Response Lab Overview

Inputs
- Statistics Reports
- DeepGuard HIPS Reports
- Customer @ & Sample Upload
- VIP Partner Cases
- Engine Tech. Partners

Security Labs

Outputs
- Security News
- Description
- Detection
- Disinfection
F-Secure Response Labs
work 24 hours a day

- 23:00 – 07:30  Shift 1
- 07:00 – 15:30  Shift 2
- 15:00 – 23:00  Shift 3
$\textit{\$\$\$ via viruses}$

- 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
Does anybody buy from spam?

“Please indicate if you have ever purchased an item or taken advantage of an offer for a product or service from an email you didn’t request or sign up for.”

Data source: www.bsa.org
<table>
<thead>
<tr>
<th>Product Type</th>
<th>Price to the User</th>
<th>Spammers Profit per Sale</th>
<th>Gross Profit for 0.0001 Percent Sales in 1 Million E-mails</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastSize, Male Penis Enlarger</td>
<td>$300</td>
<td>$75 to $125</td>
<td>$7,500 to $12,500</td>
</tr>
<tr>
<td>VigRX, Male Sexual Enhancer</td>
<td>$60 per month</td>
<td>$18 to $30</td>
<td>$1,800 to $3,000</td>
</tr>
<tr>
<td>Triplexxxcash.com, Porn Site</td>
<td>$30 per month</td>
<td>$30</td>
<td>$3,000</td>
</tr>
<tr>
<td>VegasRed, Online Casino</td>
<td>$100</td>
<td>$25 to $40</td>
<td>$2,500 to $4,000</td>
</tr>
<tr>
<td>Debt Consolidation, Financial</td>
<td>Unknown</td>
<td>$13</td>
<td>$1,300</td>
</tr>
<tr>
<td>Home Loan, Financial</td>
<td>Unknown</td>
<td>$1500 to $2000</td>
<td>$150,000 to $200,000</td>
</tr>
</tbody>
</table>
Targeted attacks
Traditional untargeted attacks

1. 
2. Sample
3. Updates

Home User  Corporate  Home User  Corporate
Targeted attacks – stealing confidential data

1. Rootkit inside an e-mail attachment
2. Confidential data
3. Confidential data
Targeted attack emails

Interesting and **relevant** email in **local** language

One attachment (DOC, EXE, CHM, XLS or PPT)

The attachment uses an exploit to drop a backdoor

**Breakdown of attachments used in attacks**
May 2005 - May 2006

- **exe, 31, 10%**
- **chm, 62, 21%**
- **doc, 206, 69%**
<table>
<thead>
<tr>
<th>Era</th>
<th>Enemy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1986 - 2003</td>
<td>Hobbyists</td>
</tr>
<tr>
<td>2003 -</td>
<td>Criminals</td>
</tr>
<tr>
<td>2006 -</td>
<td>Spies</td>
</tr>
</tbody>
</table>

New technologies to the rescue:

- F-Secure Blacklight
- F-Secure Deepguard

Expect the unexpected
Increase in spam?
Spam activity has increased 59% from September 2006 through October 2006. This increase causes email systems to experience unexpected overloads in bandwidth, server storage capacity, and loss of end-user.

*Spam percentage is based on email processed for Postini users with spam filtering enabled.

Source: Postini
Re: now Maybu

Hi

When you need it now VIAwGRA.
When you need it later CLAvvLIS.

http://www.wwatekdqrsblues.com

awoken. It had seemed so real... There had been two people he knew and one he didn't... He concentrated hard, frowning, trying to remember...
The dim picture of a darkened room came to him... There had been a snake.
- **Lowest Price Guarantee**  - **Fast Delivery**

Do not click, type in your browser **www.aaaRX.org**

<table>
<thead>
<tr>
<th></th>
<th>100mg</th>
<th>only</th>
<th>$2.00</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Viagra</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Viagra ST</strong></td>
<td>100mg</td>
<td>only</td>
<td>$2.89</td>
</tr>
<tr>
<td><strong>Valium</strong></td>
<td>10 mg</td>
<td>only</td>
<td>$2.00</td>
</tr>
<tr>
<td><strong>Xanax</strong></td>
<td>1 mg</td>
<td>only</td>
<td>$2.00</td>
</tr>
<tr>
<td><strong>Cialis</strong></td>
<td>20 mg</td>
<td>only</td>
<td>$2.00</td>
</tr>
<tr>
<td><strong>Cialis ST</strong></td>
<td>20 mg</td>
<td>only</td>
<td>$2.89</td>
</tr>
<tr>
<td><strong>Antivan</strong></td>
<td>2 mg</td>
<td>only</td>
<td>$1.90</td>
</tr>
</tbody>
</table>

Do not click, just type **www.aaaRX.org** in address bar of your browser, then click enter
Phishing
Phishing

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%
- South Korea: 14%
- China: 6%
- Great Britain: 4%
- Germany: 4%
- Russia: 3%
- India: 8%
- Brazil: 4%
- Costa Rica: 3%
- Columbia: 3%

All Other Countries < 2%
Rock phish report for 2007-03-14
---------------------------------

Domains under attack

Total number of hits per target:

<table>
<thead>
<tr>
<th>Rank</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>53.com</td>
</tr>
<tr>
<td>2</td>
<td>volksbank.de</td>
</tr>
<tr>
<td>3</td>
<td>online.bbt.com</td>
</tr>
<tr>
<td>4</td>
<td>app.nordea.se</td>
</tr>
<tr>
<td>5</td>
<td>sparkasse.de</td>
</tr>
<tr>
<td>6</td>
<td><a href="http://www.bankofamerica.com">www.bankofamerica.com</a></td>
</tr>
<tr>
<td>7</td>
<td>cantal.credit-agricole.fr</td>
</tr>
<tr>
<td>8</td>
<td><a href="http://www.citibank.de">www.citibank.de</a></td>
</tr>
<tr>
<td>9</td>
<td><a href="http://www.deutsche-bank.de">www.deutsche-bank.de</a></td>
</tr>
<tr>
<td>9</td>
<td>online.bbandt.com</td>
</tr>
<tr>
<td>11</td>
<td>global.etrade.com</td>
</tr>
<tr>
<td>12</td>
<td>citi.com</td>
</tr>
<tr>
<td>13</td>
<td>bankingportal.sparkasse.de</td>
</tr>
</tbody>
</table>
Phishing Examples
A311 Death это профессиональная система удаленного администрирования с кучей возможностей.

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

---

!!! Теперь возможен заказ профессиональной админки для организации сокс-сервиса

- свежая GEO база (IP to country-state-city)
- система аккаунтов и установка лимитов (срок действия аккаунта, количество взятых проксей)
- вывод соксов для пользователей в поштучном виде типа 197.50.***.***
- 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.
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]

«ЕПП», 2006
Ihre detaillierte GEZ Rechnung

1.12.2006 - 12.01.2007

Rechnungsnummer 012 545 124
Kundennummer 8547 0145 01

Sehr geehrter GEZ Kunde,

Die Gesamtsumme für Ihre Rechnung beträgt: **441,74** Euro.
Anbei erhalten Sie den detaillierten Rechnung sowie die alle anderen wichtigen Unterlagen zu Ihrem Bestellung im beigefügten ZIP Datei.


Mobile threats
MIRROR NEURONS AND AUTISM

A disorder of brain cells that link others’ actions to our own may explain this puzzling condition.

Constellations and Astroarchaeology

Stop Viruses That Hijack Smartphones

Bringing Seas Back from the Dead
**The Worlds Most Powerful Spy Software for Mobile Phones**

FlexiSPY is a mobile phone monitoring application that secretly records all activity on a mobile phone that has FlexiSPY installed. Protect your children, catch cheating partners, the possibilities are endless.

- Install FlexiSPY on a supported mobile phone and start to receive copies of SMS messages (sent & received), call history, and more!
- Find out [here](http://www.flexispy.com/) if your phone is supported or not.
- Symbian 9, Pocket PC and Blackberry phones will be available in March.
- Please join our mailing list to be notified of availability.

<table>
<thead>
<tr>
<th>FLEXISPY - PRO</th>
<th>FLEXISPY - LIGHT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product</strong></td>
<td><strong>Product</strong></td>
</tr>
<tr>
<td><a href="#">Details</a></td>
<td><a href="#">Details</a></td>
</tr>
<tr>
<td><a href="#">Screenshots</a></td>
<td><a href="#">Screenshots</a></td>
</tr>
</tbody>
</table>

- **PRO**
  - Remote Mic Activation
  - SM Change SMS Notification
  - SMS Logging (in/out)
  - Call History (in/out)
  - Call Duration (in/out)
  - Contact Name
  - Download Activity to Excel

- **LIGHT**
  - SMS Logging (in/out)
  - Call History (in/out)
  - Call Duration (in/out)
  - Contact Name in Address Book
  - Download Activity to Excel

**ORDER NOW**:  €150 (per year)  
**ORDER NOW**:  €50  (per year)

**STAY INFORMED**

To stay informed about the latest developments in mobile technology subscribe to our newsletter:

Insert email:  
Submit

**PRODUCT COMPARISON**

**Why Use FlexiSPY**

- RECOVER Stolen Phones. [Find out how](#)
- READ your partner's SMS.
- REVEAL their call history.
- PROTECT your children from SMS abuse.
- ARCHIVE all your own SMS for the future.
- SAVE your call history.
- MONITOR your phone charges.
- CONTROL your GPRS data charges.

**COMING SOON**

Keep checking back for the latest on our two new releases:
Net Crime
**CONTACTS**

Address: office, 202, 2 bld. 3, Predisportovaya Str., St.-Petersburg, Russia, 196240
Phone: +7 (812) 334-55-37, fax: +7 (812) 334-55-38
E-mail: info@grandlog.ru
AMY J. GREER
KINGDON KASE
TAMIS S. STARK (TS-8321)
Attorneys for Plaintiff
SECURITIES AND EXCHANGE COMMISSION
701 Market Street
Suite 2000
Philadelphia, PA 19106
Telephone: (215) 597-3100
Telefax: (215) 597-2740

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK


SECURITIES AND EXCHANGE COMMISSION,

Plaintiff,

v.

GRAND LOGISTIC, S.A. and
EVGENY GASHICHEV,

Defendants.

______________________________________

COMPLAINT

Plaintiff Securities and Exchange Commission (the “Commission”) alleges as
follows:

SUMMARY

1. This matter involves an ongoing fraudulent scheme conducted by defendant Evgeny
Gashichev, a citizen of Russia believed to be currently residing there, and his company,
defendant Grand Logistic, S.A., a foreign entity incorporated in Belize and located in
Estonia. The defendants are conducting a high-tech version of a “pump and dump”
manipulation scheme, in which they artificially inflate the market price of securities, using
### bank accounts for sale

**tabbot**

- **Verified for Bank Accounts Logins**
- **Group:** Verified Vendor
- **Posts:** 14
- **Member No.:** 3407
- **Joined:** 24-January 06

**Posted:** Jan 27 2006, 12:29 AM

- any US bank accounts for sale
- Balance from 3k and above -40$ 
- Regular Brokerage accounts from 3k and above - 70$ 
- Lots of different brokerage accounts from 3k and above with signature - 100$
- In stock accounts from other countries: CA, AU, NZ, FR, TR etc. – price negotiable
- Also I can check for other countries that interest you, please drop links to my icq

---

**bank accounts for sale**

- icq 258-954-710
- www.accs-info.com
Logins & Cob From Drax

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

**Logins:**
USA - Citibank, Washington Mutual, Wachovia, BoA, Chase
Australia - Commonwealth, National
United Kingdom - HSBC, Lloyds
Canada - TD Canada Trust

Some others 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
hi,

i sell the win32.grams trojan, a trojan that steals money from victims e-gold account and send to one of your accounts.

the price is $1000 for the EXE or $5000 for the SOURCE.

i can provide a video demo at demand.

for orders contact me on icq: 226-702-789

for more info visit
i would like to be reviewed for e-gold trojan

for the review topic visit
Review for win32.grams e-gold trojan
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
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.

Financial Manager’s news
New propositions for Financial Managers. Check out our Vacant jobs section. New conditions and offers.

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 and 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.