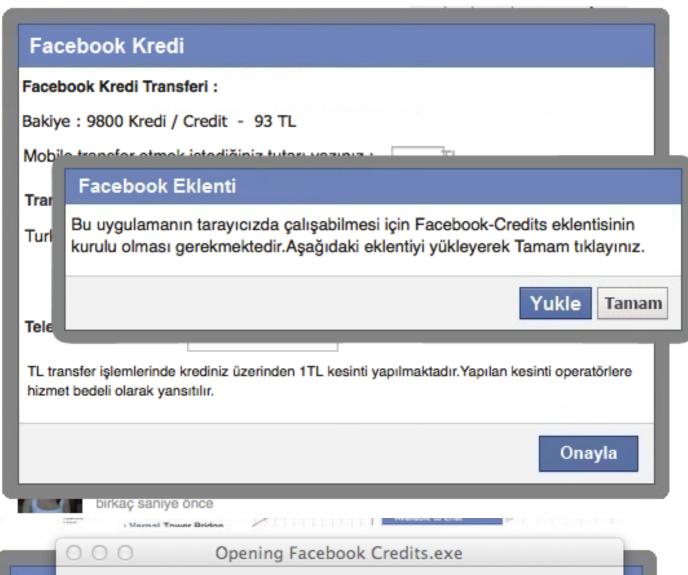
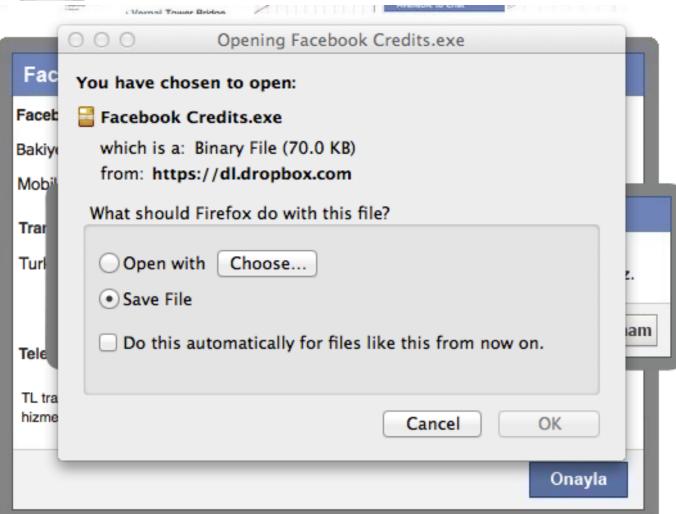
http://credits-facebook.com









https://dl.dropbox.com/s/2k259cgyqpti3vg/Facebook%20Credits.exe?dl=1



SHA256: 254155f50db89481caf7289d0b1503e34cb20b586bd985d9ac0d332f9f93b2a9

Additional information

File name: Facebook Credits.exe

Detection ratio: 0/46

Comments

Analysis date: 2013-02-14 15:13:04 UTC (23 hours, 4 minutes ago)



Antivirus Result Update Agnitum 20130214 AhnLab-V3 20130214 AntiVir 20130214

Analysis Votes Additional information

Votes

Analysis

1536:c1j9tyUHmRMkMgWHTxqZWldMYFfVb686HDUc:c1j3yUHmlWEuOYFfVb6FDUc

TrID

Generic CIL Executable (.NET, Mono, etc.) (85.3%)

Win32 Executable Generic (9.9%)

Generic Win/DOS Executable (2.3%)

DOS Executable Generic (2.3%)

Autodesk FLIC Image File (extensions: flc, fli, cel) (0.0%)

ExifTool

SubsystemVersion..... 4.0

Comments..... www.facebook.com

InitializedDataSize....: 7680 ImageVersion..... 0.0

ProductName..... www.facebook.com

FileVersionNumber....: 1.0.0.0 UninitializedDataSize....: 0 LanguageCode..... Neutral FileFlagsMask..... 0x003f CharacterSet..... Unicode



LinkerVersion....: 8.0

OriginalFilename...: Facebook Credits.exe

MIMEType...: application/octet-stream

Subsystem...: Windows GUI

FileVersion...: 1.0.0.0

TimeStamp...: 2013:02:03 02:27:12+00:00

FileType...: Win32 EXE

PEType...: PE32

InternalName...: Facebook Credits.exe

ProductVersion..: 1.0.0.0

FileDescription.: Facebook Credits

OSVersion...... 4.0 FileOS..... Win32

LegalCopyright.....: www.facebook.com Copyright 2013 MachineType...... Intel 386 or later, and compatibles

CompanyName..... www.facebook.com

ObjectFileType..... Executable application

AssemblyVersion..... 1.0.0.0

Sigcheck

publisher....: www.facebook.com
product...: www.facebook.com
internal name...: Facebook Credits.exe

copyright....: www.facebook.com Copyright (c) 2013

original name....: Facebook Credits.exe comments...: www.facebook.com

file version..... 1.0.0.0

description..... Facebook Credits

Portable Executable structural information

Compilation timedatestamp....: 2013-02-03 02:27:12

Target machine.....: 0x14C (Intel 386 or later processors and compatible processors)

Entry point address.....: 0x000117B6

PE Sections....:

 Name
 Virtual Address
 Virtual Size
 Raw Size
 Entropy
 MD5

 .text
 8192
 63420
 63488
 5.97
 03378c918aa450d3d251f188d7f7bbbf

 .rsrc
 73728
 7164
 7168
 4.84
 5de629464ccbaf468f00db00befeac2b

 .reloc
 81920
 12
 512
 0.10
 eb5f25ab117aecd4db68b0f9d44faa4e

PE Imports....:

[[mscoree.dll]] _CorExeMain

PE Resources....:

Resource type Number of resources

 RT_ICON
 2

 RT_GROUP_ICON
 1

 RT_VERSION
 1

 RT_MANIFEST
 1

Resource language Number of resources

NEUTRAL 5

Symantec Reputation

Suspicious.Insight

First seen by VirusTotal

2013-02-10 16:48:17 UTC (4 days, 21 hours ago)

Last seen by VirusTotal

2013-02-15 14:14:26 UTC (3 minutes ago)

File names (max. 25)

- 1. file-5147094 exe
- 254155f50db89481caf7289d0b1503e34cb20b586bd985d9ac0d332f9f93b2a9
- Facebook Credits.exe

Sucuri SiteCheck

Free Website Malware Scanner

Sitecheck Results

Website details

Blacklisting status



web site: credits-facebook.com

status: Site blacklisted, malware not

identified

web trust: Site blacklisted.

*This site was just scanned a few minutes ago.

Security report (Warnings found):

National Nat

Malware: No

Malicious javascript: No

Malicious iFrames: No

Drive-By Downloads: No

Anomaly detection: No

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information.

Domain Name: CREDITS-FACEBOOK.COM

Registrar: <u>INTERNET.BS</u> CORP. **Whois Server:** <u>whois.internet.bs</u>

Referral URL: http://www.internet.bs

Name Server: ELLE.NS.CLOUDFLARE.COM
Name Server: PHIL.NS.CLOUDFLARE.COM
clientTransferProhibited

Updated Date: 18-oct-2012 **Creation Date:** 18-oct-2012 **Expiration Date:** 18-oct-2013

>>> Last update of whois database: Fri, 15 Feb 2013 13:40:49 UTC <<<

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Domain credits-facebook.com

Date Registered: 2012-10-18
Date Modified: 2012-10-18
Expiry Date: 2013-10-18
DNS1: elle.ns.cloudflare.com
DNS2: phil.ns.cloudflare.com

Registrant

Fundacion Private Whois Domain Administrator

Email:508030eew8rum5kc@t02cduv4f7f99a255f64.privatewhois.net

Attn: credits-facebook.com Aptds. 0850-00056 Zona 15 Panama

Panama

Tel: +507.65995877

Administrative Contact Fundacion Private Whois Domain Administrator

Email: 508030 eed 281 gep1 @ t02 cduv4 f7 f99 a 255 f64. private who is.net to the contract of the contract

Attn: <u>credits-facebook.com</u> Aptds. 0850-00056 Zona 15 Panama

Panama

Tel: +507.65995877

Technical Contact Fundacion Private Whois Domain Administrator

 $Email: 508030 \texttt{eesf6rvtaf@} \underline{t02cduv4f7f99a255f64.privatewho is.net}$

Attn: <u>credits-facebook.com</u> Aptds. 0850-00056 Zona 15 Panama

Panama

Tel: +507.65995877

Registrar: <u>Internet.bs</u> Corp.

Registrar's Website : http://www.internetbs.net/