The Honeynet

P R O J E C T

Honeypots
Today & Tomorrow

Speaker

- Involved in information security for over 10 years, 4 with Sun Microsystems as Senior Security Architect.
- Founder of the Honeynet Project
- Published over 50 whitepapers, authored *Honeypots* and co-authored *Know Your Enemy*.
- Served 7 years in military, 4 as officer in Rapid Deployment Force.

Why Honeypots

A great deal of the security profession (and the IT world) depend honeypots, however few know it. Honeypots …

- Build anti-virus signatures.
- Intelligence gathering (Symantec / Arbor)
- Build SPAM signatures and filters.
- Build RBL's for malicious websites.
- ISP's identify compromised systems.
- Assist law-enforcement to track criminals.
- Hunt and shutdown botnets.
- Malware collection and analysis.

March 9th, 2007

How lucrative is pump-and-dump spam?

Posted by Ryan Naraine @ 10:23 am
Categories: Hackers, Browsers, Rootkits, Vulnerability research, Spam and Phishing, Spyware and Adware, Botnets, Exploit code, Data theft, McAfee, Symantec

TALKBACK ADD YOUR OPINION Worthwhile? +6 6 VOTES

Are pump-and-dump spammers really making money from hyping penny stocks in e-mails? Paul Moriarty has the answer and it's an eyebrow-raising sight.

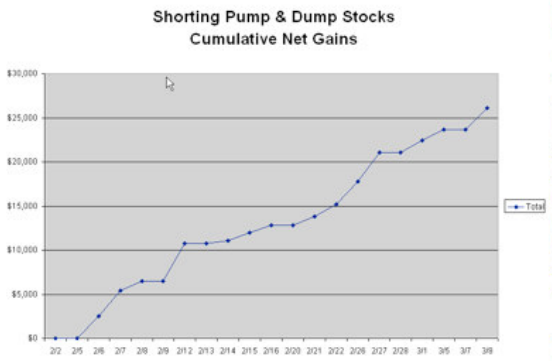
Over the last month, Moriarty, director of product development for Internet Content Security at Trend Micro, has been running a virtual portfolio of selling short on stocks found during spam runs. After 22 transactions in a five-week period, he has earned a whopping $25,610.

Short selling (shorting) a stock is the act of profiting from a stock price going down. A short seller will typically borrow a security and sell it, expecting that it will decrease in value so that they can buy it back at a lower price and keep the difference.

During Moriarty's research, he used data from pump-and-dump e-mails flooding into Trend Micro's spam honeypots. "As soon as I see activity on a particular stock, I'll short that and set a limit to cover after I've made 10%. In just over five weeks, I've turned a 25.6 percent profit on a $100,000 virtual portfolio. This is exactly what these spammers are doing. It's risky business but it's easy money," Moriarty said in an interview.

"I made money on every transaction," he added.

On the other hand, if he were to have fallen victim to "hot stock" e-mail tips and invested and held, Moriarty's portfolio would have been down 27.6 percent.



Moriarty shared his research with me after the SEC's announcement yesterday that it had suspended trading in 35 companies whose shares were promoted in spam e-mails. (See more from Larry Dignan)

Although the SEC move is to be applauded, Moriarty sees it as a double-edged sword that creates an even bigger problem.

March 08, 2007

Rinbot worm still hitting businesses

But there is 'no large global threat'

By Gregg Keizer

The Rinbot worm continues to pester and plague companies, several security organisations said, even as Symantec declared that its honeypot network had captured traffic showing that a botnet was spreading the malware.

News

Spam at all time high

Nine out of 10 e-mails will be spam by end 2007

Darren Pauli (Computerworld) 22 February, 2007 12:36:28

Up to 90 percent of all e-mails will be spam by the end of this year, according to research released yesterday.

Security vendor Marshal's Threat Research and Content Engineering (TRACE) team monitored spam traffic from honeypots located across 18 countries and recorded a 30 percent increase over the last week which smashed global record levels.

Print thi
Digg thi
More by Dar
ARN Distrib Distributors
Express Dat
Top Stori
Sarato filtering

ATLAS Dashboard: Global Summary

http://atlas.arbor.net/

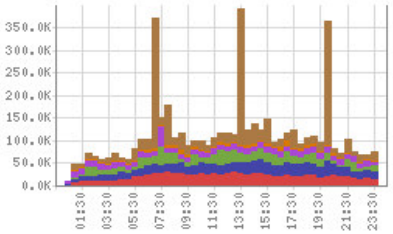
ATLAS Dashboard: Global Sum...

02 VULNERABILITY RISK INDEX (past 24 hours)

CVE	Age	Severity	Affected Products
CVE-2006-4696	163 Days	Medium	Microsoft Windows Server 2003, Windows 2000, Windows XP
CVE-2006-4691	128 Days	High	Microsoft Windows 2000, Windows XP
CVE-2006-4688	128 Days	High	Microsoft Server 2003, XP, Windows 2000
CVE-2006-3439	226 Days	High	Microsoft Windows Server 2003, Windows 2000, Windows XP
CVE-2006-2371	282 Days	High	Microsoft Windows Server 2003, Windows 2000, Windows XP

[more]

03 TOP SCANNED SERVICES (past 24 hours)



Key	Service	Traffic per subnet	Latest CVE
	TCP/139 (netbios-ssn)	1.05 MB	CVE-2006-5276
	TCP/445 (microsoft-ds)	941.19 kB	CVE-2006-5276
	ICMP/8	793.97 kB	
	TCP/1433 (ms-sql-s)	585.43 kB	CVE-2004-1560
	UDP/137 (netbios-ns)	228.88 kB	CVE-2004-0445
	other	1.62 MB	

04 TOP THREAT SOURCES (past 24 hours)

COUNTRY | ASN | HOST

Country	Rank	Attacks per subnet	Scans per subnet	Botnets	Phishing	DoS
US (United States)	1	788	964.85 kB	263	1842	6149
CN (China)	2	502	1.06 MB	31	216	542
KR (South Korea)	3	187	856.96 kB	56	4052	5
PL (Poland)	4	632	300.63 kB	4	0	0
TW (Taiwan)	5	90	187.62 kB	27	0	22
FR (France)	6	124	179.05 kB	9	40	59
JP (Japan)	7	56	99.15 kB	11	43	89

malicious website. These downloaders usually appear on a sy
after a browser exploit is used to force their download and
execution. This particular downloader will fetch and run a Bifrc
variant.
Source: TROJ_DELF.DWF

Title: Asterisk SIP Response Code Denial of Service
Severity Level: Normal Severity
Published: Thursday, March 22, 2007 09:44
Another Asterisk SIP denial of service has been found when
handling unexpected data. A SIP reply code of 0 is not handle
properly, and the Asterisk process will crash when a reply wit
code is received. Asterisk has released version 1.4.2 to addr
this issue.
Source: [2/5] Asterisk SIP Response Code Denial of Service

Title: Trojan.BAT.Crash.b
Severity Level: Normal Severity
Published: Thursday, March 22, 2007 05:00
This is a Trojan injected into HTML documents. When the web
is visited, it attempts to start Microsoft HTML Application host
(%System%\mshta.exe), a standard program. Because this is
missing on Windows 98, it may crash the computer.
Source: Trojan.BAT.Crash.b

[more]

What Are Honeypots

A security resource who's value lies in the unauthorized or malicious interaction with it.

Their Value

- Primary value of honeypots is to collect information.
- This information is then used to better identify, understand and protect against threats.
- Honeypots add little direct value to protecting your network.

Different Types

- Server: Put the honeypot on the Internet and let the bad guys come to you.
- Client: Honeypot initiates and interacts with servers
- Other: Honeytokens, Proxies, Honeyfarms

Low vs High Interaction

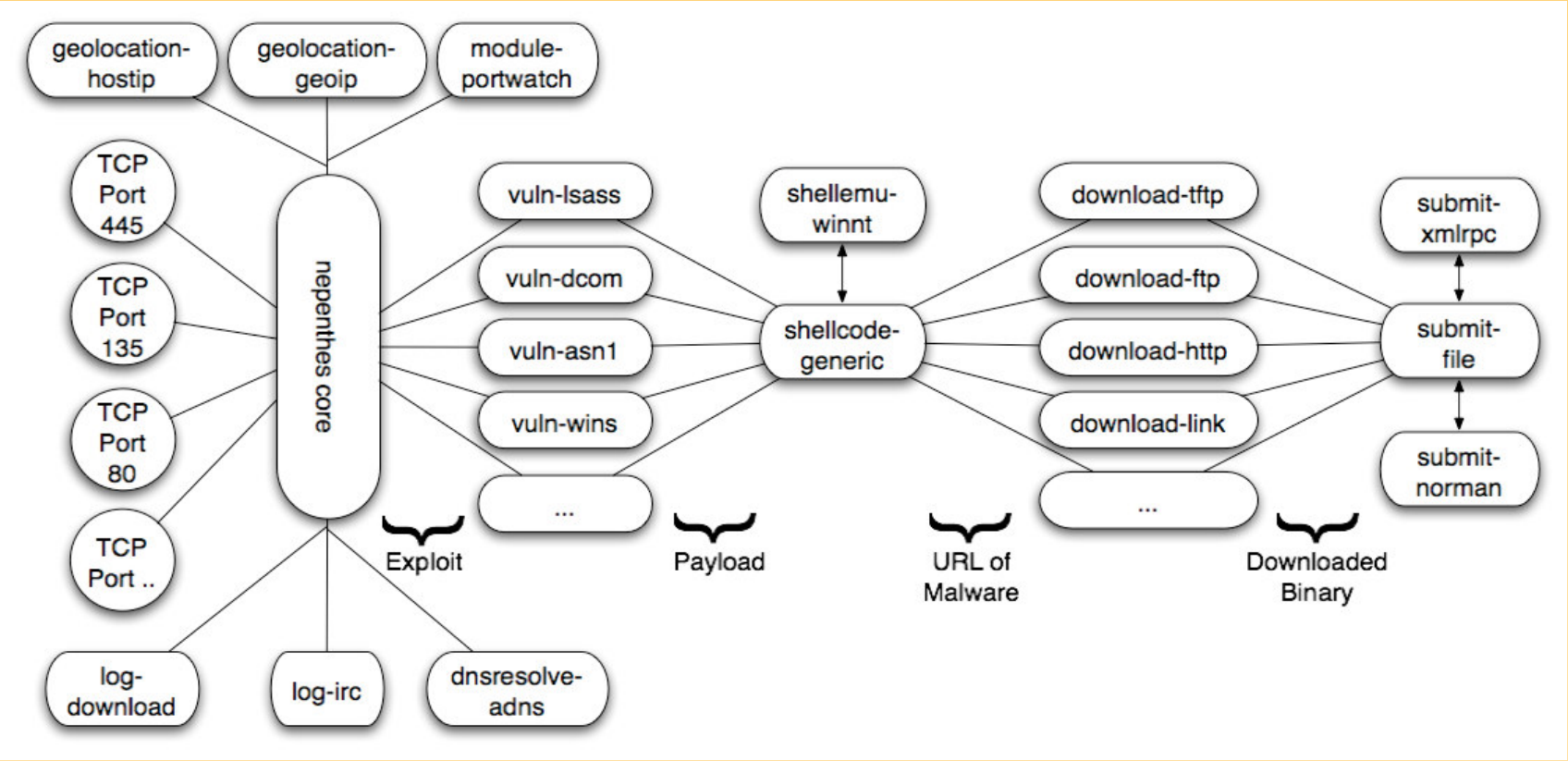
- The amount of activity a threat can have with a honeypot.
- Low-interaction emulates, high-interaction is the real thing.
- Neither solution is better, depends on what you want to achieve.

Low-Interaction Server

Software that emulates functionality. Easier to deploy and automate, less risk, but customized to more specific attacks.

- Nepenthes
- Honeyd
- Honeytrap
- Web Applications
- KFSensor

Nepenthes

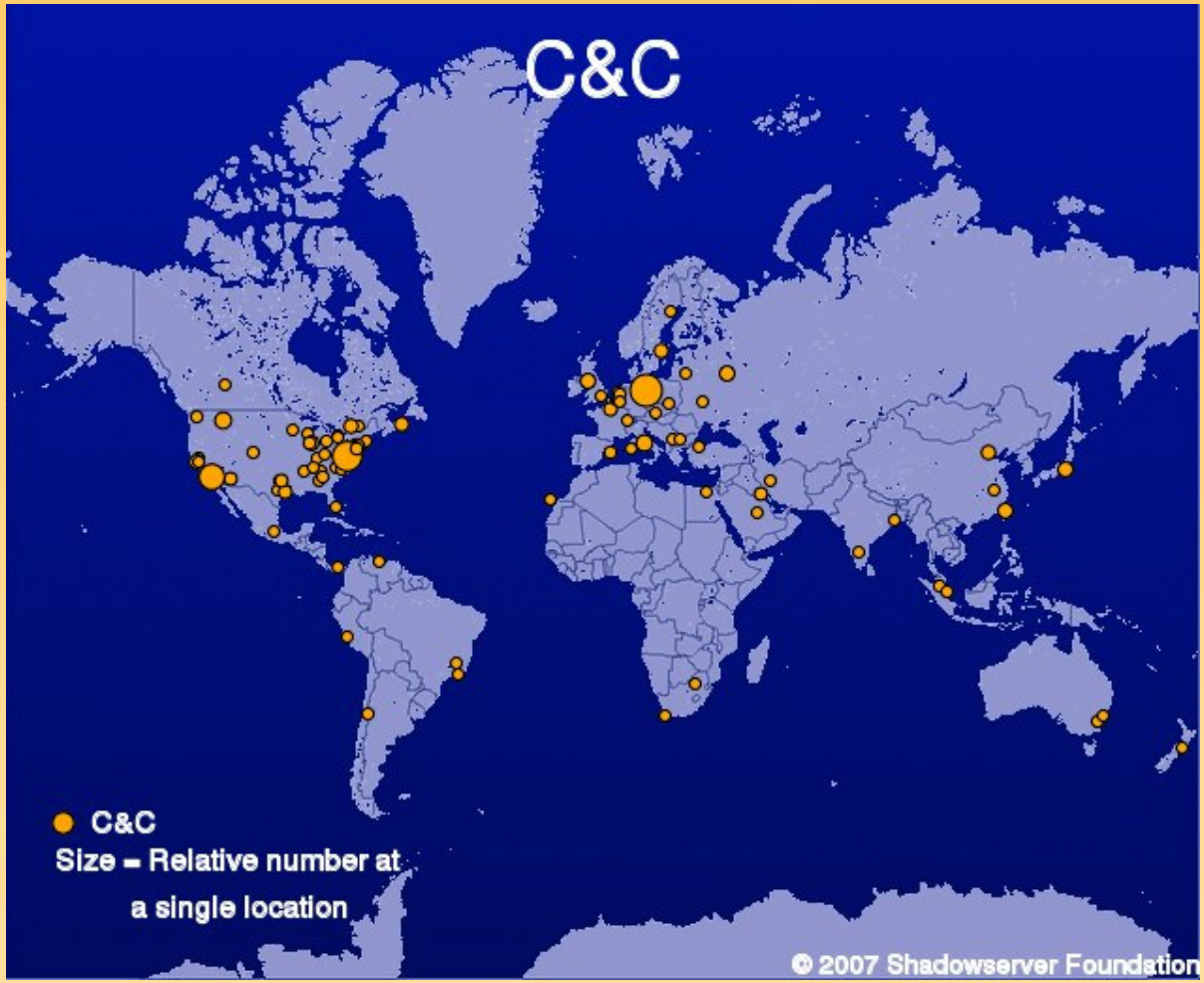

geolocation-hostip
geolocation-geoip
module-portwatch
TCP Port 445
TCP Port 135
TCP Port 80
TCP Port ..
nepenthes core
log-download
log-irc
dnsresolve-adns
vuln-lsass
vuln-dcom
vuln-asn1
vuln-wins
...
Exploit
shellemu-winnt
shellcode-generic
Payload
download-tftp
download-ftp
download-http
download-link
...
URL of Malware
submit-xmlrpc
submit-file
submit-norman
Downloaded Binary

Value: Malware Collection & Botnet Monitoring

- Nepenthes retrieves malware following a successful attack.
- Malware designed to join command channel for remote control.
- Use same information, join with botnet monitoring software.

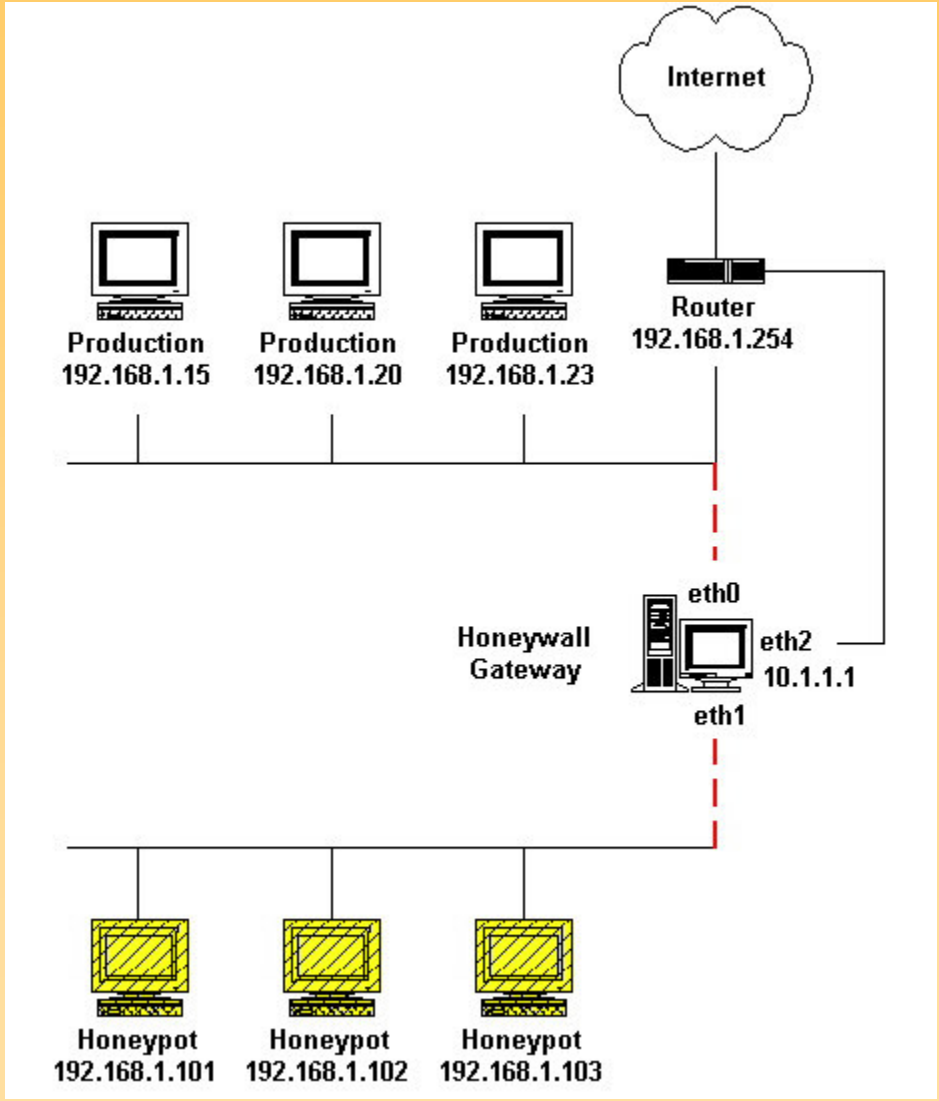
J4ck: why don't you start charging for packet attacks?
J4ck: "give me x amount and I'll take bla bla offline for this amount of time”
J1LL: it was illegal last I checked
J4ck: heh, then everything you do is illegal. Why not make money off of it?
J4ck: I know plenty of people that'd pay exorbatent amounts for packeting

```
ddos.synflood [host] [time] [delay] [port]
starts an SYN flood

ddos.httpflood [url] [number] [referrer] [recursive = true||false]
starts a HTTP flood

scan.listnetranges
list scanned netranges

scan.start
starts all enabled scanners

scan.stop
stops all scanners

http.download
download a file via HTTP

http.execute
updates the bot via the given HTTP URL

http.update
executes a file from a given HTTP URL

cvar.set spam_aol_channel [channel]
AOL Spam - Channel name

cvar.set spam_aol_enabled [1/0]
AOL Spam - Enabled?
```


C&C
C&C
Size = Relative number at a single location
© 2007 Shadowserver Foundation

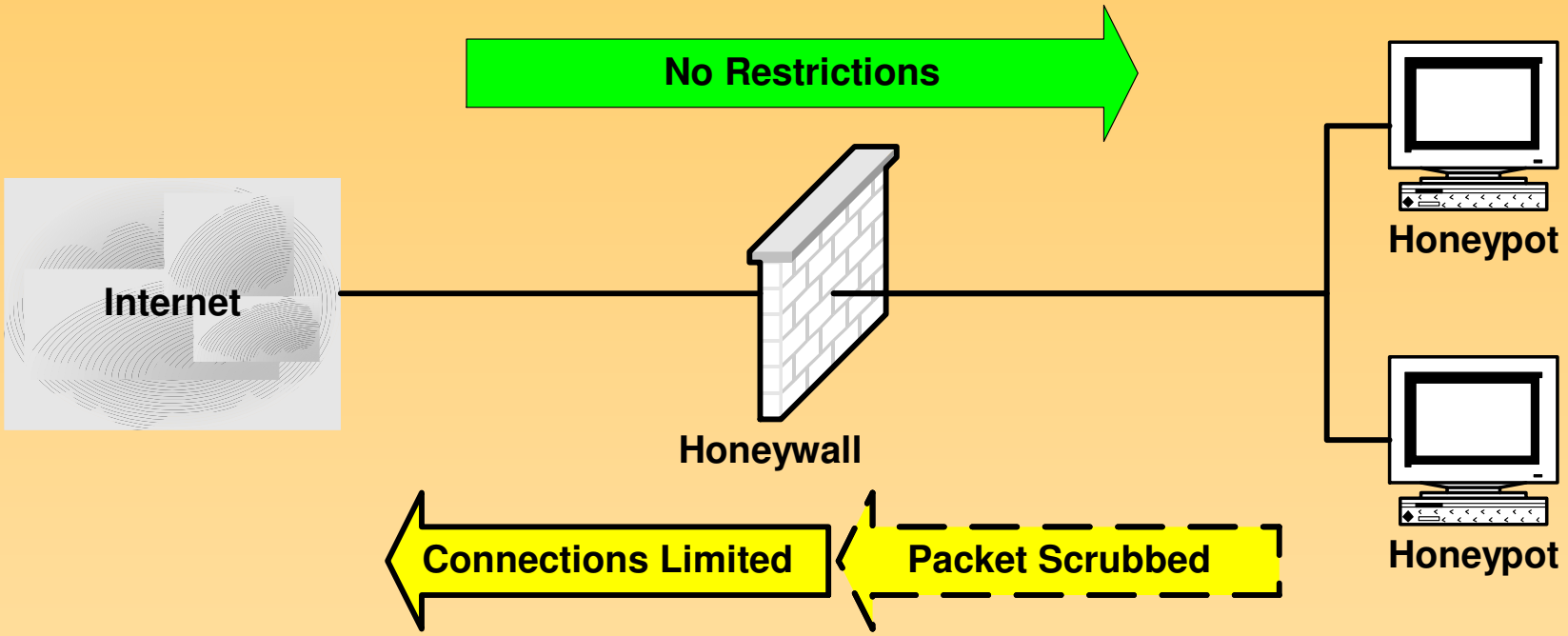
High-Interaction Servers

Typically real applications on real systems. Much more manual work, but more flexible in the data and threats it can capture.


Internet
Router
192.168.1.254
Production
192.168.1.15
Production
192.168.1.20
Production
192.168.1.23
eth0
Honeywall
Gateway
eth2
10.1.1.1
eth1
Honeypot
192.168.1.101
Honeypot
192.168.1.102
Honeypot
192.168.1.103

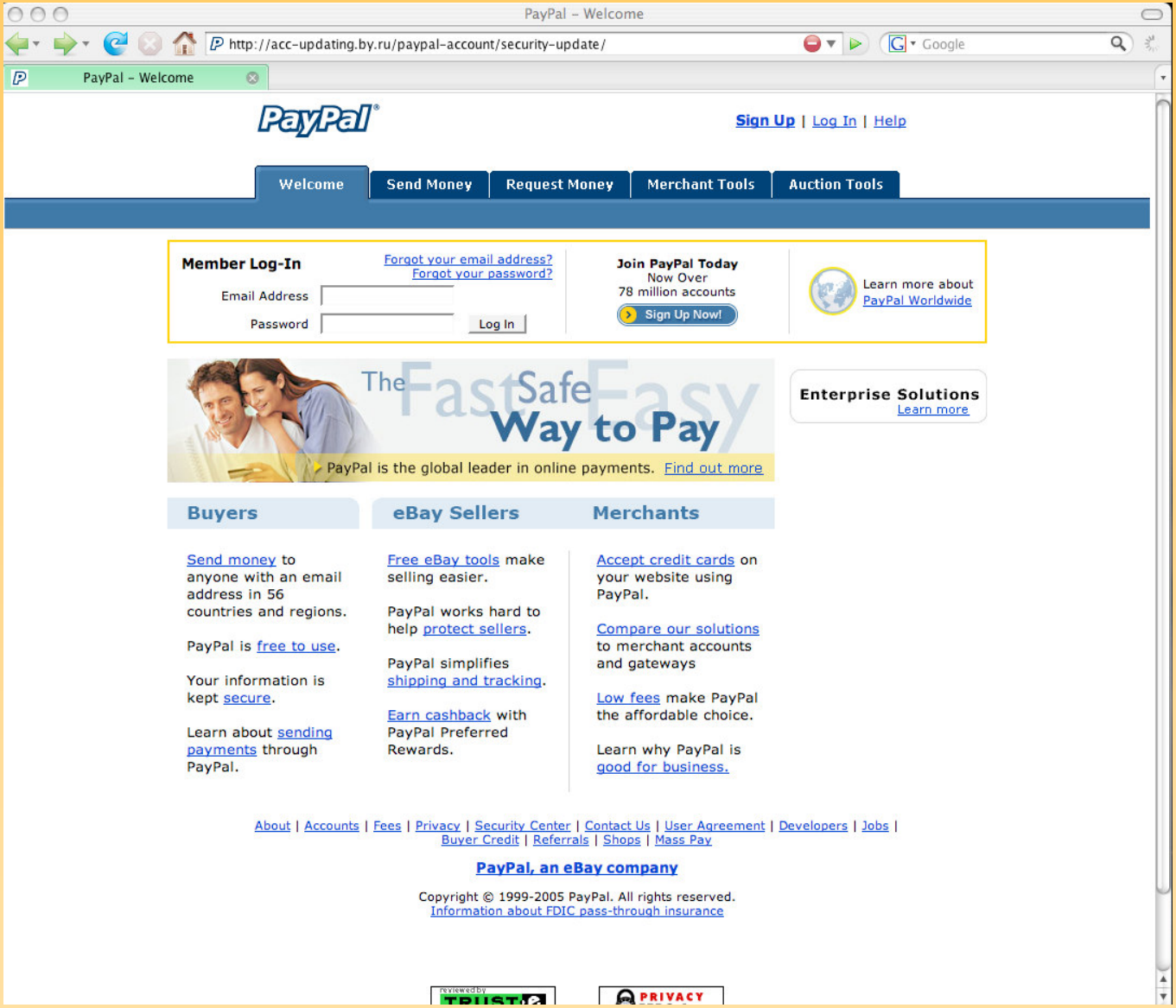
No Data Control

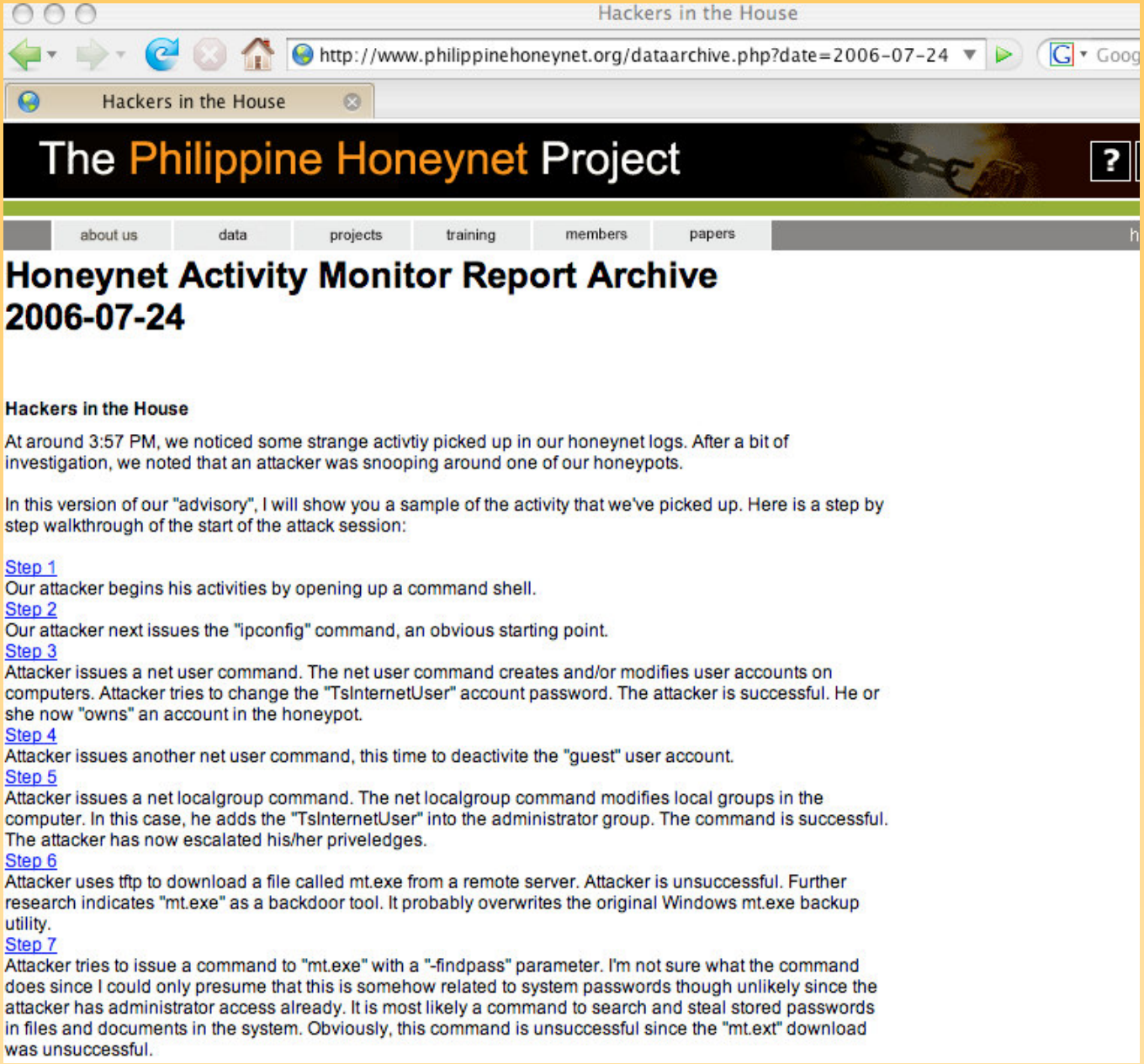
Data Control



Phishing Server

```
-rw-r--r--   1 free     web 14834 Jun 17 13:16 ebay only
-rw-r--r--   1 free     web 247127 Jun 14 19:58 emailer2.zip
-rw-r--r--   1 free     web 7517 Jun 11 11:53 html1.zip
-rw-r--r--   1 free     web 10383 Jul  3 19:07 index.html
-rw-r--r--   1 free     web 413 Jul 18 22:09 index.zip
-rw-r--r--   1 free     web 246920 Jun 14 20:38 massmail.tgz
-rw-r--r--   1 free     web 8192 Jun 12 07:18 massmail.zip
-rw-r--r--   1 free     web 12163 Jun  9 01:31 send.php
-rw-r--r--   1 free     web 2094 Jun 20 11:49 sendspamAOL1.tgz
-rw-r--r--   1 free     web 2173 Jun 14 22:58 sendspamBUN1.tgz
-rw-r--r--   1 free     web 2783 Jun 15 00:21 sendspamBUNzip1.zip
-rw-r--r--   1 free     web 2096 Jun 16 18:46 sendspamNEW1.tgz
-rw-r--r--   1 free     web 1574 Jul 11 01:08 sendbank1.tgz
-rw-r--r--   1 free     web 2238 Jul 18 23:07 sendbankNEW.tgz
-rw-r--r--   1 free     web 83862 Jun  9 09:56 spamz.zip
-rw-r--r--   1 free     web 36441 Jul 18 00:52 usNEW.zip
-rw-r--r--   1 free     web 36065 Jul 11 17:04 bank1.tgz
drwxr-xr-x   2 free     web 49 Jul 16 12:26 banka
-rw-r--r--   1 free     web 301939 Jun  8 13:17 www1.tar.gz
-rw-r--r--   1 free     web 327380 Jun  7 16:24 www1.zip
```


PayPal – Welcome
http://acc-updating.by.ru/paypal-account/security-update/
PayPal – Welcome
PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Tools
Auction Tools
Member Log-In
Forgot your email address?
Forgot your password?
Email Address
Password
Log In
Join PayPal Today
Now Over
78 million accounts
Sign Up Now!
Learn more about
PayPal Worldwide
The Fast Safe Easy
Way to Pay
PayPal is the global leader in online payments. Find out more
Enterprise Solutions
Learn more
Buyers
eBay Sellers
Merchants
Send money to anyone with an email address in 56 countries and regions.
PayPal is free to use.
Your information is kept secure.
Learn about sending payments through PayPal.
Free eBay tools make selling easier.
PayPal works hard to help protect sellers.
PayPal simplifies shipping and tracking.
Earn cashback with PayPal Preferred Rewards.
Accept credit cards on your website using PayPal.
Compare our solutions to merchant accounts and gateways
Low fees make PayPal the affordable choice.
Learn why PayPal is good for business.
About | Accounts | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs | Buyer Credit | Referrals | Shops | Mass Pay
PayPal, an eBay company
Copyright © 1999-2005 PayPal. All rights reserved.
Information about FDIC pass-through insurance
PRIVACY


Hackers in the House
http://www.philippinehoneynet.org/dataarchive.php?date=2006-07-24
Hackers in the House
The Philippine Honeynet Project
about us
data
projects
training
members
papers
Honeynet Activity Monitor Report Archive
2006-07-24
Hackers in the House
At around 3:57 PM, we noticed some strange activtiy picked up in our honeynet logs. After a bit of investigation, we noted that an attacker was snooping around one of our honeypots.
In this version of our "advisory", I will show you a sample of the activity that we've picked up. Here is a step by step walkthrough of the start of the attack session:
Step 1
Our attacker begins his activities by opening up a command shell.
Step 2
Our attacker next issues the "ipconfig" command, an obvious starting point.
Step 3
Attacker issues a net user command. The net user command creates and/or modifies user accounts on computers. Attacker tries to change the "TsInternetUser" account password. The attacker is successful. He or she now "owns" an account in the honeypot.
Step 4
Attacker issues another net user command, this time to deactivite the "guest" user account.
Step 5
Attacker issues a net localgroup command. The net localgroup command modifies local groups in the computer. In this case, he adds the "TsInternetUser" into the administrator group. The command is successful. The attacker has now escalated his/her priveledges.
Step 6
Attacker uses tftp to download a file called mt.exe from a remote server. Attacker is unsuccessful. Further research indicates "mt.exe" as a backdoor tool. It probably overwrites the original Windows mt.exe backup utility.
Step 7
Attacker tries to issue a command to "mt.exe" with a "-findpass" parameter. I'm not sure what the command does since I could only presume that this is somehow related to system passwords though unlikely since the attacker has administrator access already. It is most likely a command to search and steal stored passwords in files and documents in the system. Obviously, this command is unsuccessful since the "mt.ext" download was unsuccessful.

Client Based Honeypots

Threats change, and so to do the technologies. Bad guys have moved to client based attacks, they let the victims come to them.

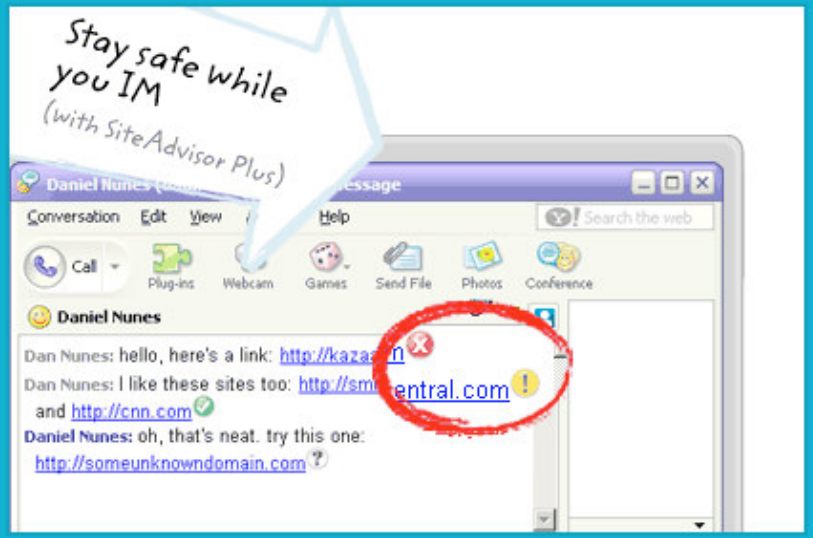
- Capture-HPC (high interaction)
- HoneyC (low interaction)
- Microsoft Strider Honeymonkey

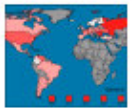
McAfee SiteAdvisor™

HOME | DOWNLOAD | ANALYSIS | SUPPORT | BLOG | ABOUT US

We test the Web to help keep you safe from spyware, spam, viruses and online scams.

- Why trust us?
- Why isn't the security software you already have enough?
- Do sites pay us to be rated?





Mapping the Mal Web:
Which domains are the riskiest?

Download SiteAdvisor now
For Firefox
It's free!

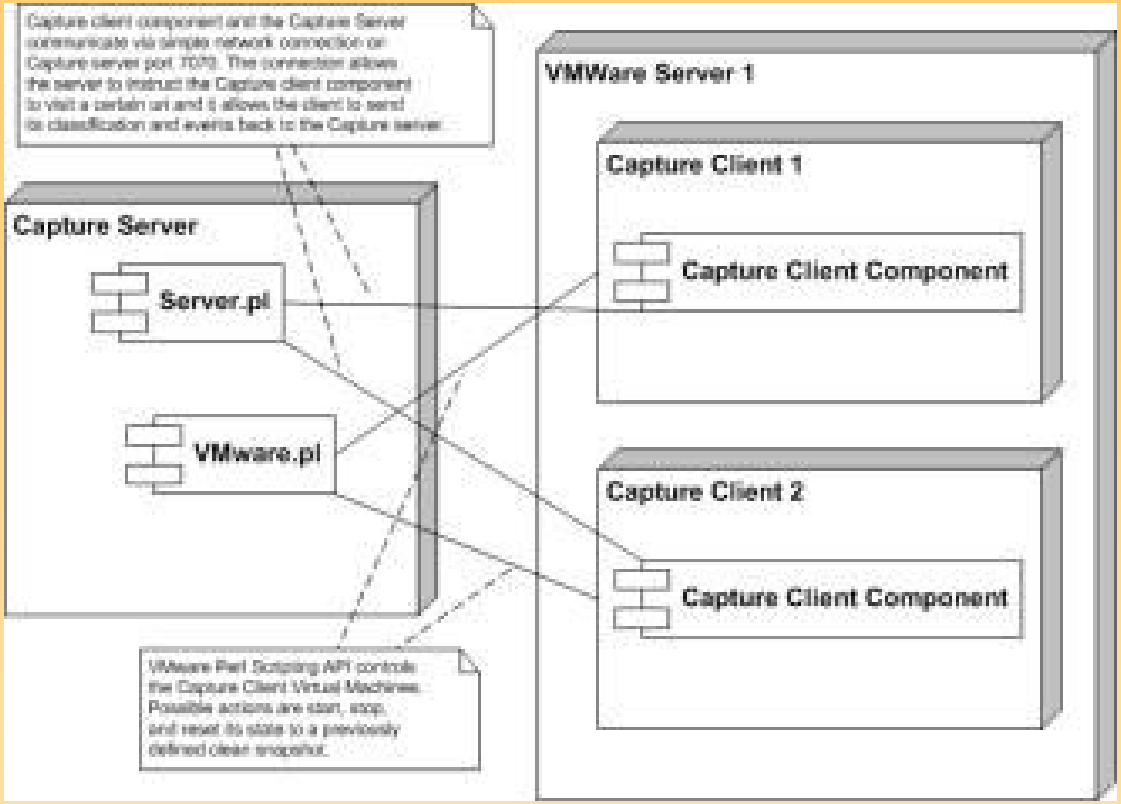
Be a Web safety hero:
Play SiteAdvisor WebQuest!

Look up a site report: Enter a site address (e.g. yahoo.com) Go

Home | Download | Analysis | Support | About us | Privacy policy | Terms of service | Sitemap | Blog

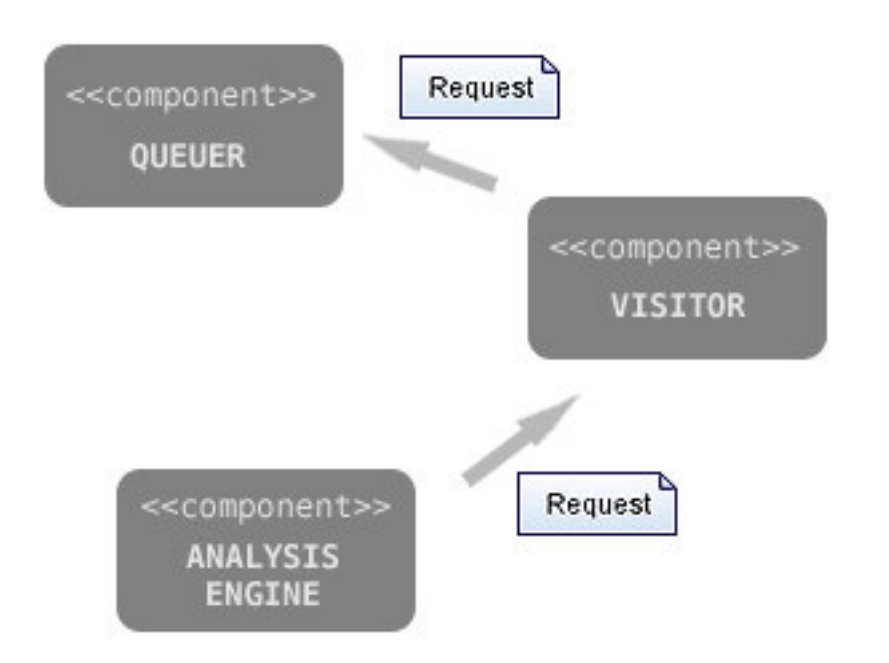
Pick a language

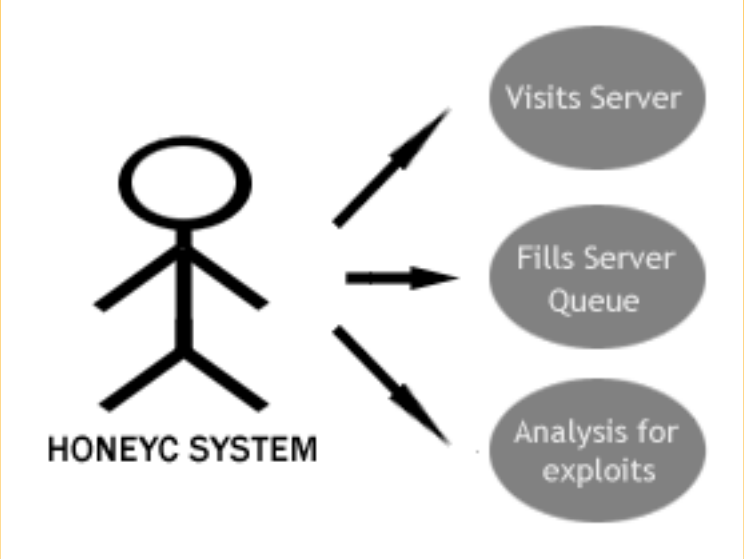
Capture-HPC



http://www.nz-honeynet.org/capture.html

HoneyC





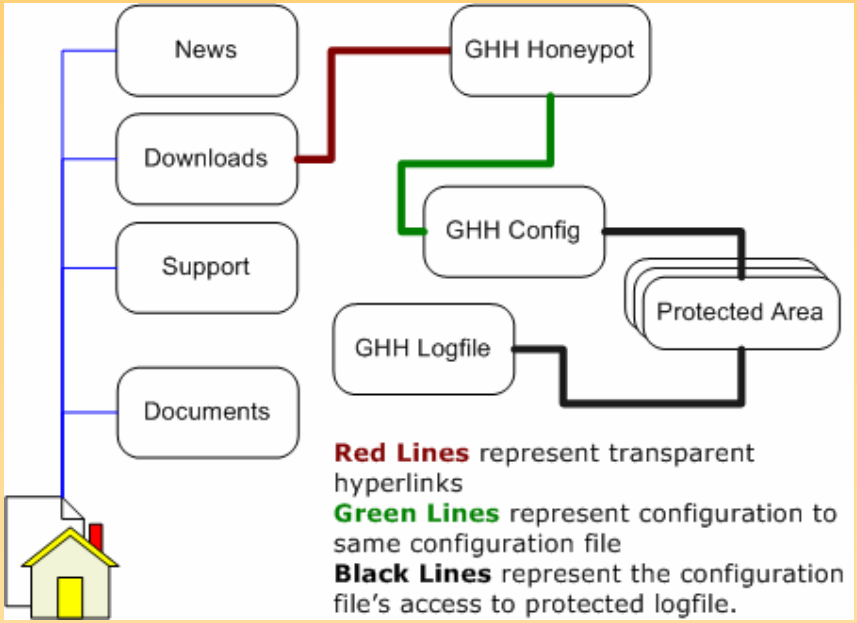
http://www.nz-honeynet.org/honeyc.html

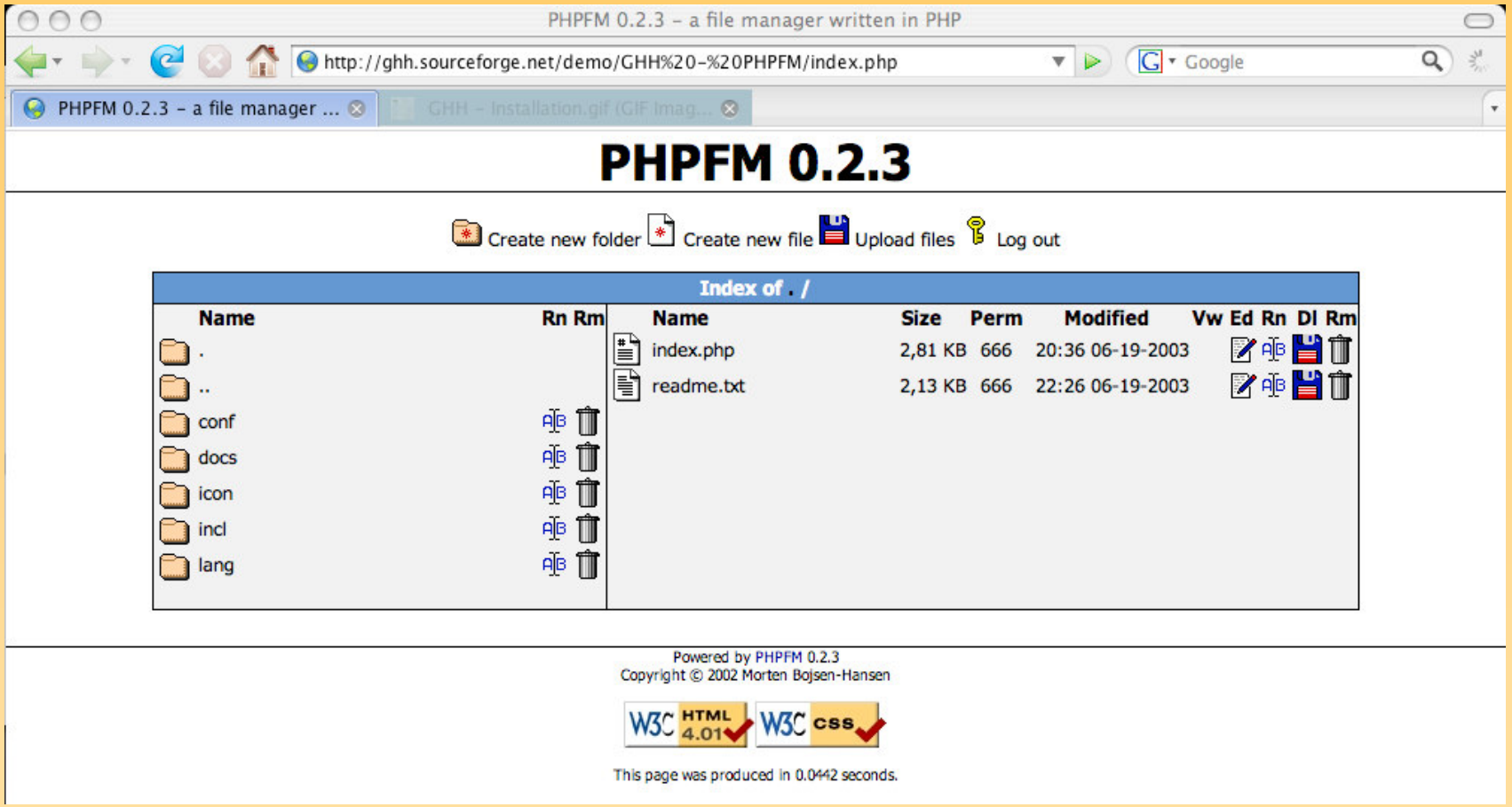
Microsoft Strider HoneyMonkey

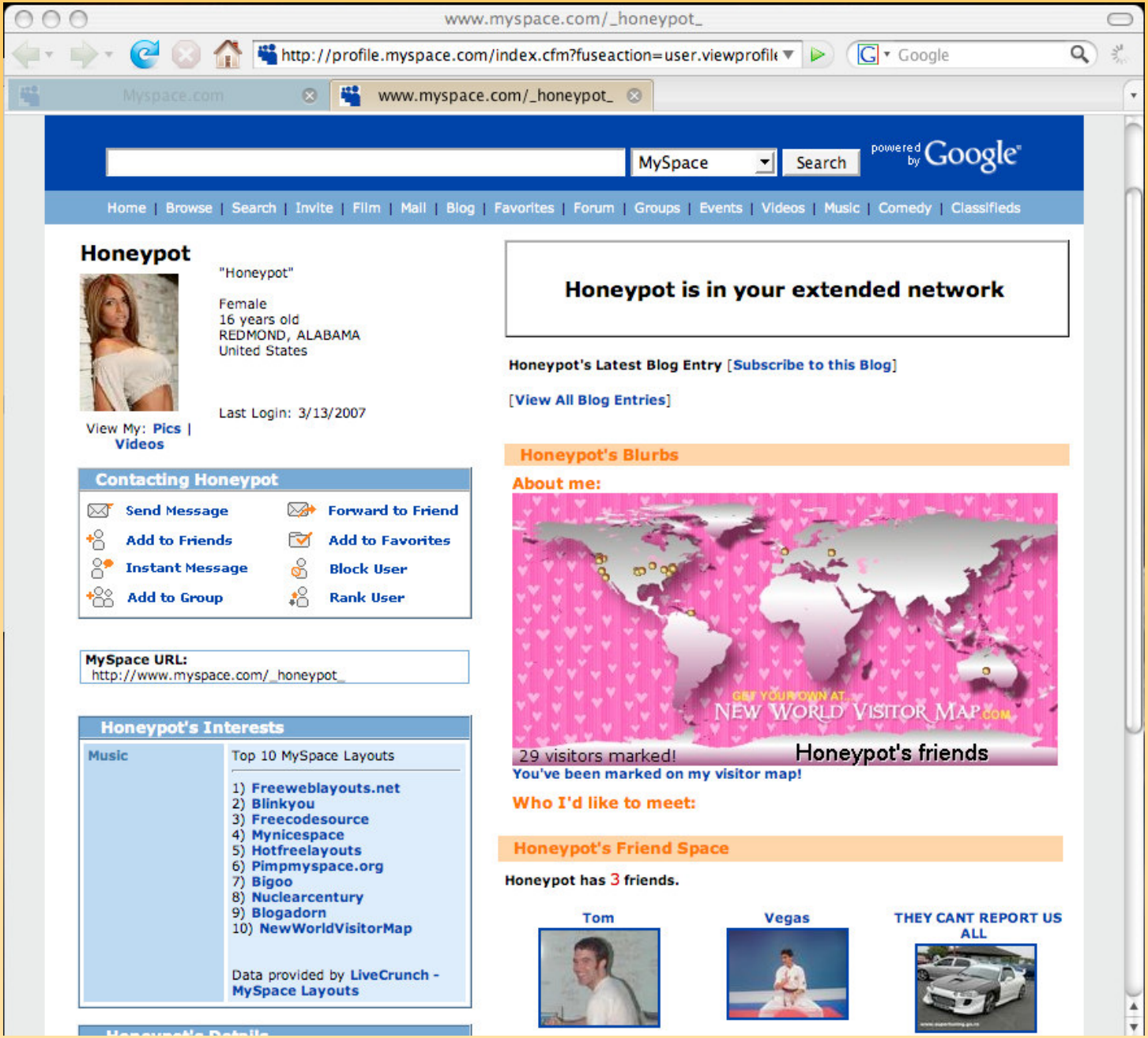
Other

- Web 2.0 - Fake Myspace accounts
- Google Honeypot (search engine entries)
- Honeyfarms - Honeymole
- Honeytokens
- Proxy Honeypots
- Anti-Spam Honeypots

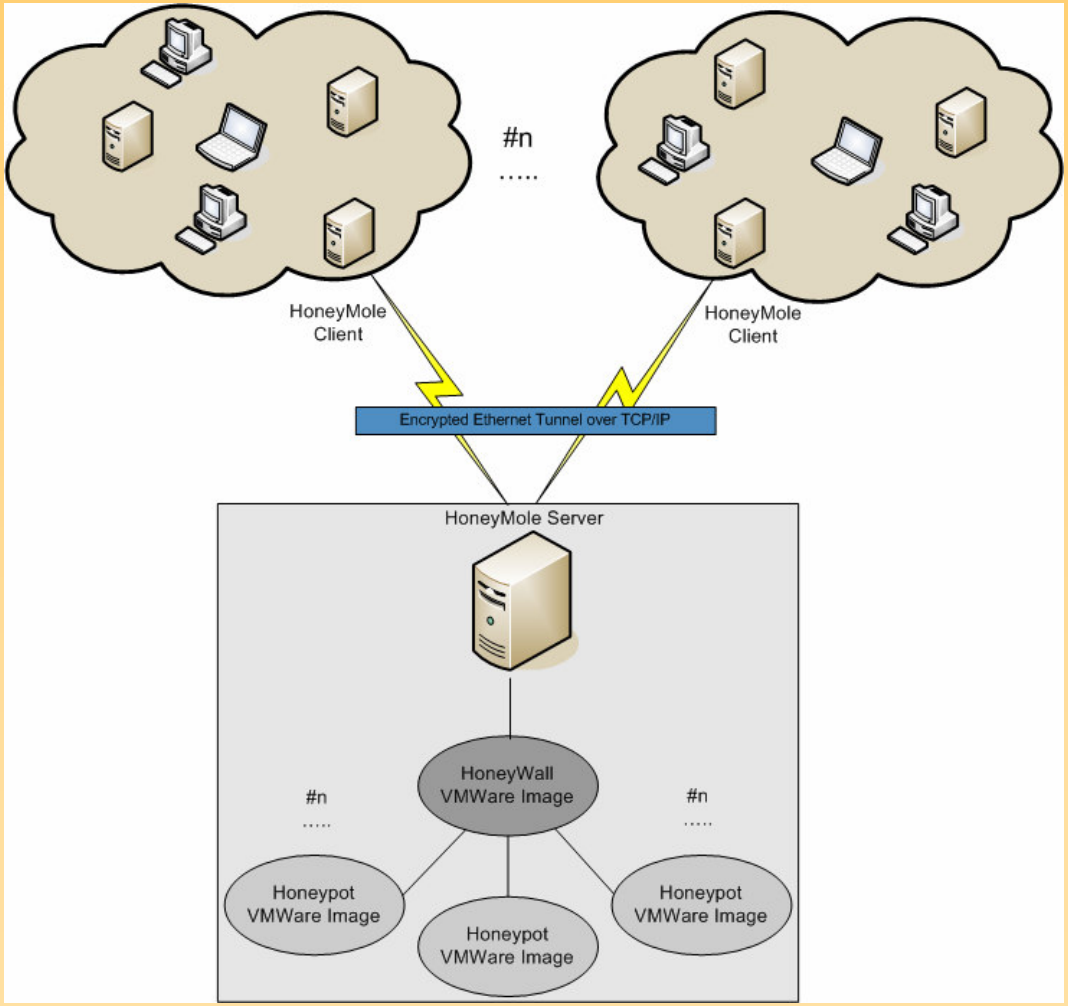
Google Honeypot



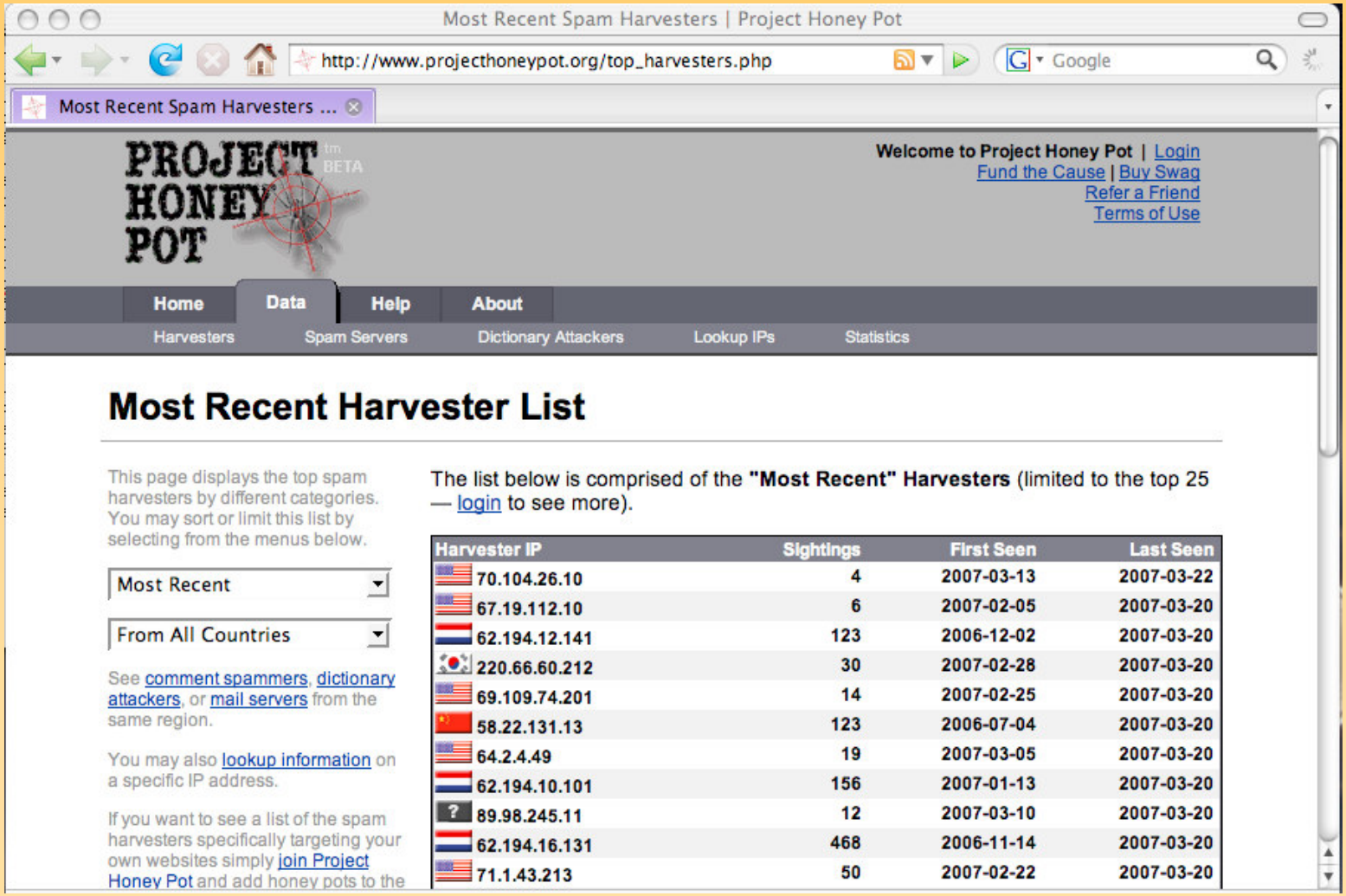

PHPFM 0.2.3 - a file manager written in PHP
http://ghh.sourceforge.net/demo/GHH%20-%20PHPFM/index.php
Google
PHPFM 0.2.3 - a file manager ...
GHH - Installation.gif (GIF Imag...
PHPFM 0.2.3
Create new folder
Create new file
Upload files
Log out
Index of . /
Name
Rn Rm
.
..
conf
docs
icon
incl
lang
Name
Size
Perm
Modified
Vw Ed Rn Dl Rm
index.php
2,81 KB
666
20:36 06-19-2003
readme.txt
2,13 KB
666
22:26 06-19-2003
Powered by PHPFM 0.2.3
Copyright © 2002 Morten Bojsen-Hansen
W3C HTML 4.01
W3C CSS
This page was produced in 0.0442 seconds.


www.myspace.com/_honeypot_
http://profile.myspace.com/index.cfm?fuseaction=user.viewprofile
Google
Myspace.com
www.myspace.com/_honeypot_
MySpace
Search
powered by Google
Home | Browse | Search | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds
Honeypot
"Honeypot"
Female
16 years old
REDMOND, ALABAMA
United States
Last Login: 3/13/2007
View My: Pics | Videos
Contacting Honeypot
Send Message
Forward to Friend
Add to Friends
Add to Favorites
Instant Message
Block User
Add to Group
Rank User
MySpace URL:
http://www.myspace.com/_honeypot_
Honeypot's Interests
Music
Top 10 MySpace Layouts
1) Freewebslayouts.net
2) Blinkyou
3) Freecodesource
4) Mynicespace
5) Hotfreelayouts
6) Pimpmyspace.org
7) Bigoo
8) Nuclearcentury
9) Blogadorn
10) NewWorldVisitorMap
Data provided by LiveCrunch - MySpace Layouts
Honeypot is in your extended network
Honeypot's Latest Blog Entry [Subscribe to this Blog]
[View All Blog Entries]
Honeypot's Blurbs
About me:
GET YOUR OWN AT NEW WORLD VISITOR MAP.COM
29 visitors marked!
Honeypot's friends
You've been marked on my visitor map!
Who I'd like to meet:
Honeypot's Friend Space
Honeypot has 3 friends.
Tom
Vegas
THEY CANT REPORT US ALL

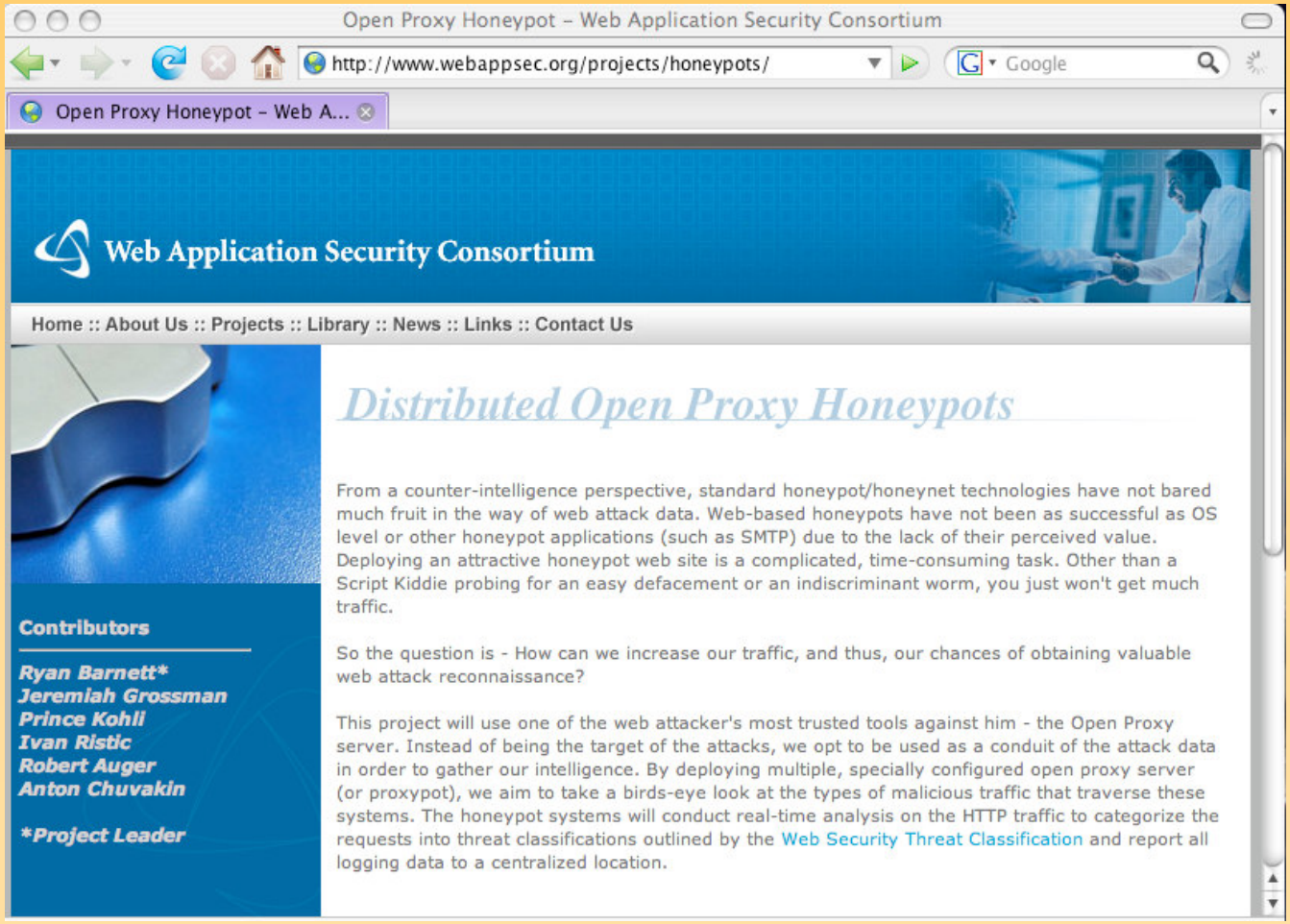
Honeymole


#n
.....
HoneyMole
Client
HoneyMole
Client
Encrypted Ethernet Tunnel over TCP/IP
HoneyMole Server
HoneyWall
VMWare Image
#n
.....
#n
.....
Honeypot
VMWare Image
Honeypot
VMWare Image
Honeypot
VMWare Image

Spam Honeytokens



Proxy Honeypot



Future

- Continue to grow in use, but not in the public eye.
- Continue to diversify, solutions designed around specific threats.
- Better automated data analysis.

Summary

- Honeypots very powerful and heavily used, but not widely known.
- Many different types, each with own advantages and disadvantages.

Contact Us

http://www.honeynet.org

<project@honeynet.org>