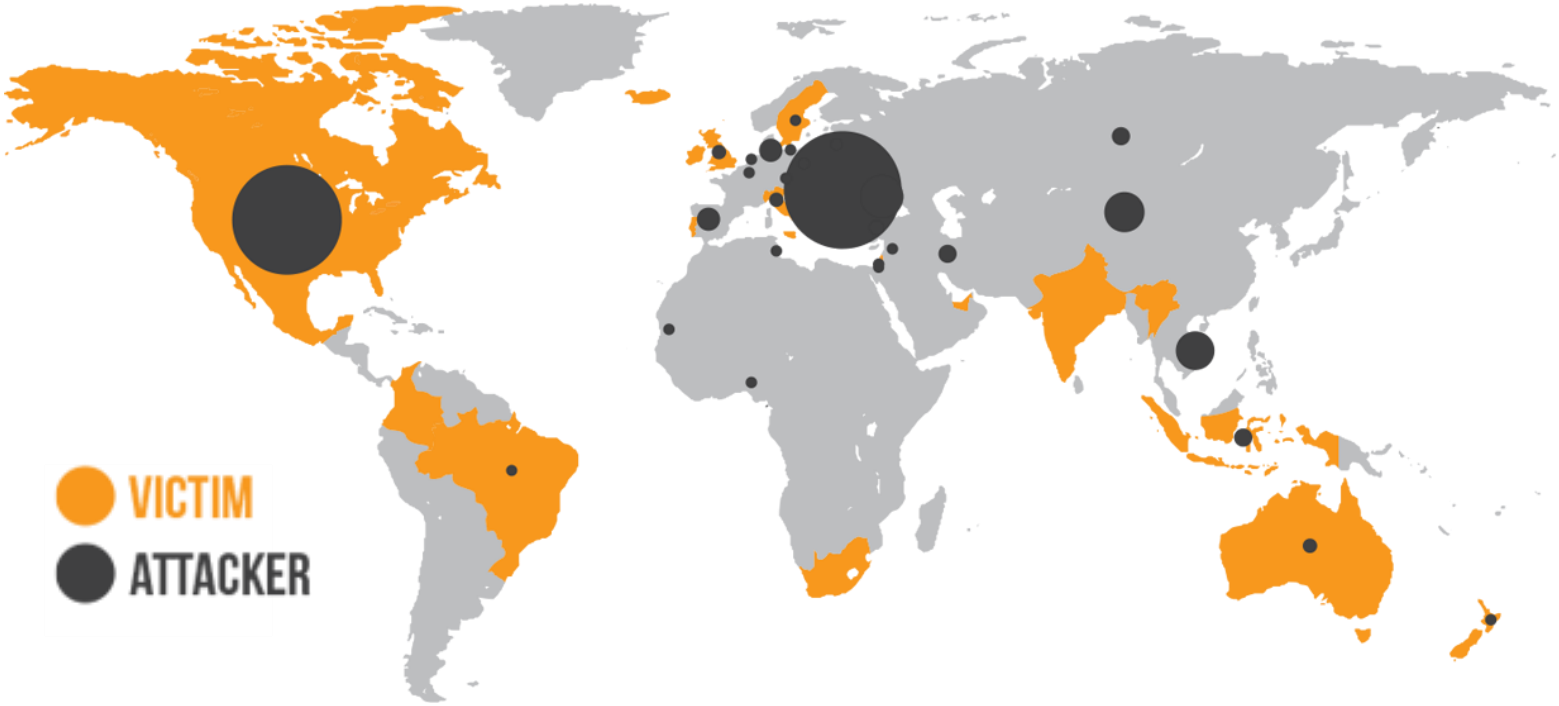
THE BAD BOYS OF CYBERCRIME

Christopher Pogue, Director

Trustwave®

SMART SECURITY ON DEMAND

A GLOBAL PROBLEM



TOP VICTIM LOCATIONS:	
UNITED STATES	73.0%
AUSTRALIA	7.0%
CANADA	3.0%
UNITED KINGDOM	2.0%
BRAZIL	1.2%

TOP ATTACKER LOCATIONS:	
ROMANIA	33.4%
UNITED STATES	29.0%
UNKNOWN	14.8%
UKRAINE	4.4%
CHINA	3.9%

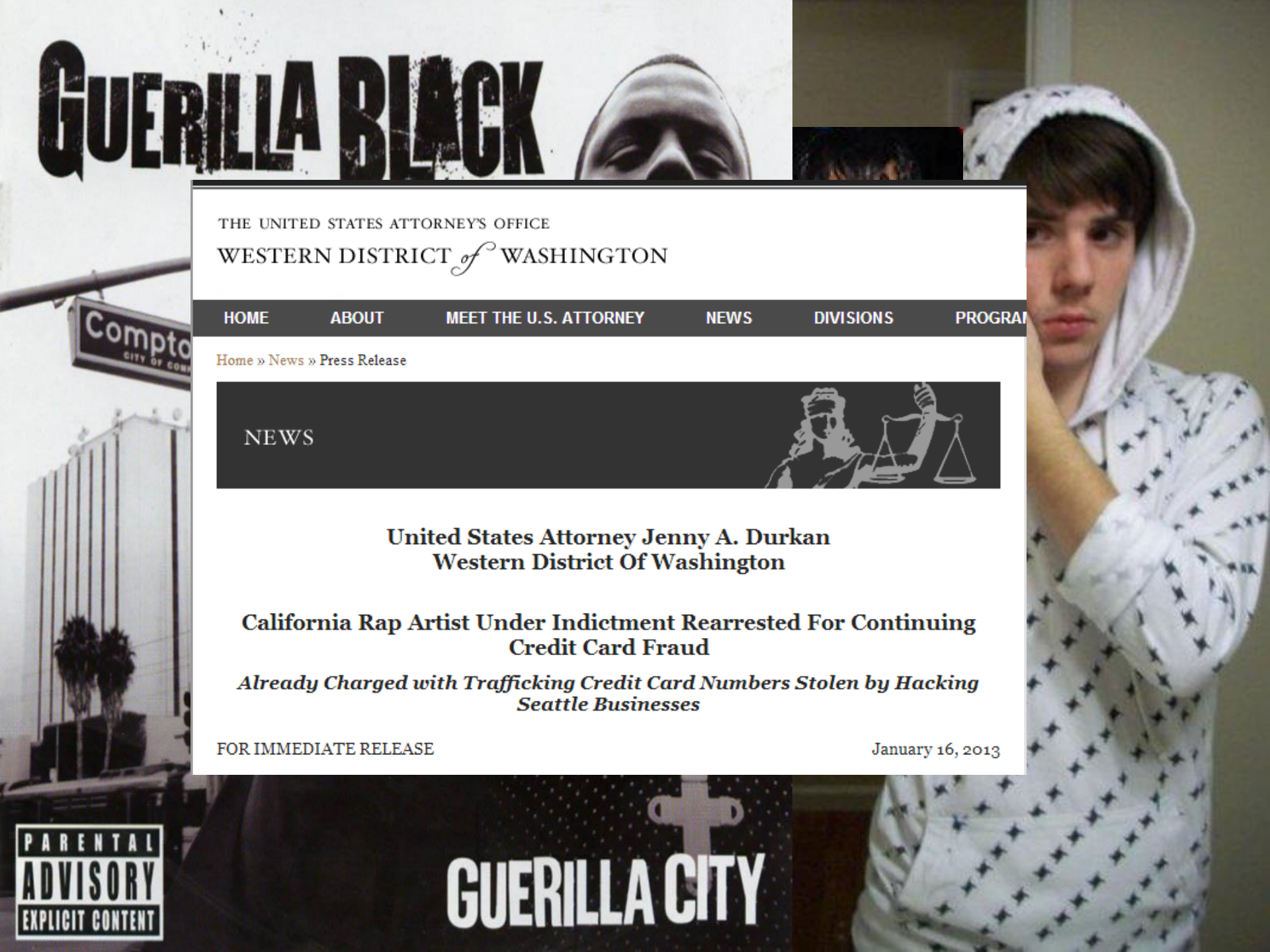
ACKNOWLEDGEMENTS

This presentation was written by the SpiderLabs in conjunction with United States Secret Service, Special Agent Mike Burgin.

The Original "Original Gangsters"

"I rob banks…what do you do?"
- John Dillinger

"Why do I rob banks? Because that's where the money is."
- Willie Sutton



THE UNITED STATES ATTORNEY'S OFFICE
WESTERN DISTRICT of WASHINGTON

HOME ABOUT MEET THE U.S. ATTORNEY NEWS DIVISIONS PROGRAM

Home » News » Press Release

NEWS

United States Attorney Jenny A. Durkan
Western District Of Washington

California Rap Artist Under Indictment Rearrested For Continuing Credit Card Fraud

Already Charged with Trafficking Credit Card Numbers Stolen by Hacking Seattle Businesses

FOR IMMEDIATE RELEASE

January 16, 2013

ADVANTAGE
OUTSIDE
pocket

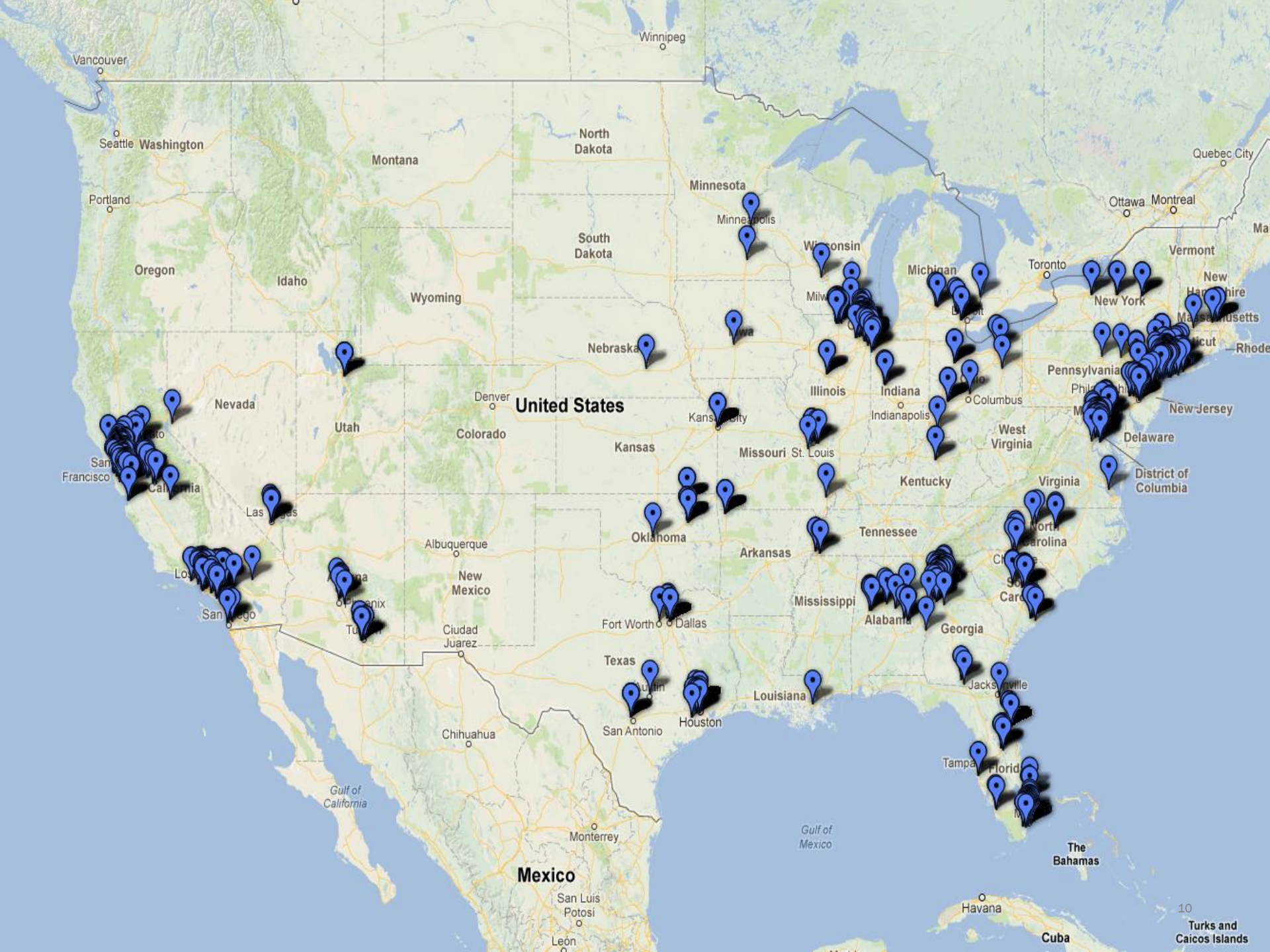
MSR206

MSR206u

IT'S PRETTY BAD

- Billions in fraud loss per year
- Huge impact to an already instable global economy
- International law enforcement involvement
- Thousands of businesses impacted world wide
- Massive criminal underground
- Mature criminal process
- Supplanting drug sales as the #1 source of revenue for organized crime
- No signs of slowing down

Trustwave®


Winnipeg
Vancouver
Seattle
Washington
Montana
North Dakota
Minnesota
Quebec City
Portland
Minneapolis
Ottawa
Montreal
South Dakota
Wisconsin
Vermont
Oregon
Idaho
Michigan
Toronto
Wyoming
New York
Nebraska
Pennsylvania
Illinois
Indiana
Columbus
Denver
United States
Nevada
Utah
Colorado
Indianapolis
New Jersey
Kansas
Missouri
St. Louis
West Virginia
Delaware
Kentucky
Virginia
District of Columbia
Las Vegas
Oklahoma
Tennessee
Albuquerque
Arkansas
New Mexico
Mississippi
Alabama
Georgia
Fort Worth
Dallas
Ciudad Juarez
Texas
Louisiana
Houston
San Antonio
Chihuahua
Gulf of California
Gulf of Mexico
Monterrey
The Bahamas
Mexico
San Luis Potosi
Havana
Cuba
León
Turks and Caicos Islands

CURRENT OPERATING ENVIRONMENT

- Not taken as seriously
- Largely overshadowed in the media by APT
- Often thought to be a “victimless” crime
- Limited focus on stopping the quantity of breaches
- Limited success for arbitration
- As opposed to a “threat”, this is an all out “assault”
- “Organized Cybercrime Assault” – The OCA

Trustwave®

WHY THINGS AREN'T GETTING BETTER

Trustwave®

SMART SECURITY ON DEMAND

TOP 25 PASSWORDS

BY PERCENT

Password1	38.7%
password	34.5%
Welcome1	16.0%
123456	12.6%
P@ssw0rd	11.8%
Passw0rd	10.9%
Password123	10.9%
Password2	10.1%
Summer12	10.1%
password1	10.1%

12345678	9.2%
Welcome2	7.6%
Spring2012	6.7%
Summer2012	6.7%
Password3	6.7%
Hello123	5.9%
Welcome3	5.9%
Fall2012	5.9%
Spring12	5.9%
pa$$w0rd	5.9%
p@ssw0rd	5.9%
p@ssword	5.0%
p@ssword1	5.0%
Summer11	5.0%
password9	5.0%

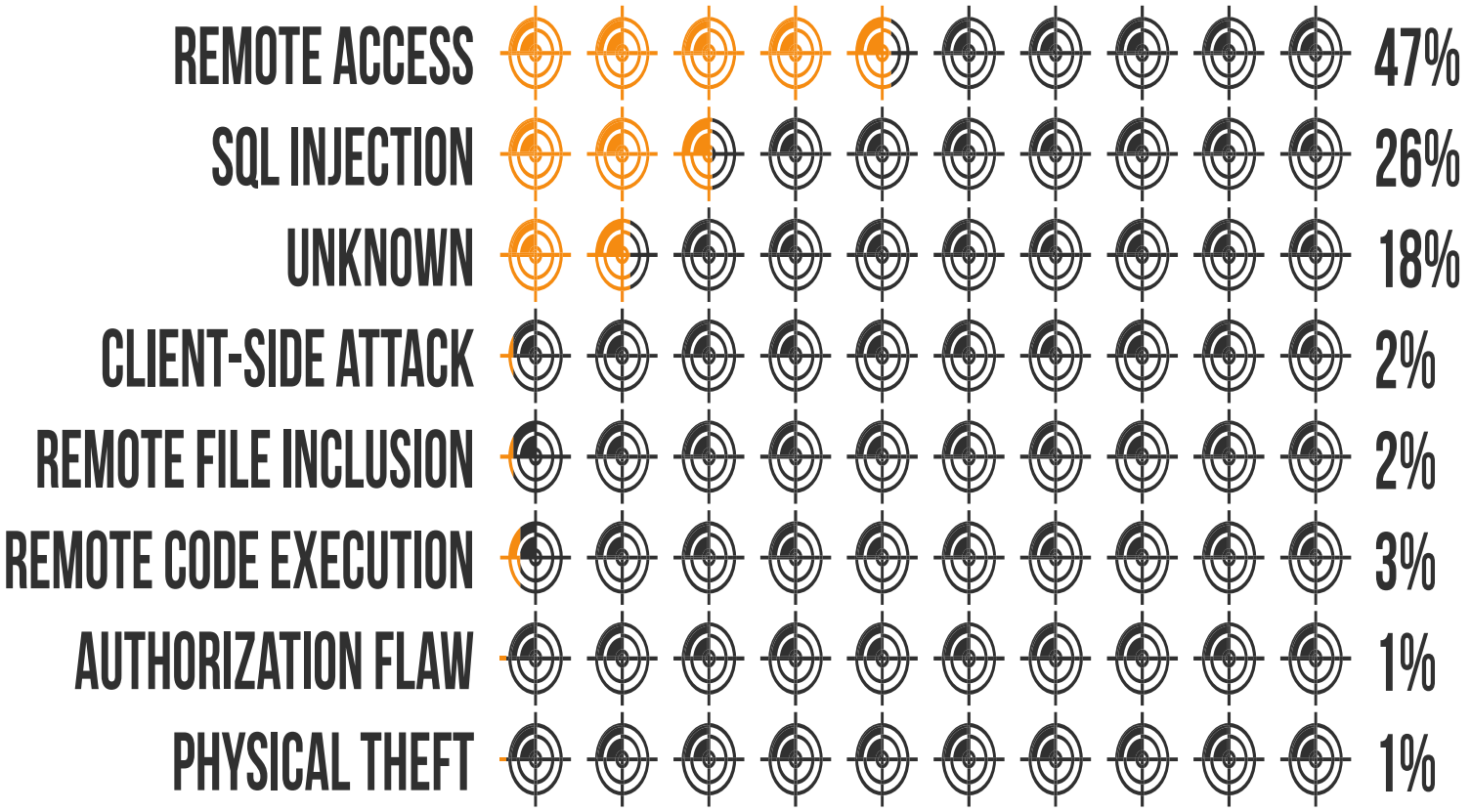
TOP PASSWORDS BY COUNT

BY COUNT

Welcome1	30,465
STORE123	21,362
Password1	15,383
password	9,466
Hello123	9,400
12345678	7,008
training	5,281
Welcome2	4,181
holiday	3,063
Happy123	2,987
123456	2,972
summer11	2,610
Welcome01	2,512
Welcome123	2,438
Changeme1	2,336
job12345	2,317
Welcome4	2,183
Password2	2,056
password1	2,053
Welcome3	2,047
Welcome22	2,029
Spring10	1,907
abcd1234	1,849
Password123	1,714
Summer11	1,473

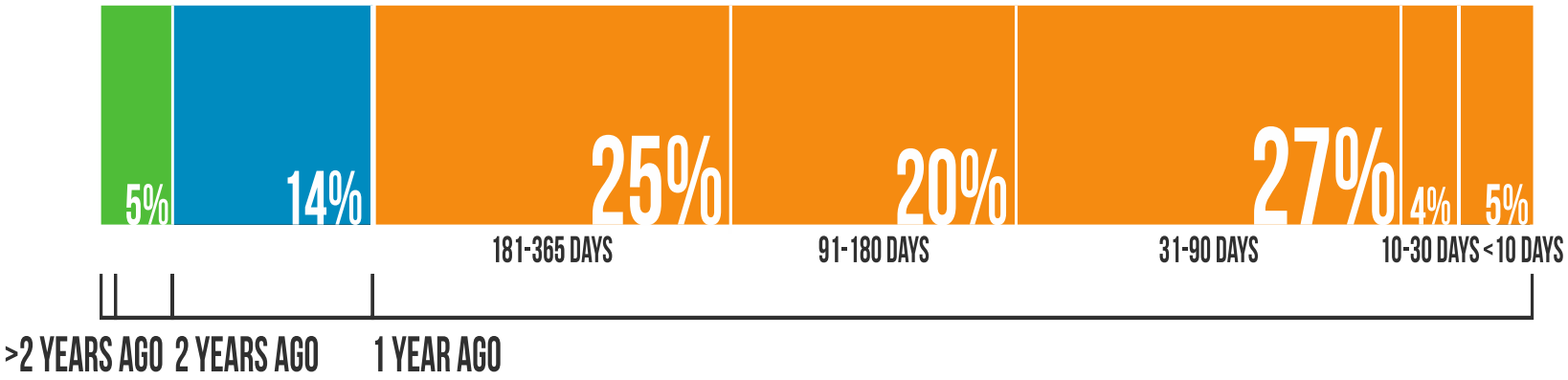
Trustwave®

METHOD OF ENTRY



BUSINESSES SLOW TO DETECT

TIMELINE: INTRUSION TO CONTAINMENT



Average of 210 days to detection.

Trustwave®

WHY THINGS AREN'T GETTING BETTER

- Not the core competency of the victim
- Third party outsourcing
- Naïve yet pervasive belief that, "It won't happen to me"
- Lack of understanding of how the OCA really works
- Lack of a broad pre-breach compliance incentive program
- Financial risks unknown, and often unquantifiable

Trustwave®

THE ORGANIZED CYBERCRIME ASSAULT

Trustwave®

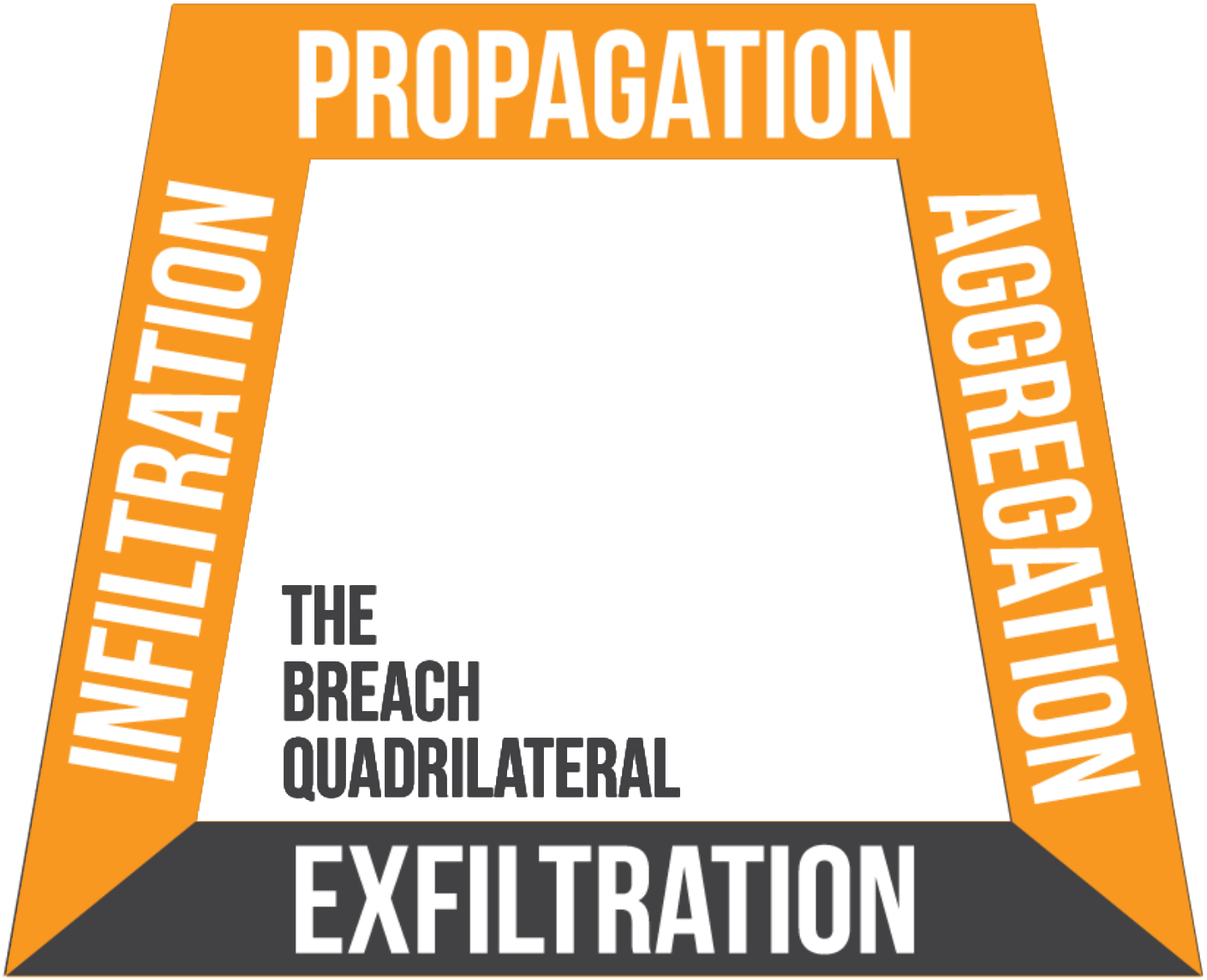
SMART SECURITY ON DEMAND

THE OCA

- Extremely organized
- Well Funded
- Large, trust based networks (largely Russian language)
- Multiple components (Recon, deployment, harvesting, exfil, sales, fraud)
- Difficult to pursue
- MLAT process takes time
- Low risk, high reward

Trustwave®

Trustwave®


PROPAGATION
INFILTRATION
AGGREGATION
THE
BREACH
QUADRILATERAL
EXFILTRATION

THE BREACH QUADRILATERAL

- Infiltration
  - Bad guy in
- Propagation
  - Bad guy pivot
- Aggregation
  - Bad guy take stuff
- Exfiltration
  - Bad guy out with wtuff

Trustwave®

THE BREACH QUADRILATERAL

Understanding the BQ

- Is a constant (must always be in place)
- Has clearly defined phases
- Once defined, can be addressed
  - Investigations
  - Remediation
  - Defense

Commonalities with the APT

- Same methodology (actors or target data is irrelevant)
- Not smoke and mirrors
- Must play by the rules

Trustwave®

INTELLIGENCE HAND-OFF

Trustwave®

SMART SECURITY ON DEMAND

The APT is Coming for You!

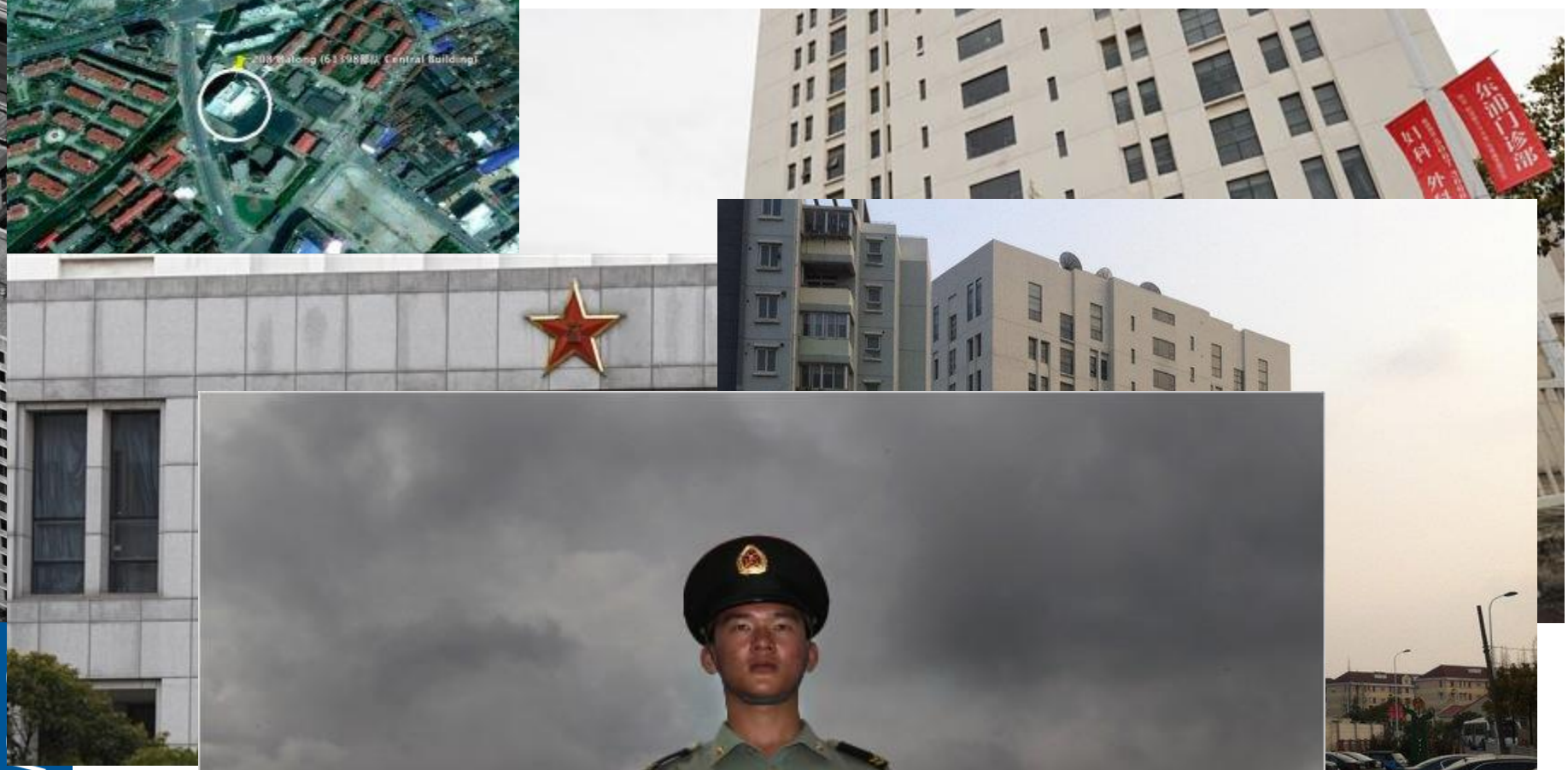


PHOTO: DALE DE LA REY/AFP/GETTY IMAGES

Trustw

The OCA is Already Here!

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOP

The New York Times

Global Bu

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIE

Hacker

By ANDREW E.
Published: Aug

MOSCOW
criminal fli
numbers d

THREAT LEVEL | crime | hacks ar

Ukrainian Carding King Arrest

BY KIM ZETTER 07.28.10 10:00 AM

Guerilla Black Fraud

The Compton rapper is allegedl

By Reggie Ugwu
Posted: 01/17/2013 12:06 PM EST
Filed Under Music News, Notorious B.I.G., Ga

LAW & DISORDER / CIVILIZATION & DISCONTENTS

Another Romanian hacker arrested for breaching NASA servers

An unemployed 26-year old who goes by "Iceman" has been charged with causing a …

by Sean Gallagher - Nov 16, 2011 5:38 pm UTC

Share
Tweet this
Email

20

ed for damaging computer systems at NASA,
orate for Investigating Organized Crime and
h breaking into an unspecified number of servers at

Australia's biggest ever da credit card crime

November 29, 2012

Tweet | Pin it | submit

Email article | Print | Reprints & permissions

Met police investigating computer hacking arrest 52-year-old man

Man suspected of business espionage under the Computer Misuse Act as part of Operation Kalmyk

Josh Halliday
guardian.co.uk, Tuesday 29 January 2013 07.49 EST

Scotland Yard said the man, who is not a journalist, will be interviewed at an Oxfordshire police station. Photograph: Facundo Arrizabalaga/EPA

Romanian hackers busted with half a MILLION credit cards from Australia - how could THAT have happened?

by Paul Ducklin on November 30, 2012 | 7 Comments
FILED UNDER: Data loss, Featured, Law & order

The Australian Federal Police (AFP) are cock-a-hoop this week, announcing the bust of a gang of Romanian credit card hackers.

According to reports, 200 Romanian cops pounced on 36 locations, detained 16 people and ultimately arrested seven of them.

The carding crew had allegedly made off with half a million Aussie credit card numbers, racking up charges averaging more than $1000 each on 30,000 of them.

At this point, I'm sure you're thinking what I am. "Half a MILLION cards from Australia. And the crooks didn't even need to leave Romania. How could THAT have happened?"

The answer, according to the Australian cops, is RDP.

Why do you hack?

Cybercrime More Lucrative Than Drug Trade

by Tim Stevens, posted Sep 19th 2007 at 11:05AM

Getty

If you've ever had your computer hacked, or credit card or other personal details stolen online, congratulations: You're now a statistic in a crime wave that has officially surpassed the international drug trade in terms of overall value. Cybercrime like those and various other technology-related scams have become a $105 billion per year business, thanks largely to losses relating to major data breaches at financial services companies such as Citigroup and Ameritrade.

According to David DeWalt, CEO of computer security firm McAffe, the big problem is that laws punishing the perpetrators of such crimes are simply not keeping up with the volume of these misdeeds. "If you rob a 7-11 you'll get a much harsher punishment than if you stole millions online," DeWalt says. "The cross-border sophistication in tracking and arresting cyber-criminals is just not there." This statistic comes on the heels of a report earlier this month that Britons were the victims of

Because that's where the money is!

Trustwave®

ATTACK SOPHISTICATION

- Community sustains—and develops—professional community of well-paid attackers
- Honing skills to attack financial systems = full-time job
- Reflected in intercepted communications (e.g., HSMs)
  - “пряму тут на вебе нашел кое какую информацию SWIFT значит система гдето в сетке есть.. помимо того как будешь искать хсм поглядывай и на свифты тоже”
  - “he found way to interact with hsm // sending pinblocks and get pins”
  - “he found atala HSM inside // and working keys for them // updating balance works perfect, it`s really sweet place”

RECRUITING TOP TALENT

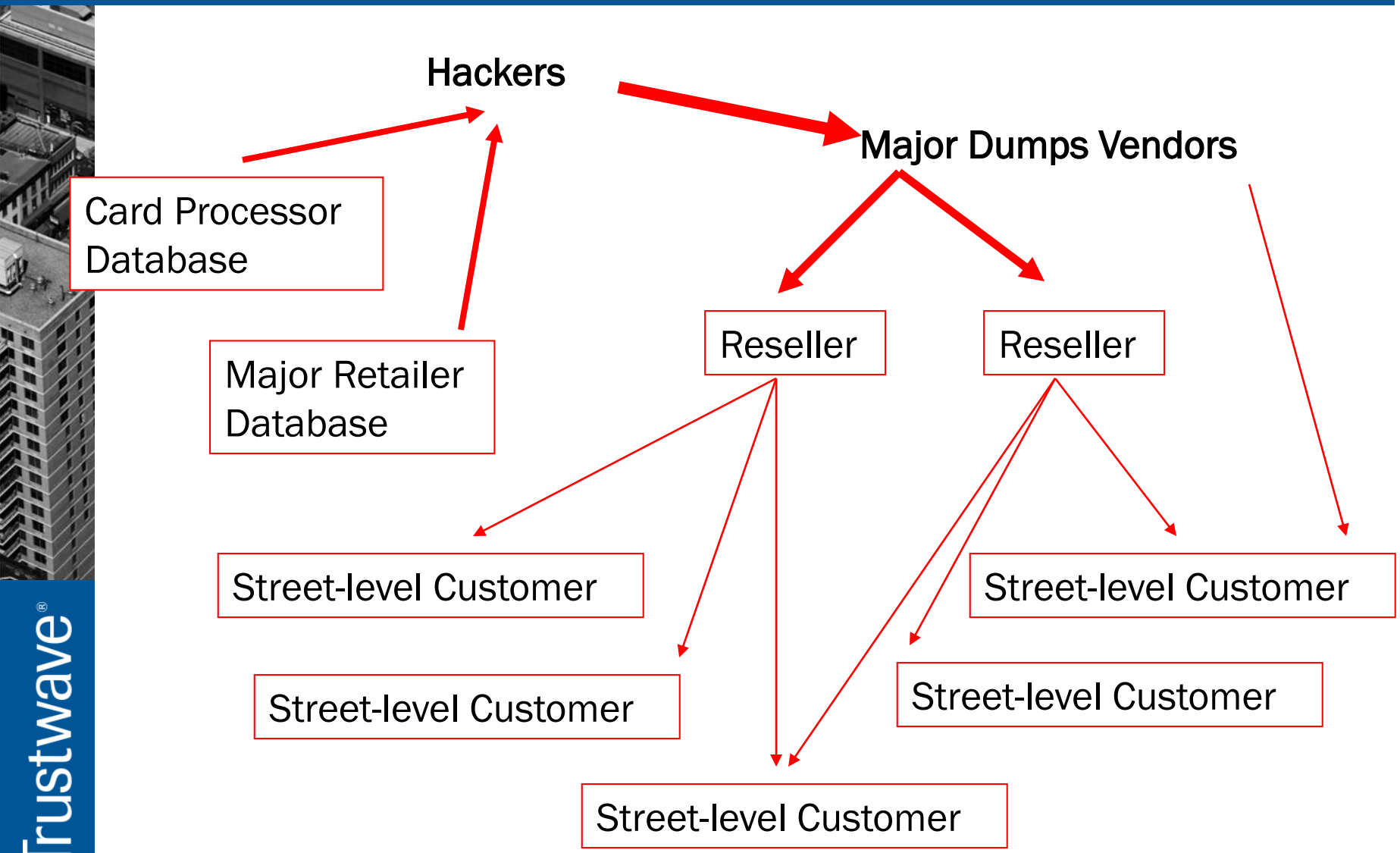
received	2005.04.20 01:13:00	its not a secret im 26 old
sent	2005.04.20 01:13:10	you're my age
received	2005.04.20 01:13:37	i finished russia kgb academy of cryptography)
received	2005.04.20 01:13:54	but i dont want to servethem)
received	2005.04.20 01:14:02	now im here)

GOOD NEWS / BAD NEWS

- Online criminals generally do not want to destroy or debilitate financial infrastructure or institutions
- However, criminal organizations do want to attack institutions and their customers to siphon off as much money as possible
  - Bankrupting customers through fraud enabled through technology and/or social engineering
  - Infecting financial systems with various malware
  - Intruding into networks for theft and recon

Trustwave®

“DUMPS” BUSINESS CYCLE



Trustwave®

29-06-2010, 10:53 AM

BadB
SELLER of:
DUMPS

BadB is offline

Join Date: Nov 2009

Posts: 86

Reputation: 5 +/-

Quote selected

The Single Controling Source as shown in past Cyber Crime Trend Reports

Big update will be done of 1st of July!

Since all update made not from freshest base in association with one of biggest dealer online the validity is about 60%. But there is very much really good bins and goods.

Base is good, but we are still suggest to use the checker.

Big booooooooooooooooooo action will take a part in the 30 of June, this time it will be interactive and arranged as game. Freebie action will also be provided even for no

Now a little about the bases currently in stock.
1. Big base of 40mln of dumps, we putting only dumps expiring next month, validity is about 60%, some bins dead, but if good - still good. Since it all cant ba blocked due am
expensive ones, both 101 and 201.
2. USA base, from couple of pos terminals, about 500 pcs daily income, updates every week.
3. Couple of small EU bases, updates from time to time.

---------- Сообщение добавлено в 07:53 AM ---------- Предыдущее сообщение размещено в 07:52 AM ----------

Very soon we planing to put a lot of UK dumps.

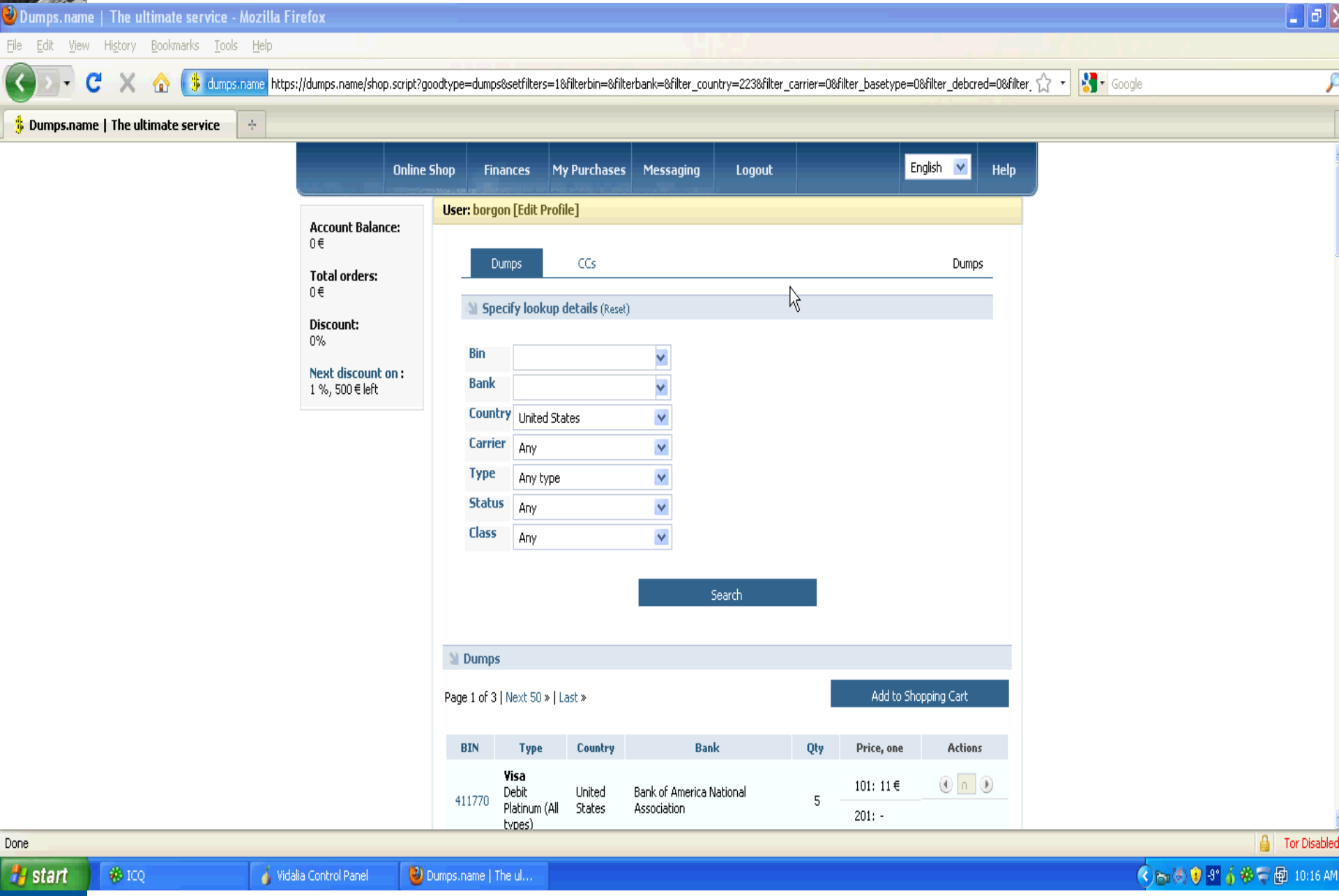
Main Base is 40 million dumps mixed with several smaller bases. this helps the bad guys hide from the main source from the banks

First online dumps shop https://dumps.name

ICQ: 49162552
Jabber: badb@badb.biz
E-mail: badb@badb.biz

Web: http://badb.biz and http://dumps.name

BadB's fully automated dumps vending website

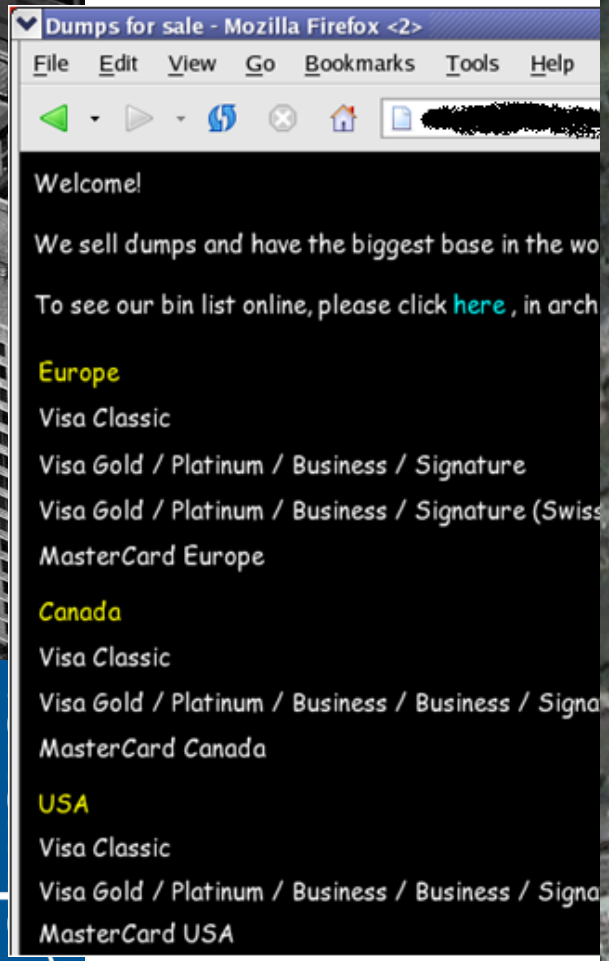


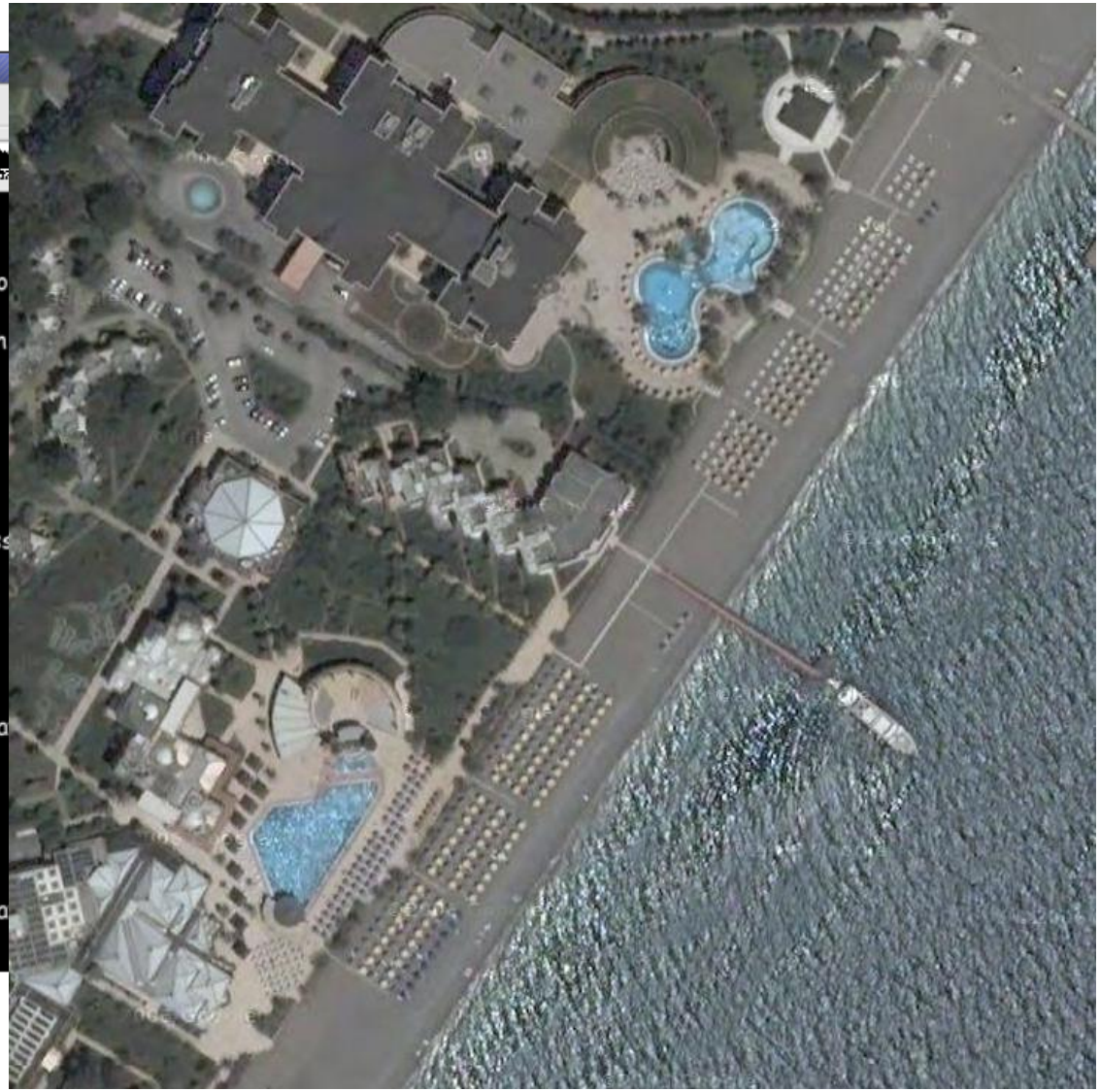
AUTOMATING STOLEN CARD SALES

- Dumps.name
- Trackservices.biz
- Zukkoshop.net
- CardRockCafe.biz
- Track2.name
- Cvvshop.com
- Cvv2shop.com
- Dumps.ws
- Darkservices.cc
- Autosell.cc
- FreshShop.su
- Mn0g0.su
- Hqcc.biz
- Cardt.ru
- CCshop.su
- Vaultmarket.org
- LTDcc.com
- Cvv2.su
- CC.am
- Killa.cc
- Bigseller.cc
- CCsell.biz

Trustwave®

FROM THE FRONT LINES





ENTIRE HOUSING DEVELOPMENT

CONCLUSION

Trustwave®

SMART SECURITY ON DEMAND

THE OCA IS REAL

- Replacing drug sales
- Organized, capable, and effective
- Difficult to pursue
- Must “follow the rules” of cybercrime
- The Breach Quadrilateral

Trustwave®

FIGHTING THE OCA

Get in the fight

- Understand how the OCA works
- Implement smart security controls

Combined Arms Effort

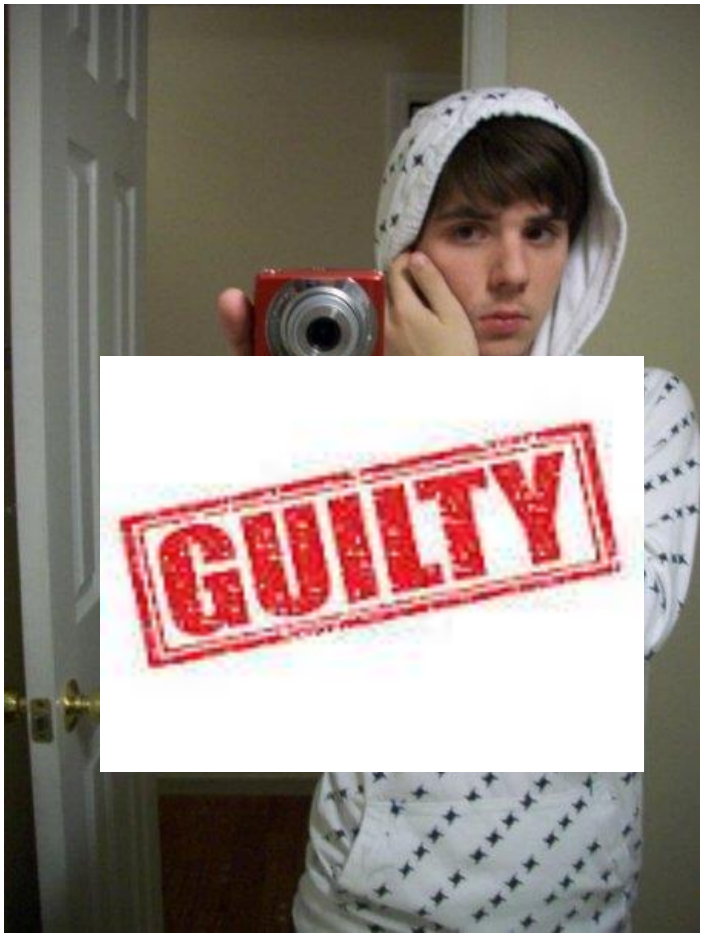
- Law Enforcement
- Private Industry

Spread Awareness

- Not a victimless crime
- Billions in fraud loss

Trustwave®

UPDATE!



Christopher Schroebel - 21
A.K.A. “Junkie”

Serving 7 years for
“Obtaining Information From a Protected Computer”
Captured with 84,000 credit card numbers in his possession.

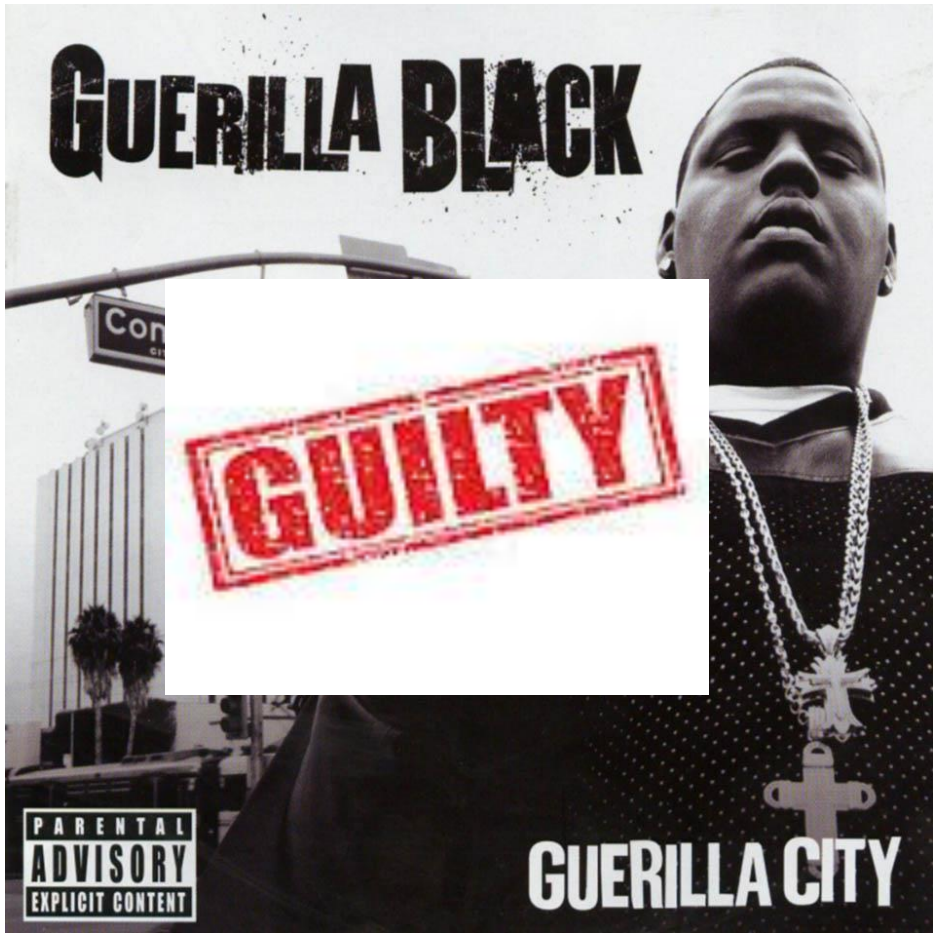
Rolled on his homies

UPDATE!

David Benjamin Schrooten
A.K.A. “Fortezza”
Dutch National
Head of the carding forum
“Kurupt.su”

Sentenced to 12 years after pleading guilty to “Conspiracy to Commit Access Device Fraud and Bank Fraud, Access Device Fraud, Bank Fraud, Intentional Damage to a Protected Computer, and Aggravated Identity Theft.”

UPDATE!



Charles Williamson
A.K.A. “Guerilla Black”

Pled Guilty to federal “Conspiracy, unauthorized access to a protected computer to facilitate fraud, access device fraud, bank fraud, and aggravated identity theft” charges on July 9, 2013 – To be sentenced in October 2013.

QUESTIONS

Trustwave®

THANK YOU!

CEPOGUE@TRUSTWAVE.COM
@SPIDERLABS
@CPBEEFCAKE

Trustwave®

SMART SECURITY ON DEMAND