The Honeynet Project

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.
How lucrative is pump-and-dump spam?

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

Over the last month, Moriaty, 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 $25,810.

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 Moriaty'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," Moriaty said in an interview.

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

On the other hand, if the were to have fallen victim to "hot stock" e-mail tips and invested and held, Moriaty's portfolio would have been down 27.5 percent.

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 Paul (Computeworld) 22 February, 2007 12:36:28

Up to 80 percent of all e-mails will be spam by the end of this year, according to research released yesterday.

Security vendor Marsha'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.
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
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 exorbitant 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?
High-Interaction Servers

Typically real applications on real systems. Much more manual work, but more flexible in the data and threats it can capture.
No Data Control

Internet

No Restrictions

No Restrictions

Honeypot

Honeypot
Data Control

Internet

No Restrictions

Honeywall

Connections Limited

Packet Scrubbed

Honeypot

Honeypot
Phishing Server
Honeynet Activity Monitor Report Archive
2006-07-24

Hackers in the House
At around 3:57 PM, we noticed some strange activity 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. Attackers try 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 disable 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 privileges.
Step 6
Attacker uses FTP to download a file called mt.exe from a remote server. Attackers 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 "mtext" downloaded 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™

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 iciest?

Be a Web safety hero:
Play SiteAdvisor WebQuest!

Download SiteAdvisor now
For Firefox

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

- **Red Lines** represent transparent hyperlinks
- **Green Lines** represent configuration to same configuration file
- **Black Lines** represent the configuration file’s access to protected logfile.
## PHPFM 0.2.3

### Index of /.

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Perm</th>
<th>Modified</th>
<th>Vw</th>
<th>Ed</th>
<th>Rn</th>
<th>Dl</th>
<th>Rm</th>
</tr>
</thead>
<tbody>
<tr>
<td>index.php</td>
<td>2.81 KB</td>
<td>666</td>
<td>20:36 06-19-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>readme.txt</td>
<td>2.13 KB</td>
<td>666</td>
<td>22:26 06-19-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Create new folder
- Create new file
- Upload files
- Log out

Powered by PHPFM 0.2.3

Copyright © 2002 Morten Bojsen-Hansen

This page was produced in 0.0942 seconds.
Honeymole
Spam Honeytokens

Most Recent Harvester List

This page displays the top spam harvesters by different categories. You may sort or limit this list by selecting from the menus below.

Most Recent
From All Countries

See comment spammers, dictionary spammers, or mail servers from the same region.

You may also lookup information on a specific IP address.

If you want to see a list of the spam harvesters specifically targeting your own websites simply join Project Honey Pot and add honey pots to the

The list below is comprised of the "Most Recent" Harvesters (limited to the top 25 — login to see more).

<table>
<thead>
<tr>
<th>Harvester IP</th>
<th>Sightings</th>
<th>First Seen</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>70.104.26.10</td>
<td>4</td>
<td>2007-03-13</td>
<td>2007-03-22</td>
</tr>
<tr>
<td>67.19.112.10</td>
<td>6</td>
<td>2007-02-05</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>62.194.12.141</td>
<td>123</td>
<td>2006-12-02</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>220.66.60.212</td>
<td>30</td>
<td>2007-02-28</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>69.109.74.201</td>
<td>14</td>
<td>2007-02-25</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>58.22.131.13</td>
<td>123</td>
<td>2006-07-04</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>64.2.4.49</td>
<td>19</td>
<td>2007-03-05</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>62.194.10.101</td>
<td>156</td>
<td>2007-01-13</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>89.98.245.11</td>
<td>12</td>
<td>2007-03-10</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>62.194.16.131</td>
<td>468</td>
<td>2006-11-14</td>
<td>2007-03-20</td>
</tr>
<tr>
<td>71.1.43.213</td>
<td>50</td>
<td>2007-02-22</td>
<td>2007-03-20</td>
</tr>
</tbody>
</table>
Proxy Honeypot

Distributed Open Proxy Honeypots

From a counter-intelligence perspective, standard honeypot/honeynet technologies have not bore much fruit in the way of web attack data. Web-based honeypots have not been as successful as OS level or other honeypot applications (such as SMTP) due to the lack of their perceived value.

Deploying an attractive honeypot web site is a complicated, time-consuming task. Other than a Script Kiddie probing for an easy defacement or an indiscriminate worm, you just won't get much traffic.

So the question is - How can we increase our traffic, and thus, our chances of obtaining valuable web attack reconnaissance?

This project will use one of the web attacker's most trusted tools against him - the Open Proxy server. Instead of being the target of the attacks, we opt to be used as a conduit of the attack data in order to gather our intelligence. By deploying multiple, specially configured open proxy servers (or proxyps), we aim to take a bird's-eye look at the types of malicious traffic that traverse these systems. The honeypot systems will conduct real-time analysis on the HTTP traffic to categorize the requests into threat classifications outlined by the Web Security Threat Classification and report all logging data to a centralized location.
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>