

The Russian Hacker Case

AO 89 (Rev. 7/95) Subpoena in a Criminal Case

United States District Court
WESTERN WASHINGTON

DISTRICT OF

UNITED STATES OF AMERICA
v.
VASILIY GORSHKOV, et al.

SUBPOENA IN A
CRIMINAL CASE

CASE NUMBER: CR00-550C

TO: RAY POMPON

☒ YOU ARE COMMANDED to appear in the United States District Court at the place, date and time specified below, or any subsequent place, date and time set by the court, to testify in the above referenced case. This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court.

<p>PLACE United States Courthouse Fifth and Madison 1010 Fifth Avenue Seattle, Washington</p>	<p>COURTROOM Room 609 Chief Judge Coughenour</p> <hr/> <p>DATE AND TIME April 29, 2001 May 29, 2001 9:00 a.m.</p>
---	--

"The Civilian"

Despite claims by King5 News, I am **not** an FBI Agent.

Many details on the case in this presentation.

Some details have been withheld.



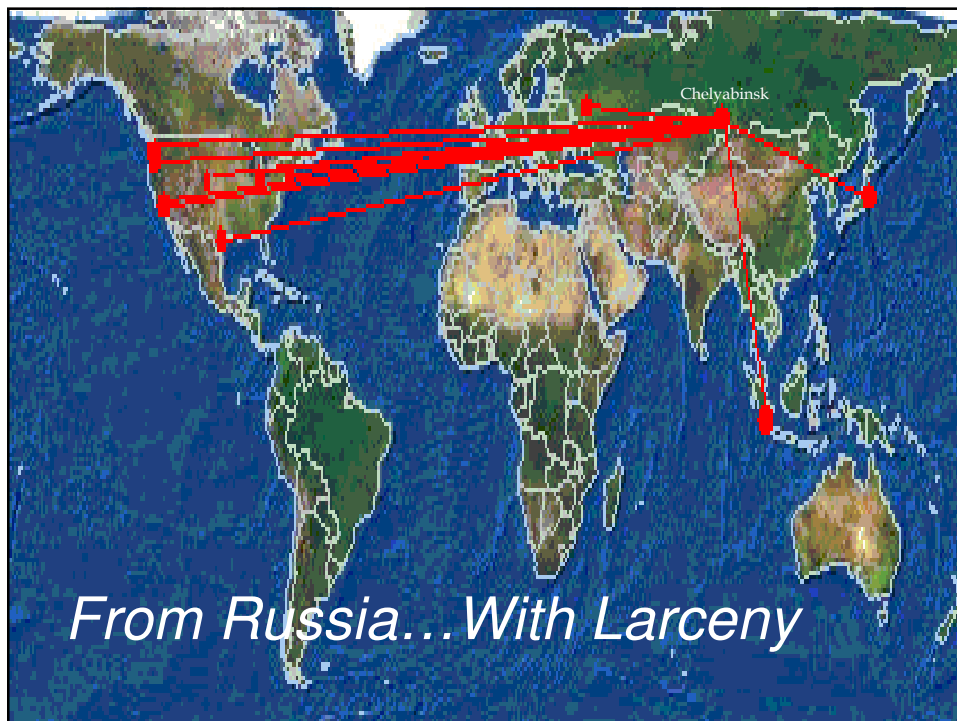
Just a small player, on a winning team

- Federal Bureau of Investigation
- United States Attorney's Office
- United States Secret Service
- Federal Trade Commission

Computer forensics assist
from Boeing and U.Washington



U.S. Department of Justice
Federal Bureau of Investigation



Winter, 1999

ISPs are hacked:

- Verio in Colorado
- LightRealm in Kirkland
- CTS in San Diego
- Speakeasy Networks in Seattle.

In some cases, ISP hosting customers' credit card data is stolen and posted on the Internet.

The hacker IRCs...



The hacker asked Speakeasy for a "security" job and weekly payments of \$1,000-1,500.

He said he would tell Speakeasy how he got in, and fix the security holes.

Speakeasy refused to pay, refused to give him a job.

As with any job seeker, he sent a resume' ...

Resume

Alexey V. Ivanov

Address: Russian Federation, Chelyabinsk, Severnaya st. 6-24
Office Phone: +7-(3512)-653600, Home Phone: +7-(3512)-364496
Email: subbsta@surnet.ru

Experience

Dec 1997 - Present, JSC "ChelyabSvyazInform" - regional telephony company (PTT), internet service provider
Russian Federation, Chelyabinsk, 454000, Kirov st. 161,
phone: +7-(3512)-653600

- * Developed financial accounting and goods inventory applications. Tools: Visual Basic For Applications.
- * Developed WWW report server that used over web browser or MS Excel Web Query. Tools: Java/servlet toolkit.
- * Developed user verification software (UNIX, GCC, SQL)
- * Installed and maintained:
 - LAN on 3Com Hub
 - US Robotics Total Control Rack
 - File server on UNIX and Windows NT
 - Dialin (SLIP/PPP/UUCP) server on UNIX
 - Mail/News server on UNIX and Windows NT
 - Proxy server on UNIX and Windows NT
 - DNS (Domain Name Server) on UNIX and Windows NT
 - WWW (World Wide Web server) on UNIX and Windows NT
 - Print server on UNIX and Windows 3.11/95/98
 - Tacacs/Radius server on UNIX and Windows NT
 - Quake/RealAudio server on UNIX and Windows NT
 - Windows 3.11/95/98 workstation
 - IP routing from local subnet to InterNet on UNIX (with network address translation) and Cisco
 - Firewall on UNIX and Cisco

Spring, 2000

The hacking continues,
but not to cash-strapped ISPs.



Target-rich sites such as financial-institutions:

- OIB, an online credit-card processing company
- Nara Bank of Korea (located in Los Angeles)
- Central National Bank of Waco, Texas

Same M.O.: The ole Hack and Blackmail

Lesson #1



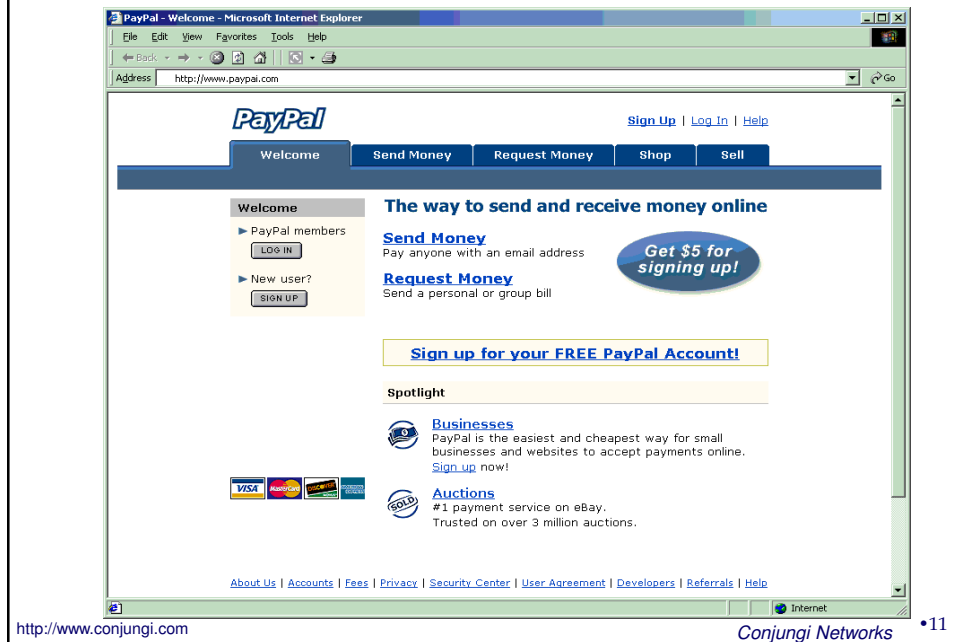
*Never store confidential data
(like credit card numbers)
on an Internet accessible server
without **encrypting** the data.*

Summer, 2000

It becomes obvious that for these hackers, it's all about the Benjamins.

They are now ready to pull off their biggest crime yet... against one of the largest financial services companies on the Internet.

Do you use this service?



•11

This e-mail was sent out

Subject: PayPal Cash Give-Away

From: Friend <CashGiveAway at Paypal dot com>

Reply-To: cheapercommunications at yahoo dot com PayPal

Congratulations You were chosen from over 30,000 contestants for our \$500.00 cash give-away from PayPal. If you are already a member simply click the link below to Accept the Cash Give-Away. Even if you are not a PayPal member you can sign-up for Free, and still accept the \$500.00 Cash Give-Away today!

Amount: \$500.00

Note: Enter Your Info Below To Accept.

To Process: Click link below or copy and paste into browser window.

<https://www.paypal.com/prq?id=H1aDsQ-6vwg7w1YaVZjb.hGJmz0uOz6pb.omew>

Paypai.com

Turns out Paypai.com was really being hosted off a server in Moscow and a server at LightRealm.

LightRealm?

Hey, where have I heard that name before?

Questions to think about:

Did PayPal **actually** get hacked?

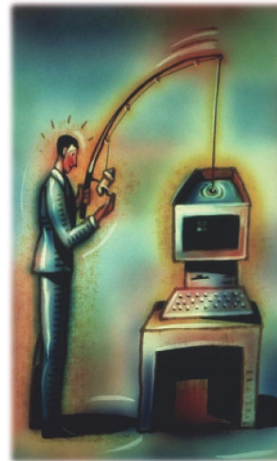
How much could they have done to prevent this?

Could this happen to your site?

Phishing

***Average users lack
expertise
to verify e-mail senders.***

***Internet's mail protocol
SMTP
has no mechanism
for the verification of
sender.***



*Fool some of the people...
some of the time... profitable!*



Ten thousand customers

Steal fifty dollars from one percent

Pretty much the average take from a bank robbery

And nearly negligible risk of getting caught

Lesson #2



*Don't believe everything you
read on the Internet. It's easy
to fake e-mail and websites.
When in doubt, check it out.*

June - Nov 7th, 2000

Remember when Alexey asked Speakeasy for a job?
The FBI takes him up on that.

UC e-mails Alexey about coming to work
for a security company called Invita.

After phone interviews and hacking demos,
"Invita" invites Alexey to Seattle to interview.

Alexey accepts and says he's bringing an associate.

Nov 9th, 2000

Need someone to qualify their hacker expertise

Someone who can talk the talk

Someone to be an Invita security consultant

Someone who knows hackers and their tools

And where's **my** flak jacket?

Nov 10th, 2000

- 3 FBI Undercover agents and me
- Posing as a security company
- “Show us your stuff”
- Full surveillance operation:
Helicopters overhead, cameras rolling,
and keyboard sniffers running
- They brought a laptop,
but we gave them a machine to use as well.



“The FBI cannot get us in Russia”

- Were more afraid of “the agencies” in Russian.
- They downloaded some tools from a Russian server
and used them to scan the Invita building network.
- They quickly deleted their tools when I asked about it.
- Remember the keystroke logger?
- A few hours later, they were both in FBI custody.



Alexey Ivanov

"Subbsta"

19 years old

Technical guy

<http://www.conjungi.com>



Vassiliy Gorshkov

"kvankin"
24 years old

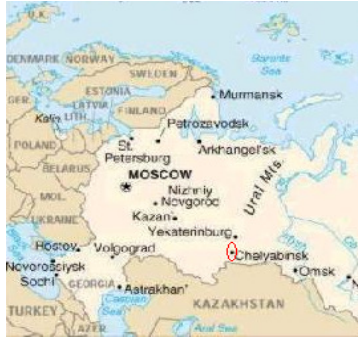
Business
development

<http://www.conjungi.com>



Chelyabinsk

“Here it is difficult for a person to live on honest wages.”



Deep in the Ural Mountain river valley.
Industrial city of 1.2 million people.
Heavily polluted, radioactive from an accident in the 50's

Inside Tech.Net.Ru

Little office in Chelyabinsk Textile Factory

They had approximately 5 employees:
three hackers, two programmers.

There were six others involved as well.

Everyone feared the Russian Mafiya.



Hacking tools on the laptop

Included such popular and easy to acquire tools like MSADC, L0phtCrack and FuckIIS

- 18 **B. FILES, SCRIPTS AND PROGRAMS FROM ALEXEY IVANOV'S TOSHIBA**
19 **LAPTOP COMPUTER**
20 50. Chart of directories, subdirectories, and files from c: drive of Alexey Ivanov's Toshiba
21 laptop computer
22 51. SPEAK.TXT (c:\work\soft\SCANNER\SPEAK.TXT)
23 52. SPEAK1.TXT (c:\work\soft\SCANNER\SPEAK1.TXT)
24 53. SPEAKE~1.TXT (c:\work\soft\SCANNER\SPEAKE~1.TXT)
25 54. SPEAK2.TXT (c:\work\soft\SCANNER\SPEAK2.TXT)
26 55. memphis.k12.mi.us (c:\work\soft\ucfjohn\john-15\run\memphis.k12.mi.us)
27 56. memphis.k12.mi.us-dec (c:\work\soft\ucfjohn\john-15\run\memphis.k12.mi.us-dec)
28

GOVT'S EXHIBIT LIST/GORSHKOV-- 5
CR00-350C

UNITED STATES ATTORNEY
801 Union Street, Suite 2100
Seattle, Washington 98101-3003
(206) 553-7970

December, 2000



ADVISORY 00-060

"E-Commerce Vulnerabilities"

December 01, 2000

Based on FBI investigations and other information, the NIPC has observed that there has recently been an increase in hacker activity specifically targeting U.S. systems associated with e-commerce and other Internet-hosted sites. The majority of the intrusions have occurred on Microsoft Windows NT systems, although Unix based operating systems have been victimized as well. The hackers are exploiting at least three known system vulnerabilities to gain unauthorized access and download propriety information. Although these vulnerabilities are not new, this recent activity warrants additional attention by system administrators. In most cases, the hacker activity had been ongoing for several months before the victim became aware of the intrusion. The NIPC strongly recommends that all computer network systems administrators check relevant systems and apply updated patches as necessary. Specific emphasis should be placed on systems related to e-commerce or e-banking/financial business. The following types of exploits have been observed:

Unauthorized Access to IIS Servers through Open Database Connectivity (ODBC) Data Access with Remote Data Service (RDS):

<http://www.conjungi.com>

Conjungi Networks

•27

Lesson #3



*Pay attention to warnings.
There's usually a reason as to
why they've been issued.*

<http://www.conjungi.com>

Conjungi Networks

•28

The FBI hacks back?

The FBI goes to the Russian server that Vassily accessed.

Over several hundred gigabytes of data is collected, but not examined until a search warrant could be obtained.

During the trial, defense calls this “the FBI hacking them”.

No expectation of privacy because they were there to demonstrate his skills and be watched.

Many sophisticated hacking tools were found

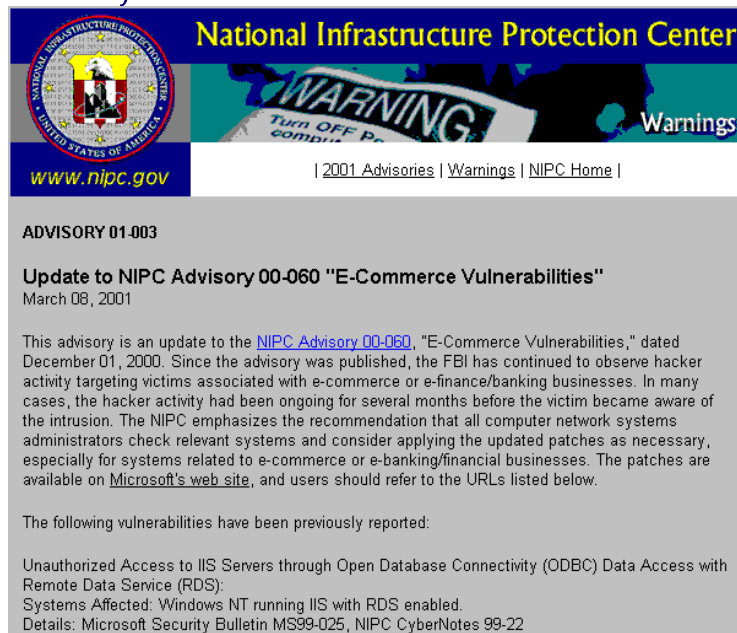
- 132. List of files in /home/kvakin/http directory (CD reference: 1b7/kvakin-home/http)
- 133. auto_web-agent.pl (tech.net.ru: /home/kvakin/http/auto_web-agent.pl)
- 134. Electronics.txt (tech.net.ru: /home/kvakin/http/Electronics.txt)
- 135. fuckIIS (tech.net.ru: /home/kvakin/http/fuckIIS)
- 136. http (tech.net.ru: /home/kvakin/http/http)
- 137. iis_hosts.txt (tech.net.ru: /home/kvakin/http/iis_hosts.txt)
- 138. net_ssl_test (tech.net.ru: /home/kvakin/http/net_ssl_test)
- 139. sslproxy (tech.net.ru: /home/kvakin/http/sslproxy)
- 140. sslproxy_socket (tech.net.ru: /home/kvakin/http/sslproxy_socket)

“These guys are some of the best system integrators I’ve ever seen”

Completely new exploits, rootkits and tools were found.

The FBI needed call in outside expertise from the University of Washington and Boeing to assist with the forensics.

March, 2001



The screenshot shows the NIPC website with a blue header. On the left is the NIPC seal. To its right is the text "National Infrastructure Protection Center" in yellow. Below the header is a banner with a "WARNING" sign and the text "Turn OFF Power to computer". To the right of the banner is the word "Warnings". Below the banner is a navigation bar with links: "2001 Advisories", "Warnings", and "NIPC Home". Below the navigation bar is the text "www.nipc.gov". Below that is the text "ADVISORY 01-003". Below that is the text "Update to NIPC Advisory 00-060 'E-Commerce Vulnerabilities'" and "March 08, 2001". Below that is a paragraph of text: "This advisory is an update to the NIPC Advisory 00-060, 'E-Commerce Vulnerabilities,' dated December 01, 2000. Since the advisory was published, the FBI has continued to observe hacker activity targeting victims associated with e-commerce or e-finance/banking businesses. In many cases, the hacker activity had been ongoing for several months before the victim became aware of the intrusion. The NIPC emphasizes the recommendation that all computer network systems administrators check relevant systems and consider applying the updated patches as necessary, especially for systems related to e-commerce or e-banking/financial businesses. The patches are available on Microsoft's web site, and users should refer to the URLs listed below." Below that is the text "The following vulnerabilities have been previously reported:". Below that is the text "Unauthorized Access to IIS Servers through Open Database Connectivity (ODBC) Data Access with Remote Data Service (RDS):". Below that is the text "Systems Affected: Windows NT running IIS with RDS enabled." Below that is the text "Details: Microsoft Security Bulletin MS99-025, NIPC CyberNotes 99-22".

National Infrastructure Protection Center

Warnings

[2001 Advisories](#) | [Warnings](#) | [NIPC Home](#)

www.nipc.gov

ADVISORY 01-003

Update to NIPC Advisory 00-060 "E-Commerce Vulnerabilities"
March 08, 2001

This advisory is an update to the [NIPC Advisory 00-060](#), "E-Commerce Vulnerabilities," dated December 01, 2000. Since the advisory was published, the FBI has continued to observe hacker activity targeting victims associated with e-commerce or e-finance/banking businesses. In many cases, the hacker activity had been ongoing for several months before the victim became aware of the intrusion. The NIPC emphasizes the recommendation that all computer network systems administrators check relevant systems and consider applying the updated patches as necessary, especially for systems related to e-commerce or e-banking/financial businesses. The patches are available on [Microsoft's web site](#), and users should refer to the URLs listed below.

The following vulnerabilities have been previously reported:

Unauthorized Access to IIS Servers through Open Database Connectivity (ODBC) Data Access with Remote Data Service (RDS):
Systems Affected: Windows NT running IIS with RDS enabled.
Details: Microsoft Security Bulletin MS99-025, NIPC CyberNotes 99-22

As well as evidence of all the aforementioned hacks

E. NARA BANK

NARA BANK EVIDENCE RECOVERED FROM TECH.NET.RU

401. dirlist_c (tech.net.ru: /home/subbsta/enc/disk1.tar >

disk1/subbsta/hack/sites/narabankna.com/dirlist_c)

402. dirlist_d (first 11 and last pages) (tech.net.ru: /home/subbsta/enc/

disk1/subbsta/hack/sites/narabankna.com/dirlist_d)

403. accounts.txt (tech.net.ru: /home/subbsta/1/1/narabankna/accounts.txt)

i21. PayPal account activity records re: Nara Bank Account 400715807 (Eui

i21A. Nara Bank records re: Nara Bank Account 400715807 (Eui

i22. PayPal account activity records re: Nara Bank Account 75076706 (Inhw

i22A. Nara Bank records re: Nara Bank Account 75076706 (Inhw

i23. PayPal account activity records re: Nara Bank Account 301346406 (Yoi

i23A. Nara Bank records re: Nara Bank Account 301346406 (Yoi

i24. PayPal account activity records re: Nara Bank Account 1050469406 (Di

i24A. Nara Bank records re: Nara Bank Account 1050469406 (Di

F. CENTRAL NATIONAL BANK-WACO

CNB-WACO EVIDENCE RECOVERED FROM TECH.NET.RU COMPUTER

502. DDA697 (CNB-Waco Daily Account Activity for August 7, 2000) (first 10 and last

pages) (tech.net.ru: /home/subbsta/a.zip > 08/DDA697)

1072. credit_cards (tech.net.ru: /home/subbsta/enc/disk1.tar > /disk1/subbsta/s.tgz >

/Stuff/Stuff/Hack/Domains/com/lightrealm/credit_cards)

"What are these PERL scripts?"

PERL robots designed
to launder stolen credit cards
through phished PayPal accounts.

Send Money

[See Demo](#)

Send Money allows you to pay anyone with an email address.

Common uses for Send Money:

- Pay for an auction item
- Split a restaurant bill or rent
- Pay for an online purchase (or send money to your family or friends)
- Pay bills online

Just enter the recipient's email address and the amount you wish to send. You can pay with a credit card or checking account.

The recipient gets an email that says "You've Got Cash!" Recipients can then collect their money by clicking a link in the email that takes them to PayPal.

SEP 19 2001

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

VASILY VYACHESLAVOVICH
GORSHKOV, a/k/a VASSILI
GORCHKOV, a/k/a "kvakin"

Defendant.

NO. CR00-550C

GOVERNMENT'S EXHIBIT LIST

CR 00 00550 -00000085

A. INVITA EVIDENCE AND SUMMARY EXHIBITS

- I. Video tape of Invita meeting, November 10, 2000, *with* superimposed transcript
- 1A Video tape of Invita meeting, November 10, 2000, *without* superimposed transcript
- 1B. Audio recording of Invita meeting, November 10, 2000 (7 tapes)
- 1C Transcript of Invita meeting, November 10, 2000

Summer-Fall, 2001

The trial ran for 3 weeks

I. SUMMARY OF THE CASE

This defendant, VASILY GORSHKOV, together with his coconspirator, ALEXEY IVANOV, were arrested in Seattle on November 10, 2000, and, on November 16, 2000, GORSHKOV was indicted in a one-count Indictment charging him with conspiracy. On April 5, 2001, a Superseding Indictment was returned charging him and IVANOV with conspiracy and nineteen substantive counts of violations of the Computer Fraud and Abuse Act and the wire fraud statute. Trial is set on the Superseding Indictment before the Honorable John C. Coughenour and a jury on September 17, 2001.

GOVERNMENT'S TRIAL BRIEF/GORSHKOV— 1
CR00-550C

UNITED STATES ATTORNEY
601 Union Street, Suite 5100
Seattle, Washington 98101-3903
(206) 553-7970

The swag

Earned as much as \$500,000
over nine months of hacking and extortion.

Used stolen credit cards to
purchased computers and high-value goods
from places in America, Canada, Guatemala and Israel.

The goods were shipped to addresses in
Romania and Cyprus and
then smuggled over the border in Kazakhstan
into the Russian Federation to Chelyabinsk.

Lesson #4



*These aren't bored "hacker" kids.
These are well-trained,
professional criminals who use
the Internet to rip you off.*

Convicted

Gorshkov guilty of extorting 3 companies.

Ivanov guilty of hacking 16 companies,
extortion and wire fraud.

Ivanov feared for his family:
In exchange for pleading out, his mother, sister
and girlfriend were relocated to America.

Some of the victims:

CD Universe
Western Union
Glen Rock Financial Services
Company
VPM, Inc.
NaraBank
Central National Bank of Waco
Online Information Bureau
St. Clair School District
Speakeasy Networks
Lightrealm Communications
PayPal
FSI Systems
Sterling Microsystems
Transmark

Victim group 1: Customers

- All those whose credit cards were stolen
- All those who got scammed out of their PayPal accounts
- 56,000 individual card #'s found in the hacker's stash.

Victim group 2: E-Commerce sites

- E-commerce website which was hacked or spoofed.
- Hackers extort money or else they would release customer information and destroy the site.
- Whether paid or not, usually used the credit card data anyway.
- In addition to big companies mentioned earlier, many smaller e-commerce sites were hit.

Victim group 3: Proxies

- “When I hack a site, I look and think if they can pay me. If cannot, then I save for later.”
- Many schools and ISPs were hacked so machines could be used in hacks against others.
- Sometimes fake sites were hosted there too.
- Victims spread all over the world... lots of schools.

Lesson #5

Been owned?
Subex must've gotcha

"The brotherhood cannot be wiped out because it is not an organization in the ordinary sense. Nothing holds it together except an idea which is indestructible" - Eric Blair's "1984"



Even if there is nothing of value on your computer, it is still useful to hackers to hijack and use against others.

Summer, 2004

- The battle was won.. The war goes on.
- Banks and e-commerce sites are still getting hacked
- Credit cards are still getting stolen en-masse.
- Extortion payments are still being demanded.
- Phishing and fraud are still going on

Where is everyone now?

Prosecutors - US Attorneys

AUSA Floyd Short

- Working on CyberCrime task force
- Current Infragard member
- His team also worked on the Blaster case

AUSA Stephen Schroeder

- Retired
- Teaching at Seattle University

FBI Agents

SA Marty Prewitt

SA Michael Schuler

Recipient of the
FBI Director's Annual Award for Outstanding
Criminal Investigation for their work on this case.

This was the first case in the bureau's history to
utilize the technique of extra-territorial seizure.

But no good deed goes unpunished

Russia's Federal Security Service (FSB)
started criminal proceedings against
FBI Agent Michael Schuler
for unauthorized access
to computer information..

And Alexy and Vasiliy?

Vasily Gorshkov
Sentenced to 4 years in federal prison.

Alexei Ivanov,
sentenced to 4 years in federal prison
with three years of supervised release .

Alexey wrote a letter to SpeakEasy

“I promise that upon my release
I will work hard to
compensate for damages
caused by my criminal behavior.”

The third hacker

Aka “Hermit”

Michael, a classmate of Alexey’s

Around 22 years old now

He was their reconnaissance hacker

A wanted man but in hiding in Russia

Michael said via e-mail:

“By tricking the Russians to Seattle to arrest them, the FBI had started a war. We’ll keep stealing just like we did in the past. Better leave us alone.”

Both Alexey and Vassiliy say there is another hacker group loosely affiliated with them.

This group was “more serious”

That group is still out there.

Questions?

