

Malware, Organized Crime, and Ties to Pharmaceutical Spam Campaigns

December 04, 2008

Matt Ziemniak, Program Director

National Cyber Forensics and Training Alliance



The National Cyber-Forensics and Training Alliance provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia, and law enforcement.

What We'll Cover

- Introduction to Malware
- Organized Crime on the Internet
- Pay-per-install Services
- Case Study

Objective:

To Understand How Malware is Utilized to
Advertise Fraudulent Pharmaceutical Websites

What is Malware?



Computer Viruses

Computer Worms

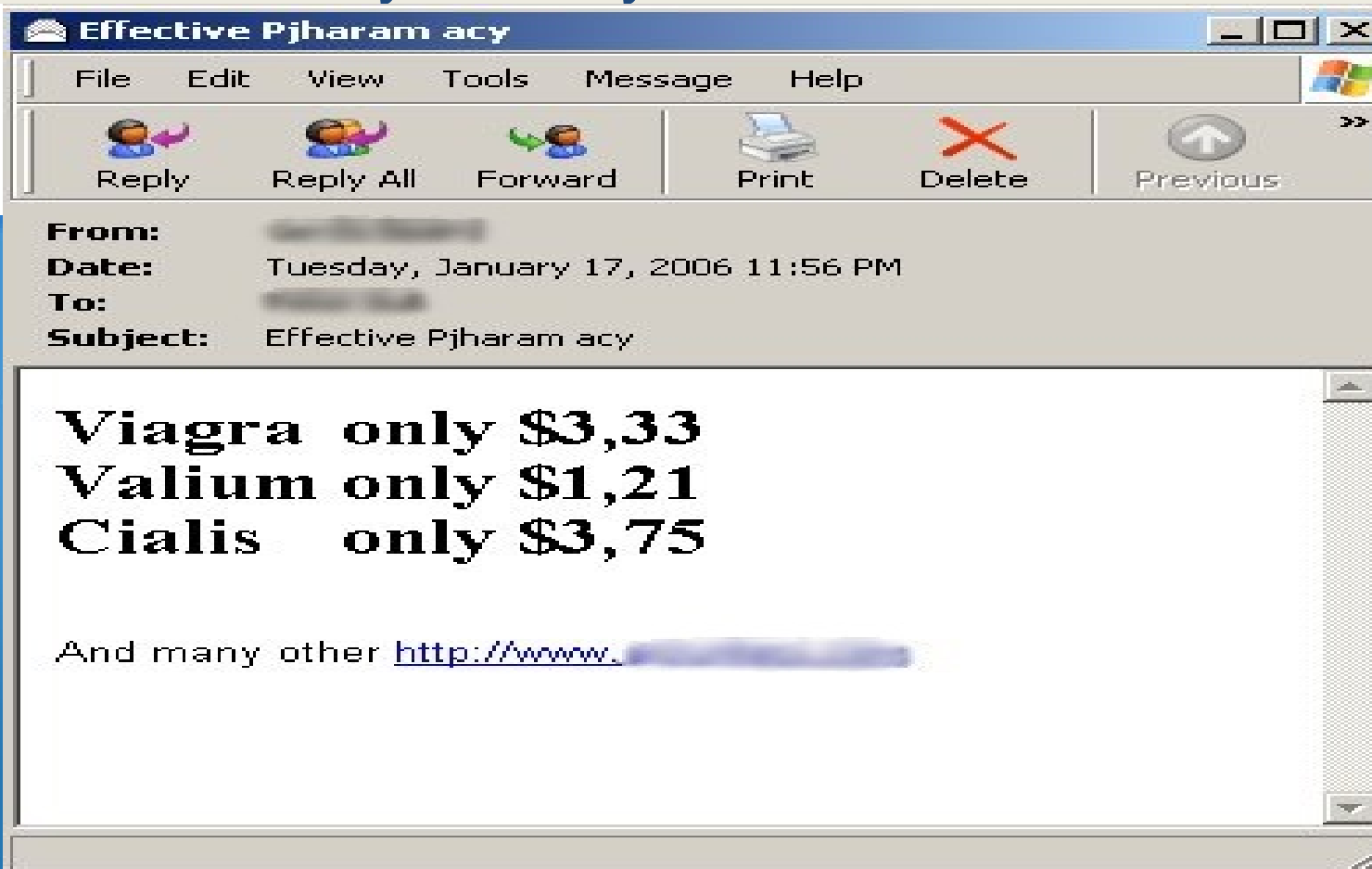
Trojans/Backdoors

Spyware/Adware

Malicious Software that does something the user did not intend for it to do!

What Can Malware Do?

- ~~Redo~~ ~~Copy~~ ~~Paste~~ ~~Key~~ ~~Strokes~~ ~~Websites~~



Taking Cyber Crime Seriously

FBI: Cybercriminals taking cues from Mafia

The FBI estimates cybercrime cost the U.S. more than \$67 billion last year

By Robert McMillan, IDG News Service

August 07, 2006

[E-mail](#) [Printer Friendly](#) [Reprints](#) [Slashdot It!](#)

Your Google search for *"international carders alliance"* has brought you to this InfoWorld page.

Sign up today for the FREE InfoWorld Daily newsletter.

SIGN UP

I understand and agree to the Terms of Service and Privacy Policy

The Web site offered to sell stolen credit card information for \$100, but it was the title of the poster that caught FBI agent Thomas X Grasso Jr.'s attention. The cybercriminal identified himself as a "Capo di capo" -- a boss of bosses, in Mafia parlance.

Free IT resource

Virtualization Insights from Top Experts - Learn how virtualization gets real!

Sponsored by Dell

Free IT resource

TechNet: More ways to know it, share it, and keep it running.

Sponsored by Microsoft

As money has become the driving force behind online threats, [cyber criminals](#) have been taking a page from organized crime, adopting the same kind of organizational structures as these older crime groups, Grasso told an audience Friday at the Defcon hacker conference. Defcon immediately follows Black Hat, its sister show.

"This organized crime group, Carderplanet, organized themselves into the same structure as the Italian Mafia," said Grasso, a supervisory special agent who works at the National Cyber Forensics & Training Alliance.

And the costs of cybercrime are steep. The FBI estimates that it cost the U.S. more than

\$67 billion last year, Grasso said.

To illustrate how sophisticated these cyber criminals are, Grasso then played a slick promotional video offering Carderplanet "business" services. It could easily have been mistaken for a legitimate IT consulting ad.

"Just so there's no confusion here, these guys are not doing something legal," he told the audience after playing the video.

The Carderplanet Web site has now been shut down and the FBI is working with other law enforcement agencies in eastern Europe to put the group completely out of business.

But Carderplanet is just one part of a larger confederation of online criminals called the International Carder's Alliance. They use known Web sites and IRC (Internet Relay Chat) channels to coordinate their online attacks.



RELATED STORIES

- Thousands hit in broad Web hack
- French President Sarkozy's bank account hacked
- Cerf: Internet is a reflection of society

Popular Tags:

cybercrime, hackers, onlinefraud

[» COMPLETE LIST OF TAGS](#)

SEE ALSO

- Analysts wary of U.K. cybercrime law revamp
- Analysts wary of U.K. cybercrime law revamp

FIND PRODUCTS AND COMPANIES

[» COMPLETE PRODUCT GUIDE](#)

Search Jobs [MORE OPTIONS](#) [careerbuilder.com](#)

IT Jobs

Enter City

US

SEARCH

TECHNOLOGY INDEX

- Applications
- Application Development
- Security
- Networking
- Wireless
- Platforms
- Hardware
- Data Management
- Storage
- Web Services
- Business

http://www.infoworld.com/article/06/08/07/HNcybercriminals_1.html

Organized Crime on the Internet



HTTP://CARDERS.NE1.NET

THE CARDERS ARMY

- 1. Credit Cards
- 2. Bank Accounts
- 3. COB's & Dumps
- 4. Venues
- 5. Discovers
- 6. Shopping

TISA



www.carderportal.org

INTERNATIONAL CARDER'S ALLIANCE

ORGANIZED CRIME IN THE 21ST CENTURY

SHADOWCREW

"FOR THOSE WHO WISH TO PLAY IN THE SHADOWS....."

The International Association
For The Advancement of Criminal Activity

Where is this site?
We searched half the Europe already!
Who knows where is it?

CARDERPLANET.COM

International Carder's Alliance

PROFILE REGISTER FAQ BB HOME SEARCH

MEMBERS USERGROUPS LOGIN LOGOUT

The Enemy is Worldwide...



Pay

Pain Relief / Muscle Relaxant

Soma



Soma (Carisoprodol) is a muscle relaxant, used to relieve the pain and stiffness of muscle spasms.

Package	Price	Per item	Savings	Order
Soma 250 mg				
90 pills x 250mg +2 Free Viagra pills	\$47.22	\$0.52 per pill		Add to cart
120 pills x 250mg +2 Free Viagra pills	\$56.22	\$0.47 per pill	Your save: \$7	Add to cart
180 pills x 250mg +4 Free Viagra pills	\$79.32	\$0.44 per pill	Your save: \$15	Add to cart
270 pills x 250mg +4 Free Viagra pills	\$112.32	\$0.42 per pill	Your save: \$28	Add to cart
Soma 350 mg				
60 pills x 350mg +2 Free Viagra pills	\$42.7	\$0.71 per pill		Add to cart
90 pills x 350mg +2 Free Viagra pills	\$52.47	\$0.58 per pill	Your save: \$12	Add to cart
120 pills x 350mg +2 Free Viagra pills	\$62.7	\$0.52 per pill	Your save: \$23	Add to cart
180 pills x 350mg +4 Free Viagra pills	\$88.47	\$0.49 per pill	Your save: \$40	Add to cart
270 pills x 350mg +4 Free Viagra pills	\$125	\$0.46 per pill	Your save: \$68	Add to cart

Viagra + Cialis

69⁹⁹\$



10 x Viagra
100 mg
10 x Cialis
20 mg

[ORDER NOW](#)

Bestsellers



Viagra

Our price: **\$1.15**

[More info](#)



Cialis

Our price: **\$2.18**

[More info](#)



Viagra Professional

Our price: **\$3.73**

[More info](#)



Cialis Professional

Our price: **\$4.17**

[More info](#)



Viagra Super Active

Our price: **\$2.82**

[More info](#)

Easy Mass Mailer

Message

Message

Subject:

Attachments:

Body Text:

Sender Info

Name:

Email:



IC InstallsCash

Our day has more than 24 hours

Eng | Rus



[Home](#)

[Terms](#)

[Faq](#)

[Sign Up](#)

[About us](#)

[Rates](#)

[Login](#)

26/02/08:

New crypted exe's!

We solved problem with our crypted exe's! Now they will be updating every 3 days and they will be invisible for every antivirus!

Anybody can work with our partnership program InstallsCash!

We pay \$3 (asia) and much more for every 1000 installs!

You have to do only one thing! Put a short one line game code on ur page(s) and **START MAKING MONEY!**

... a cheat and system of uniqueness that you see is independent data from others

16/02/08:

Increasing rates!

We're increasing our price for USA *2(50\$)! Now any mix of countries is about 30\$!

You won't lose your unique visitors with us! You can also have your own exe.

We have the best percentage of installs (10-40% of the total traff OR \$4-\$15 FOR 1000 UNIQUE VISITORS)

3 reliable high-speed servers!

Real-time statistic of!

Payment via: Fethard, Webmoney, Wire, E-gold, Western Union (WU), MoneyGram, Anelik and Epassporte

10/12/07:

Finally WE ARE WORKING!

Here's our main SITE. At numerous requests we've cancelled system of uniqueness! Now everyone can see number of unique loadings irrespective of others adverts!

More than 300 webmasters work with us already!

Friendly support service!

We have four-year experience!

WE PAY WITHOUT ANY DELAY!

Individual approach to everybody!

Everyone's glad, working with us. And that's the main thing for Your decision!

206.53.51.12



Get video

finjan



21.7 MB / 24 MB

Spam Sample

I am a underwear model, and in our industry, everyone uses this.
<http://www.wisodene.com/>

Who is Our Badguy?

Brand Name Meds
Free Shipping on
Orders Over \$99
www.CanadaDrugs.com

Canada RX Drugs Online

Buy Prescriptions
and Save over 70%
We Will Beat All
Competitors Prices
CanadianPharmacyMeds.com

Rx Meds - Free Shipping

USA online meds.
Free Shipping
1-800 Support. All
orders processed
AmericanRxLeader.com

Canadian Pharmacy Online

Canadian Pharmacy
Online Directory.
Find Canadian
Pharmacy Online
Fast.
TopSellingDrugs.com

Buy Advantage Online

America's Largest

[edit](#) Title

Canadian Meds Llc

[edit](#) Description

Excerpted from the website:

Generic means using a different name for the same ingredients. The contents of the pills are absolutely the same in our generic version and the branded analogue.

[read more](#)

[edit](#) Address

200-1765 W 8th Ave
Vancouver BC V6J 5C6 Canada

[edit](#) Contact

Canadian Meds Llc
info@thecanadianmeds.com

[edit](#) Logos



[edit](#) Additional Information

[edit](#) [edit](#) [edit](#) [edit](#)

Russian Business Network

washingtonpost.com

NEWS | OPINIONS | SPORTS | ARTS & LIVING | Discussions | Photos & Video | City Guide | CLASSIFIEDS | JOBS | CA

Shadowy Russian Firm Seen as Conduit for Cybercrime

By Brian Krebs

washingtonpost.com Staff Writer

Saturday, October 13, 2007; A15

An Internet business based in [St. Petersburg](#) has become a world hub for Web sites devoted to computer security experts. They say Russian authorities have provided little help in efforts to shut

The Russian Business Network **sells Web site hosting to people engaged in criminal activity** the

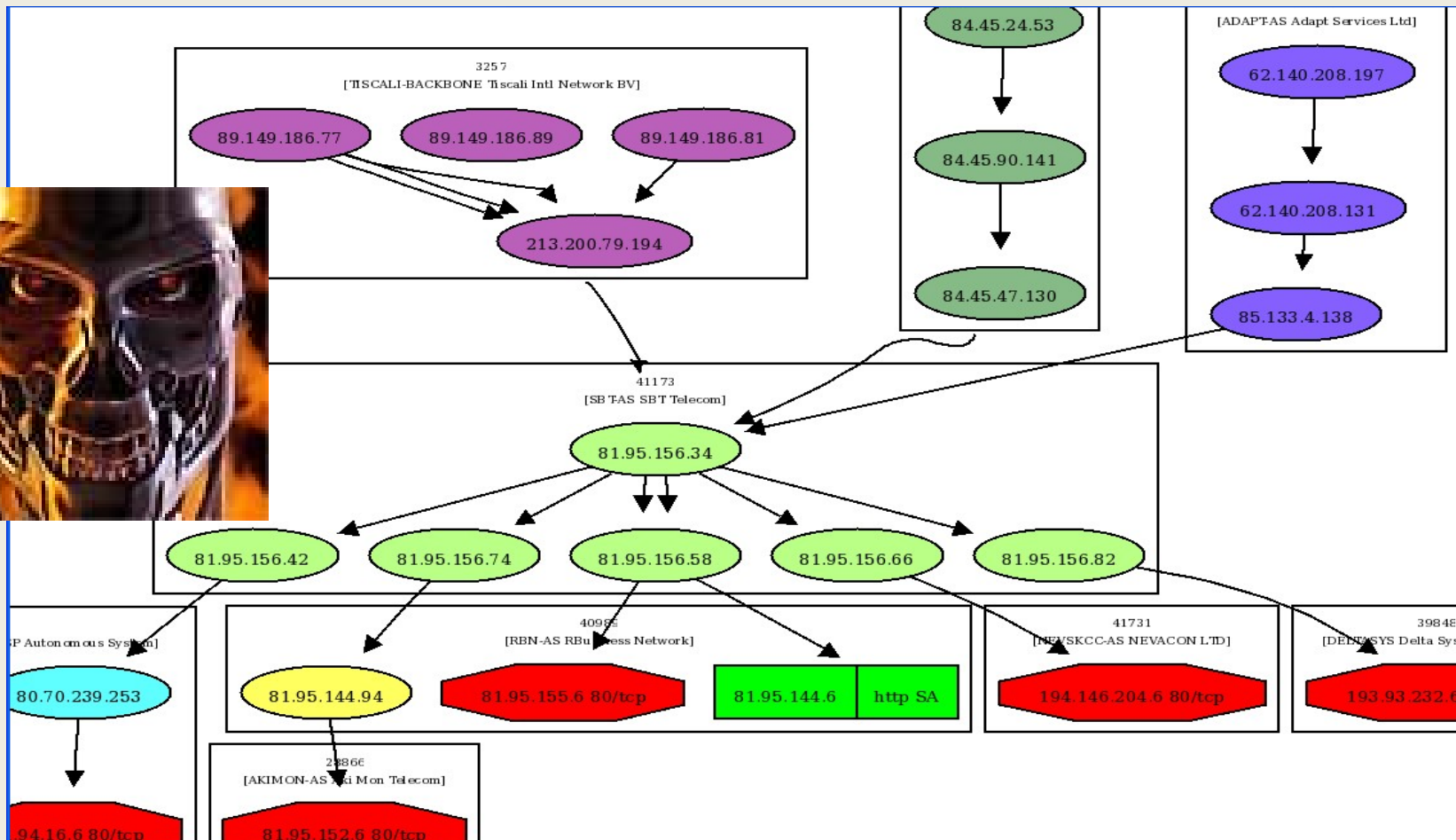
Groups operating through the company's computers are thought to be responsible for about half of the cyberattacks which cybercrooks use e-mail to lure people into entering personal and financial data at fake co-

One group of phishers, known as the Rock Group, used the company's network to steal about \$10 million, a report by [VeriSign](#) of [Mountain View, Calif.](#), one of the world's largest Internet security firms.

In another recent report, the [Cupertino, Calif.](#)-based security firm [Symantec](#) said that the Russians carry out a major portion of the world's cybercrime and profiteering.

http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html

Complex and Organized



Crimes Overlap

HACKING/INTRUSION

MALWARE
INFECTION/BOTNET

CRIMINAL

ILLEGAL SPAM

PHARMACEUTICAL
FRAUD

Questions

Matthew Ziemniak

Program Director- Cyber Operations
National Cyber-Forensics and Training
Alliance

mziemniak@ncfta.net

412-802-8000 ext. 229