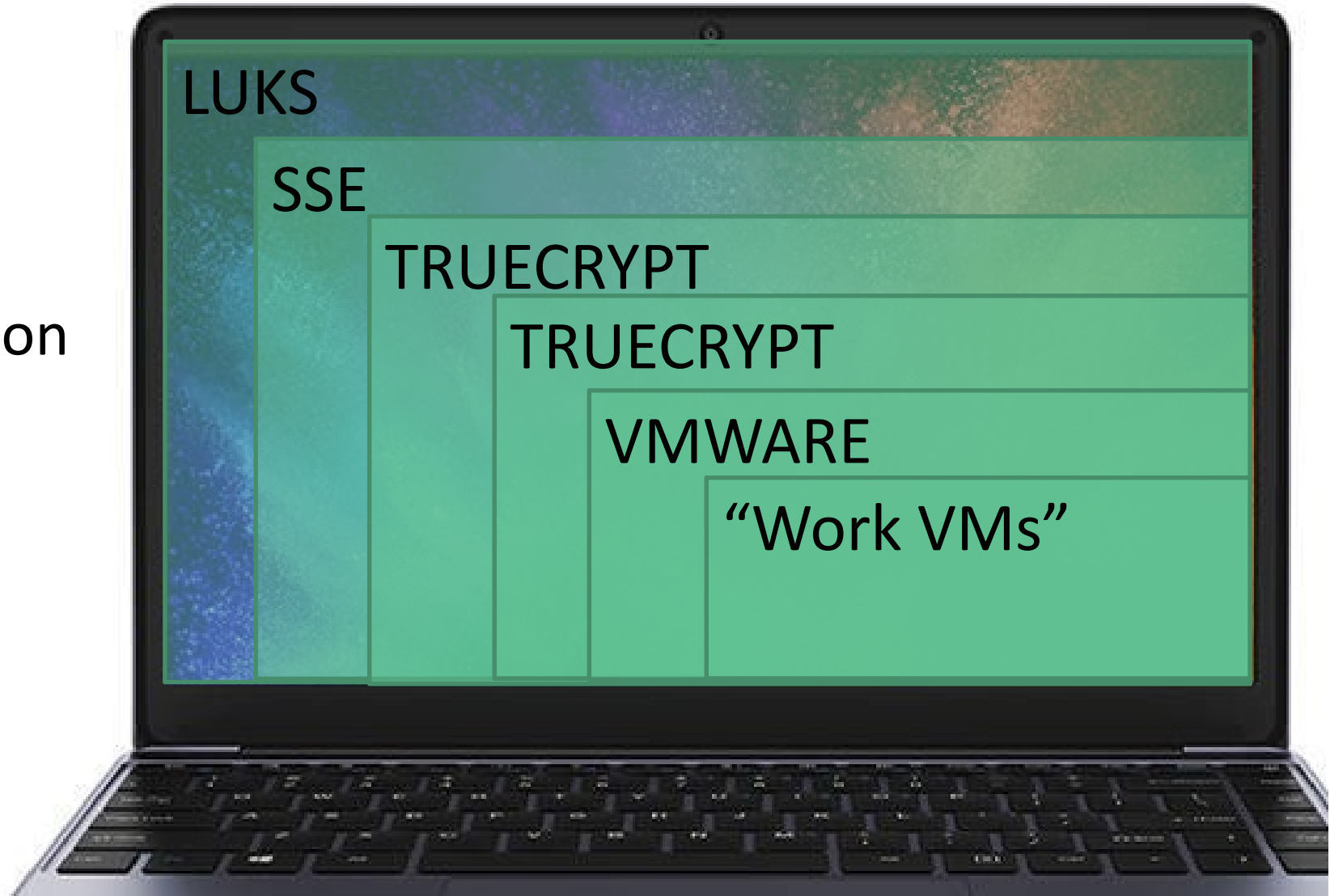
RSAConference2020

Let’s talk about their OPSEC (and what we did about it)

You are right to ask: *Why did this case take so long…*

Computer OPSEC

- Linux Distro (UB)
- Custom boot integrity
- LUKS disk encryption
  - Kali & networking here
- SSE – Custom Encryption
- TrueCrypt - 2 Layers
- VMWARE
  - “work” images (Win)




TP-LINK

Secure Comms

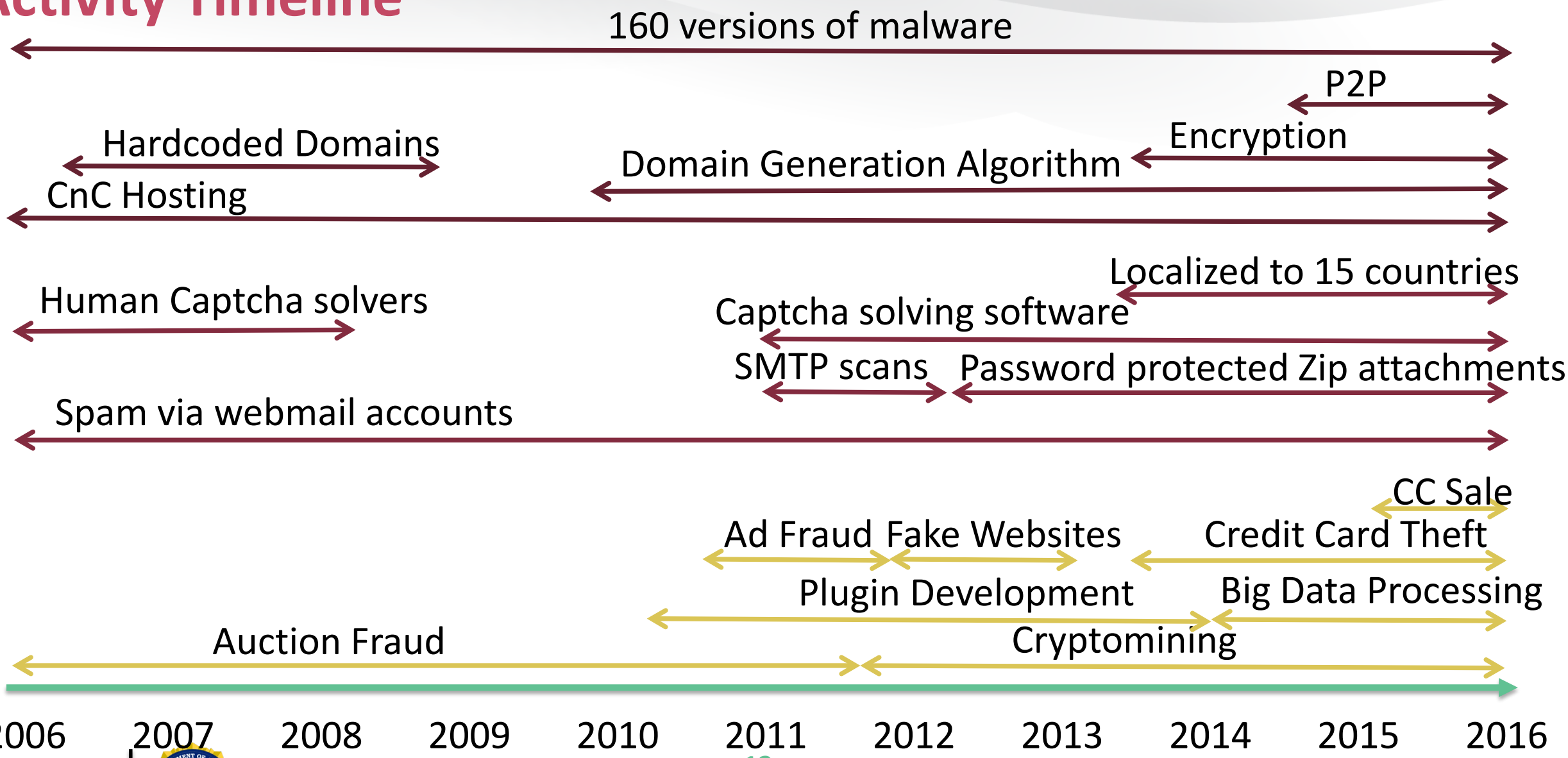
- Stolen wifi
- Proxychains in different countries
- TOR
- VPNs
- SSH
- Sftp
- PGP
- OTR/Jabber

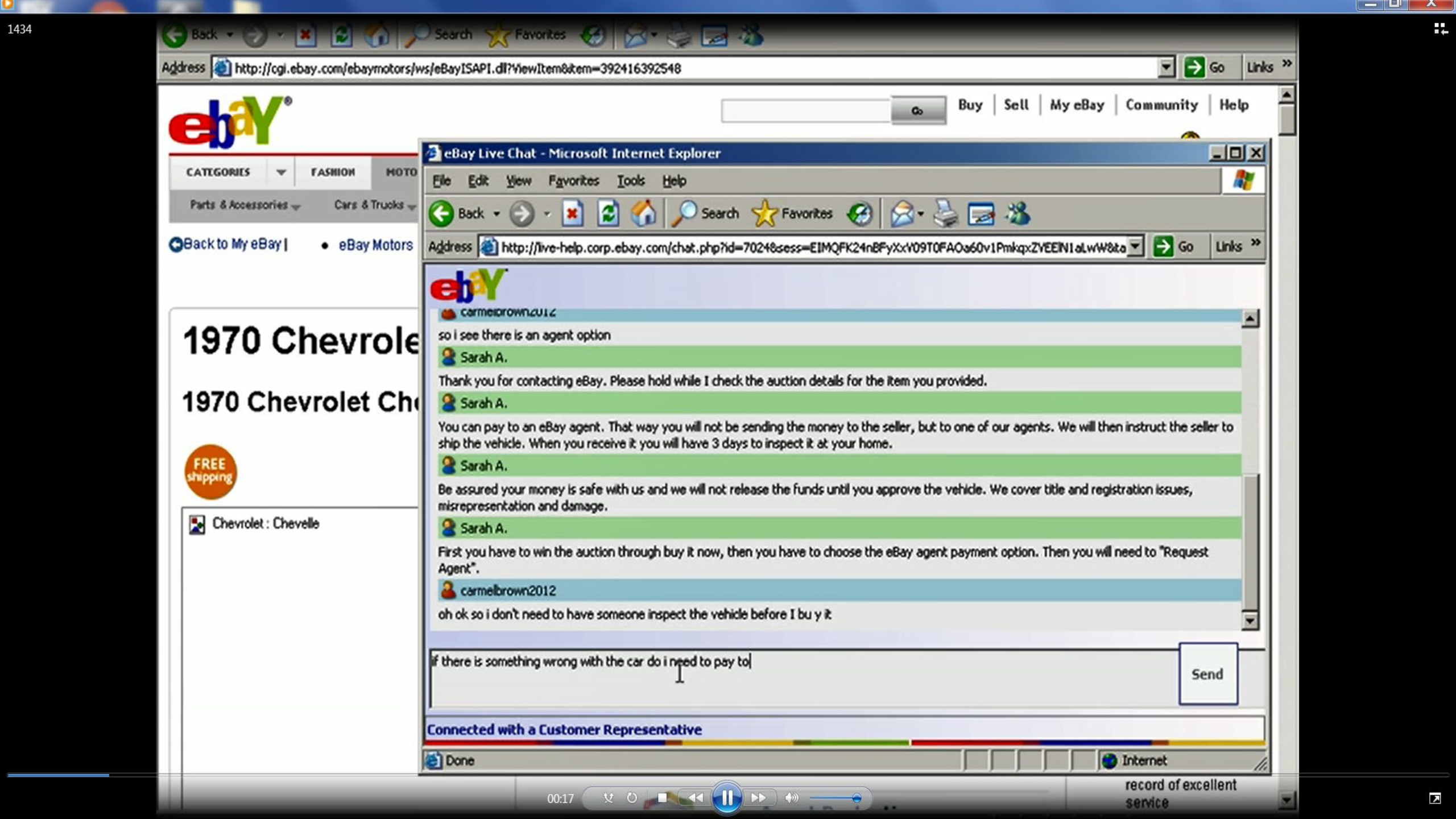
RSAConference2020

So much OPSEC.

So much crime.

Activity Timeline

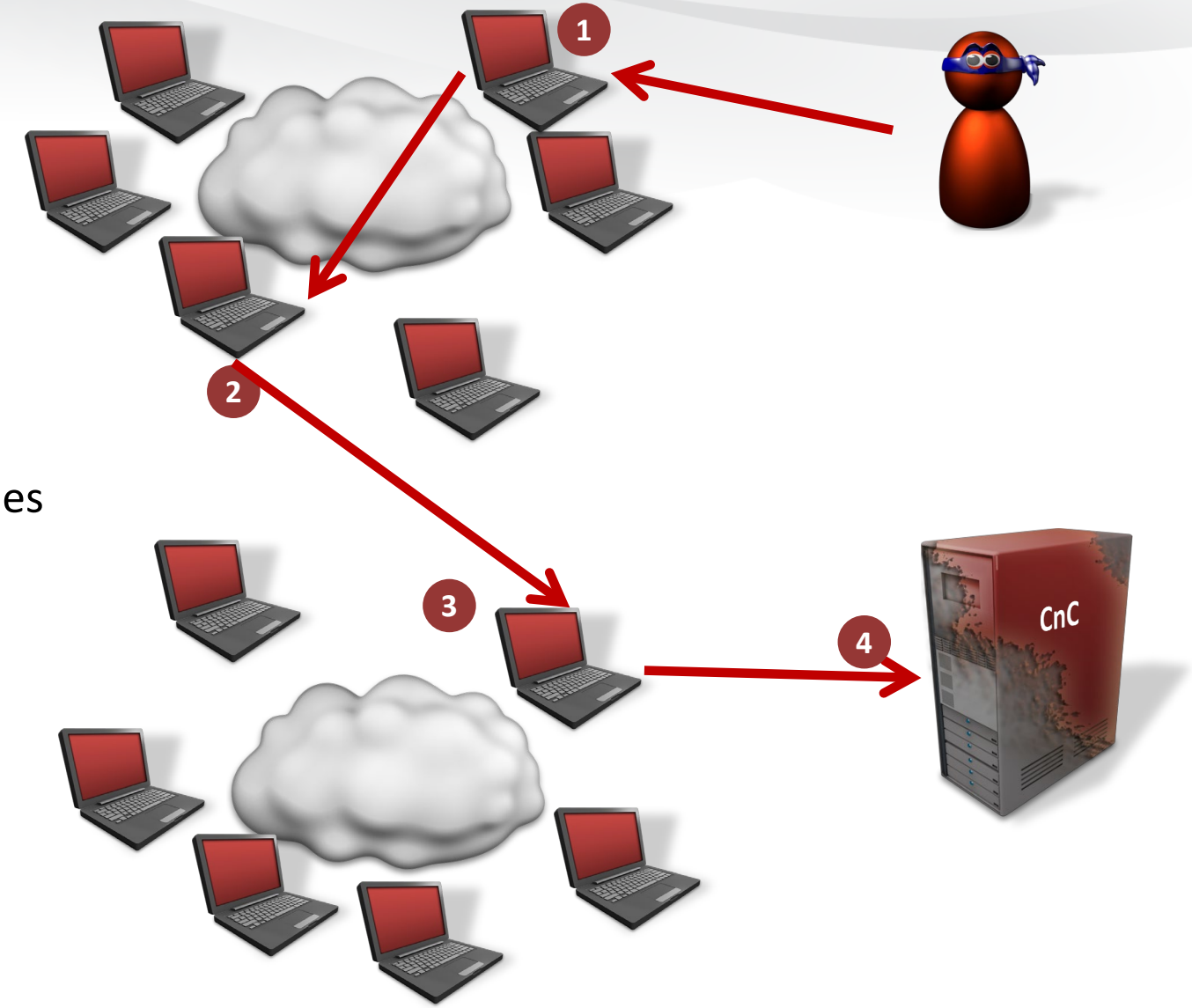



1434
Address http://cgi.ebay.com/ebaymotors/ws/eBayISAPI.dll?ViewItem&item=392416392548
Buy | Sell | My eBay | Community | Help
CATEGORIES | FASHION | MOTO
Parts & Accessories | Cars & Trucks
Back to My eBay | eBay Motors
1970 Chevrole
1970 Chevrolet Che
FREE shipping
Chevrolet : Chevelle
eBay Live Chat - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://live-help.corp.ebay.com/chat.php?id=70248&sess=EIMQFK24nBFyXxW09T0FAOs60v1PmkqxZYEEIN1aLwW&ta
carmelbrown2012
so i see there is an agent option
Sarah A.
Thank you for contacting eBay. Please hold while I check the auction details for the item you provided.
Sarah A.
You can pay to an eBay agent. That way you will not be sending the money to the seller, but to one of our agents. We will then instruct the seller to ship the vehicle. When you receive it you will have 3 days to inspect it at your home.
Sarah A.
Be assured your money is safe with us and we will not release the funds until you approve the vehicle. We cover title and registration issues, misrepresentation and damage.
Sarah A.
First you have to win the auction through buy it now, then you have to choose the eBay agent payment option. Then you will need to "Request Agent".
carmelbrown2012
oh ok so i don't need to have someone inspect the vehicle before I bu y it
if there is something wrong with the car do i need to pay to
Send
Connected with a Customer Representative
Done
Internet
00:17
record of excellent service

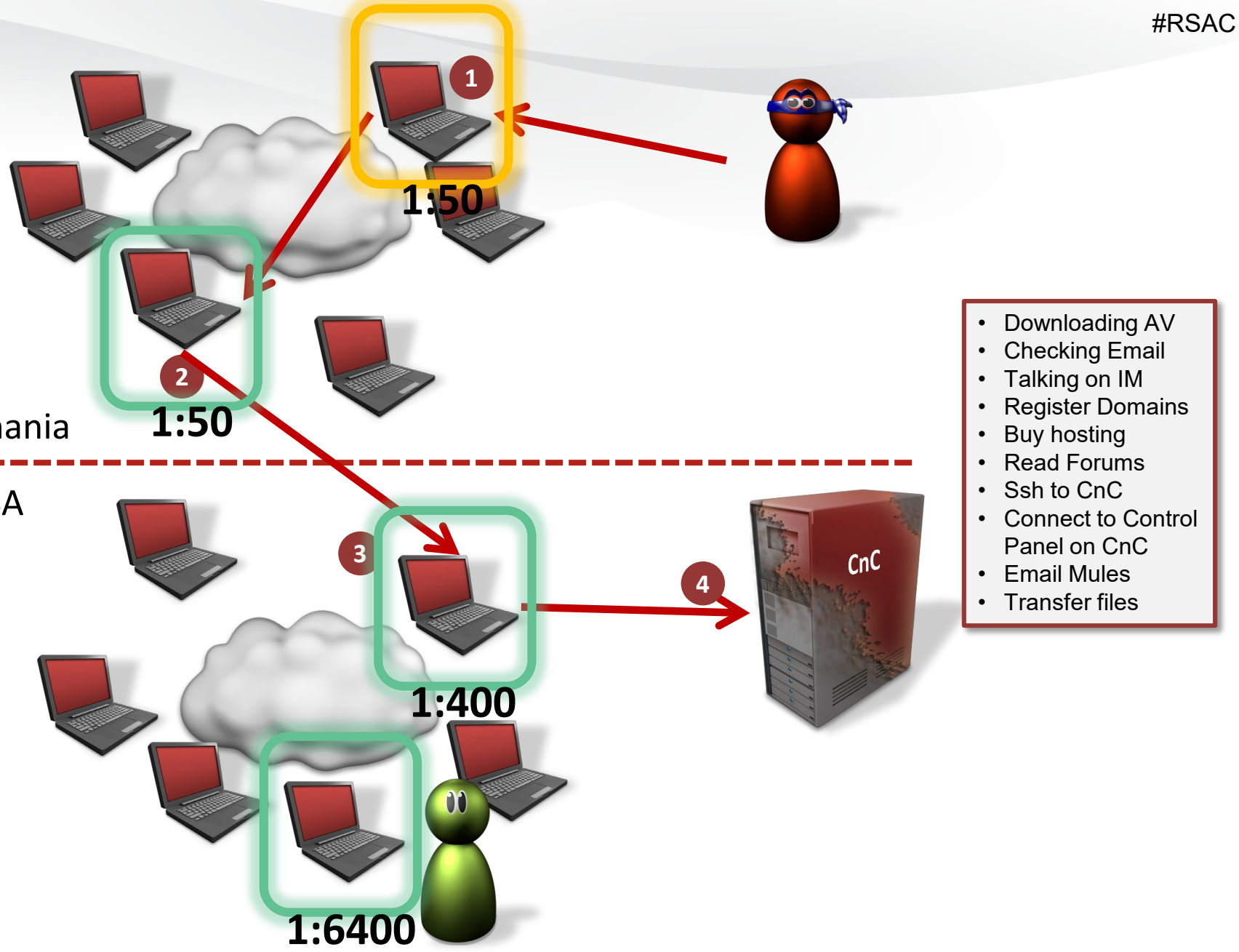
2016: Bayrob Browser + Big Data


F9 40 00-5E F9 40 00-18 06 41 00
06 41 00-AF 06 41 00-DC 06 41 00
07 41 00-7A 07 41 00-BE 07 41 00
14 41 00-56 17 41 00-0D 1C 41 00
00 00 00-00 00 00 00-DA 2C 41 00
A0 41 00-45 8C 41 00-00 00 00 00
36 41 00-00 00 00 00-00 00 00 00
00 00 00-00 00 00 00-00 00 00 00
41 54 41-4B 45 59 3A-BE F9 22 BB
A0 02 00-6B 75 74 72-6F 6E 67 40
2E 63 6F-6D 00 00 00-00 00 00 00
DATAKEY:
kutrong@
yahoo.com
D2C--a53a_002f4b6a.tmp-400000.bin
PE .0053A360|Hiew 8.41 (c)SEN
5C-44 69 73 70-61 74 63 68
viceCtrlDispatch
5E-53 43 4D 61-6E 61 67 65
erA OpenSCManage
5E-67 65 53 65-72 76 69 63
rA ChangeServic
32-41 00 00 00-53 74 61 72
eConfig2A Star
55-41 00 00 00-43 72 65 61
tServiceA Crea
53-65 41 00 00-00 00 00 00
teServiceA
53-20 74 65 61-6D 20 69 73
symantec team is
68-65 6E 2D 63-6F 6F 70 2C
a big hen-coop,
5E-20 73 6D 61-72 74 20 20
chicken smart
20-20 20 20 20-20 20 20 20
20-20 20 20 20-44 41 54 41
DATA

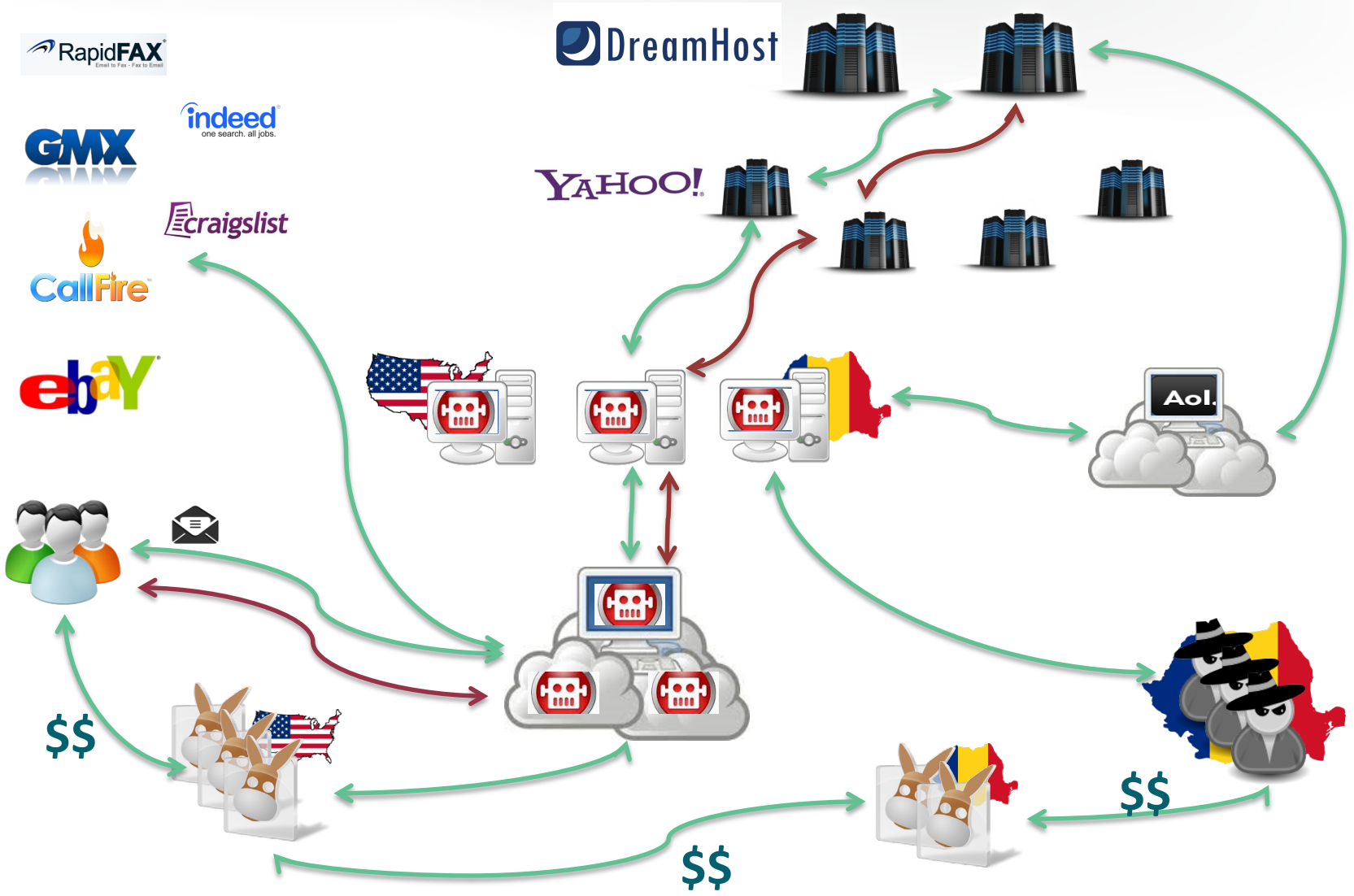
- Infected Machines Used as Proxies
- Always at least 3 hops



- Not all proxies are equal!
- Speed
- Open ports
- Uptime
- Geographic location

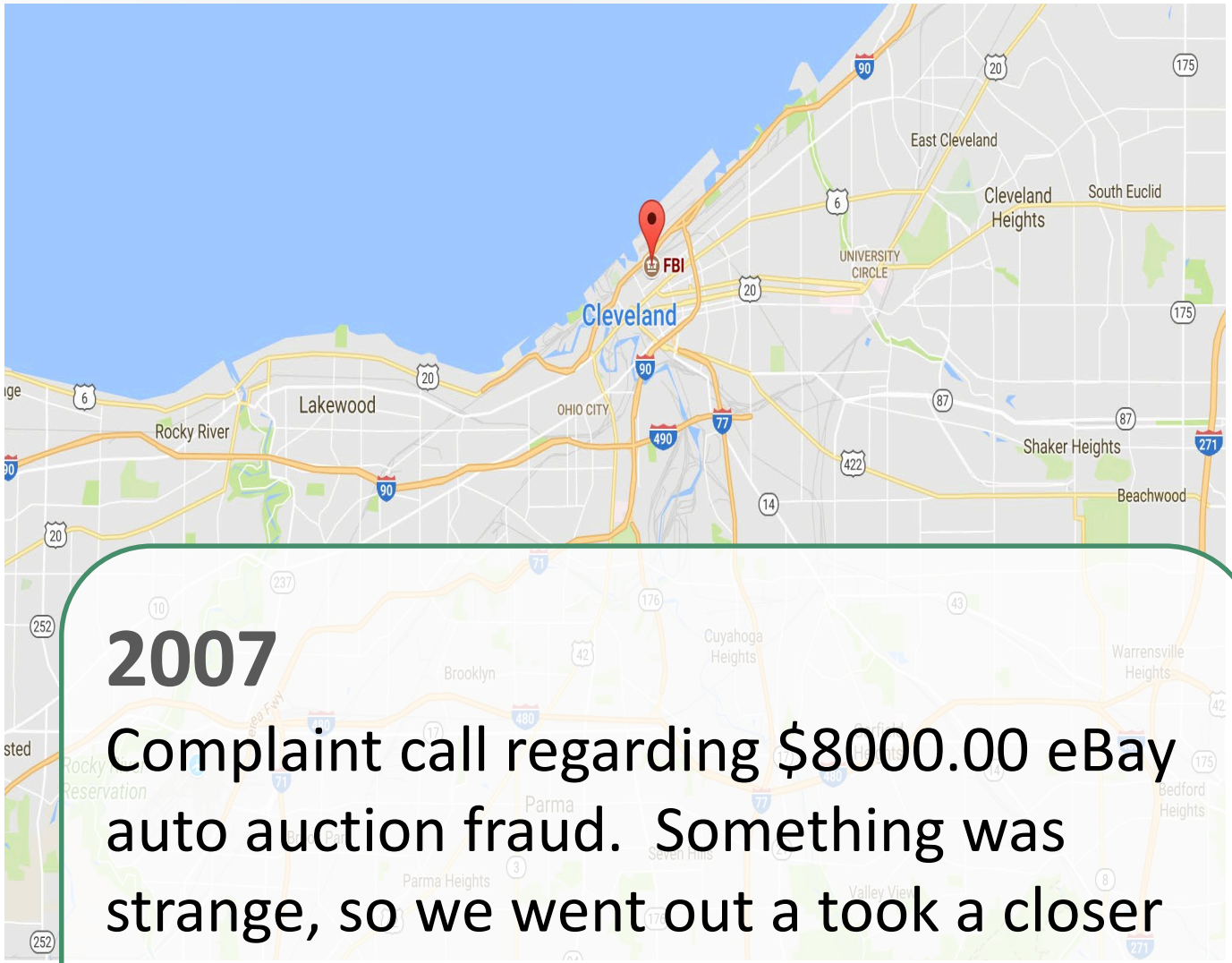


Infrastructure Overview



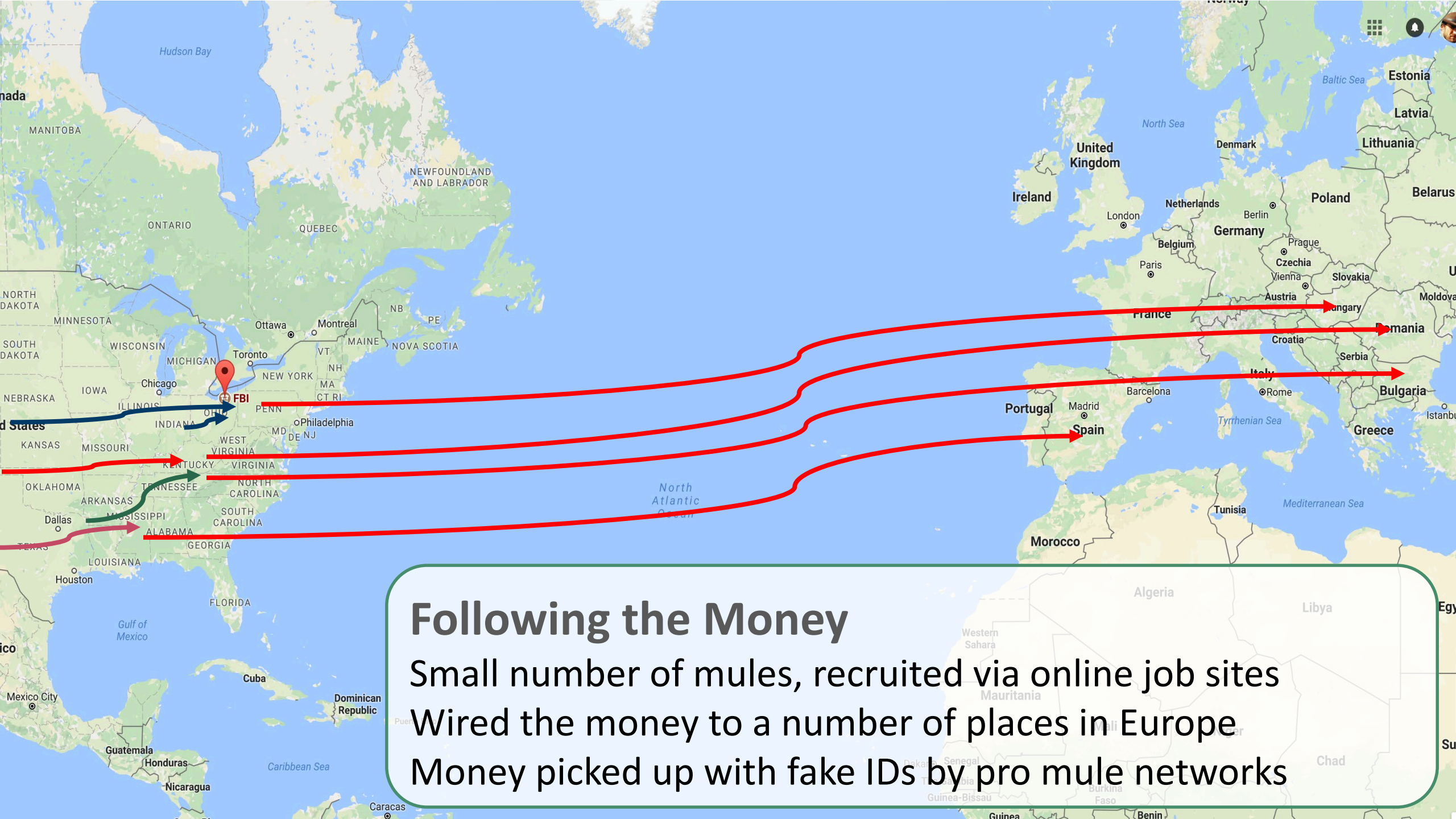
How the FBI got involved…

- Local complaint call
- Lots of initial legal process related to the mules
- Trying to follow the money
- Working with Western Union
- Coordinating with International partners
- Applied to be a mule



2007

Complaint call regarding $8000.00 eBay auto auction fraud. Something was strange, so we went out a took a closer look. Found what is now called Bayrob.



Following the Money

Small number of mules, recruited via online job sites

Wired the money to a number of places in Europe

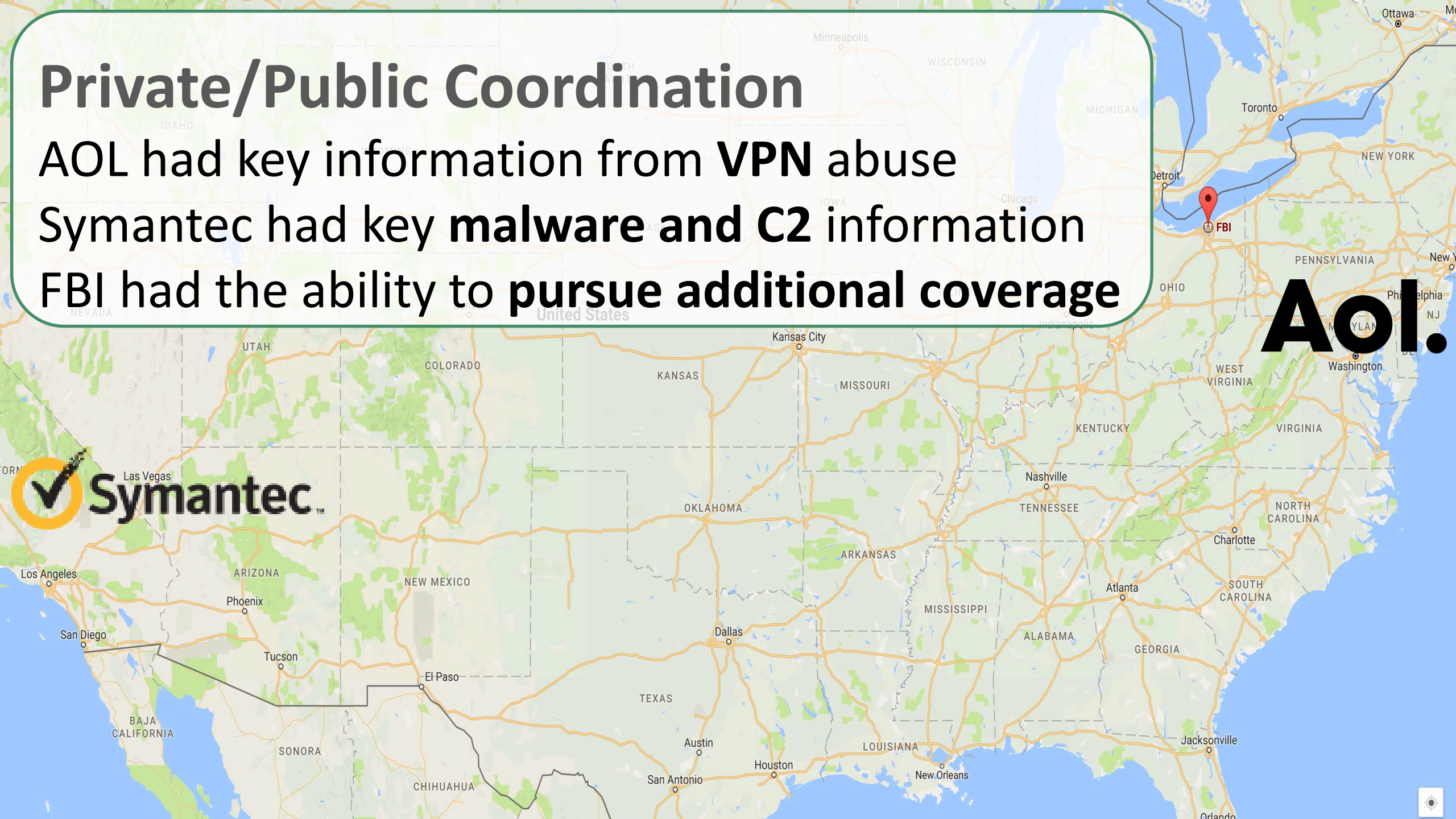
Money picked up with fake IDs by pro mule networks

Private/Public Coordination

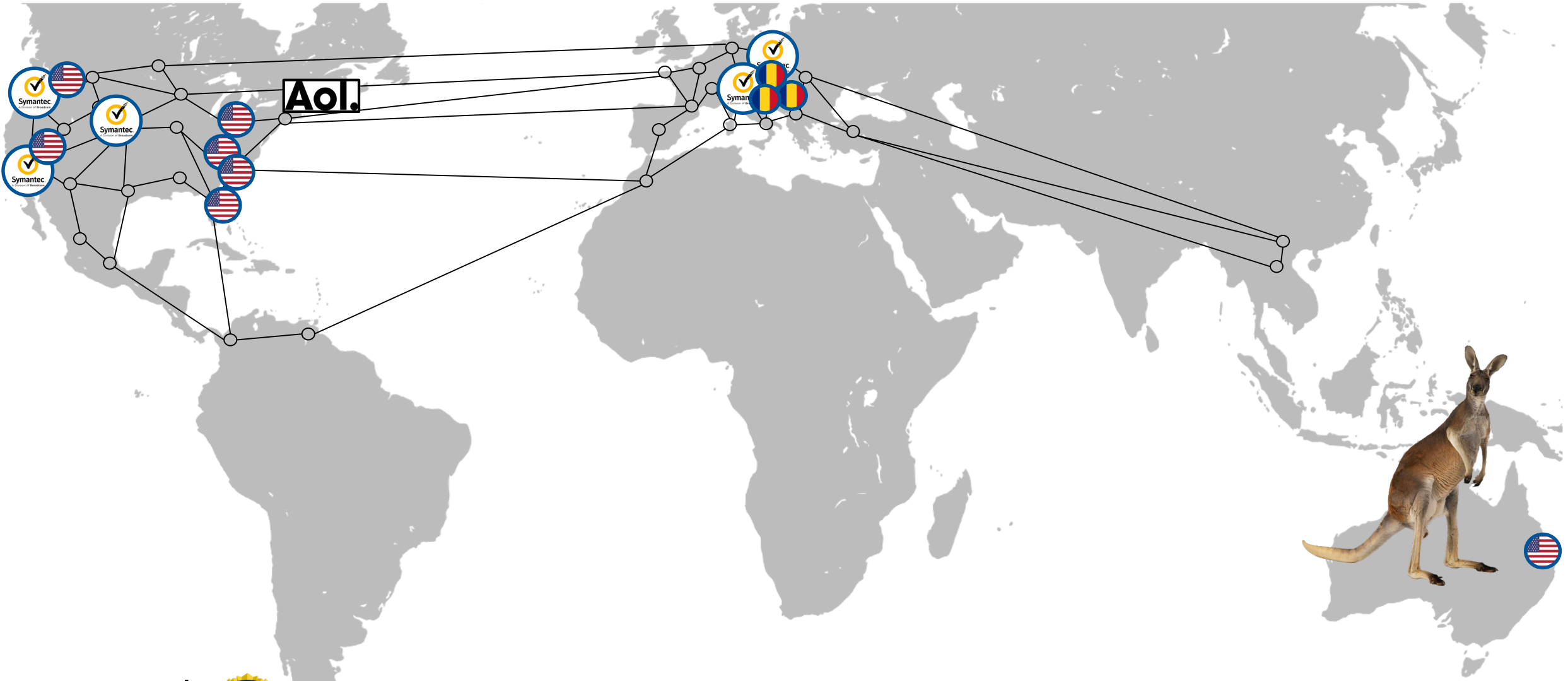
AOL had key information from **VPN** abuse

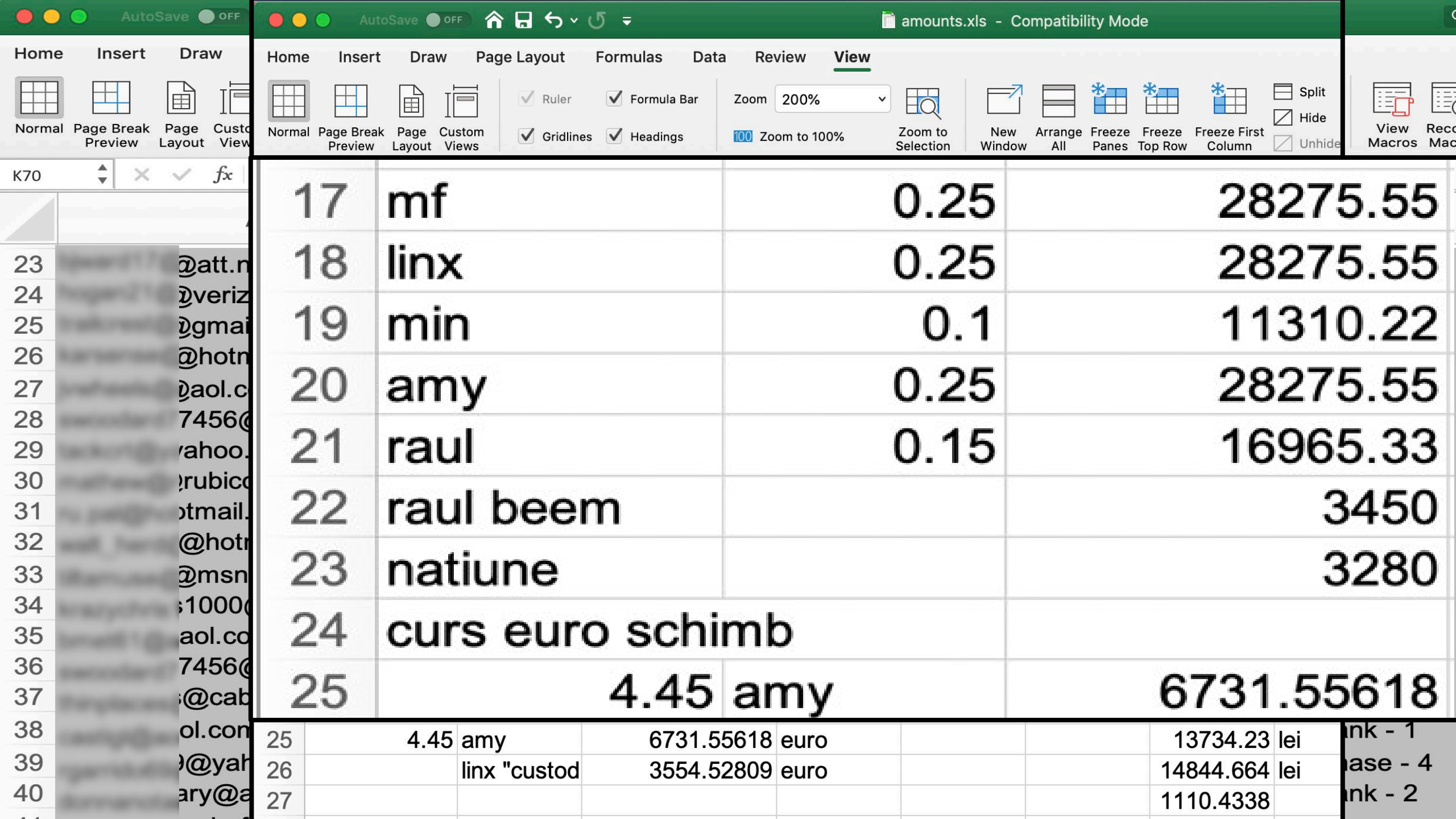
Symantec had key **malware and C2** information

FBI had the ability to **pursue additional coverage**



Our shared visibility




amounts.xls - Compatibility Mode
Home Insert Draw Page Layout Formulas Data Review View
Normal Page Break Preview Page Layout Custom Views
Ruler Formula Bar Gridlines Headings
Zoom 200% Zoom to 100% Zoom to Selection
New Window Arrange All Freeze Panes Freeze Top Row Freeze First Column
Split Hide Unhide
View Macros
17 mf 0.25 28275.55
18 linx 0.25 28275.55
19 min 0.1 11310.22
20 amy 0.25 28275.55
21 raul 0.15 16965.33
22 raul beem 3450
23 natiune 3280
24 curs euro schimb
25 4.45 amy 6731.55618
25 4.45 amy 6731.55618 euro 13734.23 lei
26 linx "custod 3554.52809 euro 14844.664 lei
27 1110.4338


PenguiNet
Total Com...
(1) Faceba...
masterfraud
my - Secur...
vps - Secur...
my - Secur...


sox3 - Win...
sox3 - Wind...
aol_jobs - v...
yahoohosti...
Calculator
8:10 PM
4/4/2013

Raduspr Traffic

Connection 1 (TCP)

```
Start: 2013-05-13 14:27:05.085097 UTC
  End: 2013-05-13 14:28:36.109303 UTC

172.190.235.81:2935 -> 74.208.5.85:80 (15766 bytes)
74.208.5.85:80 -> 172.190.235.81:2935 (35935 bytes)

Referer: http://www.gmx.com/
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
                                                                    4.0;
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
InfoPath.2)
Host: www.gm
TextfieldEma l=minolta9797&TextfieldPassword=[redacted]ttonLogin=1

Referer: http://www.gmx.com/
```

Twitter, Inc. [US] | https://twitter.com/raduspr

Home Moments Search Twitter Have an account? Log in

Tweets 2 Following 3 Followers 5 Follow

Radu Bogdan

@raduspr

Joined January 2011

New to Twitter?

Sign up now to get your own personalized timeline!

Sign up

You may also like · Refresh

Los Angeles Times
@latimes

Tweets & replies

Radu Bogdan @raduspr · 7 Dec 2013
Replying to @ypool_net
@ypool_net any updates?
1

Radu Bogdan @raduspr · 1 Dec 2013
@ypool_net server down? or what happened?

Loading seems to be taking a while.
Twitter may be over capacity or experiencing a momentary hiccup. Try again or visit Twitter Status for more information.

RSAConference2020

Are we done here, or just getting started?

Expectations and perspectives vary widely based on where you sit

Server Search Warrants

- Found lots of stuff!
- PHP framework, with plugin architecture
- CasperJS for client side scripting +JSON command and data messages
- Vast database with really solid tracking by soxid (unique to infected system)

Turns out they created a completely self-documenting cyber criminal enterprise!

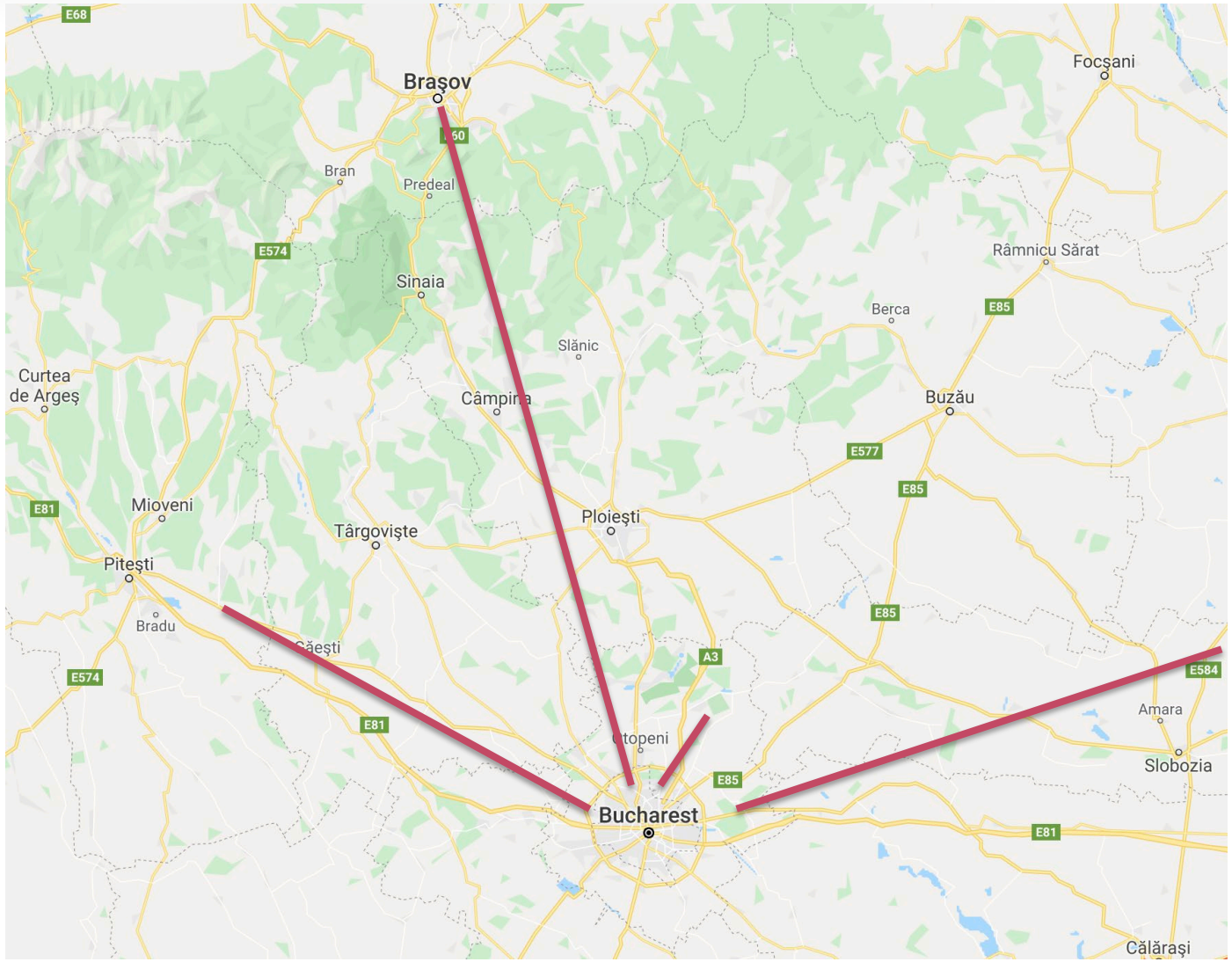
Title III Data Intercept of multiple dedicated C2 servers

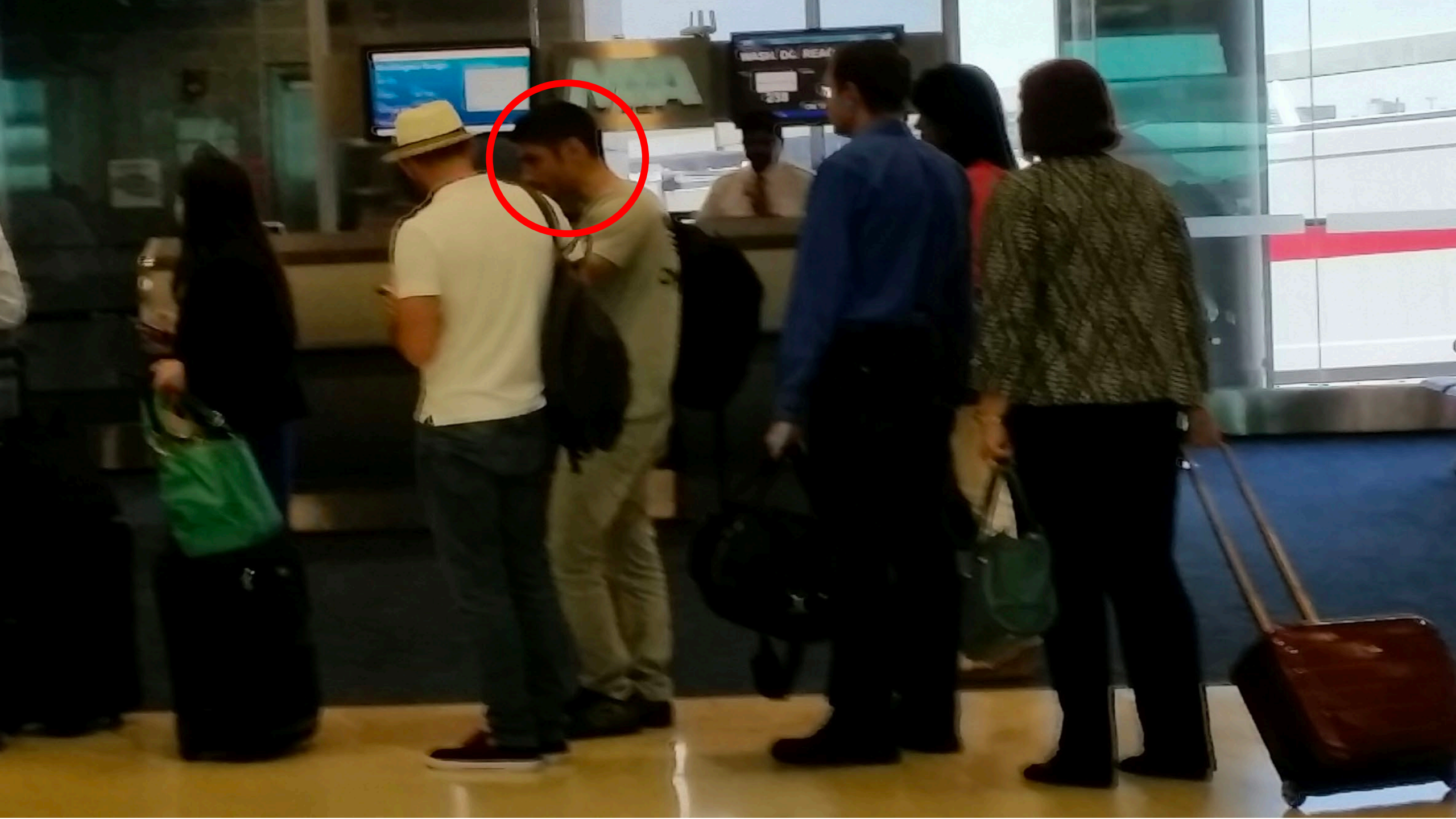
- 180 million products in our traffic collection tool, which was not designed for 180 million products
- TIII's are hard
  - 4 months for approval, met Deputy Attorney General
  - 30 day renewals, 15 days report updates, for 6 months
- There is no substitute for TIII data
  - Realtime evolution, **ID'ed victims** and **cashout guy**

BROADCOM

RNP Coverage identifies connections

- Identifies a house leased by raduspr in Brasov
  - Lived in by some who rarely ever comes out of the house
- Identifies encrypted connections to an apartment in Bucharest
- Bucharest location has other encrypted connections
- **No connections to Bayrob infected systems, VPNs, etc**
- Little Internet traffic





26514	romeo-mobil@ro.	obe.m@ro.remote.mx	"ba"	hey
26515	romeo-mobil@ro.	obe.m@ro.remote.mx	"pai ce vrei sa faci"	Well, what do you want to do?
26516	romeo-mobil@ro.	obe.m@ro.remote.mx	"Sal spawnez"	To spawn it
26				
26	I have fixar and sql		I have fixar [*sic*] and sql	
26	it was something stupid at epoll		it was something stupid at epoll	
26	Aha		Uh-huh.	
26	Sunt im avion		I am on the plane.	
26	Decolez acu		I am taking off now.	
26	hehe		Hihi.	
26	team prins		I got you!	
26	da ba acu la preturile astea		Yes, dude, now at these prices…	
26	"face fo 6000 pe luna"		making about 6,000 per month	
26	"Ce?"		What?	
26	"Mining?"		Mining?	
26	"da"		yeah	
26	"6000$?"		$6000?	
26537	romeo-mobil@ro.	obe.m@ro.remote.mx	"Si prima data fac scanf"	And first I do scanf
26538	romeo-mobil@ro.	obe.m@ro.remote.mx	"Si rulez cu runpipe?"	And I run with runpipe?
26539	romeo-mobil@ro.	obe.m@ro.remote.mx	"dar tu vrei sal lasi in background"	but you want to leave it in the *background*
26540	romeo-mobil@ro.	obe.m@ro.remote.mx	"nu merge cu pipe"	it doesn't work with pipe

RSAConference2020

Prosecution Phase

Hard decisions need to be made about when to go with what we have, how to introduce evidence, etc…

BAYROB GANG: THE SUSPECTS

SUSPECTS FROM ROMANIA FACE CHARGES FOR A RANGE OF CYBERCRIME OFFENCES

BOGDAN NICOLESCU

Alleged aliases: "Masterfraud", "mf"
Alleged role:
- Group leader
- Strategic direction

DANET TIBERIU

Alleged aliases: "Amightysa", "amy"
Alleged role:
- Technical lead
- Botnet development & infrastructure

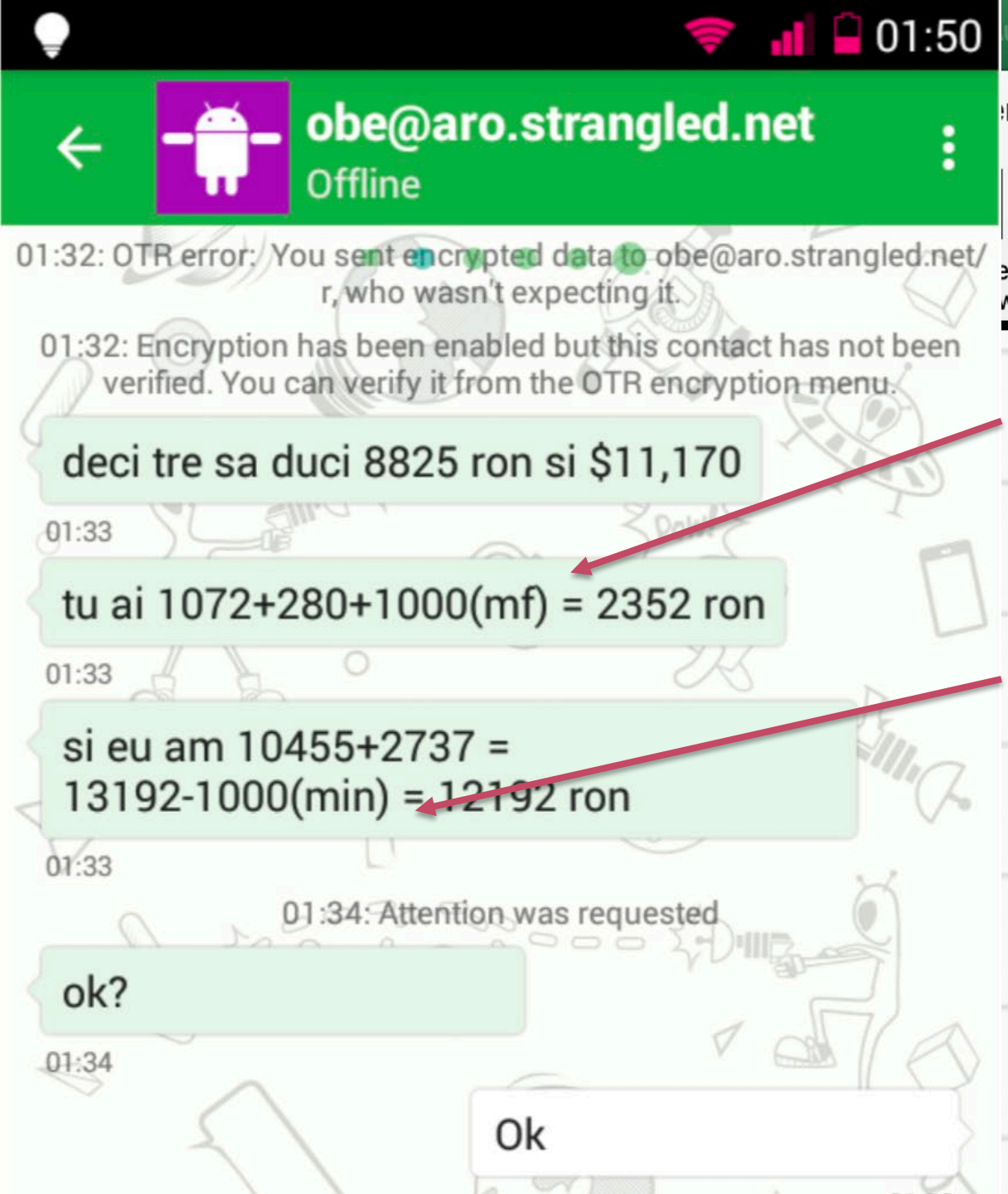
RADU MICLAUS

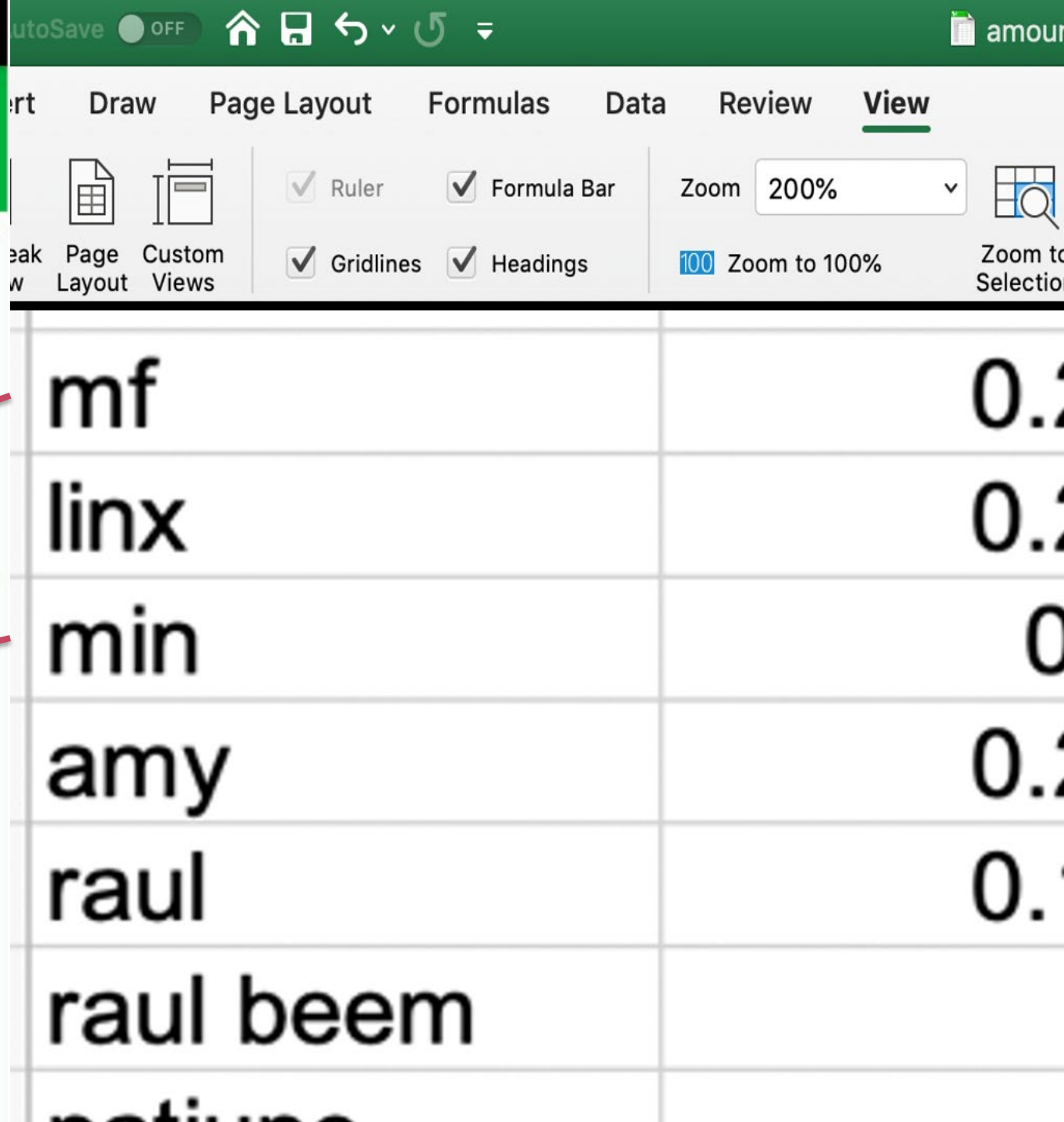
Alleged aliases: "Minolta", "min"
Alleged role:
- Junior technical member
- Managing auction fraud

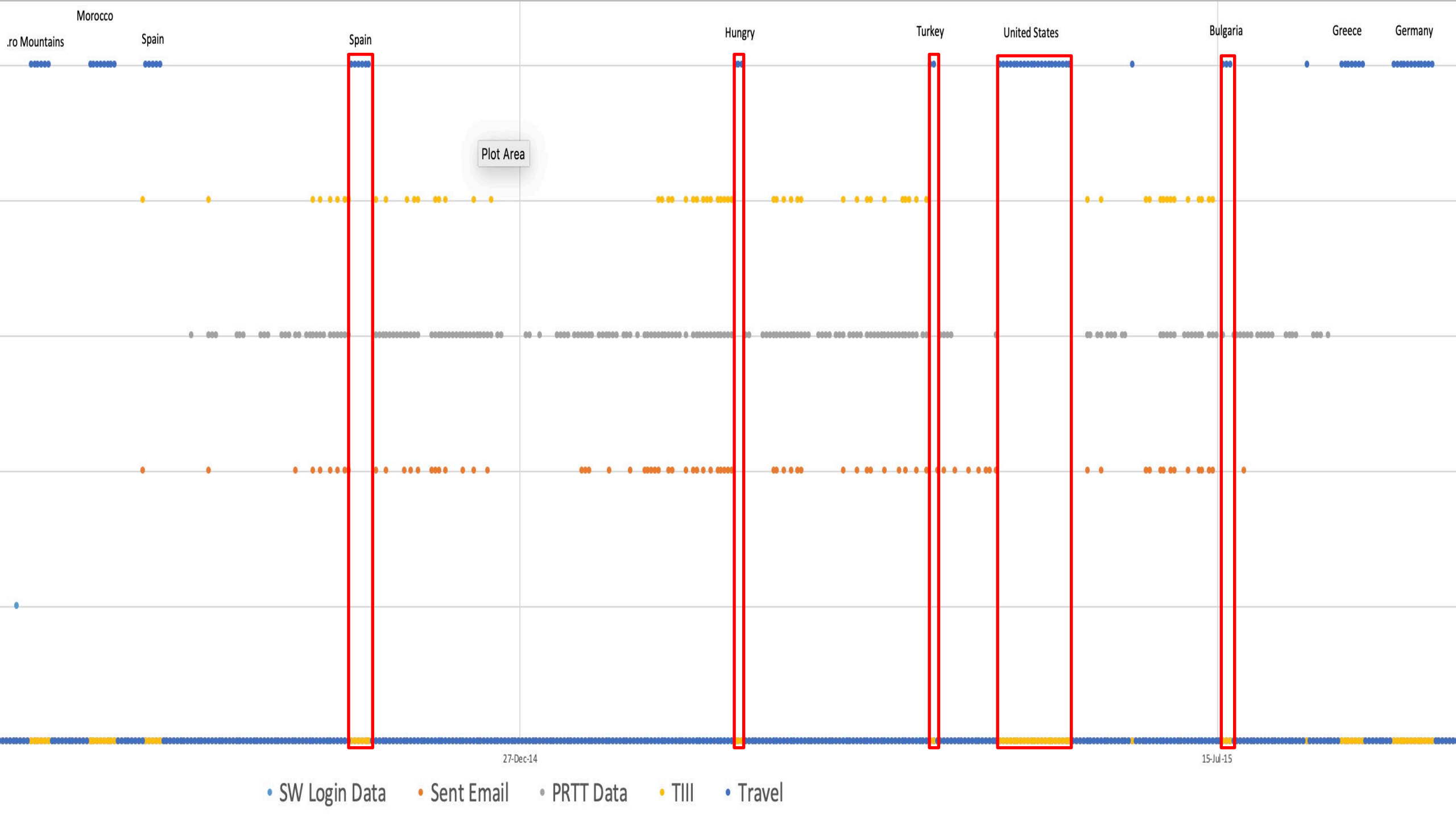
CHARGES

- Auction fraud
- Credit card theft
- Money laundering
- Operating a botnet
- Trafficking in counterfeits


DTF Criminal Division
U.S. Attorney's
DTF


01:50
obe@aro.strangled.net
Offline
01:32: OTR error: You sent encrypted data to obe@aro.strangled.net/
r, who wasn't expecting it.
01:32: Encryption has been enabled but this contact has not been
verified. You can verify it from the OTR encryption menu.
deci tre sa duci 8825 ron si $11,170
01:33
tu ai 1072+280+1000(mf) = 2352 ron
01:33
si eu am 10455+2737 =
13192-1000(min) = 12192 ron
01:33
01:34: Attention was requested
ok?
01:34
Ok


Draw
Page Layout
Formulas
Data
Review
View
Page Layout
Custom Views
Ruler
Formula Bar
Gridlines
Headings
Zoom
200%
Zoom to 100%
mf
linx
min
amy
raul
raul beem

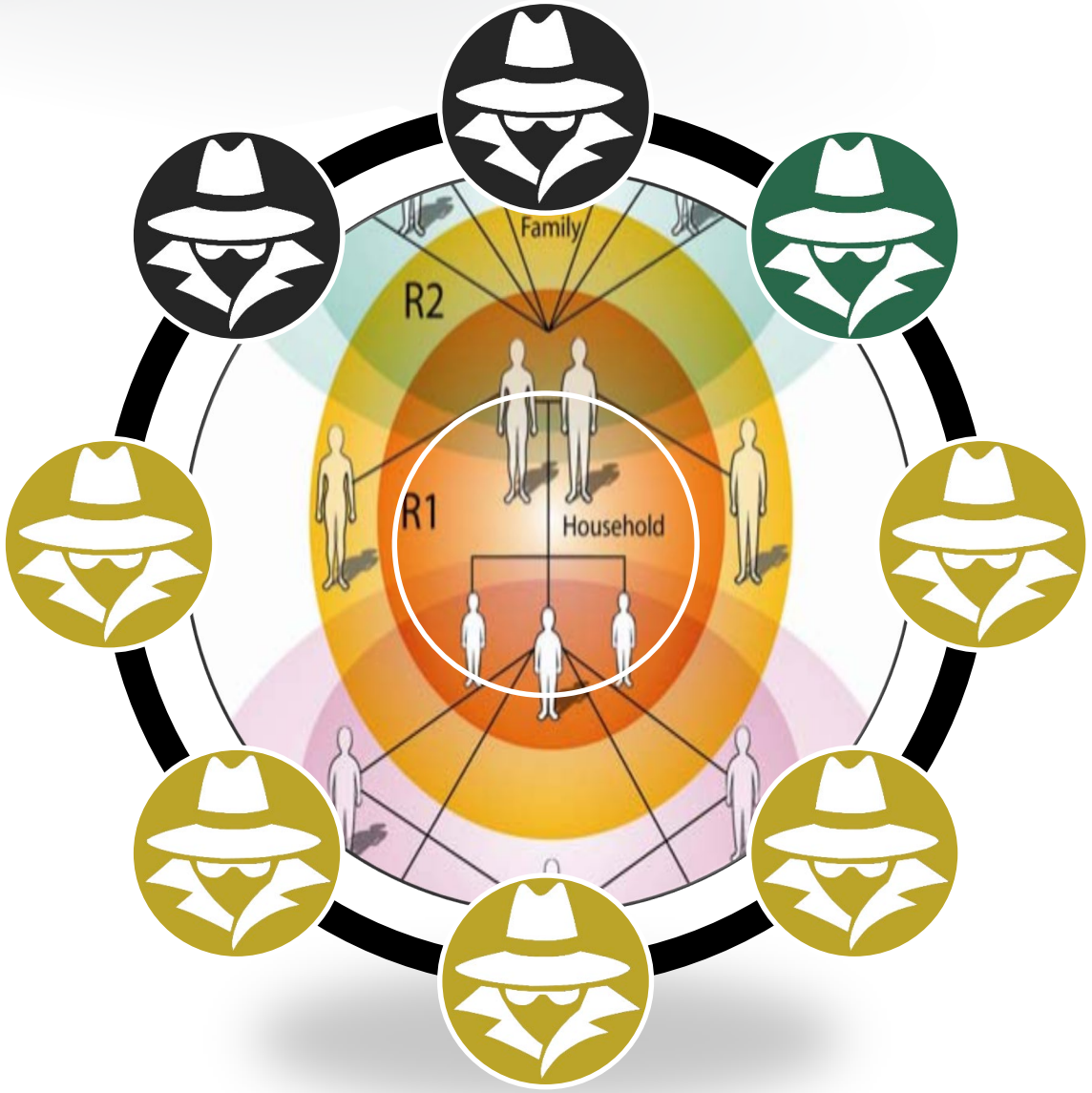

.ro Mountains
Morocco
Spain
Spain
Hungry
Turkey
United States
Bulgaria
Greece
Germany
Plot Area
27-Dec-14
15-Jul-15
SW Login Data
Sent Email
PRTT Data
TIII
Travel

DANET PLEAS

- Confirms everything we know
- Identifies the majority of the group we didn't know
- Describes the setup
- Provides passwords he remembers

Working the human element

- Associates often the weakest link in OPSEC
- Create a significant surface area
- Tell the story from the inside



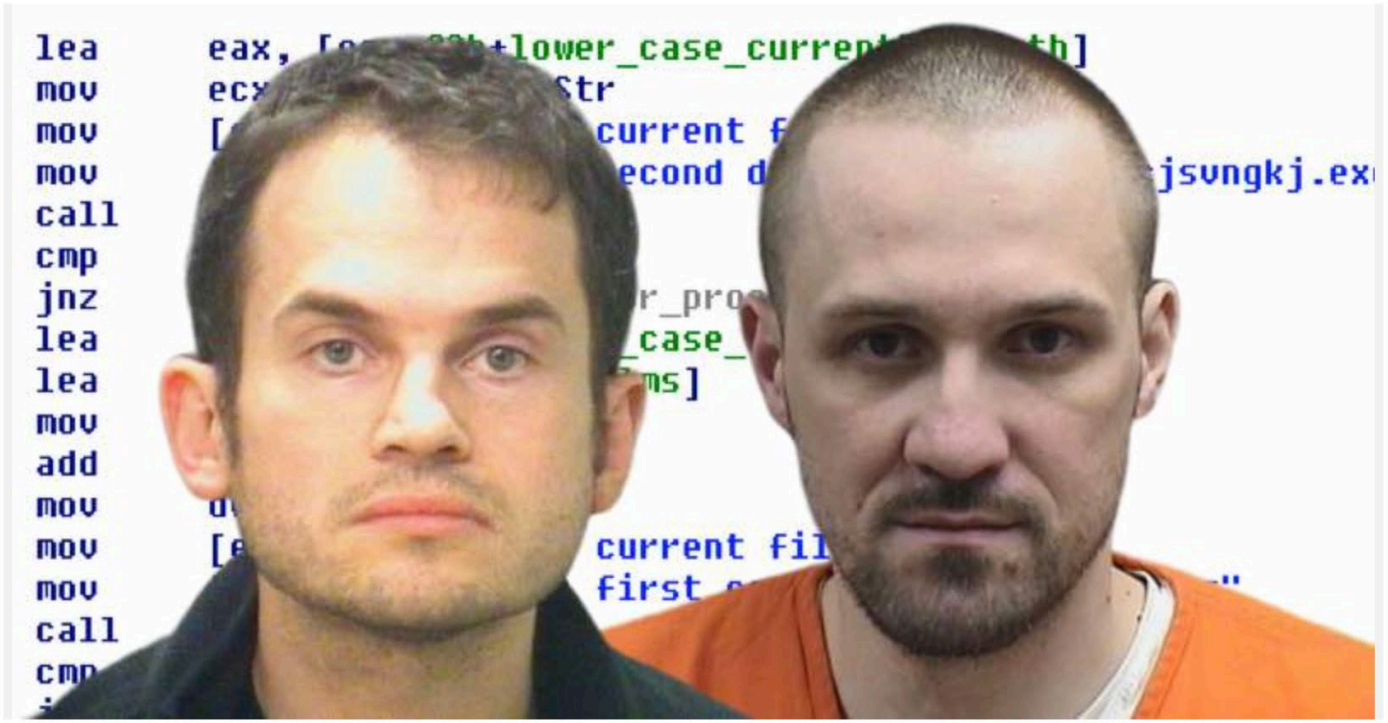
Trial outcome

- Each Guilty on 21 counts
  - Wire fraud (12 counts)
  - Traffic in Counterfeit Service Marks (1 count)
  - Aggravated Identity Theft (5 counts)
  - Money Laundering (1 count)
  - Conspiracy counts on the available statutes (2)

INDUSTRY NEWS

Bayrob malware gang convicted of infecting over 400,000 computers worldwide, stealing millions through online auction fraud

1 day ago 4 Min Read



A US court has convicted two Romanian hackers belonging to the Bayrob malware gang after they infected over 400,000 computers around the world, and stole millions of dollars.

Some good rules

1. Don’t talk openly
2. Don’t operate from home
3. Encrypt everything
4. No logs
5. Create Personas
6. Don’t contaminate
7. Don’t trust
8. Be paranoid
9. Don’t talk to police
10. Don’t give people power over you

1. OTR, radio noise, no phone talk ✓
2. Stolen wifi, hacked routers, proxies, TOR ✓
3. SFTP, SSH, PGP, OTR, LUKS, Truecrypt,+ ✓
4. Logging disabled ✓
5. Hacker Handles ✓
6. Isolated hacking environment ✓
7. Built all tech themselves ✓
8. Triple encrypted drives, proxychaining ✓
9. A lot of pressure ✓
10. Limited inner circle ✓

RSAConference2020

Questions?

Thank you RSA!