Security Engineering

2. Attack tools. Malicious software

COSEC
www.seg.inf.uc3m.es

CHAPTER 2. Programme

1. Attack tools. Features and types
2. Malicious software. Classification
3. Kits, Cryptovirus, APT

CYBERATTACKS. Stages and procedures

Scanning of networks, systems and services

Identification of vulnerabilities

Exploitation, consolidation and spread Harvesting, handling and inspection of network

traffic

Code injection attacks Denial of

service attacks

Malware

Social engineering

CHAPTER 2. Programme

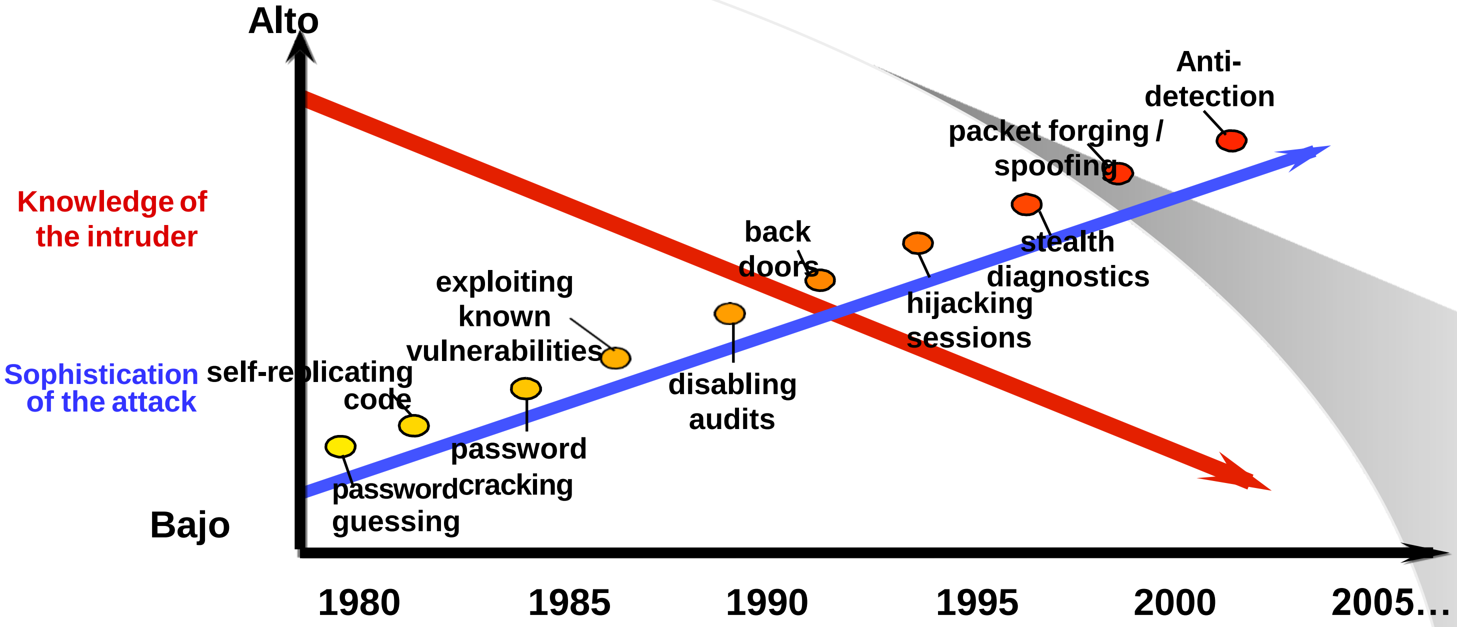
1. Attack tools. Features and types
   - Sophisticated
   - Automated
   - Social Engineering
2. Malicious software. Classification
3. Kits, Cryptovirus, APT

HYBRID TOOLS. Spyware

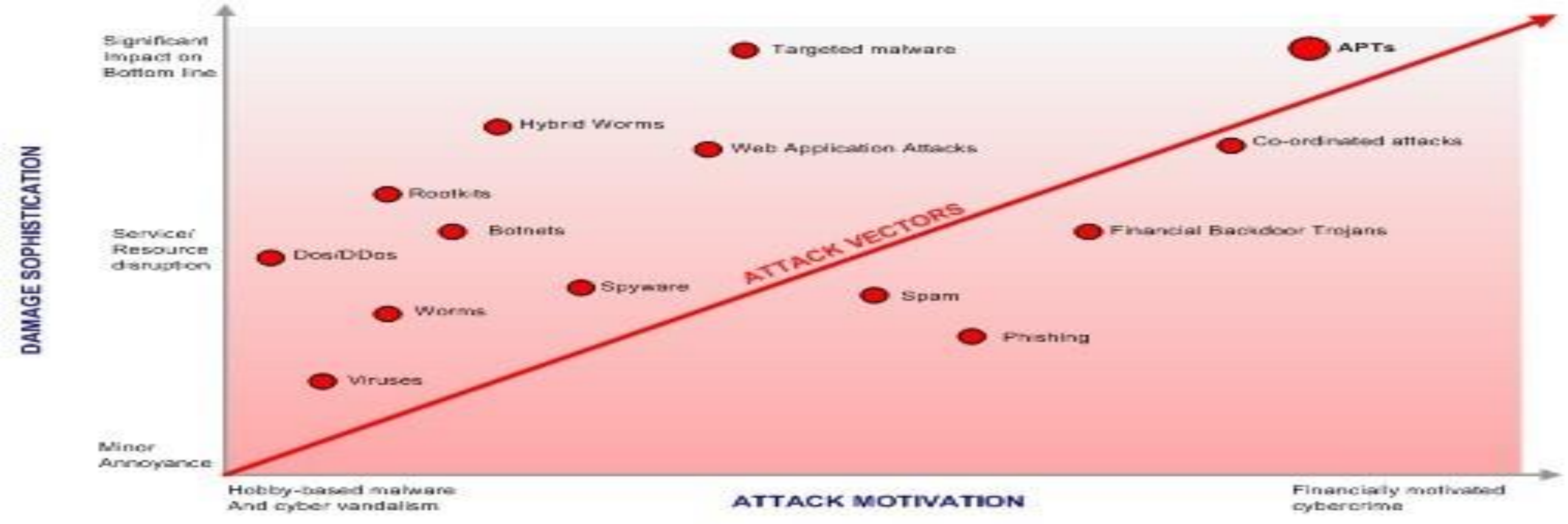
Usually malicious software, included in downloaded Internet software, that get installed on your computer, collecting information from your browsing habits or keystrokes, in order to send it to its creator

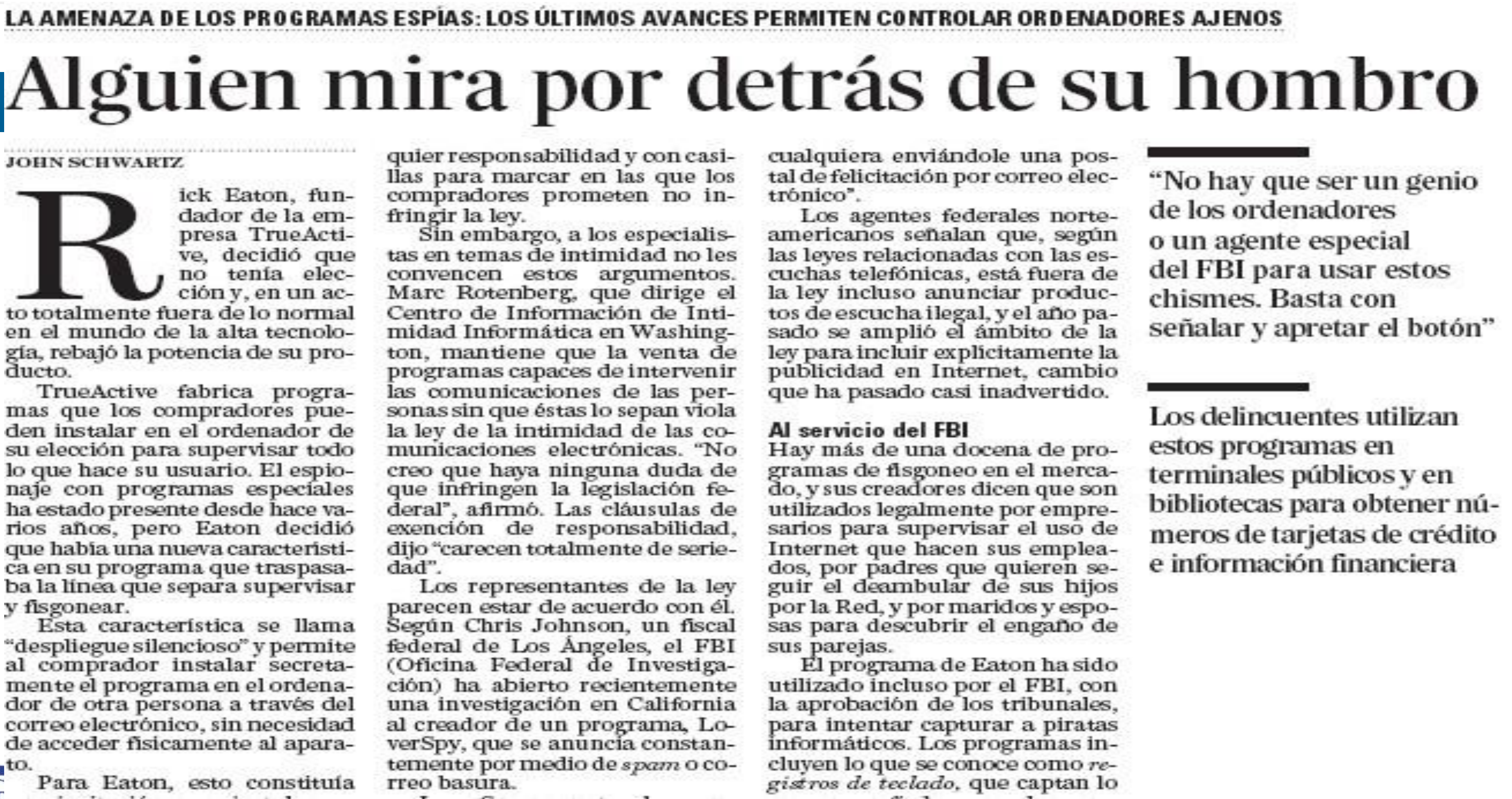
HYBRID TOOLS. Spyware

SOPHISTICATION. Attack vs. knowledge



SOPHISTICATION vs. MOTIVATION





LA AMENAZA DE LOS PROGRAMAS ESPÍAS: LOS ÚLTIMOS AVANCES PERMITEN CONTROLAR ORDENADORES AJENOS

Alguien mira por detrás de su hombro

JOHN SCHWARTZ

Rick Eaton, fundador de la empresa TrueActive, decidió que no tenía elección y, en un acto totalmente fuera de lo normal en el mundo de la alta tecnología, rebajó la potencia de su producto.

TrueActive fabrica programas que los compradores pueden instalar en el ordenador de su elección para supervisar todo lo que hace su usuario. El espionaje con programas especiales ha estado presente desde hace varios años, pero Eaton decidió que había una nueva característica en su programa que traspasaba la línea que separa supervisar y fisgonear.

Esta característica se llama "despliegue silencioso" y permite al comprador instalar secretamente el programa en el ordenador de otra persona a través del correo electrónico, sin necesidad de acceder físicamente al aparato.

Para Eaton, esto constituía

quier responsabilidad y con casillas para marcar en las que los compradores prometen no infringir la ley.

Sin embargo, a los especialistas en temas de intimidad no les convencen estos argumentos. Marc Rotenberg, que dirige el Centro de Información de Intimidad Informática en Washington, mantiene que la venta de programas capaces de intervenir las comunicaciones de las personas sin que éstas lo sepan viola la ley de la intimidad de las comunicaciones electrónicas. "No creo que haya ninguna duda de que infringen la legislación federal", afirmó. Las cláusulas de exención de responsabilidad, dijo "carecen totalmente de seriedad".

Los representantes de la ley parecen estar de acuerdo con él. Según Chris Johnson, un fiscal federal de Los Ángeles, el FBI (Oficina Federal de Investigación) ha abierto recientemente una investigación en California al creador de un programa, LoverSpy, que se anuncia constantemente por medio de *spam* o correo basura.

cualquiera enviándole una postal de felicitación por correo electrónico".

Los agentes federales norteamericanos señalan que, según las leyes relacionadas con las escuchas telefónicas, está fuera de la ley incluso anunciar productos de escucha ilegal, y el año pasado se amplió el ámbito de la ley para incluir explícitamente la publicidad en Internet, cambio que ha pasado casi inadvertido.

Al servicio del FBI

Hay más de una docena de programas de fisgoneo en el mercado, y sus creadores dicen que son utilizados legalmente por empresarios para supervisar el uso de Internet que hacen sus empleados, por padres que quieren seguir el deambular de sus hijos por la Red, y por maridos y esposas para descubrir el engaño de sus parejas.

El programa de Eaton ha sido utilizado incluso por el FBI, con la aprobación de los tribunales, para intentar capturar a piratas informáticos. Los programas incluyen lo que se conoce como *registros de teclado*, que captan lo

"No hay que ser un genio de los ordenadores o un agente especial del FBI para usar estos chismes. Basta con señalar y apretar el botón"

Los delincuentes utilizan estos programas en terminales públicos y en bibliotecas para obtener números de tarjetas de crédito e información financiera

CHAPTER 2. Programme

1. Attack tools. Features and types
   - Sophisticated
   - **Automated**
   - Social Engineering
2. Malicious software. Classification
3. Kits, Cryptovirus, APT

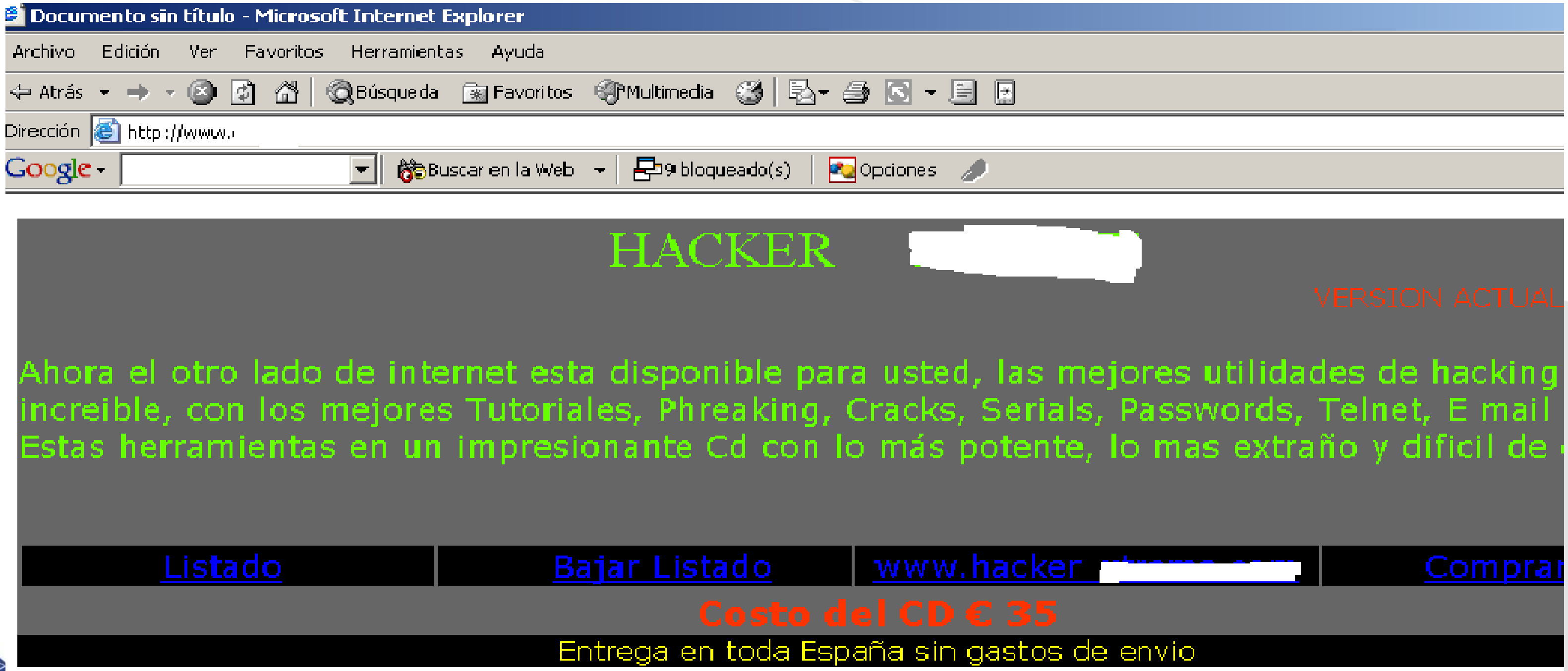
AUTOMATED TOOL: Evolution

Script Kiddies

Exploiting of specific vulnerabilities

Attack kits (interlocking modules)

AUTOMATED TOOLS: Eg



HACKER [redacted]

VERSION ACTUAL

Ahora el otro lado de internet esta disponible para usted, las mejores utilidades de hacking
increible, con los mejores Tutoriales, Phreaking, Cracks, Serials, Passwords, Telnet, E mail
Estas herramientas en un impresionante Cd con lo más potente, lo mas extraño y dificil de

Listado	Bajar Listado	www.hacker [redacted]	Comprar

Costo del CD € 35

Entrega en toda España sin gastos de envio

AUTOMATED TOOLS: Eg

2003 UPDATED VERSION

CD HACKER content

- **MANUALES Y TUTORIALES HACKERS Y COMUNICACIONES**
- **SNIFFERS**
- **IP TOOLS**
- **SCANNERS**
- **CONTROL A DISTANCIA**
- **PROGRAMAS VARIOS HACKING**
- **HERRAMIENTAS ANTI SPYWARE**
- **HERRAMIENTAS ANTI HACKER**
- **ATAQUES**
- **SERIALS Y CRACKERS**
- **KEYLOGGERS**
- **PASSWORDS (utilitarios para develar claves, generadores de combinaciones de claves, fuerza bruta)**
- **FUERZA BRUTA (para forzar el login / password de sitios protegidos)**
- **PHREAK (conexion telefonica)**
- **CORREO ELECTRONICO (utilitarios para e mail , ICQ y Chat)**
- **ENCRIPTADORES**
- **BROMAS PESADAS (utilidades que generan falsos errores, deshabilitan funciones windows, simulan virus, etc)**
- **SPOOFING**
- **CURSOS (para desarrollas sus propios programas, utilitarios y virii)**
- **DECODIFICADORES AUDIO Y VIDEO (para Divx - Mp3)**
- **TUTORIALES PARA GRABACION CD**
- **COMPILACION DE TRUCOS**
- **VIRII (detectores, creadores, codigo fuente, tutoriales sobre virus)**
- **MP3Z (tutoriales sobre creacion y manejo de MP3)**
- **PROGRAMAS PARA GRABACION CD**

ATTACK KITS (*CRIMEWARE* KIT)

- Assemblers modules
  - Executables for specific attacks
  - Functions of antivirus evasion
  - Creating infrastructures of C & C
- Sent of malicious code: spam (botnet?), Spear phishing, compromised web, etc.

ATTACK KIT. Zeus

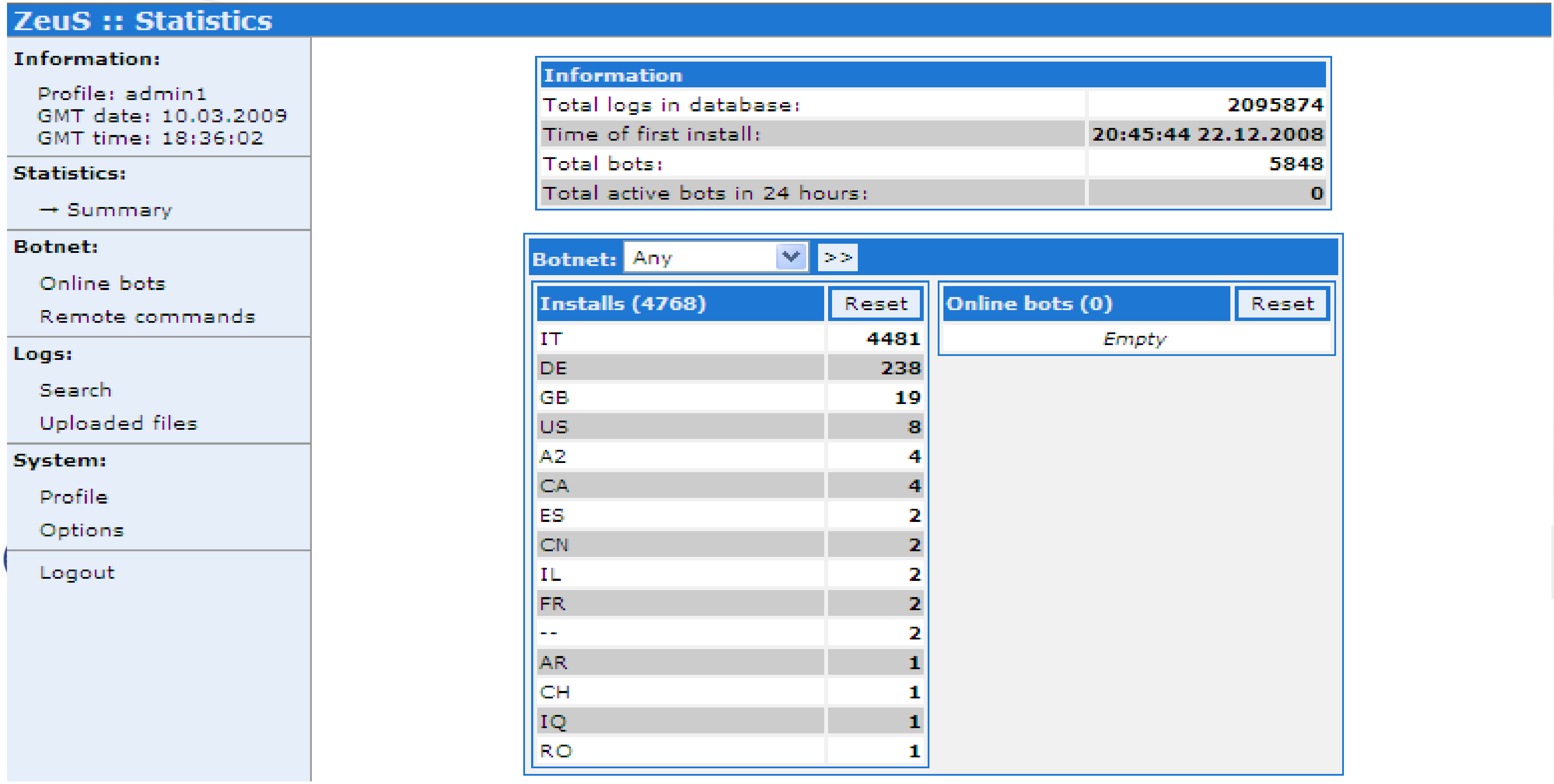
Banking Trojan: Redirects to fraudulent websites

Cost ≅2000-10000 $ (some versions include maintenance)

Ignores certain two-factor authentications

http://www.thetechherald.com/articles/Overview- Inside-the-Zeus-Trojans-source-code/13567/

Zeus GUI



ZeuS :: Statistics

Information:

Profile: admin1
GMT date: 10.03.2009
GMT time: 18:36:02

Statistics:

→ Summary

Botnet:

Online bots
Remote commands

Logs:

Search
Uploaded files

System:

Profile
Options

Logout

Information	
Total logs in database:	2095874
Time of first install:	20:45:44 22.12.2008
Total bots:	5848
Total active bots in 24 hours:	0

Botnet: Any >>

Installs (4768)	Reset
IT	4481
DE	238
GB	19
US	8
A2	4
CA	4
ES	2
CN	2
IL	2
FR	2
--	2
AR	1
CH	1
IQ	1
RO	1

Online bots (0)	Reset
Empty	

ATTACK KIT. Firesheep

TCP session hijacking (session hijacking) Firefox

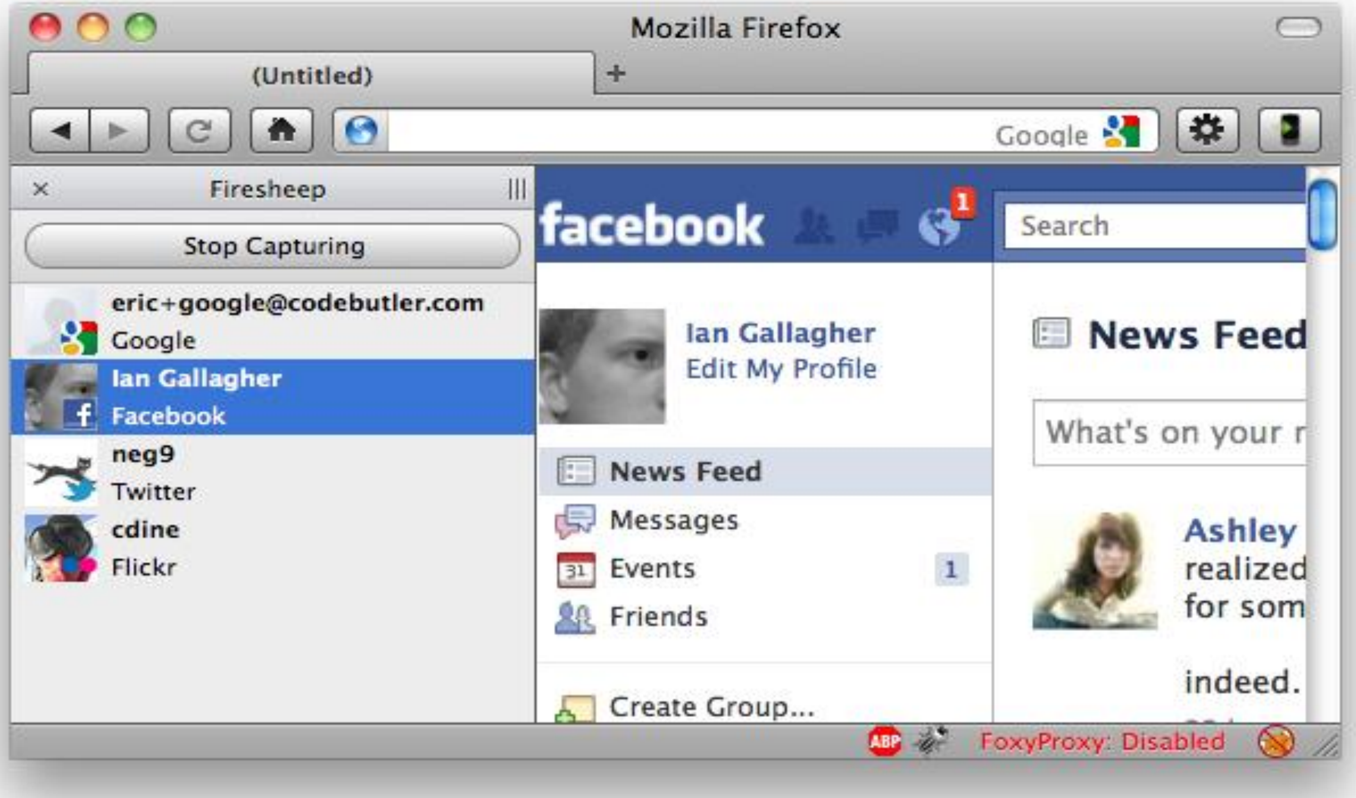
systems- Posted in Fall 2010

Main threat: Secure connections (SSL) only during authentication

Android Description: FaceNiff

Firesheep hacking user accounts with a click

Google, Twitter...



eric+google@codebutler.com
Google

Ian Gallagher
Facebook

neg9
Twitter

cdine
Flickr

Ian Gallagher
Edit My Profile

News Feed

What's on your r

Ashley
realized
for som

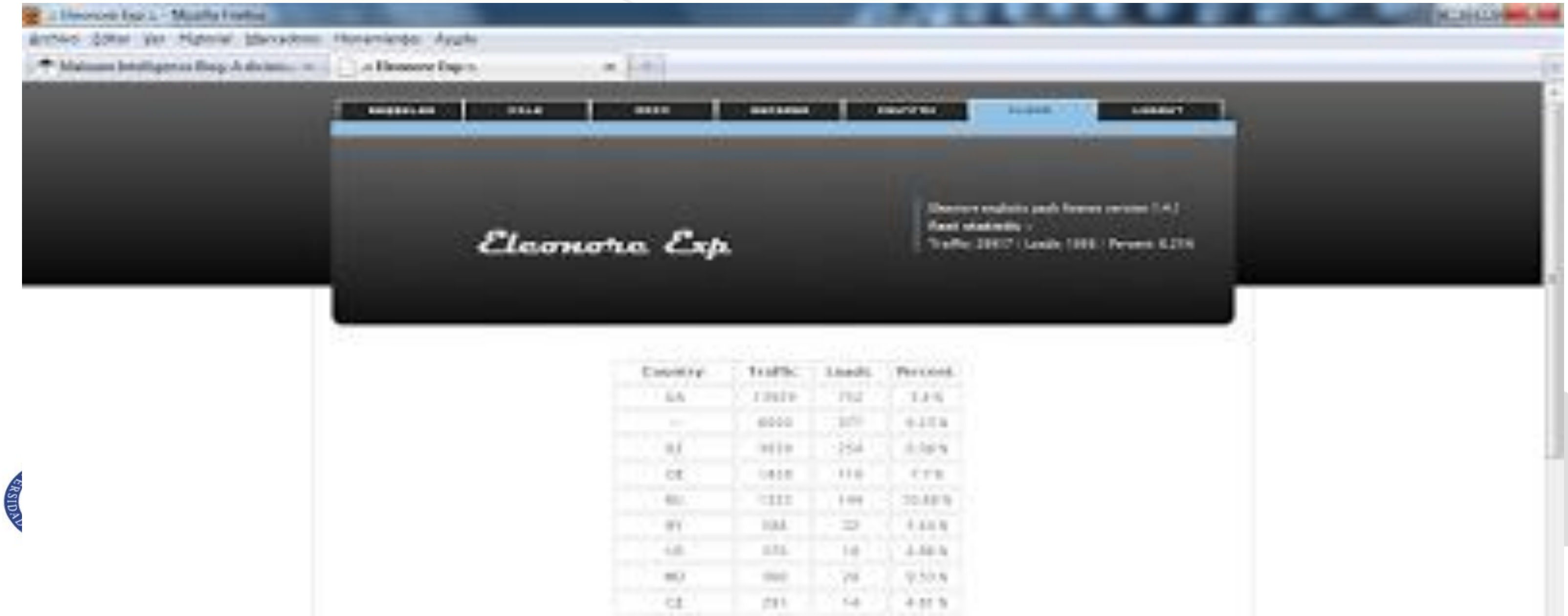
indeed.

ATTACK KIT. Eleonor

Track the web for known vulnerabilities

Use one of them to install the malware

Eleanor Exploit Pack


:: Eleonore Exp :: - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Malware Intelligence Blog: A dissem...
:: Eleonore Exp ::
Eleonora Exp

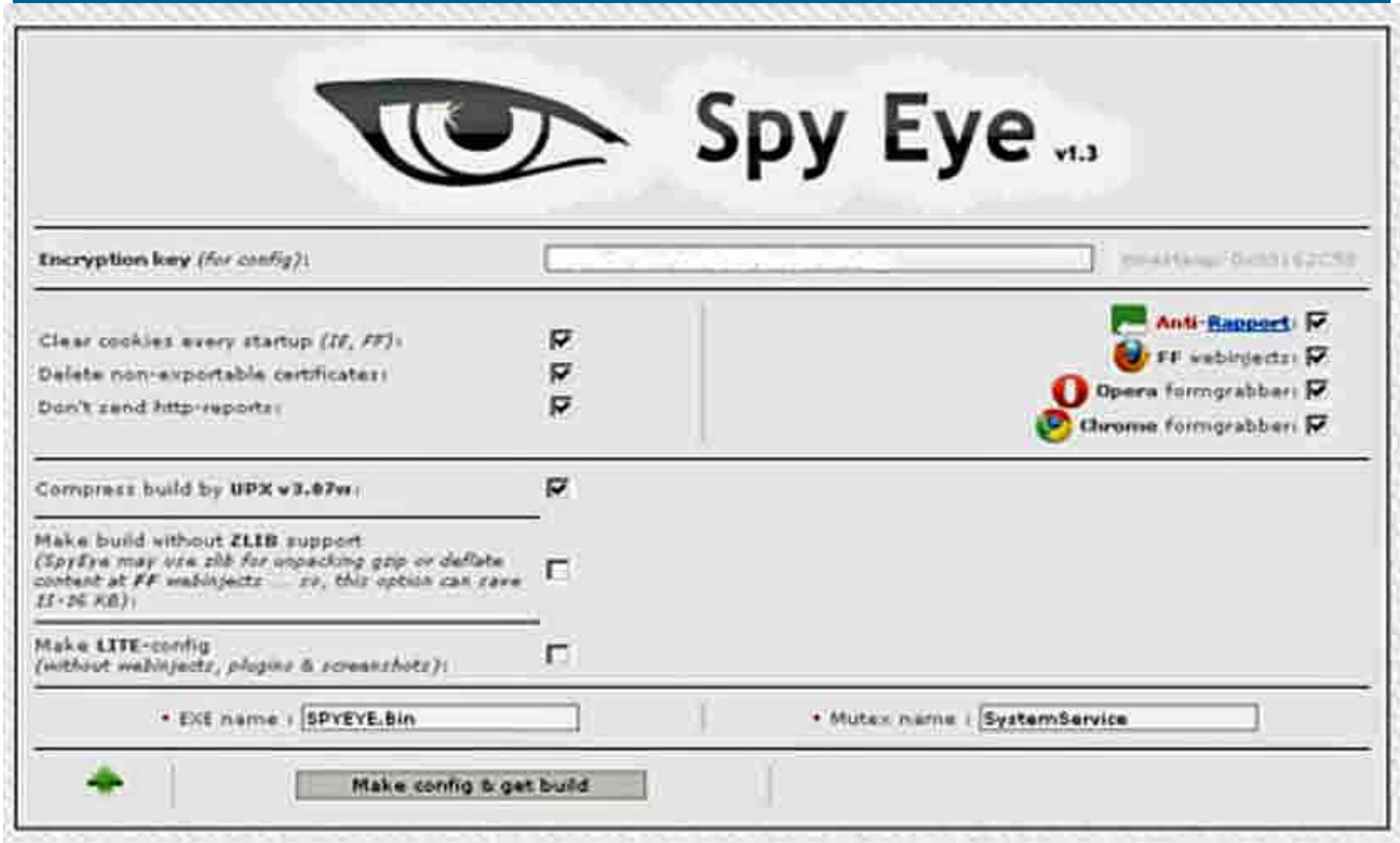
Eleonore exploits pack license version [illegible]
Real statistic :
Traffic: [illegible] | Loads: [illegible] | Percent: [illegible]

Country	Traffic	Loads	Percent
[illegible]	[illegible]	[illegible]	[illegible]
--	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
DE	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
US	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
CZ	[illegible]	[illegible]	[illegible]

ATTACK KIT. Spyeye

Feature: You can start the webcam to record the attack

Video demo: http://www.youtube.com/watch?v=lJzcguH76Wg



Encryption key *(for config)*: [illegible]

Clear cookies every startup *(IE, FF)*: ☑

Delete non-exportable certificates: ☑

Don't send http-reports: ☑

Anti-Rapport: ☑

FF webinjects: ☑

Opera formgrabber: ☑

Chrome formgrabber: ☑

Compress build by **UPX v3.07w**: ☑

Make build without **ZLIB** support
(SpyEye may use zlib for unpacking gzip or deflate content at FF webinjects ... so, this option can save 11-36 KB): ☐

Make **LITE**-config
(without webinjects, plugins & screenshots): ☐

• EXE name : SPYEYE.bin

• Mutex name : SystemService

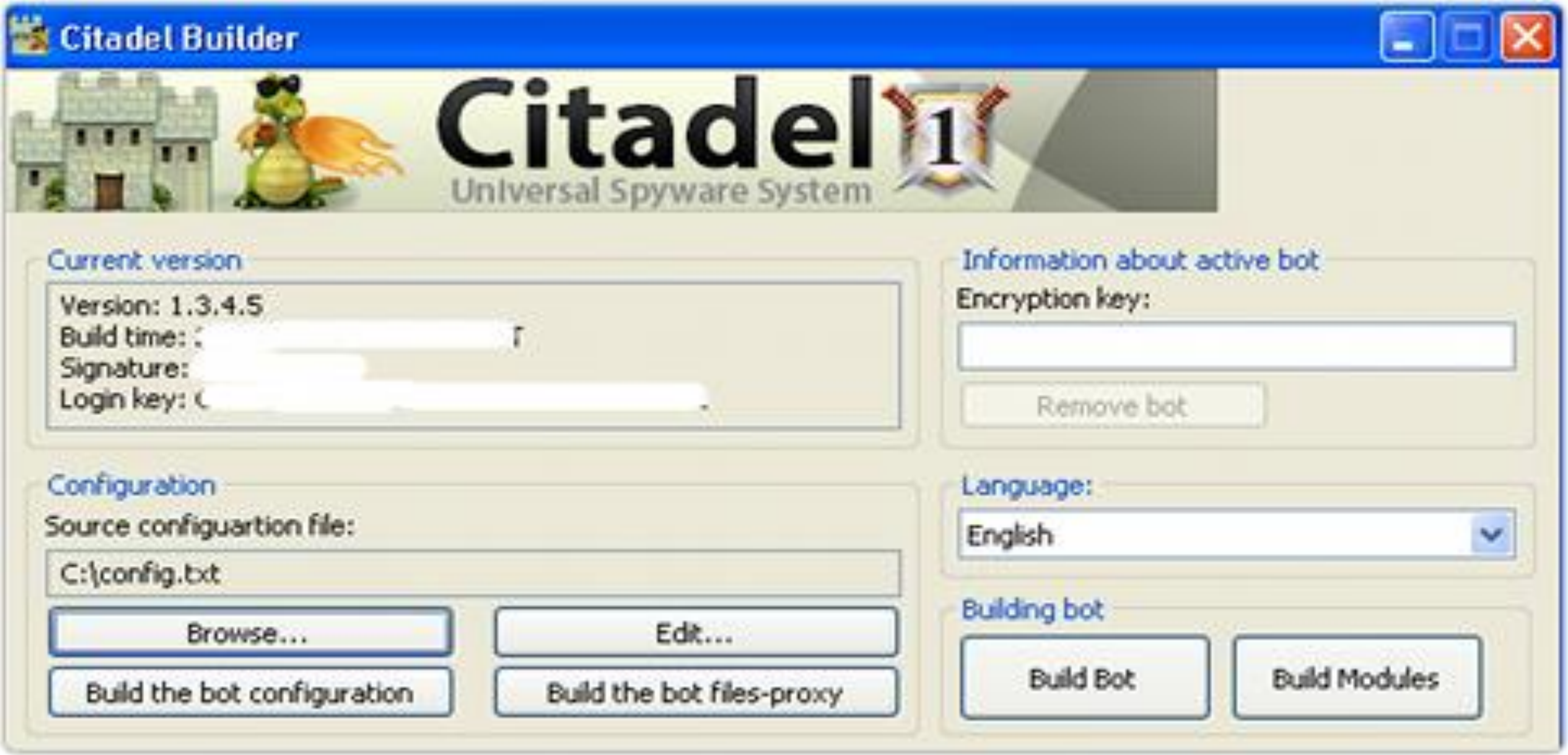
ATTACK KITS. Others

Blackhole: web threat

Mpack: key logger

Phishing kits

CRIMEWARE KIT



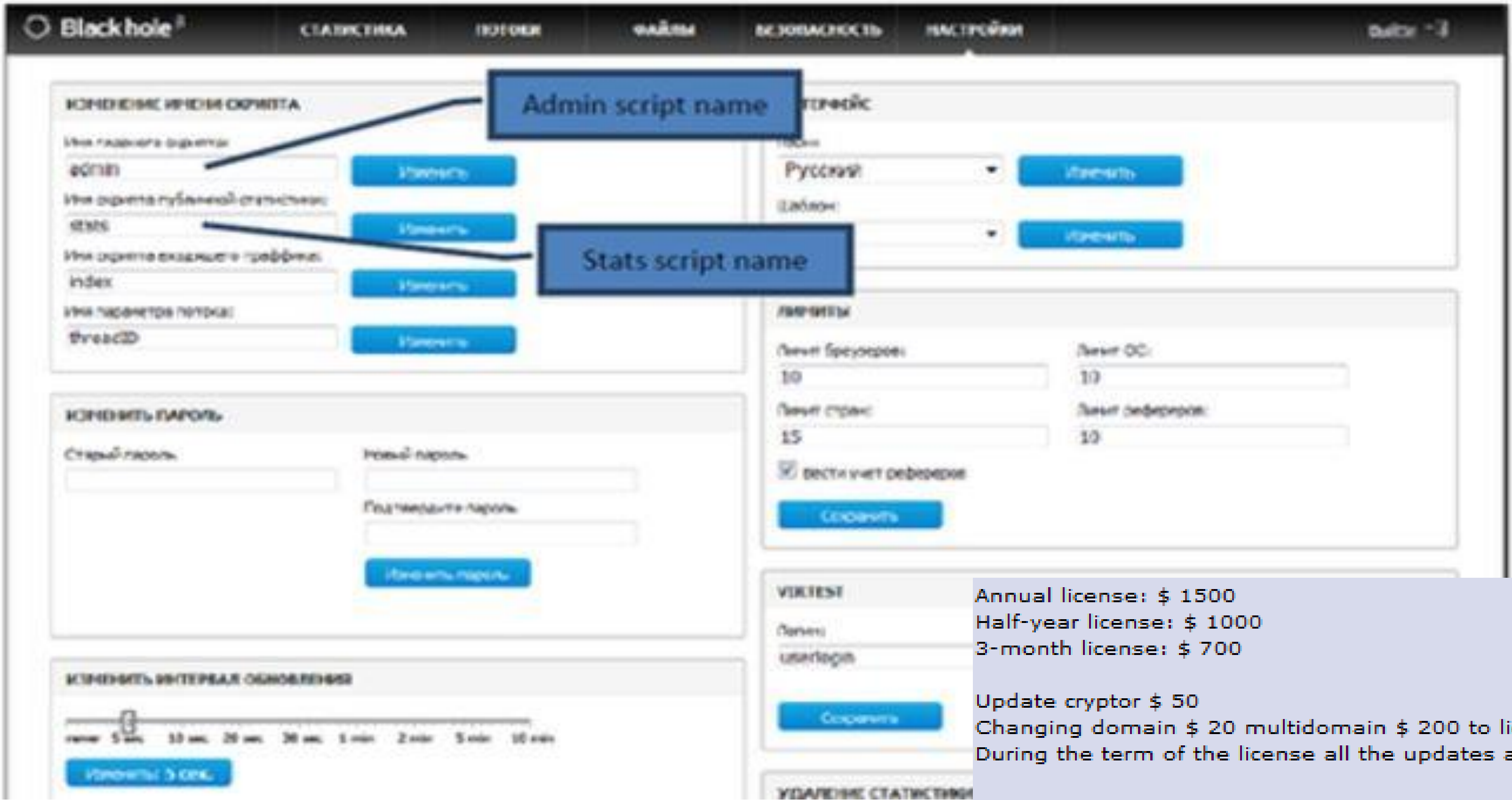
Version: 1.3.4.5
Build time: [redacted]
Signature: [redacted]
Login key: [redacted]

Encryption key:

Source configuartion file: C:\config.txt

Language: English

Blackhole



ИЗМЕНЕНИЕ ИМЕНИ СКРИПТА

Имя главного скрипта: admin

Имя скрипта публичной статистики: stats

Имя скрипта входящего трафика: index

Имя параметра потока: threadID

Admin script name

Stats script name

ИЗМЕНИТЬ ПАРОЛЬ

Старый пароль:

Новый пароль:

Подтвердите пароль:

Изменить пароль

ИЗМЕНИТЬ ИНТЕРВАЛ ОБНОВЛЕНИЯ

Изменить: 5 сек.

ИНТЕРФЕЙС

Язык: Русский

Шаблон:

ЛИМИТЫ

Лимит браузеров: 10

Лимит ОС: 10

Лимит стран: 15

Лимит рефереров: 10

☑ вести учет рефереров

Сохранить

VIRTEST

Логин: userlogin

Сохранить

УДАЛЕНИЕ СТАТИСТИКИ

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $ 20 multidomain $ 200 to license.
During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): $ 200
2 weeks (14 full days): $ 300
3 weeks (21 full day): $ 400
4 weeks (31 full day): $ 500
24-hour test: $ 50

- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: $ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

CHAPTER 2. Programme

1. Attack tools. Features and types
   - Sophisticated
   - Automated
   - **Social Engineering:**
     - **Phishing, spear phishing**
2. Malicious software. Classification
3. Kits, Cryptovirus, APT

TOOLS. Social engineering

BASIC PRINCIPLES[1]

We all want to help

We trust in others

We do not like to deny ourselves

We love praises

1. Kevin Mitnick

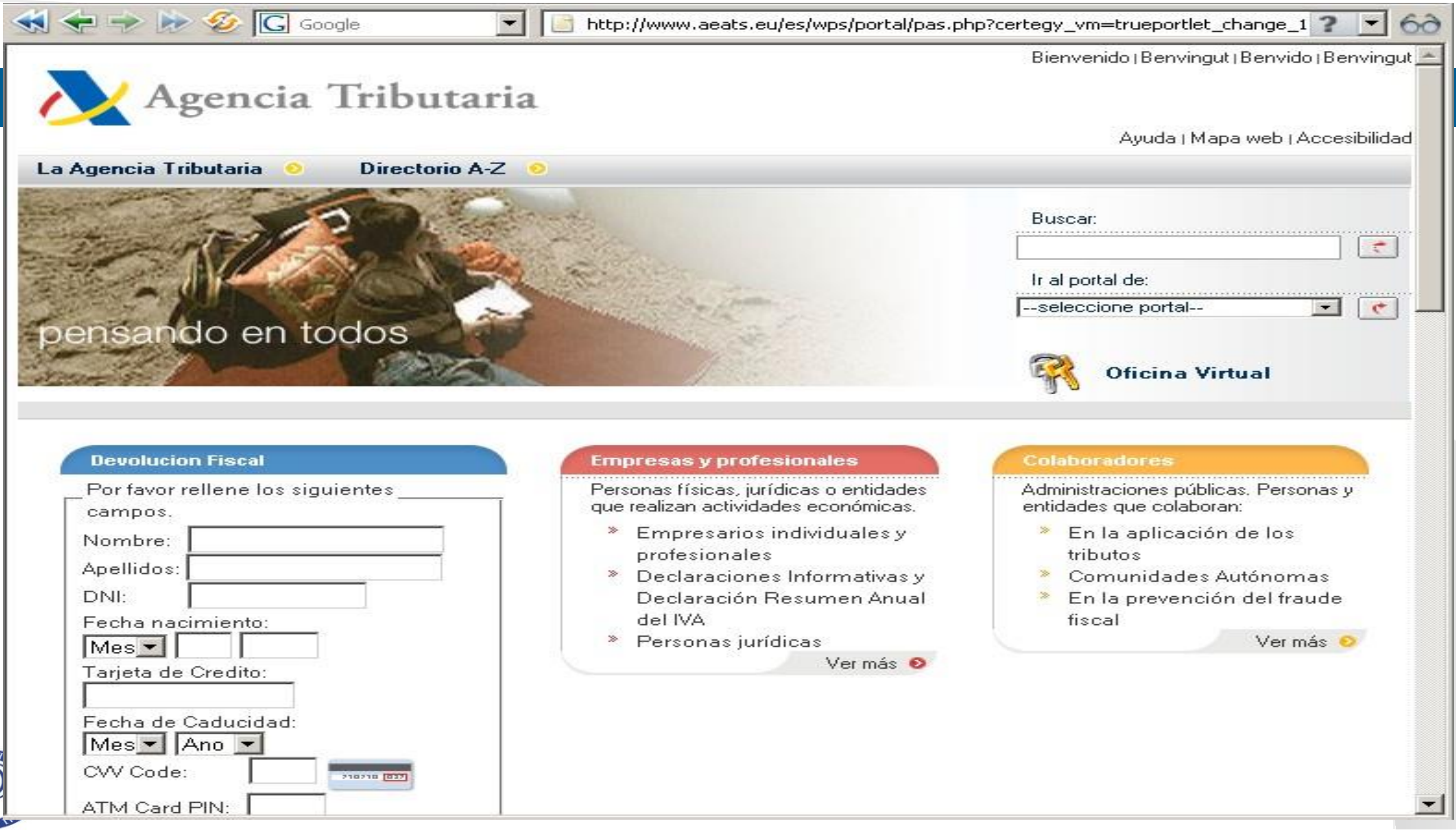
SOCIAL ENGINEERING

Panda Software ha detectado en las últimas horas el envío masivo de un correo electrónico no solicitado referente a la captura del líder de Al-Qaeda, Osama Bin Laden, que tiene como objetivo hacer que el usuario visite una supuesta página web publicitaria que descarga un troyano en el ordenador.

El asunto del citado email es "Osama Bin Laden Captured" y su remitente suele ser variable, aunque siempre simula proceder de la radio televisión británica BBC o la cadena estadounidense CNN.

En cuanto al cuerpo del texto, que aparece en inglés, intenta convencer al internauta para que acuda a la dirección web que adjunta para ver las fotografías o el vídeo de Bin Laden.

En caso de que el usuario visite la citada dirección se abre una página supuestamente publicitaria. Sin embargo, contiene un código que aprovecha una vulnerabilidad (Exploit/MIE.CHM) que, a su vez, descarga y ejecuta un fichero (VBS/Psyme.C). Finalmente, éste baja desde Internet un archivo llamado "EXPLOIT.EXE", que contiene al troyano "Trj/Small.B".


Google
http://www.aeats.eu/es/wps/portal/pas.php?certegy_vm=trueportlet_change_1

Bienvenido | Benvingut | Benvido | Benvingut

Agencia Tributaria

Ayuda | Mapa web | Accesibilidad

La Agencia Tributaria

Directorio A-Z

pensando en todos

Buscar:

Ir al portal de:

--seleccione portal--

Oficina Virtual

Devolucion Fiscal

Por favor rellene los siguientes campos.

Nombre:

Apellidos:

DNI:

Fecha nacimiento:

Mes

Tarjeta de Credito:

Fecha de Caducidad:

Mes Ano

CVV Code:

ATM Card PIN:

Empresas y profesionales

Personas físicas, jurídicas o entidades que realizan actividades económicas.

- Empresarios individuales y profesionales
- Declaraciones Informativas y Declaración Resumen Anual del IVA
- Personas jurídicas

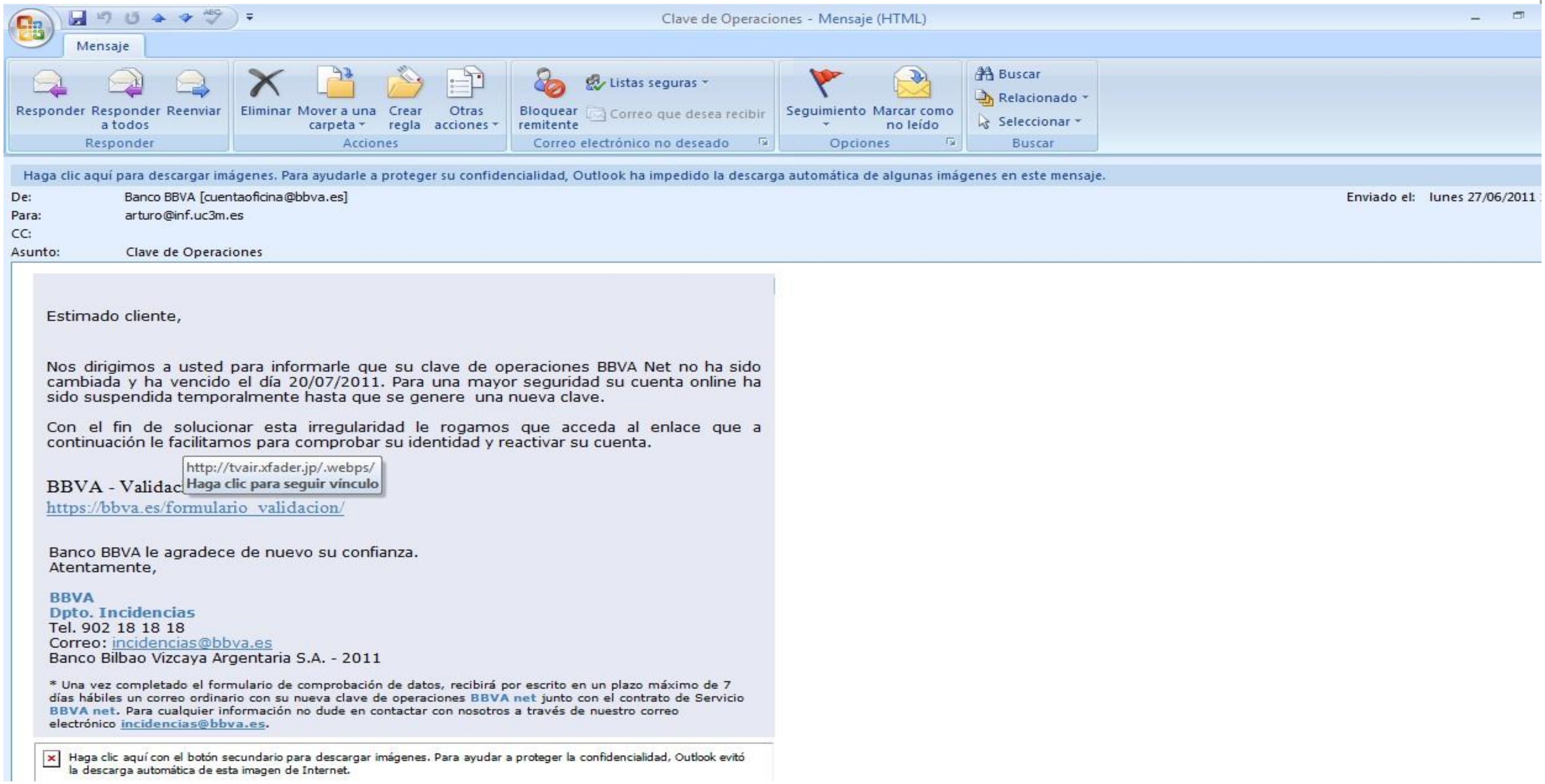
Ver más

Colaboradores

Administraciones públicas. Personas y entidades que colaboran:

- En la aplicación de los tributos
- Comunidades Autónomas
- En la prevención del fraude fiscal

Ver más



Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

De: Banco BBVA [cuentaoficina@bbva.es]
Para: arturo@inf.uc3m.es
CC:
Asunto: Clave de Operaciones

Enviado el: lunes 27/06/2011

Estimado cliente,

Nos dirigimos a usted para informarle que su clave de operaciones BBVA Net no ha sido cambiada y ha vencido el día 20/07/2011. Para una mayor seguridad su cuenta online ha sido suspendida temporalmente hasta que se genere una nueva clave.

Con el fin de solucionar esta irregularidad le rogamos que acceda al enlace que a continuación le facilitamos para comprobar su identidad y reactivar su cuenta.

http://tvair.xfader.jp/.webps/
Haga clic para seguir vínculo

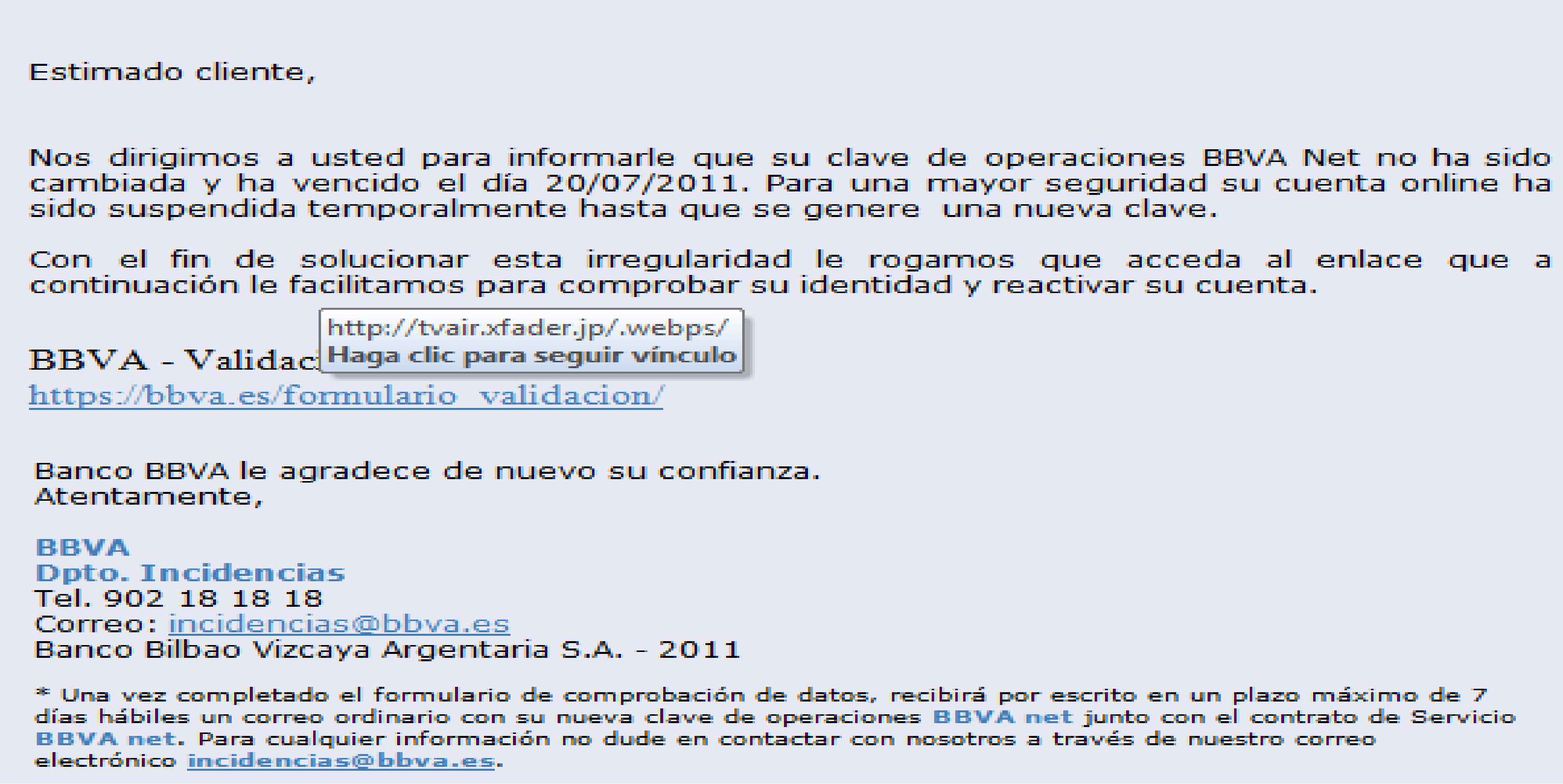
BBVA - Validac
https://bbva.es/formulario_validacion/

Banco BBVA le agradece de nuevo su confianza.
Atentamente,

BBVA
Dpto. Incidencias
Tel. 902 18 18 18
Correo: incidencias@bbva.es
Banco Bilbao Vizcaya Argentaria S.A. - 2011

* Una vez completado el formulario de comprobación de datos, recibirá por escrito en un plazo máximo de 7 días hábiles un correo ordinario con su nueva clave de operaciones **BBVA net** junto con el contrato de Servicio **BBVA net**. Para cualquier información no dude en contactar con nosotros a través de nuestro correo electrónico **incidencias@bbva.es**.

☒ Haga clic aquí con el botón secundario para descargar imágenes. Para ayudar a proteger la confidencialidad, Outlook evitó la descarga automática de esta imagen de Internet.



Estimado cliente,

Nos dirigimos a usted para informarle que su clave de operaciones BBVA Net no ha sido cambiada y ha vencido el día 20/07/2011. Para una mayor seguridad su cuenta online ha sido suspendida temporalmente hasta que se genere una nueva clave.

Con el fin de solucionar esta irregularidad le rogamos que acceda al enlace que a continuación le facilitamos para comprobar su identidad y reactivar su cuenta.

BBVA - Validaci

https://bbva.es/formulario_validacion/

Banco BBVA le agradece de nuevo su confianza.
Atentamente,

BBVA
Dpto. Incidencias
Tel. 902 18 18 18
Correo: incidencias@bbva.es
Banco Bilbao Vizcaya Argentaria S.A. - 2011

* Una vez completado el formulario de comprobación de datos, recibirá por escrito en un plazo máximo de 7 días hábiles un correo ordinario con su nueva clave de operaciones **BBVA net** junto con el contrato de Servicio **BBVA net**. Para cualquier información no dude en contactar con nosotros a través de nuestro correo electrónico **incidencias@bbva.es**.

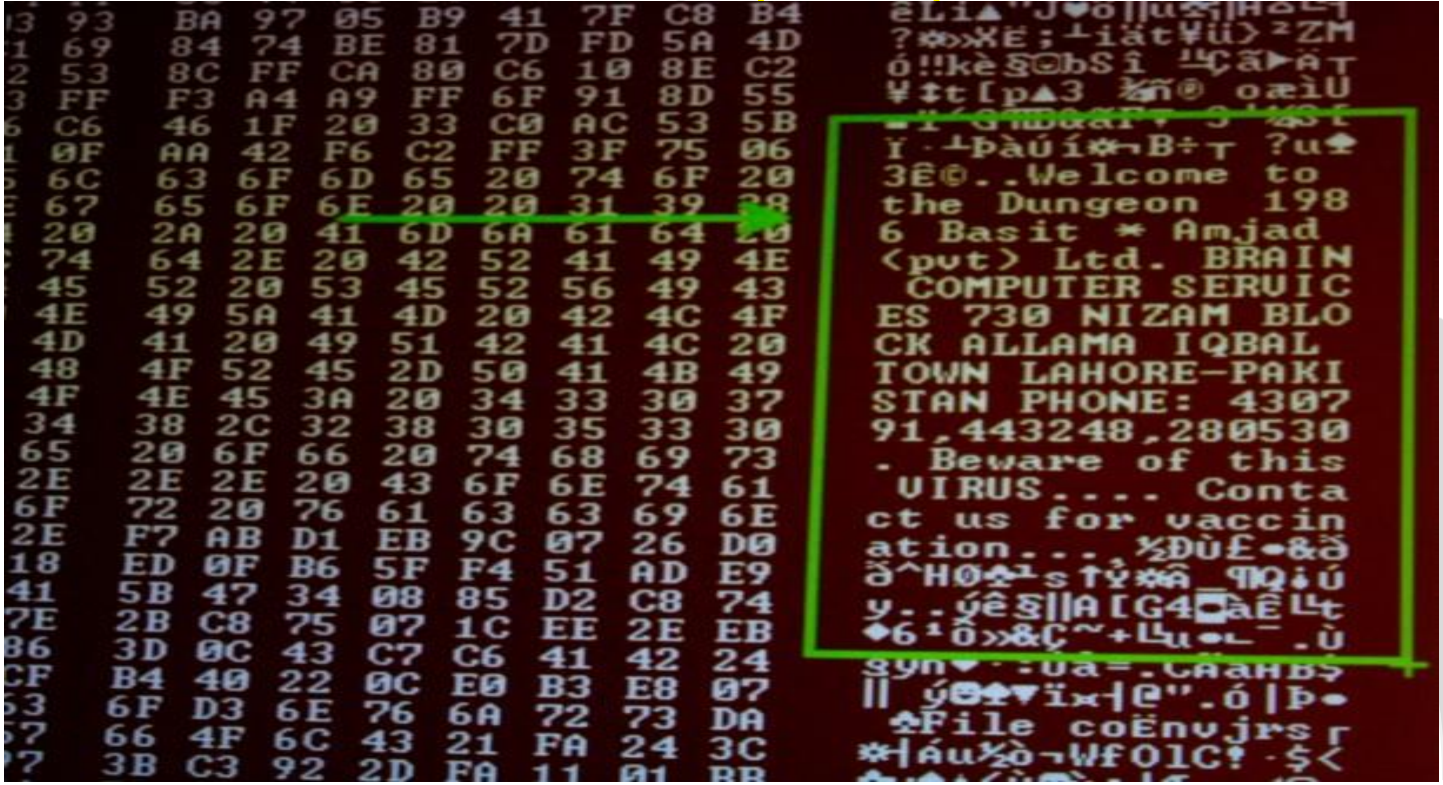
CHAPTER 2

1. Tools of attack. Features and types
2. **Malicious software. Classification**
3. Kits, Criptovirus, APT

MALICIOUS SOFTWARE. Brief History

- Von Neumann. Theoretical Concept
- AT&T Labs (1960): *Core Wars*
- Fred Cohen (Doctoral thesis,1983): Construction
- *Elk Cloner* (1985): First virus propagated. Apple II
- *Brain* (1986): Basit and Amjad Farooq. Lahore (Pakistan)
- *Morris Worm (November 2nd, 1988)*

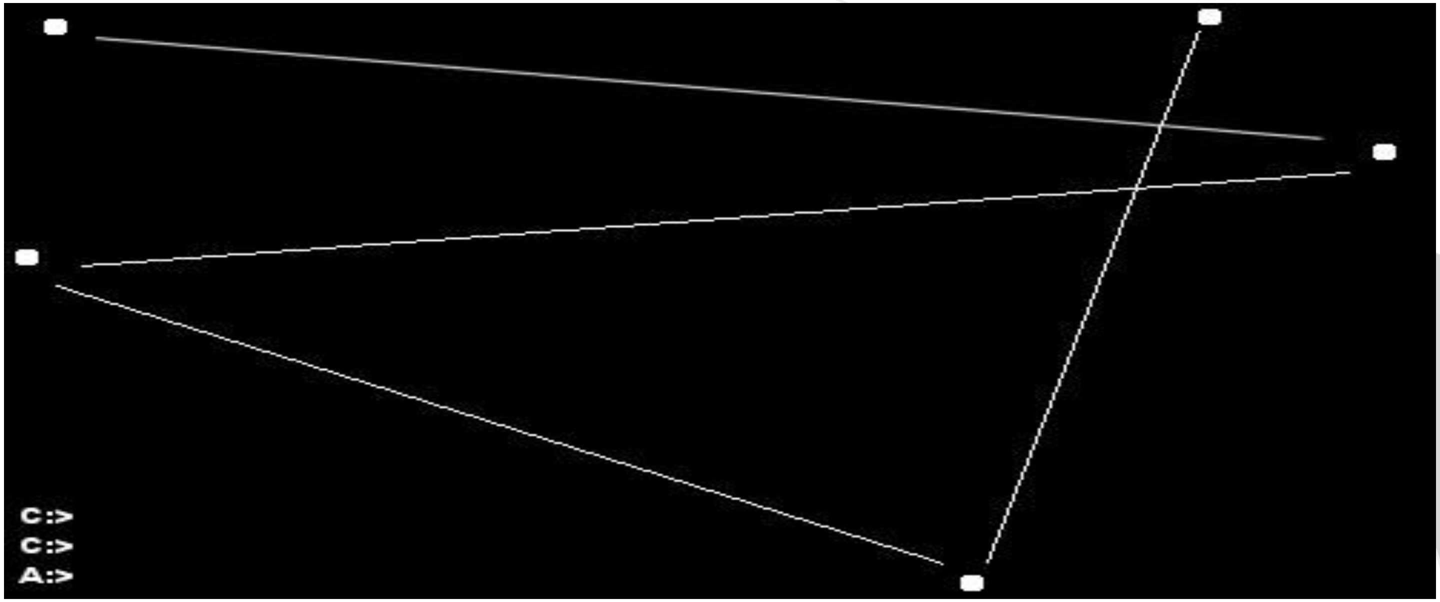
VIRUS BRAIN (1986)



```
93   BA 97 05 B9 41 7F C8 B4
69   84 74 BE 81 7D FD 5A 4D
53   8C FF CA 80 C6 10 8E C2
FF   F3 A4 A9 FF 6F 91 8D 55
C6   46 1F 20 33 C0 AC 53 5B
0F   AA 42 F6 C2 FF 3F 75 06
6C   63 6F 6D 65 20 74 6F 20
67   65 6F 6E 20 20 31 39 38
20   2A 20 41 6D 6A 61 64 20
74   64 2E 20 42 52 41 49 4E
45   52 20 53 45 52 56 49 43
4E   49 5A 41 4D 20 42 4C 4F
4D   41 20 49 51 42 41 4C 20
48   4F 52 45 2D 50 41 4B 49
4F   4E 45 3A 20 34 33 30 37
34   38 2C 32 38 30 35 33 30
65   20 6F 66 20 74 68 69 73
2E   2E 2E 20 43 6F 6E 74 61
6F   72 20 76 61 63 63 69 6E
2E   F7 AB D1 EB 9C 07 26 D0
18   ED 0F B6 5F F4 51 AD E9
41   5B 47 34 08 85 D2 C8 74
7E   2B C8 75 07 1C EE 2E EB
86   3D 0C 43 C7 C6 41 42 24
CF   B4 40 22 0C E0 B3 E8 07
63   6F D3 6E 76 6A 72 73 DA
67   66 4F 6C 43 21 FA 24 3C
97   3B C3 92 2D FA 11 01 BB
```

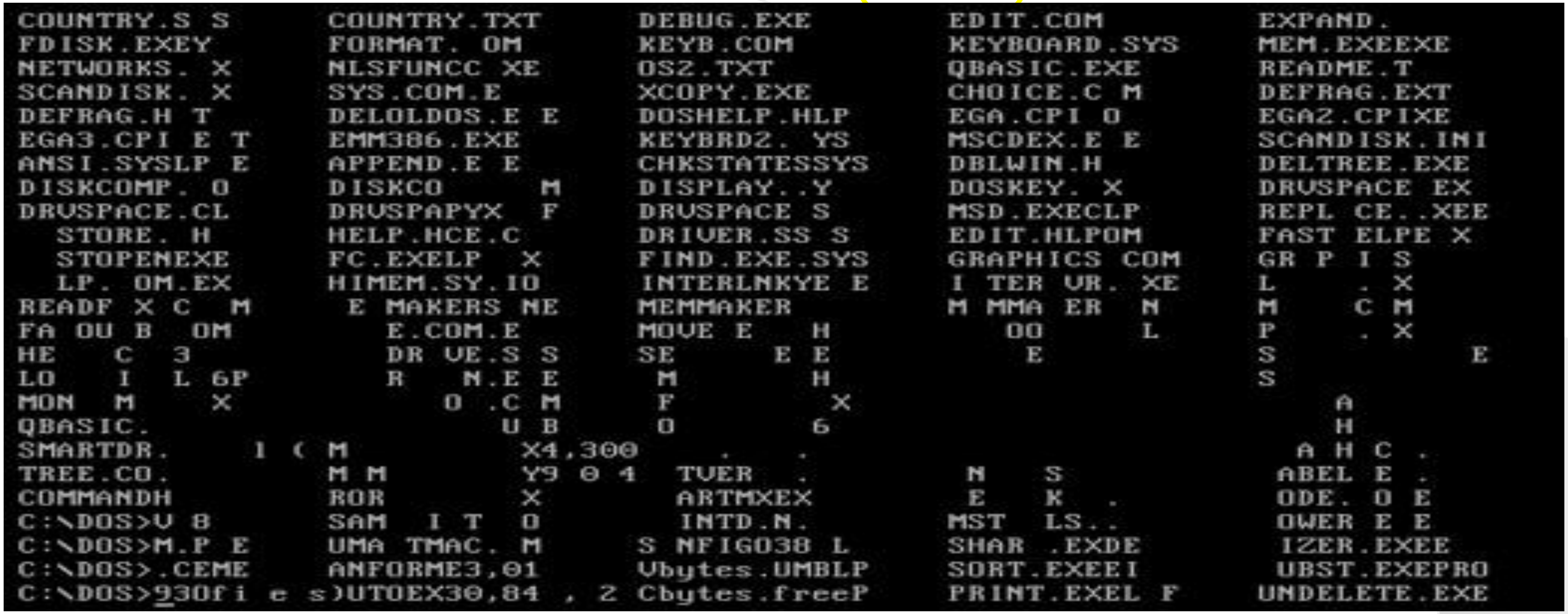
```
?☼»XË;┴iät¥ü>²ZM
ó!!kè§☺bSî ╧Çã►ÂT
¥↕t[p▲3 ¼ñ® oæìU
Ï·┴þàúí☼¬B÷┬ ?u♠
3Ê©..Welcome to
the Dungeon  198
6 Basit * Amjad
(pvt) Ltd. BRAIN
 COMPUTER SERVIC
ES 730 NIZAM BLO
CK ALLAMA IQBAL
TOWN LAHORE-PAKI
STAN PHONE: 4307
91,443248,280530
. Beware of this
 VIRUS.... Conta
ct us for vaccin
ation...,½ÐÙ£•&ð
ð^HØ♠┴s↑Ÿ☼Â_¶Q¿Ú
y..ýê§||A[G4▄àÊ╚t
♦6¹Ö»&Ç~+╚u•└¯.Ù
|| ý☻♠▼ïx┤@".ó|Þ•
 ♠File coËnvjrs┌
☼┤Áu½ò¬WfO1C!·$<
```

VIRUS: Ping-pong (1988)



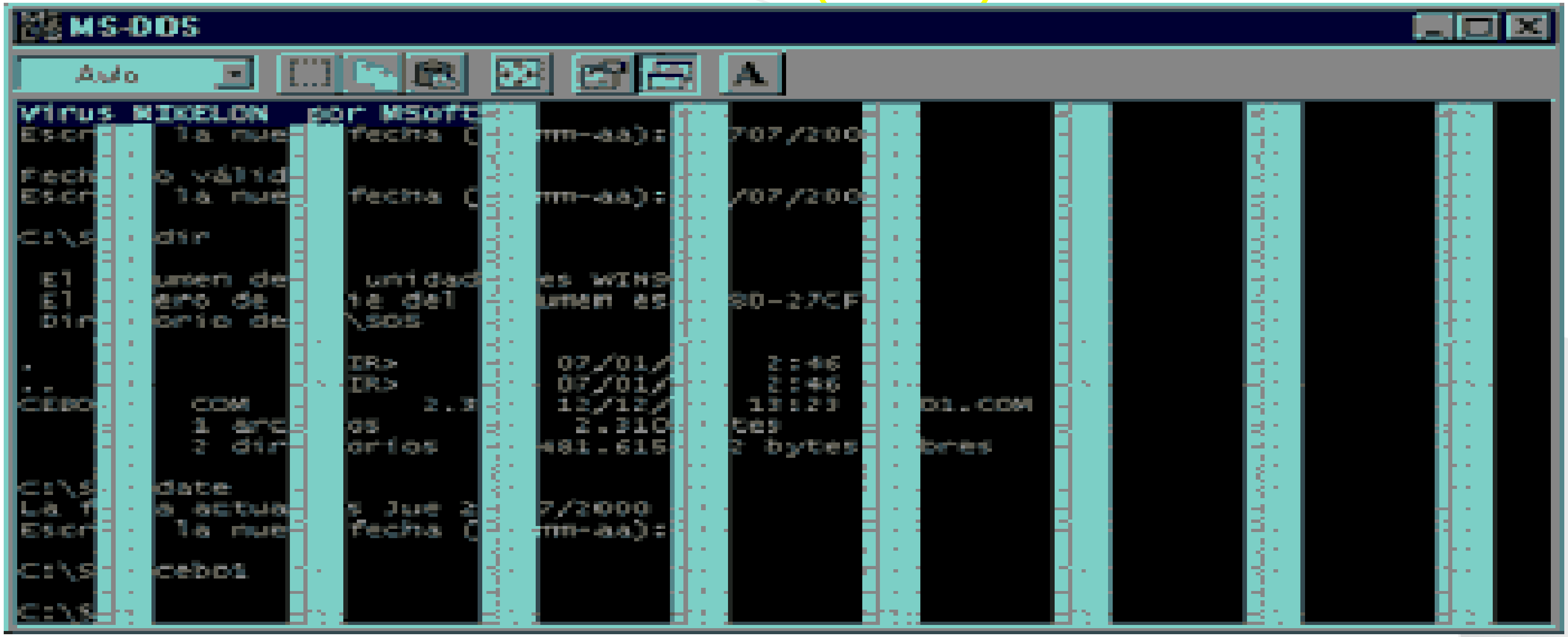
```
C:>
C:>
A:>
```

VIRUS CASCADE (1988)



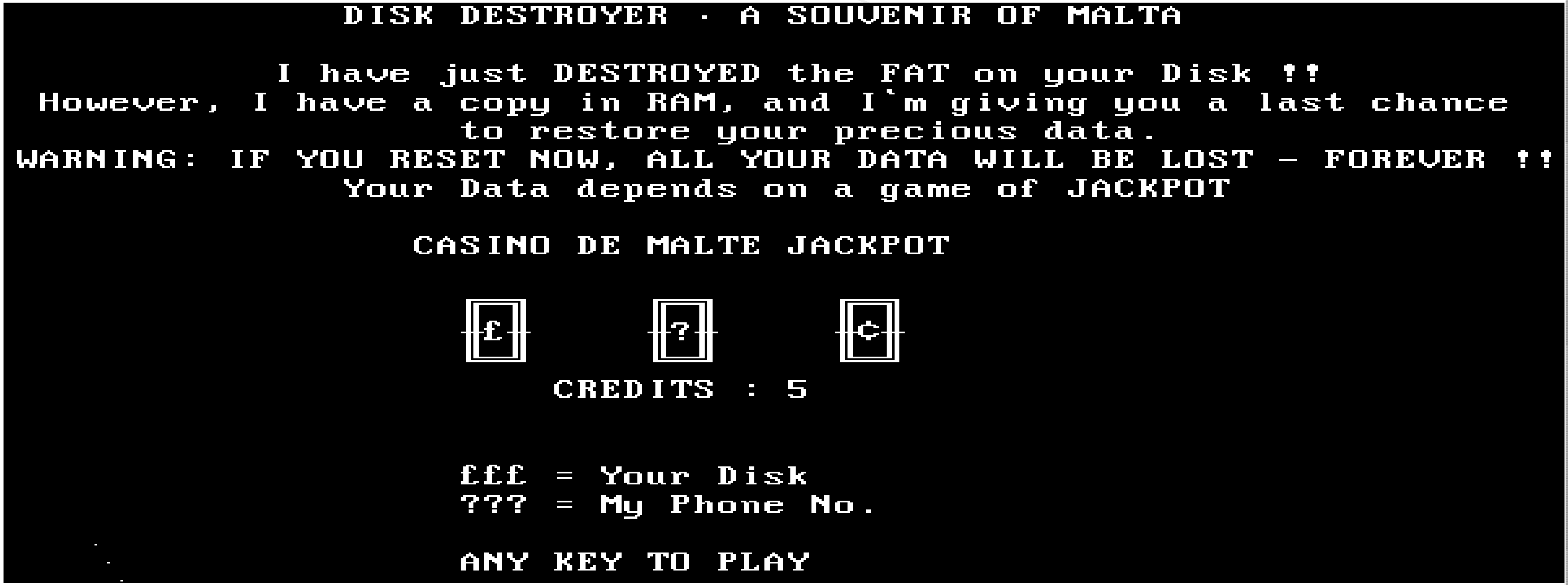
```
COUNTRY.S S     COUNTRY.TXT     DEBUG.EXE       EDIT.COM        EXPAND.
FDISK.EXEY      FORMAT. OM      KEYB.COM        KEYBOARD.SYS    MEM.EXEEXE
NETWORKS. X     NLSFUNCC XE     OS2.TXT         QBASIC.EXE      README.T
SCANDISK. X     SYS.COM.E       XCOPY.EXE       CHOICE.C M      DEFRAG.EXT
DEFRAG.H T      DELOLDOS.E E    DOSHELP.HLP     EGA.CPI O       EGA2.CPIXE
EGA3.CPI E T    EMM386.EXE      KEYBRD2. YS     MSCDEX.E E      SCANDISK.INI
ANSI.SYSLP E    APPEND.E E      CHKSTATESSYS    DBLWIN.H        DELTREE.EXE
DISKCOMP. O     DISKCO     M    DISPLAY..Y      DOSKEY. X       DRVSPACE EX
DRVSPACE.CL     DRVSPAPYX  F    DRVSPACE S      MSD.EXECLP      REPL CE..XEE
  STORE. H      HELP.HCE.C      DRIVER.SS S     EDIT.HLPOM      FAST ELPE X
  STOPENEXE     FC.EXELP  X     FIND.EXE.SYS    GRAPHICS COM    GR P I S
  LP. OM.EX     HIMEM.SY.IO     INTERLNKYE E    I TER VR. XE    L    . X
READF X C  M     E MAKERS NE    MEMMAKER        M MMA ER  N     M    C M
FA OU B  OM        E.COM.E      MOVE E   H         OO     L     P    . X
HE   C  3          DR VE.S S    SE     E E          E           S          E
LO   I  L 6P       R   N.E E     M       H                      S
MON  M    X           O .C M     F        X                         A
QBASIC.                  U B     O       6                          H
SMARTDR.    1 ( M         X4,300    .   .                         A H C .
TREE.CO.        M M       Y9 0 4  TVER  .        N   S           ABEL E .
COMMANDH        ROR       X       ARTMXEX        E   K  .        ODE. O E
C:\DOS>V 8      SAM  I T  O       INTD.N.       MST  LS..        OWER E E
C:\DOS>M.P E    UMA TMAC. M     S NFIG038 L     SHAR .EXDE       IZER.EXEE
C:\DOS>.CEME    ANFORME3,01     Vbytes.UMBLP    SORT.EXEEI       UBST.EXEPRO
C:\DOS>930fi e s)UTOEX30,84 , 2 Cbytes.freeP    PRINT.EXEL F    UNDELETE.EXE
```

VIRUS BARS (1993)



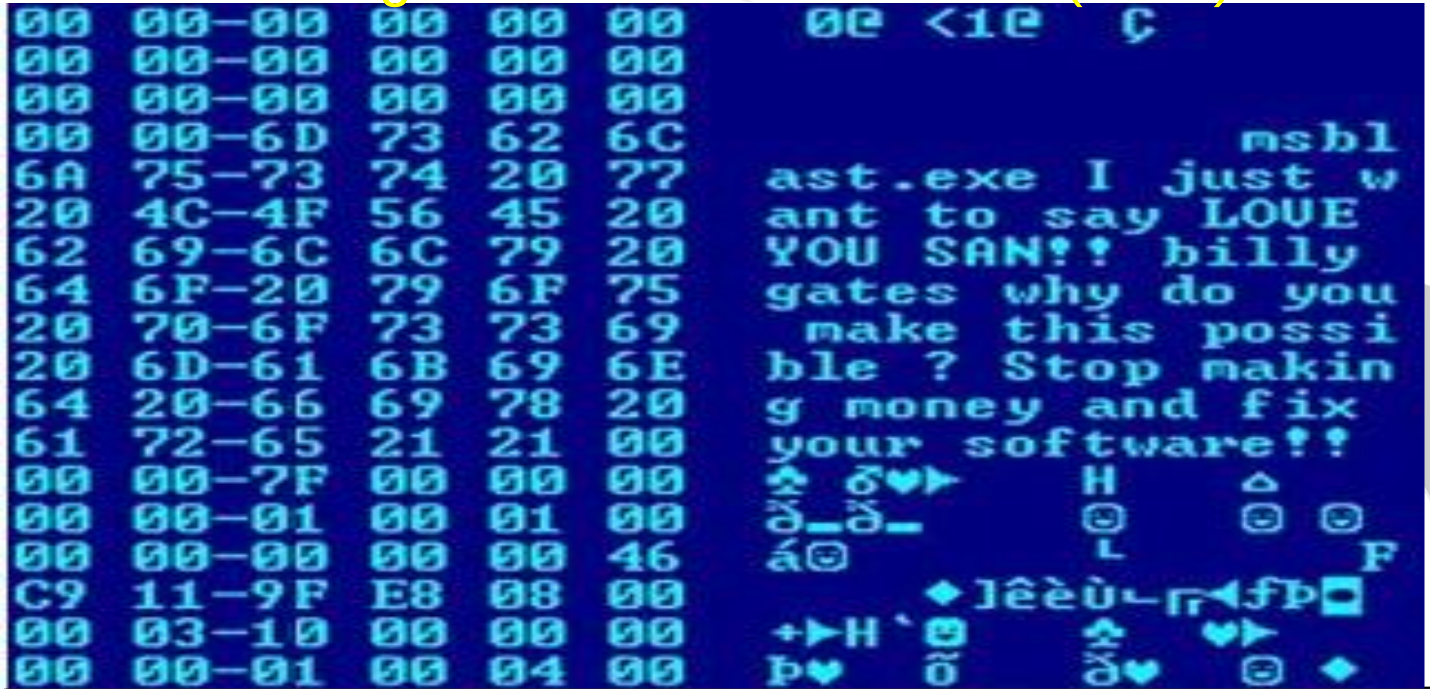
```
Virus BIKELON  por MSoft
Escr    la nue   fecha (   mm-aa):   /07/200

Fech   o válid
Escr    la nue   fecha (   mm-aa):   /07/200

C:\S   dir

 El    umen de    unidad   es WINS
 El    ero de    ie del    umen es   80-27CF
 Dir   orio de   \SOS

.               IR>          07/01/       2:46
..              IR>          07/01/       2:46
CEBO      COM          2.3   12/12/      13:23       01.COM
          1 arc    os          2.310    tes
          2 dir    orios     481.615    2 bytes    bres

C:\S   date
La f   a actua   s Jue 2   7/2000
Escr    la nue   fecha (   mm-aa):

C:\S   cebo1

C:\S
```

VIRUS CASINO (1991)



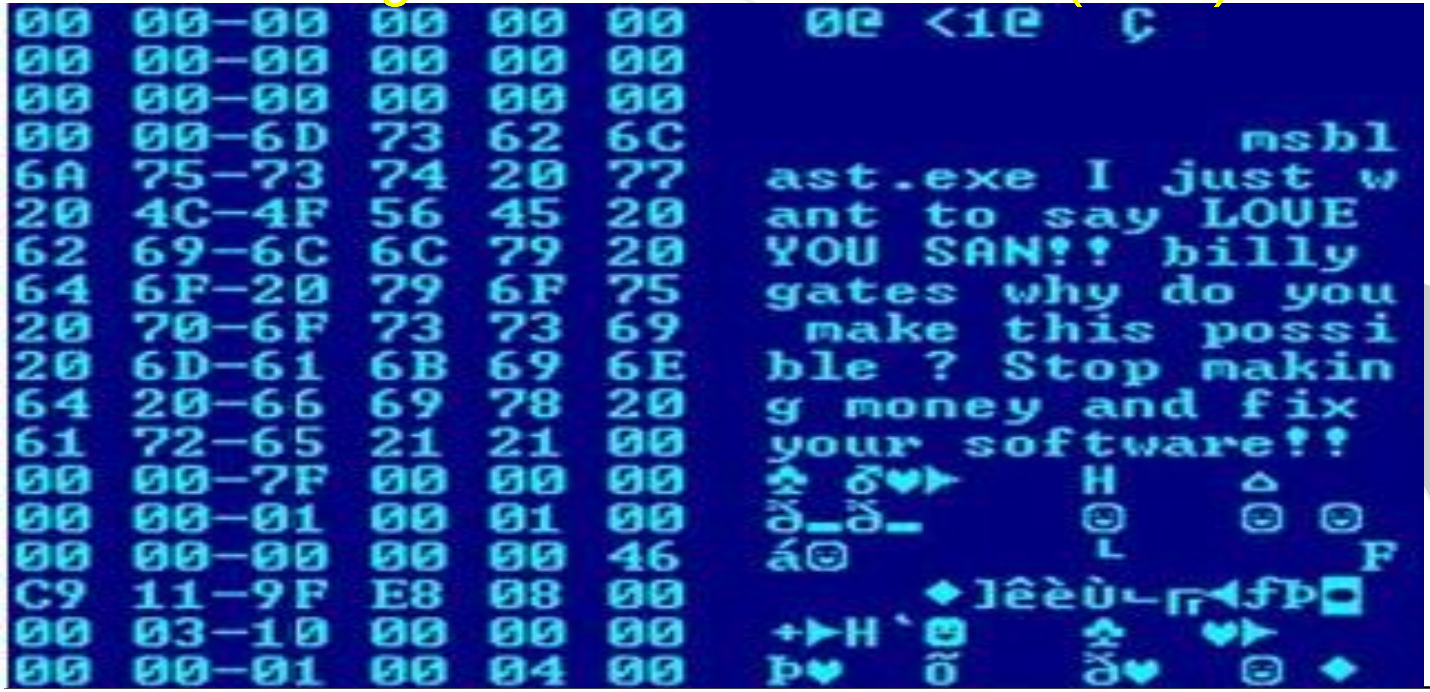
```
              DISK DESTROYER . A SOUVENIR OF MALTA

           I have just DESTROYED the FAT on your Disk !!
 However, I have a copy in RAM, and I`m giving you a last chance
                   to restore your precious data.
WARNING: IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER !!
              Your Data depends on a game of JACKPOT

                    CASINO DE MALTE JACKPOT


                      £       ?       ¢
                        CREDITS : 5


                      £££ = Your Disk
                      ??? = My Phone No.

                      ANY KEY TO PLAY
```

VIRUS: Fragment of the Blaster code (2003)



```
00 00-00 00 00 00    0@ <1@   Ç
00 00-00 00 00 00
00 00-00 00 00 00
00 00-6D 73 62 6C                msbl
6A 75-73 74 20 77  ast.exe I just w
20 4C-4F 56 45 20  ant to say LOVE
62 69-6C 6C 79 20  YOU SAN!! billy
64 6F-20 79 6F 75  gates why do you
20 70-6F 73 73 69   make this possi
20 6D-61 6B 69 6E  ble ? Stop makin
64 20-66 69 78 20  g money and fix
61 72-65 21 21 00  your software!!
00 00-7F 00 00 00  ⇞ δ♥▶    H    ⌂
00 00-01 00 01 00  ð_ð_     ☺    ☺ ☺
00 00-00 00 00 46  á☺       L       F
C9 11-9F E8 08 00      ◆]êèù└╒◀ƒP◘
00 03-10 00 00 00  +▶H`☻    ⇞    ♥▶
00 00-01 00 04 00  Þ♥   õ   ð♥   ☺ ◆
```

VIRUS: Fragment of the Blaster code (2003)

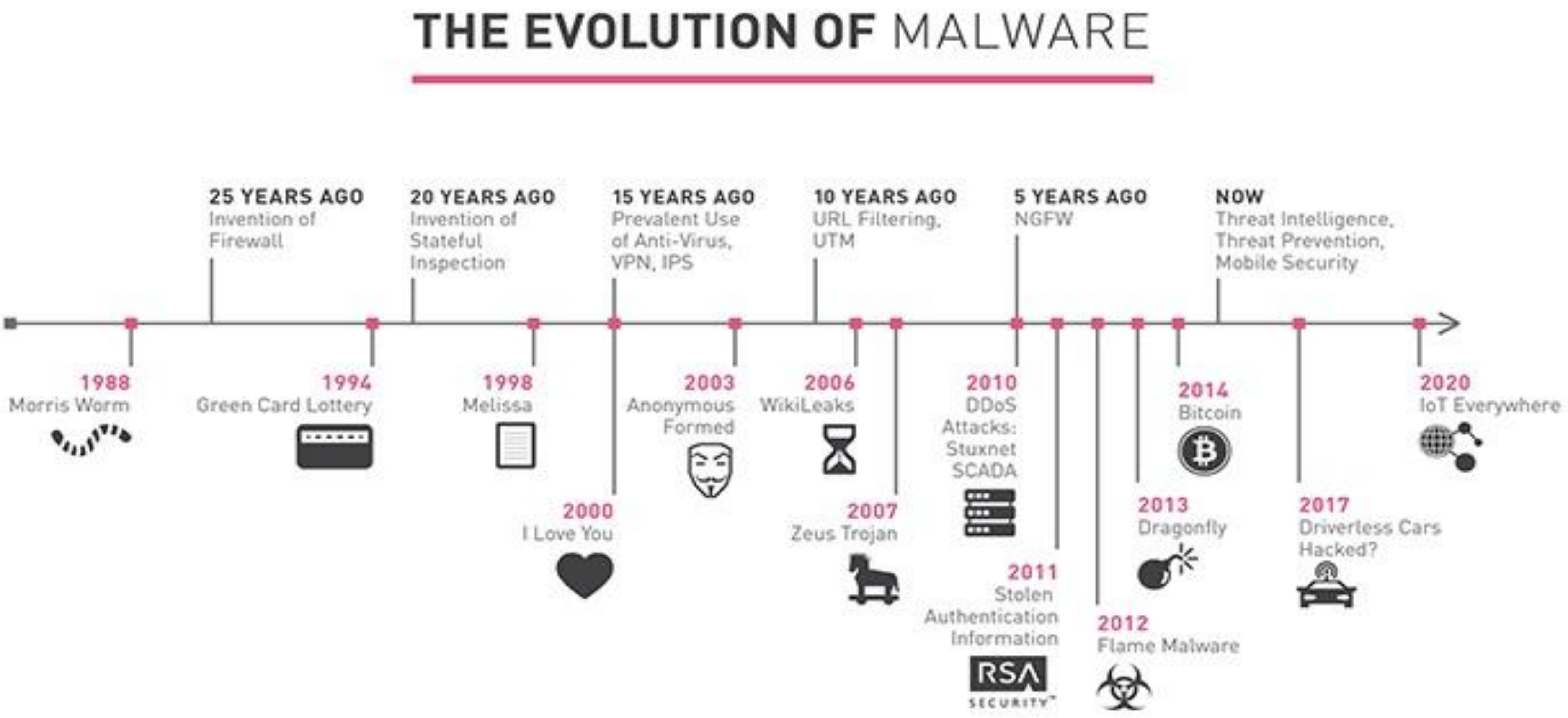


```
00 00-00 00 00 00     0@ <1@  Ç
00 00-00 00 00 00
00 00-00 00 00 00
00 00-6D 73 62 6C               msbl
6A 75-73 74 20 77   ast.exe I just w
20 4C-4F 56 45 20   ant to say LOVE
62 69-6C 6C 79 20   YOU SAN!! billy
64 6F-20 79 6F 75   gates why do you
20 70-6F 73 73 69    make this possi
20 6D-61 6B 69 6E   ble ? Stop makin
64 20-66 69 78 20   g money and fix
61 72-65 21 21 00   your software!!
00 00-7F 00 00 00   ♠ ð♥►    H    ⌂
00 00-01 00 01 00   ð_ð_     ☺   ☺ ☺
00 00-00 00 00 46   á☺       L     F
C9 11-9F E8 08 00        ◆]êèù└╓◄ƒÞ■
00 03-10 00 00 00   +►H`☻    ♠  ♥►
00 00-01 00 04 00   Þ♥  õ    ð♥  ☺ ◆
```

MALICIOUS SOFTWARE vs. ANTIVIRUS[1]

- Malicious software/day 50.000
- Signature package ≈ $2\ 10^{7}$ signatures
- Updates ≈ 5-10 minutes
- Reaper – primer antivirus - 1973

[1] David Perry. TrendMicro. Computing Jun 09



THE EVOLUTION OF MALWARE

25 YEARS AGO
Invention of Firewall

20 YEARS AGO
Invention of Stateful Inspection

15 YEARS AGO
Prevalent Use of Anti-Virus, VPN, IPS

10 YEARS AGO
URL Filtering, UTM

5 YEARS AGO
NGFW

NOW
Threat Intelligence, Threat Prevention, Mobile Security

1988
Morris Worm

1994
Green Card Lottery

1998
Melissa

2000
I Love You

2003
Anonymous Formed

2006
WikiLeaks

2007
Zeus Trojan

2010
DDoS Attacks: Stuxnet SCADA

2011
Stolen Authentication Information

2012
Flame Malware

2013
Dragonfly

2014
Bitcoin

2017
Driverless Cars Hacked?

2020
IoT Everywhere

MALICIOUS SOFTWARE: Types

- Virus
- Worms
- Trojan Horses
- Backdoors
- Logic bombs
- …

MALICIOUS SOFTWARE: Evolution

- Attacks to integrity
  - Michelangelo (1992), Brain (1985), ...
- Attacks to confidentiality
  - Smart TV attacks via DVB-T (2017)
- Attacks to availability
  - AIDS (1989), GpCode (2004)

MALICIOUS SOFTWARE: Clasification

- Autonomous:
  - Worms
- Non autonomous
  - Virus
  - Trojan Horses
  - Logic bombs
  - Rear doors

MALICIOUS SOFTWARE: Clasification

- Self-reproducing
  - Worms
  - Virus
- Unable to reproduce
  - Trojan Horses
  - Logic bombs
  - Backdoors

MALICIOUS SOFTWARE: Virus

Programs that are contained in others, capable of self-replication placing their copies on different elements of computer programs, where they spread and develop their malignant function

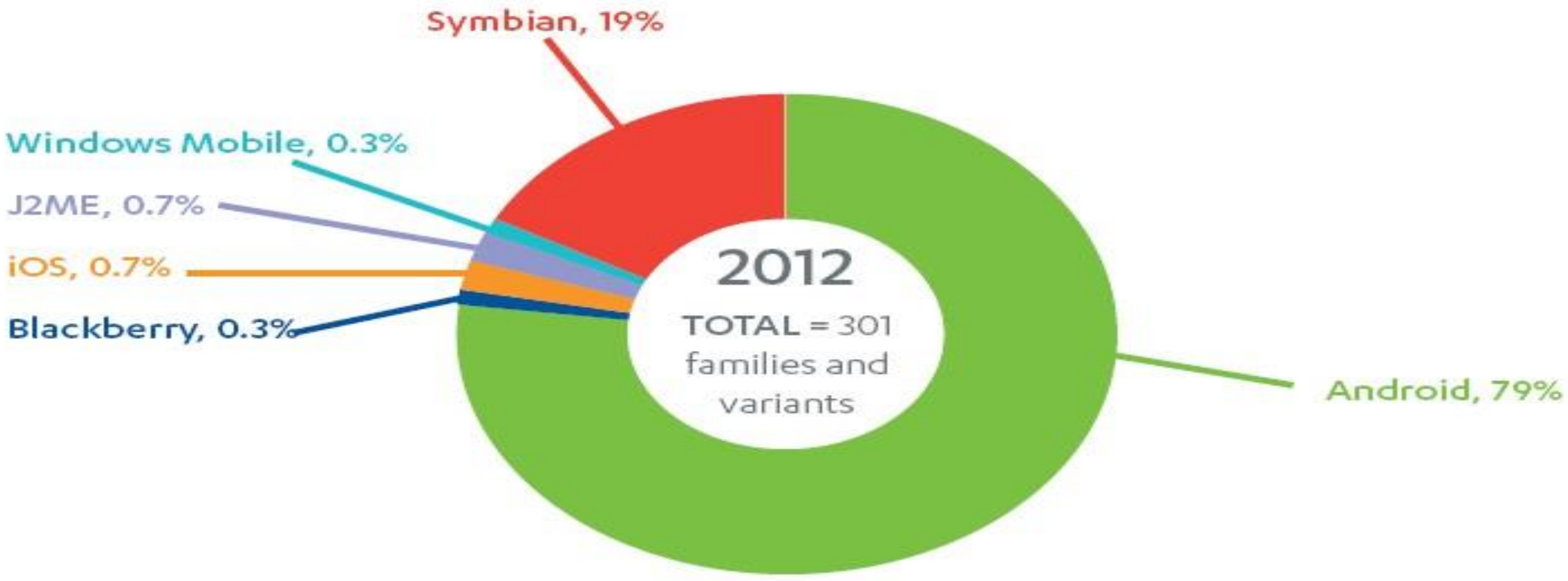
VIRUS. *Smartphone virus*

Cabir

CommWarrior

Worms (Cabir: 2004, IkeeB: 2010)

MOBILE. Malicious software 2012[1]



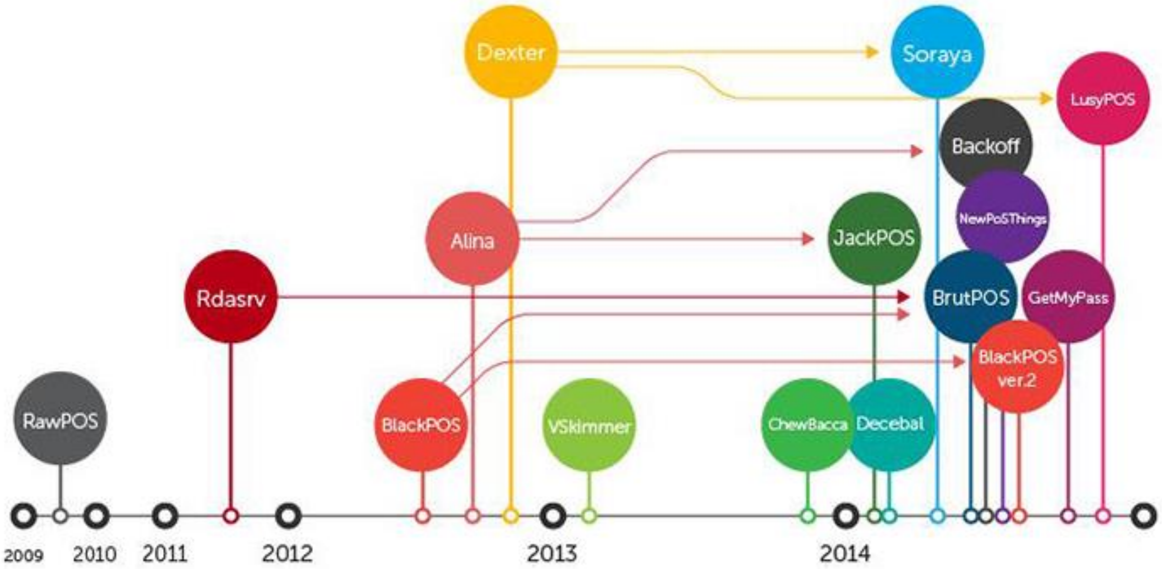
[1] F-Secure. Mobile threat report 2012 Q4

VIRUS. *Point of sale*

Kaptoxa (TrojanPOSRAM)

BlackPOS

Dexter



VIRUS. Duals

Virus.Linux.Bi.a/Virus.Win32.Bi.a (concept test). Year 2006

Smile. Year 2002

Winux (concept test). Year 2001

MALWARE: Phases of a virus

- Propagation (infection)
- Latency
- Activation
- Damage

MALWARE: code of a virus

- Self-reproducing
- Activation
- Damage

MALWARE: Virus Types

- Start (System)
- Files (Programs)
- Memory resident
- Poachers
- Polymorphic (eg criptovirus)
- Macro
- False (Hoax)

Virus

- A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected”.
- Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.

Worm

- A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers.
- Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. **Without user help**
- Unlike a computer virus, it does not need to attach itself to an existing program.
- Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Trojan

- A **Trojan horse**, or **Trojan**, in computing is a generally non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm
- Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.

VIRUSTYPES. *Hoax*

Pay attention to this message, because I had this virus without knowing it, like many other people. Follow the instructions below:

It is contained in a file called "XXX.EXE" and its removal is easy before June 1st, it is when activated ANTIVIRUS SYSTEM NOT FOUND THEN YOU ARE ON.:

- Click the START button - Select SEARCH; FILES OR FOLDERS - Write the filename:? XXX.EXE - Choose LOCAL HARD DRIVES search and then in all memory where any file can be stored

VIRUS TYPE. *Hoax*

- If you find it DO NOT open it from the spot on the ICON (little legible black-white, saying XXX), instead click the right mouse button and select DELETE. It will tell you this is a program and if you delete it, it won´t run a part of Windows. Please ignore all messages and click accept

Once in the trash, choose Empty Recycle Bin. It is important that DO NOT keep it in the trash, because there is could also be activated

PLEASE SPREAD THIS MESSAGE

VIRUS RYPES. *Hoax*

From: jamiep [jamiep@hku.hk]
Sent: Tuesday, November 22, 2011 12:24 To:
undisclosed-recipients:
Subject: King Juan Carlos University user

You have exceeded your Universidad Rey Juan Carlos e-mail quota limit account of 250MB. It is asked you to expand it within 48 hours or your Universidad Rey Juan Carlos email account will be clear from the database. Simply click here to complete information requested and extend the Universidad Rey Juan Carlos e-mail account quota to 450 MB.

Thank you for using Universidad Rey Juan Carlos email services.
Copyright © 2011 Universidad Rey Juan Carlos Clearinghouse.

VIRUS TYPES: Polymorphic

Reproduction: routines that produce different replicas (difficult to detect using signatures). The common method to achieve this is through encryption.

They consist of two parts: One (the malicious code) changes in each replica (though not its function); the other, the decryption routine, remains unchanged.

Polymorphism also occurs in worms.

VIRUS TYPES: Metamorphic

They use NOP instructions, change in records to be used, in the control flow (through jumps), rearranging separate instructions, etc.

Reproduction: routines that produce different replicas (but with the same function), preventing detection by signature, so must be used heuristics.

Rare outside research laboratories.

ADVANCED TECHNIQUES OF EVASION

Shortchange the detection techniques, for example using polymorphism and metamorphism

They aren´t attack programs, but allow them to penetrate into a system without being undetected

MALWARE: Worm

Program that acts autonomously, spreading through the networks, and replicating every time it achieves a system, from which it seeks to other systems connected, in order to continue the process indefinitely

MALWARE: Worm

- First known Worm (1988)
  - Creator: Robert Tappan Morris (23 years)
  - Exploited vulnerability: finger service
  - Infected machines:> 6000
- Sanction: 3 years probation, fined $106, 400 hours of social work

MALWARE: Trojans

Program that apparently or truelly runs a useful function, but hides a segment of harmful or unwanted code that abuses the privileges granted to the execution of that program

MALWARE: Logic Bombs

Code segment of a program that under certain, logical or temporal conditions, is activated, in order to produce an unexpected effect, usually harmful, eg the deletion of data or programs

MALWARE: Backdoor

Input code -not documented, secret and different than the one provided for enter- to a program, that is used to access to it, circumventing the controls and, usually, without the knowledge of its administrator or responsible

MALWARE: Trends

- Annual growth rate: 175%
- 100% have features from worms
- New mechanisms of propagation: P2P, social networks, mobile, ...
- Increased complexity of the malicious code.
- New objectives: PDA, smartphones, POS, ...
- Some tips:
    - Blended Threats: Multiple input vectors.
    - Disabling the protection software (AV, FW, ...)

CHAPTER 2. Programme

1. Tools of attack. Features and types
2. Malicious software. Classification
3. **Kits, Criptovirus, APT**

CRIPTOVIRUS (Ransomware). Features

Based on public key cryptography

Examples of polymorphism

Uses in blackmail

Also criptotroyas, criptoworms, etc.

CRIPTOVIRUS. Phases

Creation

- Generating a pair of keys (public-private)

Installation

- Generation (PRNG) of a secret key (ks) and IV
- Data encryption on the infected computer
- Delete (safely) of the clear data
- Encrypted with the public key (ks) and IV

CRIPTOVIRUS. Phases

Uninstall. The attacker:

- Receive (ks) and IV (encrypted with his public key)
- Check the fulfilling of his impositions
- Gets ks and IV (using his private key)
- Sends Ks and IV to the victim

CRIPTOVIRUS. Effectiveness of the attack

- None, if there are backups
- Impossible to retrieve the private key (the virus only contains the public one)
- Anonymous payment complicated: there are protocols for this (*true anonymous cash*)

CRIPTOVIRUS. Example

Trojan W32/Gpcode. NAA

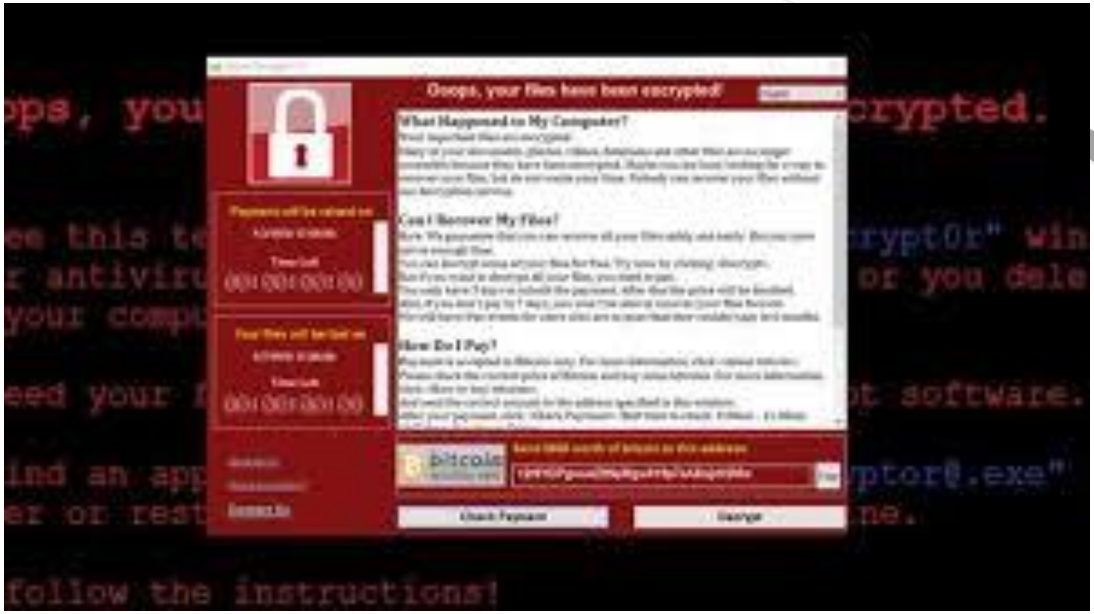
- http://www.f-secure.com/v-descs/gpcode.shtml
- Encryption Type : RSA
- Motivation: Economic Blackmail
- Rescue: Going to URL
- Discovery date: 11-06-2006

Directed Ransomware massive campaign

The CCN-CERT warns of a new massive directed ransomware campaign . Ransomware is a malicious software that, after having encrypted the user documents, displays a message requesting the payment of an specific amount for, allegedly, recover the access to all encrypted files. This campaign is being conducted through emails that try to infect the machine with a variant of **CTB-Locker.**

The email attaches a .ZIP file, which contains a file with extension .scr. It downloads malware to a temporary folder and encrypt files shared drives on the infected computer and displays a message requesting payment so that it can carry out the recovery.

The issues that have been used so far in these…



ops, you … crypted.

ee this te … crypt0r" win
r antiviru … or you dele
your compu

eed your f … t software.

ind an app … ptor@.exe"
er or rest … ne.

follow the instructions!

Ooops, your files have been encrypted!

What Happened to My Computer?

[illegible]

Can I Recover My Files?

[illegible]

How Do I Pay?

[illegible]

Payment will be raised on
Time Left
00:00:00:00
Your files will be lost on
Time Left
00:00:00:00
bitcoin
Send $300 worth of bitcoin to this address:
Check Payment
Decrypt

APTs

- An **advanced persistent threat** (**APT**) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity.
- APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time.
- The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.

ADVANCED PERSISTENT THREATS

Malware designed to act undetected, surviving during a long time

They use sophisticated design tools, some of them have been reused

PERSISTENT ADVANCED THREATS

EXAMPLES

- Stuxnet (SCADA systems)
- Flame
- RSA (SecurID)…

CREATORS (ALLEGEDLY)

- Governments: China; USA; Israel; Russia, ...
- Large corporations
- Criminal organizations

PERSISTENT ADVANCED THREATS. Possible origins

- REGIN (NSA/GCHQ?)
- GHOSTNET (China)
- OCTUBRE ROJO and Turla (Russia?)
- THE MASK (Spain?)
- STUXNET Y FLAME (NSA/GCHQ?)

PERSISTENT ADVANCED THREATS

OBJETIVES

- Countries or enemies corporations
- Critical Infrastructure
- Research centers…

PERSISTENT ADVANCED THREATS

PHASES OF ATTACK

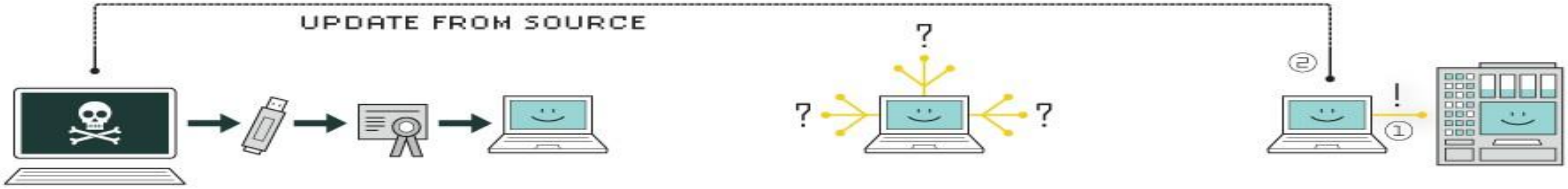
- Identification and target recognition
- Deception of a user (social engineering: spear phishing)
- Exploiting vulnerabilities
- Privilege escalation (to root)
- Installation and operation of remote administration tools (RAT)

PERSISTENT ADVANCED THREATS

DETECTION

- Repeated connections from the same IP
- Transmission of large volumes of data
- Warnings from third parties

HOW STUXNET WORKED



1. infection

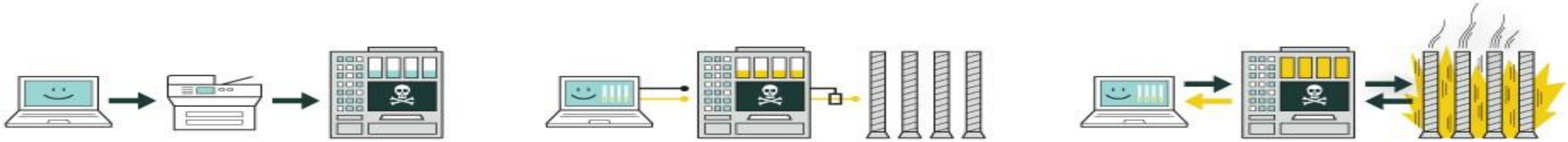
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

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.

Security Engineering

2. Attack tools. Malicious software

COSEC
www.seg.inf.uc3m.es