The Ultimate Honeypot

Philip Attfield
NWSI
July 7, 2005
The Original, Ultimate Honeypot
The Original Winnie

© Philip Attfield 2005
The Fall City Honeypot
Ultimate Honeypot?
Or is it really? ...
“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

Arrest: 11/00
EW hire: 4/01
Trial: 09/01
Sentence: 10/02 $700k
VG Release: 11/03

Amazon, CD Universe: “99/00”
CTS, Speakeasy: < 12/99 >
Sytex Honeypot
NARA, CNB, Ebay, PayPal, Email, CTS: ongoing

Ivanov Sentence: 07/03 $25M

Gorshkov Sentence: 10/02 $700k
Speakeasy

• November:
  – Receive solicitation for “security consulting” services
  – Sent photos & resume
  – Refused

• December:
  – Threats escalate to retaliation & extortion
  – Dec 24\textsuperscript{th}; (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
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 …
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 services

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:  LATLE-ORG-RIPN  
ns-server:  memphis.k12.mi.us  
ns-server:  ns.tech.net.ru.  
ns-server:  ns.tech.net.ru.  
created:  000427  
state:  Delegated  
changed:  000427  
mnt-by:  LARDYCH-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” 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
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)
<table>
<thead>
<tr>
<th>Workstation</th>
<th>User</th>
<th>Date</th>
<th>Start</th>
<th>Elapsed</th>
<th>Exe</th>
<th>Caption</th>
<th>Key strokes</th>
<th>Formatted</th>
<th>Raw</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:22:44 PM</td>
<td>0:00:00</td>
<td>C:\WINNT\Explorer.exe</td>
<td>Program Manager</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:22:44 PM</td>
<td>0:00:10</td>
<td>Program Manager</td>
<td>Command Prompt</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:22:54 PM</td>
<td>0:01:14</td>
<td>C:\WINNT\System32\ftp.exe</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:22:57 PM</td>
<td>0:00:16</td>
<td>C:\WINNT\Explorer.exe</td>
<td></td>
<td>18</td>
<td>ipconfig-all</td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:23:55 PM</td>
<td>0:00:00</td>
<td>C:\WINNT\Explorer.exe</td>
<td>ftp</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:23:55 PM</td>
<td>0:00:00</td>
<td>C:\WINNT\Explorer.exe</td>
<td>Run</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:23:58 PM</td>
<td>0:00:10</td>
<td>C:\WINNT\System32\ftp.exe</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:24:08 PM</td>
<td>0:00:13</td>
<td>C:\WINNT\Explorer.exe</td>
<td></td>
<td>24</td>
<td>kvakin &lt;ESC&gt;&lt;CTRL&gt;&lt;UP&gt;&lt;UP&gt;</td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:24:08 PM</td>
<td>0:02:44</td>
<td>C:\WINNT\System32\telnet.exe</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:26:31 PM</td>
<td>0:00:10</td>
<td>C:\WINNT\System32\ftp.exe</td>
<td></td>
<td>18</td>
<td>exit quit</td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:26:41 PM</td>
<td>0:00:10</td>
<td>C:\WINNT\System32\ftp.exe</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC02</td>
<td>Administrator</td>
<td>11/10/2000</td>
<td>3:26:51 PM</td>
<td>0:01:58</td>
<td>Program Manager</td>
<td>Command Prompt</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkStation</td>
<td>User</td>
<td>Date</td>
<td>Start Time</td>
<td>Elapsed</td>
<td>Exe</td>
<td>Key strokes</td>
<td>Formatted</td>
<td>Raw</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>------------</td>
<td>------------</td>
<td>---------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>INVC2</td>
<td>Administrator</td>
<td>11/10/2009</td>
<td>3:26:52 PM</td>
<td>0:00:21</td>
<td>C:\WINNT\System32\telnet.exe</td>
<td>kvakin\ cflevfq\ is\ telnet freebsd.tech.net.ru\ kvakin\ cflevfq\</td>
<td>110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC2</td>
<td>Administrator</td>
<td>11/10/2009</td>
<td>3:28:48 PM</td>
<td>0:00:27</td>
<td>Program Manager</td>
<td>freebsd.tech.net.ru\ kvakin\ cflevfq\ cd kvakin\ ls\ get lomscanc.exe\ n\ bin\ &lt;UP&gt;&lt;ESC&gt;&lt;BACK&gt;&lt;BACK&gt;get lomscanc.exe\ n\ bin\ &lt;MENU&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC2</td>
<td>Administrator</td>
<td>11/10/2009</td>
<td>3:28:49 PM</td>
<td>0:00:01</td>
<td>C:\WINNT\Explorer.exe</td>
<td>freebsd.tech.net.ru\ kvakin\ cflevfq\ cd kvakin\ ls\ get lomscanc.exe\ quit\ ls\ &lt;MENU&gt;&lt;TAB&gt;&lt;UP&gt;&lt;DOWN&gt;&lt;TAB&gt;&lt;MENU&gt;</td>
<td>102</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC2</td>
<td>Administrator</td>
<td>11/10/2009</td>
<td>3:28:57 PM</td>
<td>0:00:00</td>
<td>C:\WINNT\Explorer.exe</td>
<td>telnet\ ls\ telnet\ ls\ telnet\ ls\ ftp tech.net.ru\ ftp tech.net.ru</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC2</td>
<td>Administrator</td>
<td>11/10/2009</td>
<td>3:28:57 PM</td>
<td>0:00:00</td>
<td>C:\WINNT\Explorer.exe</td>
<td>C:\WINNT\Explorer.exe\ Run\ ftp tech.net.ru\ Run\ ftp tech.net.ru</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC2</td>
<td>Administrator</td>
<td>11/10/2009</td>
<td>3:28:57 PM</td>
<td>0:00:00</td>
<td>C:\WINNT\Explorer.exe</td>
<td>telnet\ 15 ftp tech.net.ru\ 6 ftp tech.net.ru</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVC2</td>
<td>Administrator</td>
<td>11/10/2009</td>
<td>3:29:15 PM</td>
<td>0:00:18</td>
<td>Program Manager</td>
<td>C:\WINNT\System32\ftp.exe</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GORSHKOV
Note: freebsd.tech.net.ru

ibm_log.csv
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/20/2005</td>
<td>12:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>12:00 AM</td>
<td>Administrator logout</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>1:00 AM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>2:00 AM</td>
<td>Administrator logout</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>3:00 AM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>4:00 AM</td>
<td>Administrator logout</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>5:00 AM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>6:00 AM</td>
<td>Administrator logout</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>7:00 AM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>8:00 AM</td>
<td>Administrator logout</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>9:00 AM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>10:00 AM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>11:00 AM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>12:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>1:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>2:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>3:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>4:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>5:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>6:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>7:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>8:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>9:00 PM</td>
<td>Administrator login</td>
</tr>
<tr>
<td>11/20/2005</td>
<td>10:00 PM</td>
<td>Administrator login</td>
</tr>
</tbody>
</table>

**Note:** The table contains multiple entries for different times and dates, indicating the login and logout times for an administrator. The entries are repeated multiple times, suggesting a pattern or a log format.
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

© Philip Attfield 2005
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 (cvcvcdn@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:localhost:3306','root', 'YtGhjcnj',{ RaiseError => 1 } ); # database
open(F,"<register.htm"); # file containing email domain names
local $/=undef;
$fullfile=

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";
    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 = $fullfile =~ m|^<option\svvalue=.*?>(.*?)</option>$|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>){
      $document.=$_; }

© Philip Attfield 2005
#!/usr/bin/perl
use IO::Socket;
use DBI;
$dbh = DBI->connect( 'DBI:mysql:myown: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>){
        $document.=$_; }

© Philip Attfield 2005
#!/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 = $fullfile =~ m|^<option\svvalue=.*?>(.*?)</option>$|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
    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
    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>){
        $document.=$_;
}
if ( $document =~ /Your\'s new\'s e-mail\'s address has been\'s established\'and\'s \is\'s ready\'sto\'s use/) {
    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="qwrtpsdfghjklzcvbnm";
    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\sn\semail\saddress\shas\sbeen\sestablished\sand\sis\sready\sto\ssuse/ ) {
    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\nTrying aborted...\n"
    redo;
}
open ( HTML, "temp1.html");
print HTML $document;
close ( HTML );
}
close ($socket) if $socket;
...
sub GetRandomName {
  local $string;
  local $alphabet1="qwrtpsdfghjklzcvbnm";
  local $alphabet2="eyuioa";
  foreach (1.. ( int(rand( 2 )) +3) ) {
    $string.=substr($alphabet1,int(rand(20)),1);
    $string.=substr($alphabet2,int(rand(6)),1);
  }
  $string.=substr($alphabet1,int(rand(20)),1);
  return $string;
}
if ($document =~ /Your\'s new email address has been established and is ready to use/) {
    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\nTrying 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 $alphabet1="qwrtpsdfghijklzcvbmn";
    local $alphabet2="eyuioa";
    foreach (1.. ( int( rand(2) ) +3) )
    {
        $string.= substr($alphabet1, int(rand(20)),1);
        $string.= substr($alphabet2, int(rand(6)),1);
    }
    $string.= substr($alphabet1, int(rand(20)),1);
    return $string;
}
if ( $document =~ /Your\'s\new\semail\saddress\shas\'\been\sestablished\sand\sis\sready\sto\sus\e/ ) {
    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 $alphabet1="qwrtpsdfghjklzcvbnm";
    local $alphabet2="eyuioa";
    foreach (1..(int(rand(2))+3)) {
        $string.=substr($alphabet1,int(rand(20)),1);
        $string.=substr($alphabet2,int(rand(6)),1);
    }
    $string.=substr($alphabet1,int(rand(20)),1);
    return $string; ## cvcv cvcv..@somedomain
}
SUCCESS!
Your new email address has been established and is ready to use!

Your new account information is as follows:

<table>
<thead>
<tr>
<th>Your New Address:</th>
<th><a href="mailto:cedotif@sportsoaddict.com">cedotif@sportsoaddict.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Your Password:</td>
<td>a1w2e3r4</td>
</tr>
</tbody>
</table>

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!

<table>
<thead>
<tr>
<th>1:</th>
<th>2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3:</td>
<td>4:</td>
</tr>
<tr>
<td>5:</td>
<td>6:</td>
</tr>
<tr>
<td>7:</td>
<td>8:</td>
</tr>
<tr>
<td>9:</td>
<td>10:</td>
</tr>
</tbody>
</table>

Tell Them!
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

<table>
<thead>
<tr>
<th>Date</th>
<th>Sender Email Address</th>
<th>Recipient Email Address</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:xksyyrix@mailroom.com">xksyyrix@mailroom.com</a></td>
<td><a href="mailto:sokybaduh@packersfan.com">sokybaduh@packersfan.com</a></td>
<td>-500</td>
</tr>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:wkezejruw@mailroom.com">wkezejruw@mailroom.com</a></td>
<td><a href="mailto:kekypys@as-if.com">kekypys@as-if.com</a></td>
<td>-500</td>
</tr>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:zozfenji@mailroom.com">zozfenji@mailroom.com</a></td>
<td><a href="mailto:rimorul@pcpostal.com">rimorul@pcpostal.com</a></td>
<td>-500</td>
</tr>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:epetsgsc@mailroom.com">epetsgsc@mailroom.com</a></td>
<td><a href="mailto:bomozyhud@sportsaddict.com">bomozyhud@sportsaddict.com</a></td>
<td>-500</td>
</tr>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:ohekjikr@mailroom.com">ohekjikr@mailroom.com</a></td>
<td><a href="mailto:witewegooq@friendsfan.com">witewegooq@friendsfan.com</a></td>
<td>-500</td>
</tr>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:mlqlgqdkj@mailroom.com">mlqlgqdkj@mailroom.com</a></td>
<td><a href="mailto:puzohaduq@sade.com">puzohaduq@sade.com</a></td>
<td>-500</td>
</tr>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:ahpizkri@mailroom.com">ahpizkri@mailroom.com</a></td>
<td><a href="mailto:poqupacij@mostlysunny.com">poqupacij@mostlysunny.com</a></td>
<td>-500</td>
</tr>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:alevlnni@mailroom.com">alevlnni@mailroom.com</a></td>
<td><a href="mailto:malohiqaj@1funplace.com">malohiqaj@1funplace.com</a></td>
<td>-500</td>
</tr>
<tr>
<td>8/24/2000</td>
<td><a href="mailto:hxtqafa@mailroom.com">hxtqafa@mailroom.com</a></td>
<td><a href="mailto:cuzyzimy@moonshinehollow.com">cuzyzimy@moonshinehollow.com</a></td>
<td>-500</td>
</tr>
</tbody>
</table>

- Note email address: cvcv(cv@…
- 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

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

© Philip Attfield 2005
“we build computers ourselves because it is much cheaper...”

--- 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'll pay you same day when we'll receive email from you with total sum we have to pay. You'll get the payment and only after that will ship the hardware.

If you are interesting 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 manager

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

Paypal $ to purchase goods, shipped to Chelyabinsk for resale

Email → Anon. Email
E-Bay → E-Bay
PayPal → PayPal

randomized proxy/relay
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

© Philip Attfield 2005
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
RUSSIAN COMPUTER HACKER CONVICTED BY JURY

Francis J. Diskin, United States Attorney for the Western District of Washington, and Charles E. Mancigo, Special Agent in Charge, Seattle Division, Federal Bureau of Investigation, announced that a jury returned guilty verdicts yesterday against VASILIY GORSHEKOV, 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 GORSHEKOV is scheduled before Chief United States District Judge John C. Coughenour in Seattle at 9:00 a.m. on January 4, 2002. GORSHEKOV 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.
The Price of Success
F SB Calls FBI Agent An Illegal Hacker

By Nabi Abdullaev

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-
FBI agent charged with hacking

Russia alleges agent broke law by downloading evidence

By Mike Brunker

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

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 Farmer
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

😊