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
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
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 worldwide
- Massive criminal underground
- Mature criminal process
- Supplanting drug sales as the #1 source of revenue for organized crime
- No signs of slowing down
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
WHY THINGS AREN’T GETTING BETTER
# Top 25 Passwords by Percent

<table>
<thead>
<tr>
<th>Password</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password1</td>
<td>38.7%</td>
</tr>
<tr>
<td>password</td>
<td>34.5%</td>
</tr>
<tr>
<td>Welcome1</td>
<td>16.0%</td>
</tr>
<tr>
<td>123456</td>
<td>12.6%</td>
</tr>
<tr>
<td>P@$sw0rd</td>
<td>11.8%</td>
</tr>
<tr>
<td>Password</td>
<td>10.9%</td>
</tr>
<tr>
<td>Password123</td>
<td>10.9%</td>
</tr>
<tr>
<td>Password2</td>
<td>10.1%</td>
</tr>
<tr>
<td>Summer12</td>
<td>10.1%</td>
</tr>
<tr>
<td>password1</td>
<td>10.1%</td>
</tr>
<tr>
<td>12345678</td>
<td>9.2%</td>
</tr>
<tr>
<td>Welcome2</td>
<td>7.6%</td>
</tr>
<tr>
<td>Spring2012</td>
<td>6.7%</td>
</tr>
<tr>
<td>Summer2012</td>
<td>6.7%</td>
</tr>
<tr>
<td>Password3</td>
<td>6.7%</td>
</tr>
<tr>
<td>Hello123</td>
<td>5.9%</td>
</tr>
<tr>
<td>Welcome3</td>
<td>5.9%</td>
</tr>
<tr>
<td>Fall2012</td>
<td>5.9%</td>
</tr>
<tr>
<td>Spring12</td>
<td>5.9%</td>
</tr>
<tr>
<td>pa$$w0rd</td>
<td>5.9%</td>
</tr>
<tr>
<td>p@$sw0rd</td>
<td>5.9%</td>
</tr>
<tr>
<td>p@$sw0rd</td>
<td>5.9%</td>
</tr>
<tr>
<td>p@$sw0rd</td>
<td>5.0%</td>
</tr>
<tr>
<td>Summer11</td>
<td>5.0%</td>
</tr>
<tr>
<td>password9</td>
<td>5.0%</td>
</tr>
<tr>
<td>Password</td>
<td>Count</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Welcome1</td>
<td>30,465</td>
</tr>
<tr>
<td>Store123</td>
<td>21,362</td>
</tr>
<tr>
<td>Password1</td>
<td>15,383</td>
</tr>
<tr>
<td>Password</td>
<td>9,466</td>
</tr>
<tr>
<td>Hello123</td>
<td>9,400</td>
</tr>
<tr>
<td>12345678</td>
<td>7,008</td>
</tr>
<tr>
<td>Training</td>
<td>5,281</td>
</tr>
<tr>
<td>Welcome2</td>
<td>4,181</td>
</tr>
<tr>
<td>Holiday</td>
<td>3,063</td>
</tr>
<tr>
<td>Happy123</td>
<td>2,987</td>
</tr>
<tr>
<td>summer11</td>
<td>2,610</td>
</tr>
<tr>
<td>Welcome01</td>
<td>2,512</td>
</tr>
<tr>
<td>Welcome123</td>
<td>2,438</td>
</tr>
<tr>
<td>Changeme1</td>
<td>2,336</td>
</tr>
<tr>
<td>job12345</td>
<td>2,317</td>
</tr>
<tr>
<td>Welcome4</td>
<td>2,183</td>
</tr>
<tr>
<td>Password2</td>
<td>2,056</td>
</tr>
<tr>
<td>password1</td>
<td>2,053</td>
</tr>
<tr>
<td>Welcome3</td>
<td>2,047</td>
</tr>
<tr>
<td>Welcome22</td>
<td>2,029</td>
</tr>
<tr>
<td>Spring10</td>
<td>1,907</td>
</tr>
<tr>
<td>abcd1234</td>
<td>1,849</td>
</tr>
<tr>
<td>Password123</td>
<td>1,714</td>
</tr>
<tr>
<td>Summer11</td>
<td>1,473</td>
</tr>
</tbody>
</table>
## Method of Entry

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access</td>
<td>47%</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>26%</td>
</tr>
<tr>
<td>Unknown</td>
<td>18%</td>
</tr>
<tr>
<td>Client-Side Attack</td>
<td>2%</td>
</tr>
<tr>
<td>Remote File Inclusion</td>
<td>2%</td>
</tr>
<tr>
<td>Remote Code Execution</td>
<td>3%</td>
</tr>
<tr>
<td>Authorization Flaw</td>
<td>1%</td>
</tr>
<tr>
<td>Physical Theft</td>
<td>1%</td>
</tr>
</tbody>
</table>
BUSINESSES SLOW TO DETECT

TIMELINE: INTRUSION TO CONTAINMENT

Average of 210 days to detection.
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
THE ORGANIZED CYBERCRIME ASSAULT
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
THE BREACH QUADRILATERAL

PROPAGATION

INfiltration

AGGREGATION

EXFILTRATION
THE BREACH QUADRILATERAL

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

SMART SECURITY ON DEMAND
The APT is Coming for You!
The OCA is Already Here!

Another Romanian hacker arrested for breaching NASA servers
An unemployed 26-year-old who goes by "Iceman" has been charged with causing a...

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 18 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?

Because that’s where the money is!
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

2005.04.20 01:13:00 its not a secret im 26 old

2005.04.20 01:13:10 you're my age

2005.04.20 01:13:37 i finished russia kgb academy of cryptography )

2005.04.20 01:13:54 but i dont want to servethem )

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
“DUMPS” BUSINESS CYCLE

- Hackers
- Major Dumps Vendors
- Card Processor Database
- Major Retailer Database
- Street-level Customer
- Street-level Customer
- Street-level Customer
- Street-level Customer
- Street-level Customer
- Street-level Customer
- Street-level Customer
Big update will be done on 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 booooooodddddddddddddd 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 not active users.

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 can't be blocked due amount of 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.

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

First online dumps shop https://dumps.name
BadB’s fully automated dumps vending website

![Website Screenshot](image_url)

### User Profile: borgon
- **Account Balance:** 0 €
- **Total orders:** 0
- **Discount:** 0%
- **Next discount on:** 1 %, 500 € left

### Dumps Section
- **Specify lookup details (optional):**
  - **Bin:**
  - **Bank:**
  - **Country:** United States
  - **Carrier:** Any
  - **Type:** Any type
  - **Status:** Any
  - **Class:** Any

### Dumps Table
<table>
<thead>
<tr>
<th>BIN</th>
<th>Type</th>
<th>Country</th>
<th>Bank</th>
<th>Qty</th>
<th>Price, one</th>
</tr>
</thead>
<tbody>
<tr>
<td>411770</td>
<td>Visa Debit Platinum (All Banks)</td>
<td>United States</td>
<td>Bank of America National Association</td>
<td>5</td>
<td>11 €</td>
</tr>
</tbody>
</table>

Add to Shopping Cart
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
Welcome!
We sell dumps and have the biggest base in the world.
To see our bin list online, please click [here](#), in archiv[...]

**Europe**
- Visa Classic
- Visa Gold / Platinum / Business / Signature
- Visa Gold / Platinum / Business / Signature (Swiss)
- MasterCard Europe

**Canada**
- Visa Classic
- Visa Gold / Platinum / Business / Business / Signature
- MasterCard Canada

**USA**
- Visa Classic
- Visa Gold / Platinum / Business / Business / Signature
- MasterCard USA
CONCLUSION

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
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
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