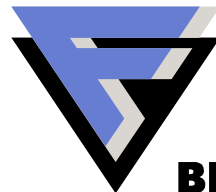


# Online Crime & Crime Online

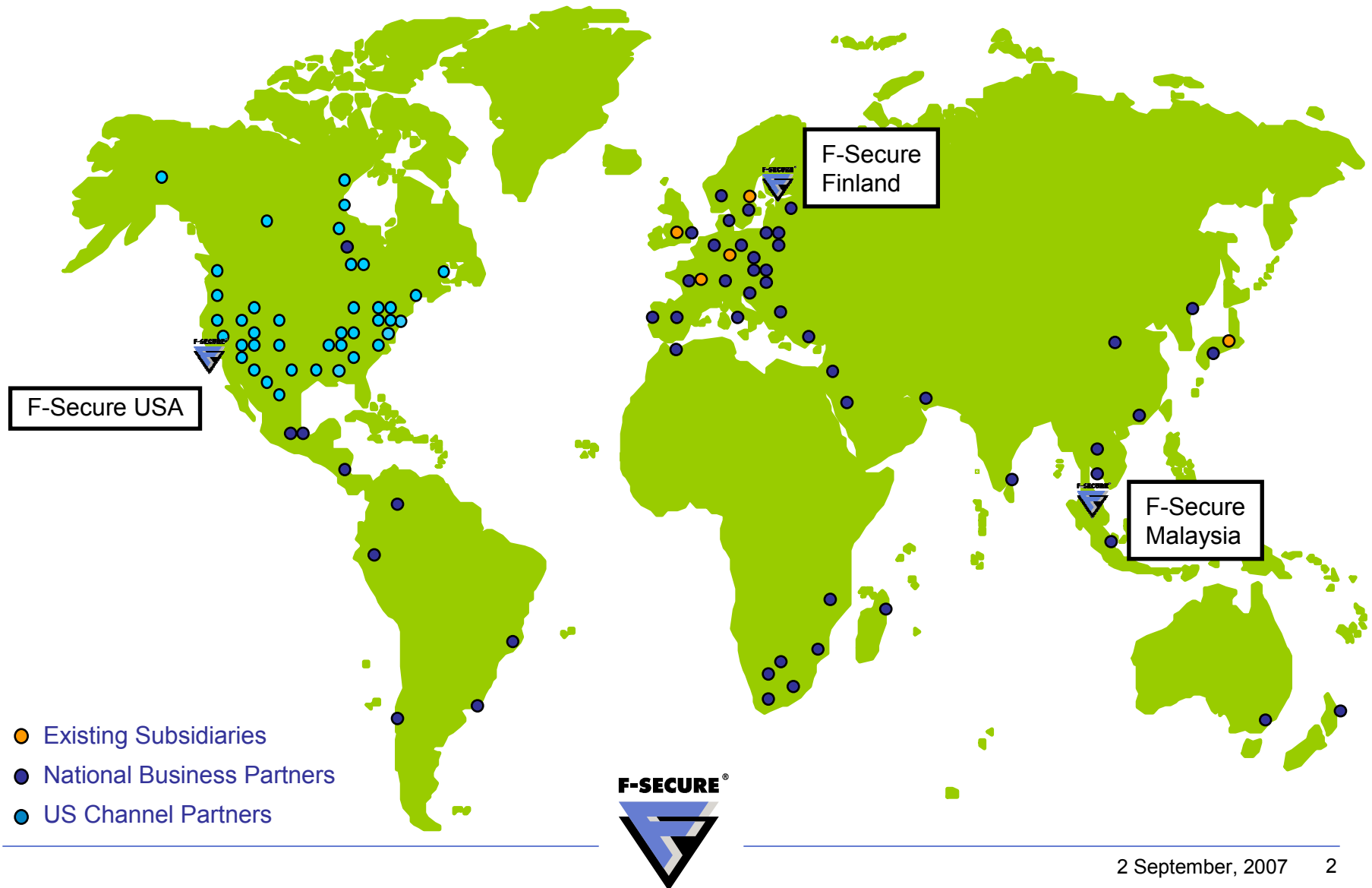
**Mikko Hypponen**  
**Chief Research Officer, F-Secure Corp**

**F-SECURE®**



**BE SURE.**

# F-Secure Corp













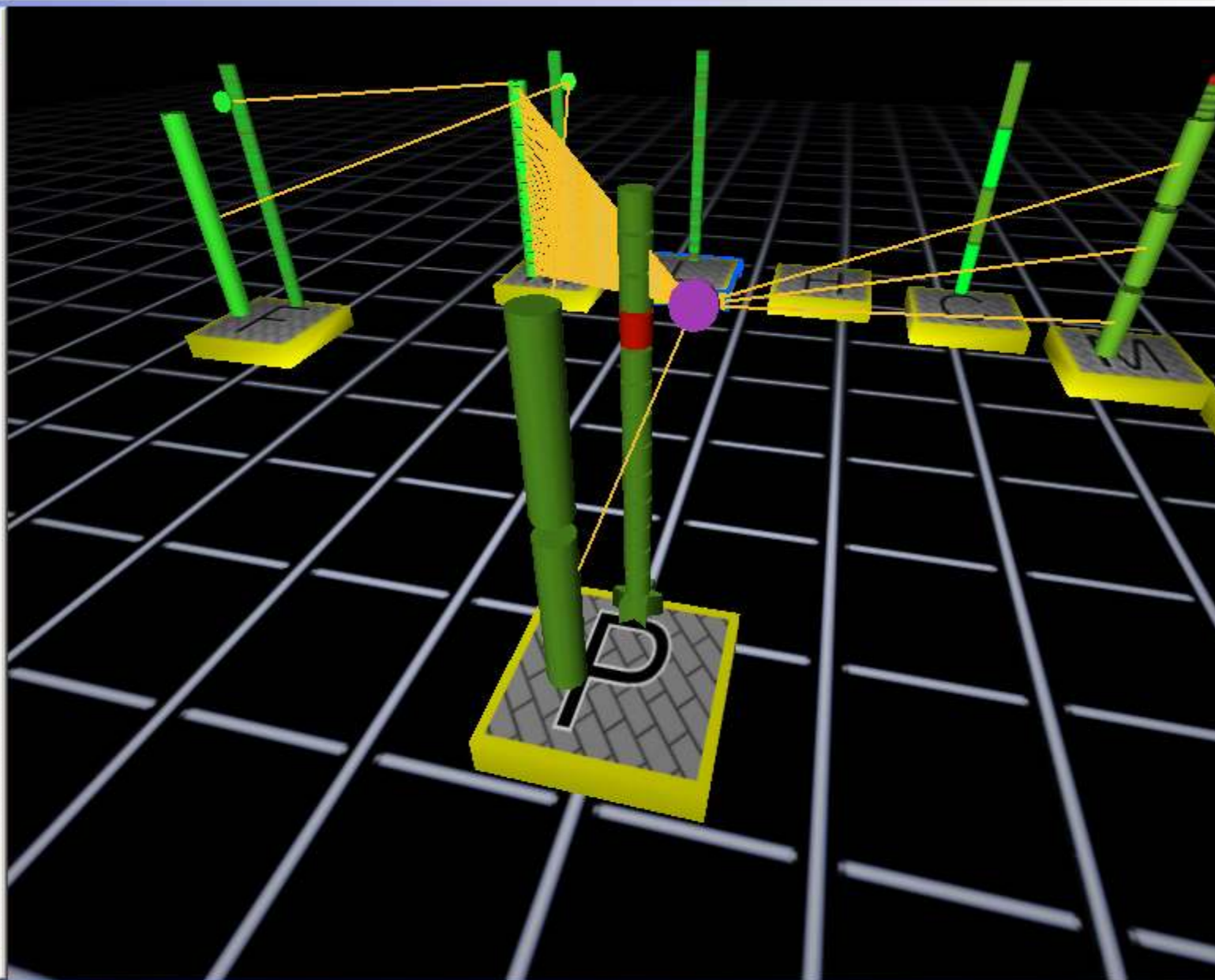
Snapshot\_breplibot\_c.xml

## Properties

|                |     |
|----------------|-----|
| Process        |     |
| PID            | 848 |
| Priority score | 36  |

## Libraries

|         |                                    |
|---------|------------------------------------|
| process | PID 676                            |
| module  | svchost.exe at 0x01000000          |
|         | BaseNamedObjects.dll at 0x00000000 |
|         | BaseNamedObjects.dll at 0x00000000 |
|         | BaseNamedObjects.dll at 0x00000000 |
|         | svchost.exe at 0x01000000          |
|         | ntdll.dll at 0x7C900000            |
|         | kernel32.dll at 0x7C800000         |
|         | advapi32.dll at 0x77C00000         |
|         | rpcrt4.dll at 0x77E00000           |
|         | shimeng.dll at 0x5CB00000          |
|         | acgenral.dll at 0x6F800000         |
|         | user32.dll at 0x77D00000           |
|         | gdi32.dll at 0x77F10000            |
|         | winmm.dll at 0x76B40000            |
|         | ole32.dll at 0x774E0000            |
|         | msvcrt.dll at 0x77C10000           |
|         | oleaut32.dll at 0x77100000         |
|         | msacm32.dll at 0x77100000          |
|         | version.dll at 0x77C00000          |
|         | shell32.dll at 0x7C900000          |
|         | shlwapi.dll at 0x77FE0000          |
|         | userenv.dll at 0x76900000          |
|         | uxtheme.dll at 0x5AC00000          |
|         | comctl32.dll at 0x77300000         |
|         | comctl32.dll at 0x5DC00000         |
|         | ntmarta.dll at 0x77690000          |
|         | wldap32.dll at 0x76F00000          |
|         | samlib.dll at 0x71BF0000           |
|         | rpcss.dll at 0x76A80000            |
|         | ws2_32.dll at 0x71A00000           |



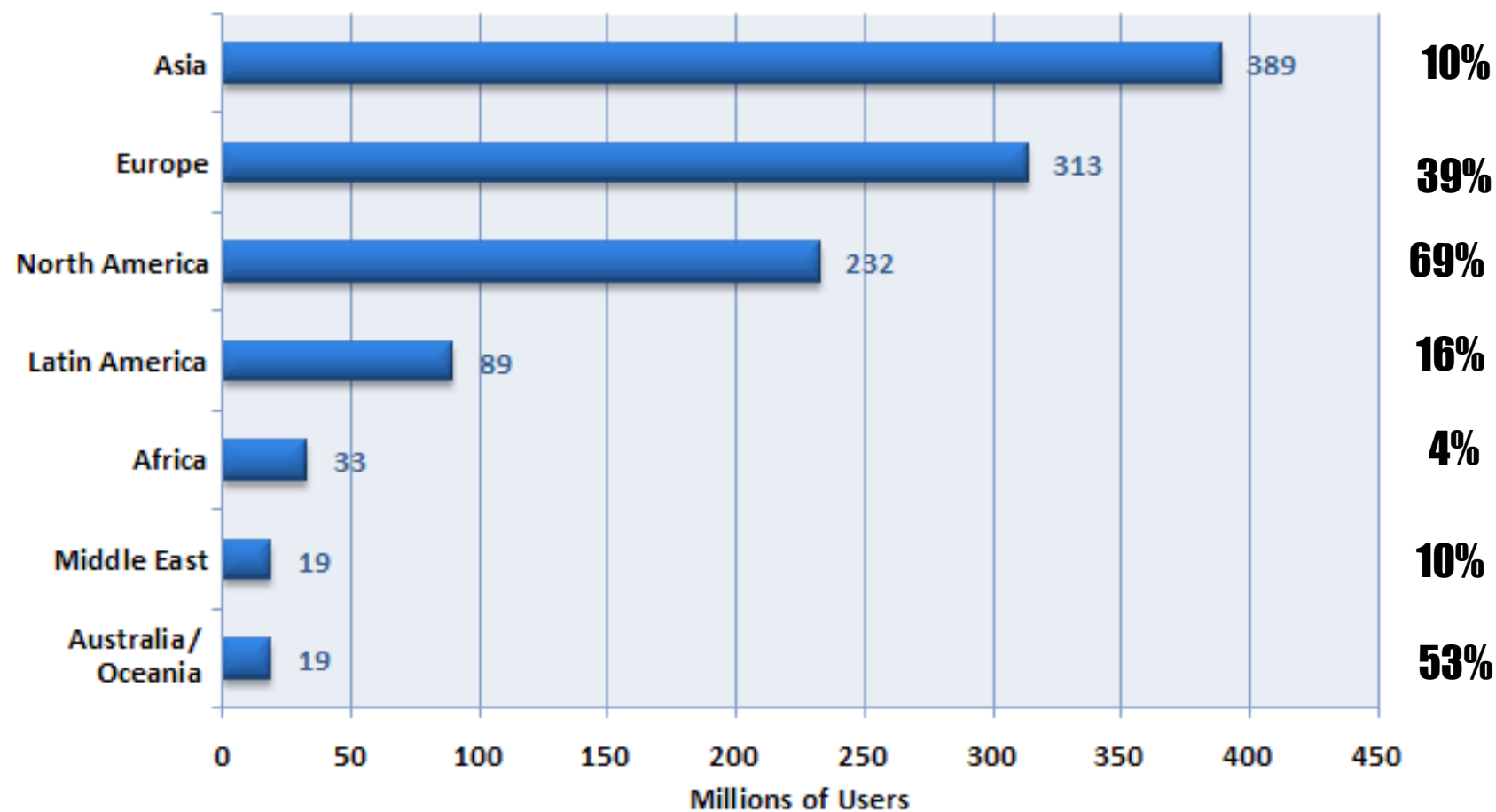
Filters Sorters

**We used to have to  
worry about the  
criminals that were  
close to us**



## Internet Users by World Region

### Penetration %



Copyright © www.internetworldstats.com - Jan 11, 2007





# **Computer crime is the fastest growing segment of the IT industry**



The background of the slide is a photograph of a large amount of US currency. There are several stacks of hundred-dollar bills, some of which are tied with rubber bands. Other bills are scattered across the surface. The lighting is somewhat dim, and the overall tone is slightly blue.

## **\$\$\$\$ via viruses**

**Spam**

**DDoS Extortion**

**Stealing credit card numbers**

**Stealing email addresses**

**Stealing passwords to Paypal + eBay**

**Stealing passwords to online banks**

**Stealing passwords to stock brokers**

**Stealing passwords to Poker sites**

**Stealing passwords to WOW+Lineage**

**Targeted attacks – industrial espionage**

**The money is good.  
And nobody is getting  
caught.**





# Does anybody buy from spam?



**Table 6.1** Revenue vs. Products Sold

| Product Type                          | Price to the User | Spammers Profit per Sale | Gross Profit for 0.0001 Percent Sales in 1 Million E-mails |
|---------------------------------------|-------------------|--------------------------|--|
| <i>FastSize</i> , Male Penis Enlarger | \$300             | \$75 to \$125            | \$7,500 to \$12,500  |
| <i>VigRX</i> , Male Sexual Enhancer   | \$60 per month    | \$18 to \$30             | \$1,800 to \$3,000   |
| Triplexxxcash.com, Porn Site          | \$30 per month    | \$30                     | \$3,000  |
| <i>VegasRed</i> , Online Casino       | \$100             | \$25 to \$40             | \$2,500 to \$4,000   |
| Debt Consolidation, Financial         | Unknown           | \$13                     | \$1,300  |
| Home Loan, Financial                  | Unknown           | \$1500 to \$2000         | \$150,000 to \$200,000                                     |

# Phishing







[Enter Information](#) → [Done](#)

## Personal Account Update

**Email Address\*:**   
**Password\*:**

### Email Address and Password

You will use these to log in to PayPal.

Please enter your full email address, for example, **name@domain.com**

Your password must be at least 8 characters long and is case-sensitive. Please do not enter accented characters.

**First Name\*:**   
**Last Name\*:**   
**Address\*:**   
**City\*:**   
**State\*:**   
**ZIP Code\*:**  (5 or 9 digits)  
**Country\*:** -- Choose a Country --

### Personal Information

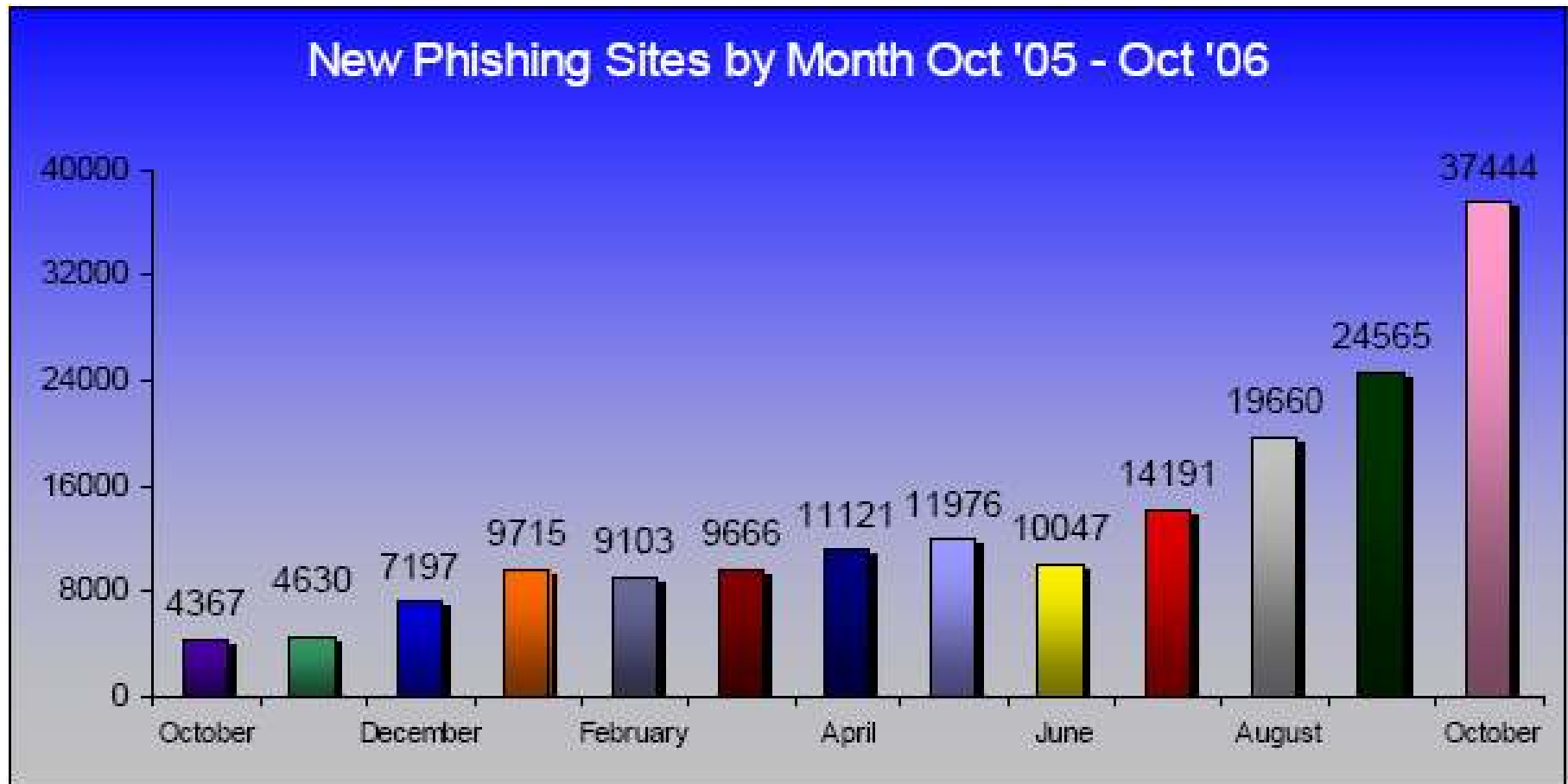
Please enter your name and address as they are listed for your debit card, credit card, or bank account.

**Card Number\*:**   
**Expiration Date\*:** --  -- --  --  
**Card Verification Number\*:**   
**ATM PIN Number\* (Credit Card Validation):**

### Card Information

Please enter your credit card number, card verification number, expiration date exactly as they appear on your credit card and PIN number.

## New Phishing Sites by Month Oct '05 - Oct '06



Source: Anti-Phishing Working Group



## Phishing Sites By Country of Host, October 2006



**United States 24%**

**Great Britain 4%**

**Russia 3%**

**Germany 4%**

**China 6%**

**South Korea 14%**

**Japan 3%**

**India 8%**

**Costa Rica 3%**

**Columbia 3%**

**Brazil 4%**

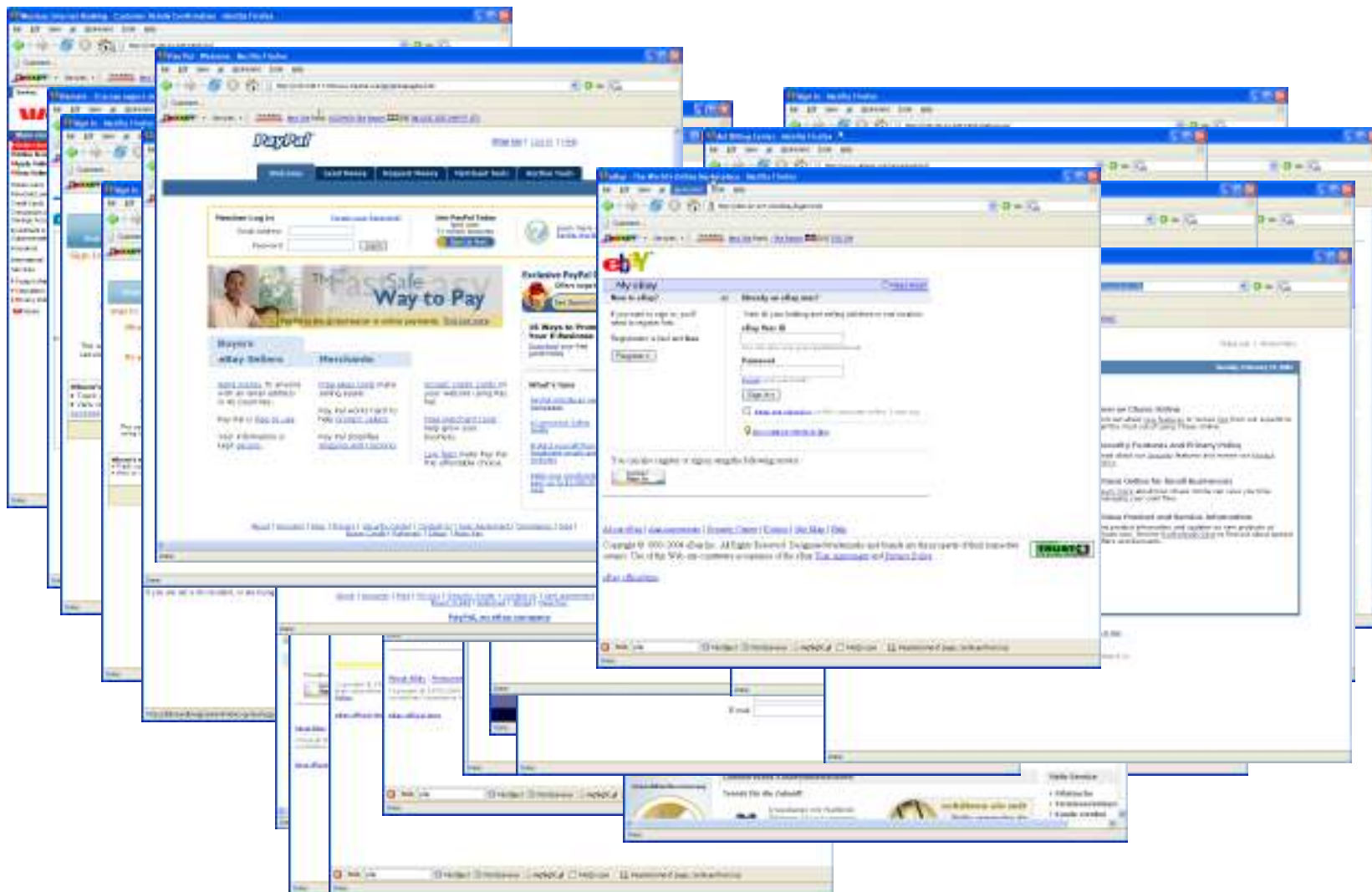
**All Other Countries < 2%**





**Education  
never  
works**





# Rock Phish





# "NEW2007" kit



A311 Death это профессиональная система удалённого администрирования с кучей возможностей.

Помните, что постоянное совершенствование средств защиты требует постоянный приток новых технологий тестирования. ТОЛЬКО свежее spyware способно обеспечить уровень функциональности, адекватный текущим потребностям.

$$- \equiv \equiv : : \equiv \equiv -$$

- СВЕЖАЯ GEO база (IP to country-state-city)
  - система аккунтов и установка лимитов (срок действия аккунта, количество взятых проксей)
  - вывод соксов для пользователей в поштучном виде типа 197.59.\*\*\*.\*\*\*
  - поиск и фильтрация по соксам
  - в цену входит установка на сервер
- цена 250 \$

[посмотреть скриншоты](#)

\*\*\* установка производится ТОЛЬКО на технически подготовленные сервера

*All information on this site is given exclusively in the educational purposes.*

*All programs are intended only for testing and revealing vulnerability on personal computers and corporate networks.*

save config

load config

save as...

exit

.a3d files

about



http://se-code.net/



Google

# SE CODE

## WARNING

правила использования нашего софта

Предлагаемый софт должен использоваться исключительно в образовательных целях или для повышения собственной безопасности, использование данного софта во всех остальных случаях преследуется законом той страны в которой вы находитесь.

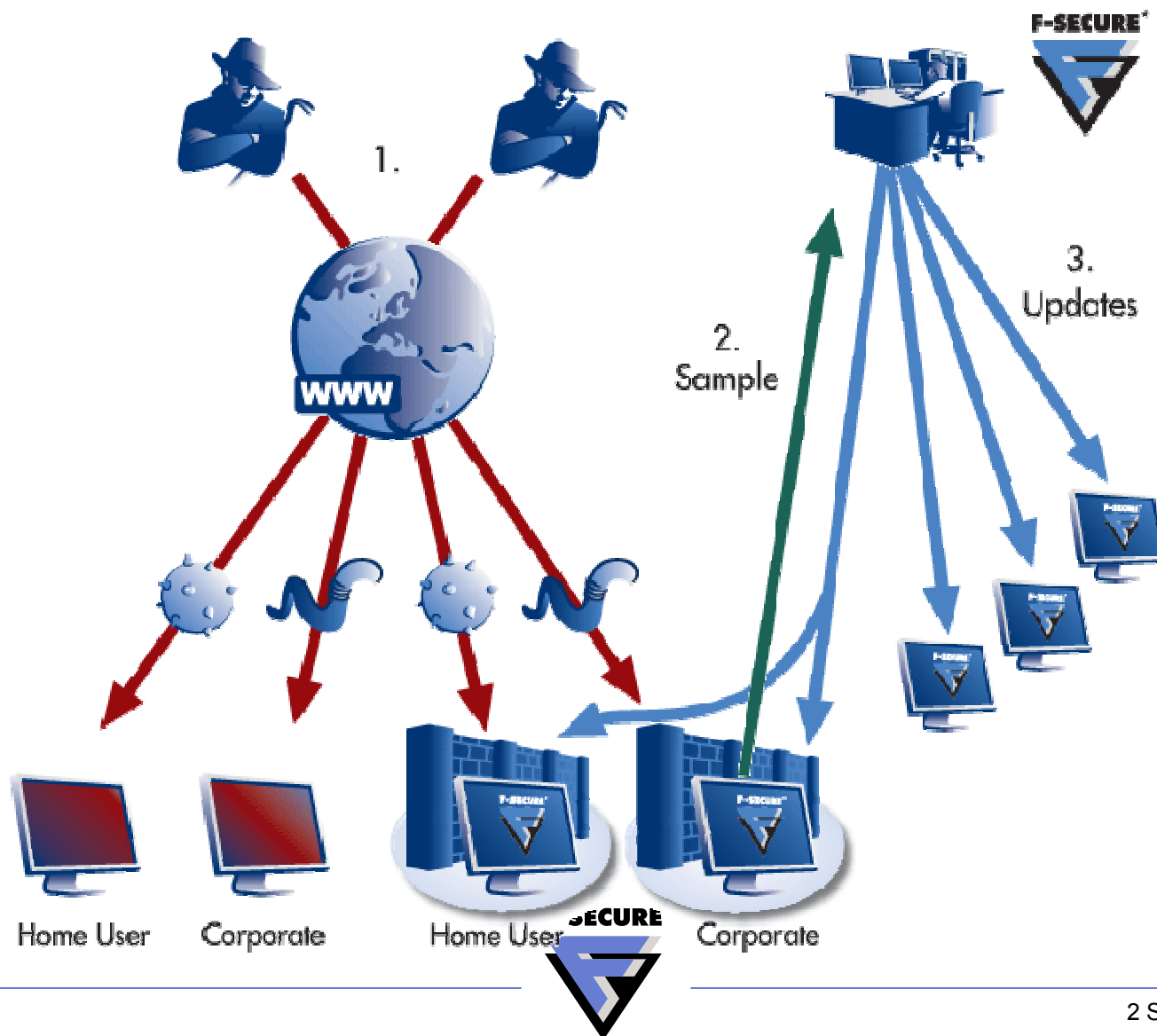
ЗАПРЕЩАЕТСЯ ИСПОЛЬЗОВАТЬ НАШ СОФТ В ПРОТИВОЗАКОННЫХ ЦЕЛЯХ

☐ [Я согласен с правилами использования] ☐ [Я не согласен с правилами использования]

# Targeted attacks

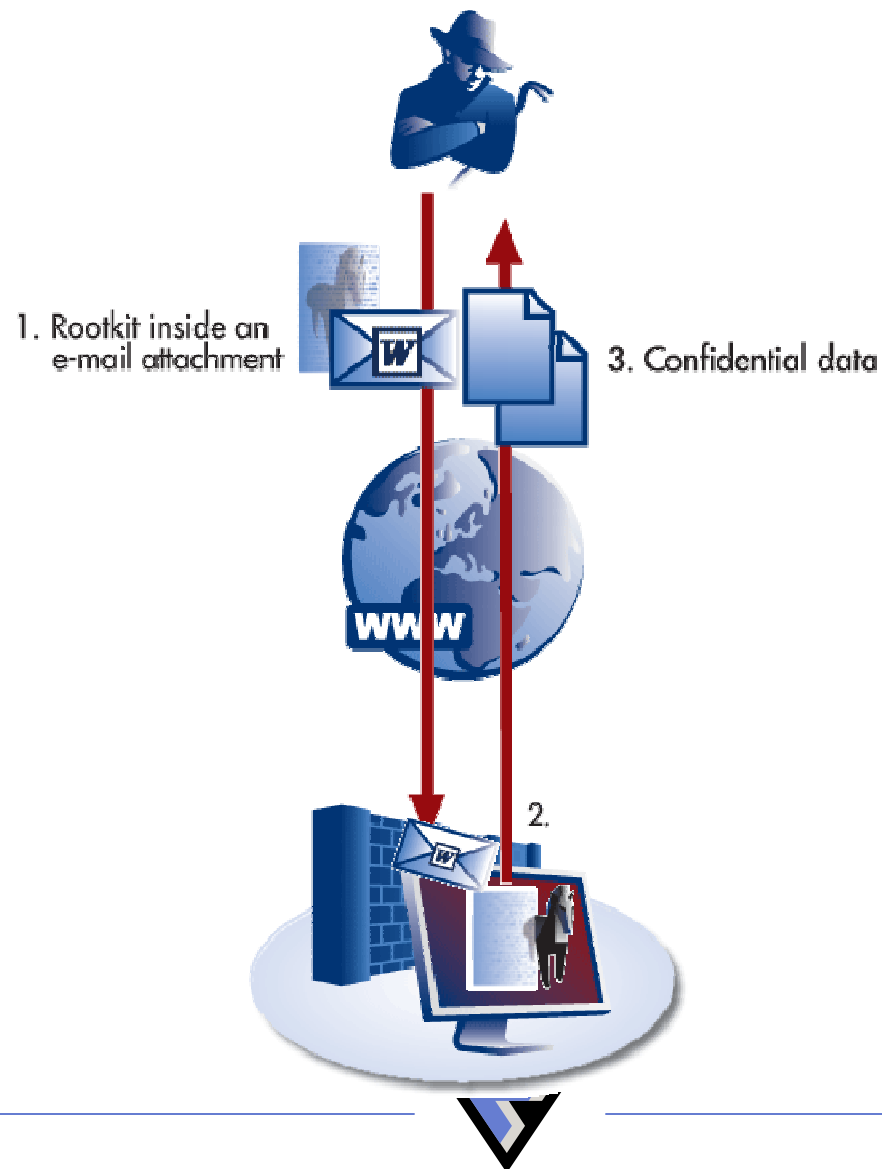


# Traditional untargeted attacks



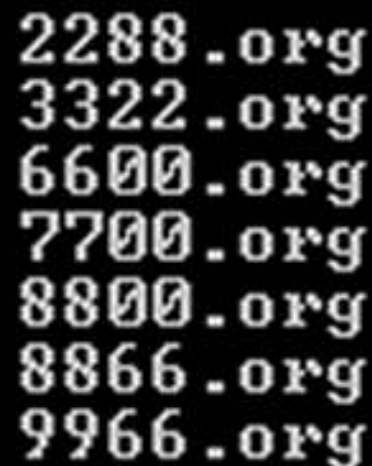


# Targeted attacks – stealing confidential data



## Known cases

|                        |                |
|------------------------|----------------|
| <b>March 2005:</b>     | <b>USA</b>     |
| <b>September 2005:</b> | <b>EU</b>      |
| <b>December 2005:</b>  | <b>USA</b>     |
| <b>Jan 2006:</b>       | <b>UK</b>      |
| <b>March 2006:</b>     | <b>UK</b>      |
| <b>April 2006:</b>     | <b>Germany</b> |
| <b>May 2006:</b>       | <b>Sweden</b>  |
| <b>June 2006:</b>      | <b>Finland</b> |
| <b>November 2006:</b>  | <b>Sweden</b>  |
| <b>November 2006:</b>  | <b>Finland</b> |
| <b>February 2007:</b>  | <b>Sweden</b>  |
| <b>March 2007:</b>     | <b>Estonia</b> |



2288.org  
3322.org  
6600.org  
7700.org  
8800.org  
8866.org  
9966.org



| <b>Era</b>  | <b>Enemy</b> |
|-------------|--------------|
| 1986 - 2003 | Hobbyists    |
| 2003 -      | Criminals    |
| 2006 -      | Spies        |

**New technologies to the rescue:**

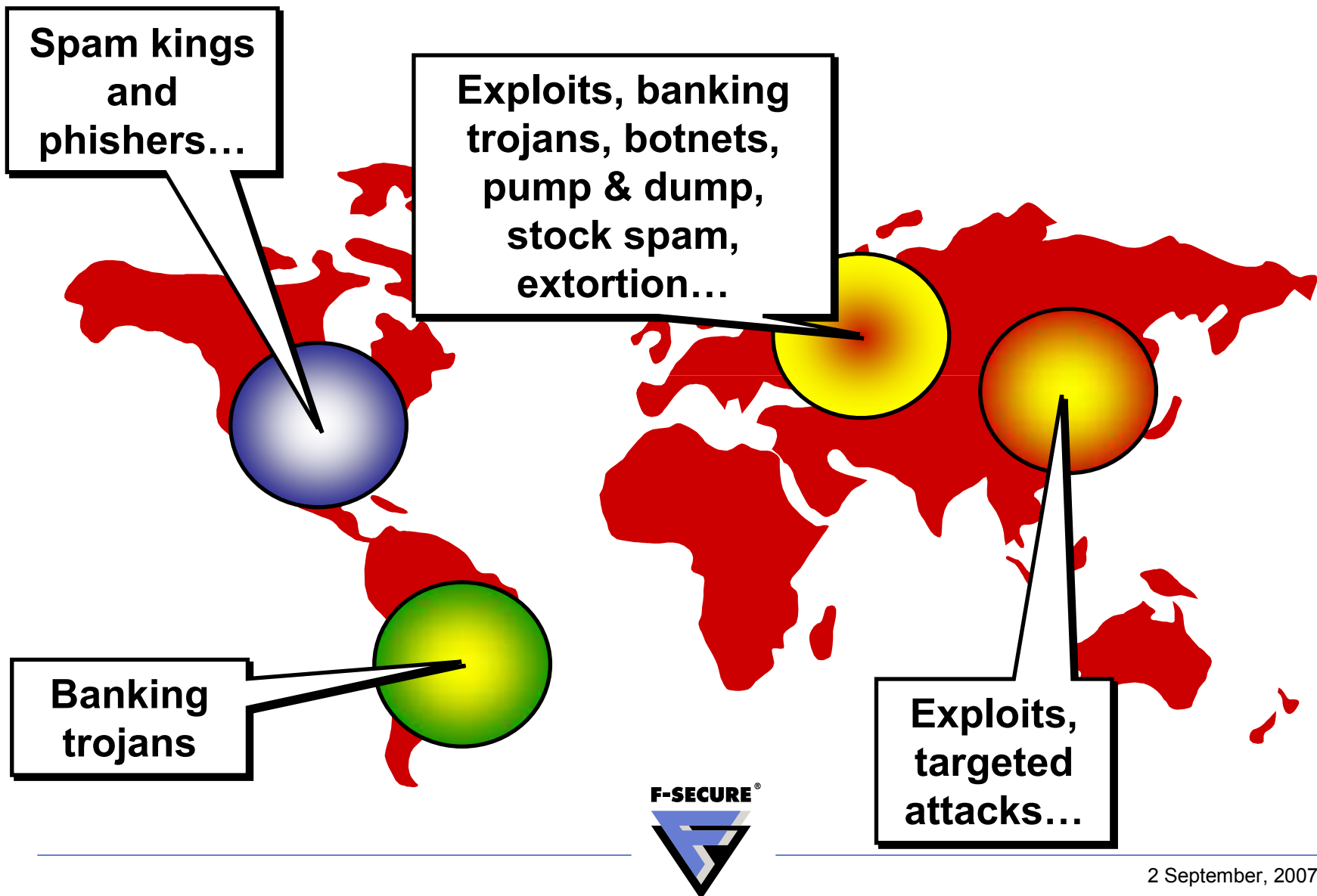
- **F-Secure Blacklight**
- **F-Secure Deepguard**

Expect the unexpected

**Today, the most likely  
place for you to be the  
target of a crime is the  
internet**



## Where are they?





# Mad Powerpoint Skills!

Who are they?



## We used to be fighting these...



**Chen-Ing Hau**  
Author of  
the CIH virus



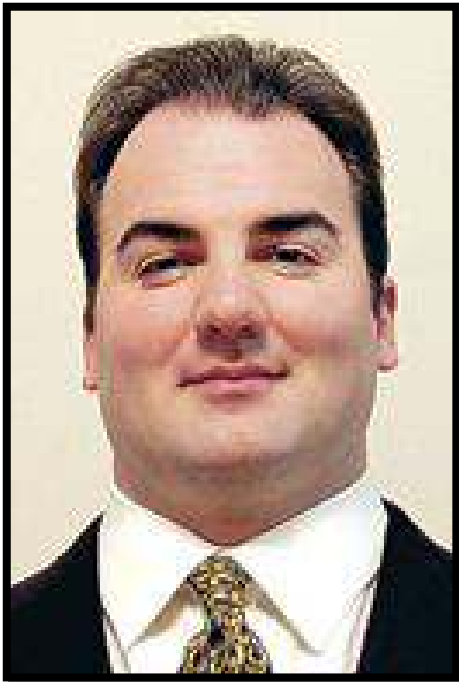
**Joseph McElroy**  
Hacked the Fermi lab  
network



**Benny**  
Ex-29A



## Today we are fighting these!



**Jeremy Jaynes**  
Millionaire,  
and a spammer



**Jay Echouafni**  
CEO,  
and a DDoS attacker

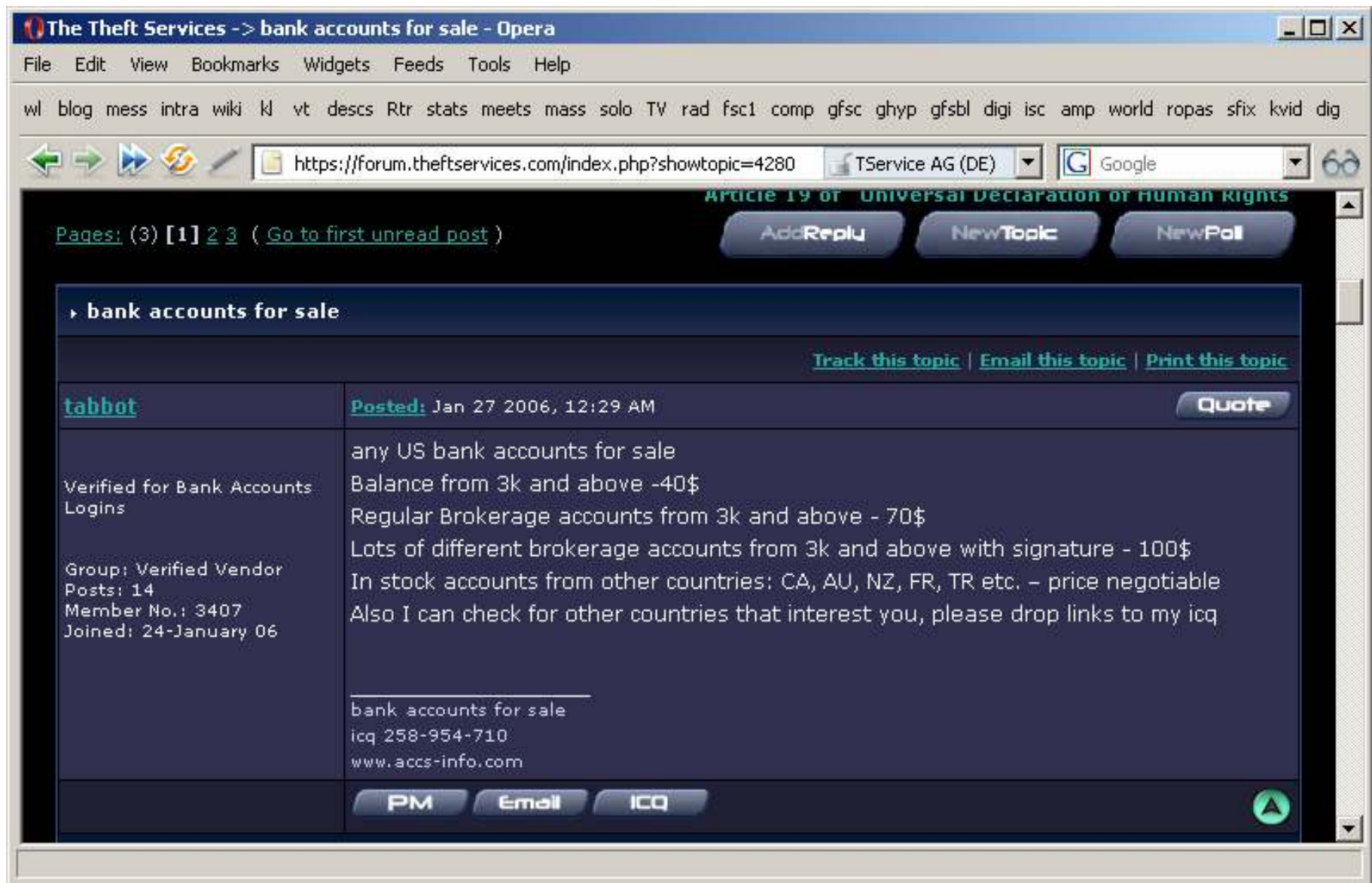


**Andrew Schwarmkoff**  
Member of Russian mob,  
and a phisher



**Where do they  
do their  
business?**







## Logins&Cob From Drax

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

**Drax**

**Posted:** Jun 22 2006, 11:26 PM

**Quote**



**Australian Logins Verified Provider**

Group: Verified Vendor  
Posts: 100  
Member No.: 3641  
Joined: 16-March 06

I'm offering for sale Bank Logins of various countries, and limited supply of cobs.

### Logins:

USA - Citi, Washington Mutual, Wachovia, BoA, Chase

Australia - Commonwealth, National

United Kingdom - HSBC, Lloyds

Canada - TD Canada Trust

Some other's in stock, Ask me if you need something specific.

### Cobs:

Discover

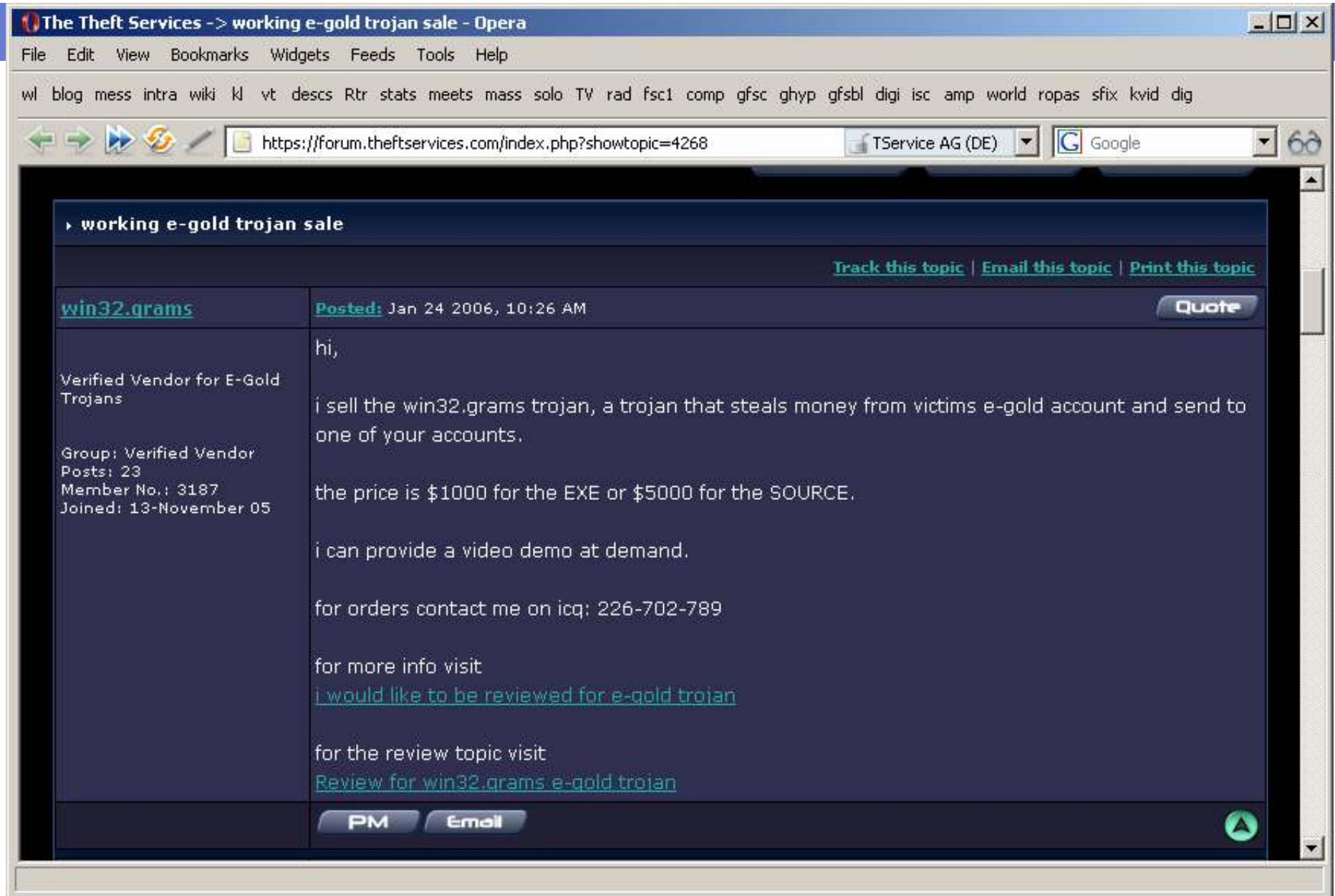
I only have Discover & Chase in stock now, Contact me if there is a specific cob you're interested in.

### Prices:

Contact for price

### Payment:

eGOLD/WMZ/WU



**How do they  
move the  
money?**



> Registration

> FAQ

> Contact

> How it works

Home

Contact Us

## Outsource Line

Great opportunity for everyone!



### Outsource Line

"If it weren't for Outsource Line I wouldn't be in business today. It's that simple."  
President, Packaging Company

#### Company's News

>> **05.12.04**

Each day brings new customers! Today we got our happy 100-th customer!

>> **21.10.04**

Finally we have made new design. Enjoy.

>> **12.10.04**

We opened a new office in Spain.

[Read more](#)

> **You guys are really the greatest!!!!...**

It works great this way!  
Thanks a lot for all the great support!!!

#### Registration:

Thank you for the shown interest about our proposal. At the moment we have a number of vacancies of GENERAL ASSISTANT in many countries and territories. We'd like to give you some information about what exactly our company doing and how would you help us. But just before that I'd like to tell you that for this job we are NOT going to ask you do ANY initial investments or send ANY kind of initial payments. And another thing to mention here that this is part-time home-based job that will require just about 5 or less hours weekly. So you can happily stay at your current position if you have any and just if you'll see a good potential to grow with us you can start work harder.

Basic methods of domestic payments we are receiving from our customers are: domestic wire transfers, cashier's checks, money orders and some others. For most of those methods it will take a long time and often significant additional charges to receive them outside the country where the payment was initiated.

Your responsibilities will include receiving these payments into your bank account and transfer them to us with the way we'll inform you. You will get 6-8% from total transferred amount as your wages.

This is fully home-based flexible hours part-time job with just minimal



>> **You have a company that cares about more than just the bottom line**  
and that is rare to find in this day and age.  
Marc & Diane Injejikian

**...thank you very much for all your support and for looking into this for me. Thats how support should be.**

Thanks  
Spencer Boydell-Butt





**TRANS WORLD PAY COMPANY**  
WE CAN ALWAYS HELP YOU.



### We have new partners

December 17 - the date we signed contract with Rietumu Bank, Riga, Latvia. Now we became Verified Partners of the bank, and are ready for new projects.

[MORE](#)

### Financial Manager's news

New propositions for Financial Managers. Check out our Vacant jobs section. New conditions and offers

[MORE](#)

### Italian and French citizens



We start cooperation with Terberg DTS company, the biggest Terberg machines spare parts supplier.

Also, we signed a contract with [www.uk-merchant-account.co.uk](http://www.uk-merchant-account.co.uk) and [www.taxcafe.co.uk](http://www.taxcafe.co.uk). Now we can offer services for these companies and new partners in Italy and France have more job offers and propositions

## ABOUT OUR VACANCIES

### About our Vacant jobs

We are proud to offer several positions for USA and EU citizens. We do not require any special education or previous experience. We do not require much time devotion for our job. Our primary condition for new partners is trust, honest and activity. Please, look at our propositions:

### EURO Financial Manager (European Union: France, Italy, etc.)

It's very important position for us. As we develop our cooperation with EU companies and new partners, and do not have our office there now, we need local representatives there. Position is very responsible. We have a list of tasks you may choose from. Being EU Financial Manager you will need to:

- establish new bank accounts for our corporations (you will be 2nd owner of our companies)
- establish merchant accounts for our corporations (and perform cashier's functions)
- receive and redirect wire transfers and cheques (you will be receiving funds directly from our customers)
- communication and customer service for our local UK partners and customers.

Salary for EU Financial Manager depends on activity and is commission based. Average it's €2,200-3,700  
Schedule is individual too. From 1 to 10 hours per week

### US Financial Manager

This position is very important too, as we have new customers every week in USA. Conditions are basically the same as for EU Financial Manager. US Financial Manager will need to:

- establish corporations and corporate accounts for us (in both positions, all fees are paid by us)
- establish merchant accounts for our corporations
- wire transfer, cheque, money order receiving and redirecting
- bank and other financial correspondence receiving and redirecting
- communication and customer service for our local US partners and customers.

Salary for US Financial Manager depends on activity and is commission based. Average it's \$2,700-4,000  
Schedule is individual too. From 1 to 10 hours per week

For applying and receiving more information - please, fill online application form at our website.



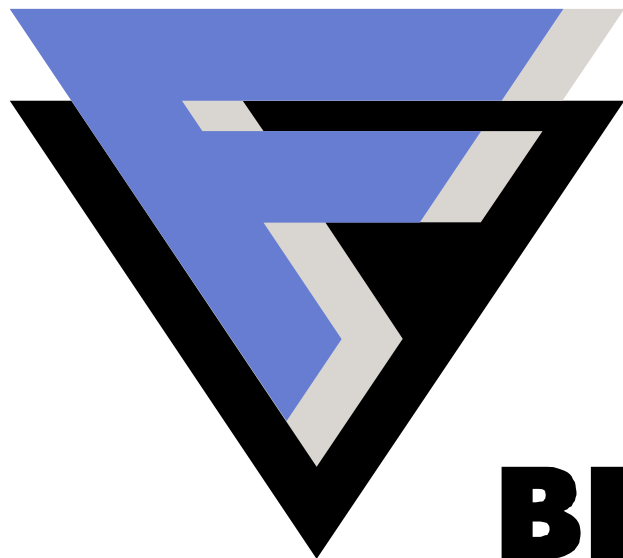


**Good  
will  
prevail**





# **F-SECURE<sup>®</sup>**



## **BE SURE.**

Mikko Hypponen  
Chief Research Officer  
F-Secure Corporation

[www.f-secure.com](http://www.f-secure.com)  
[www.hypponen.com](http://www.hypponen.com)

