

Index of /crm/css

Name	Last modified	Size	Description
 Parent Directory		-	
 TuneUpUtilities32.css	17-Apr-2013 17:49	4.4M	
 TuneUpUtilities32.gif	19-Apr-2013 16:18	3.4M	

Apache/2.2.3 (CentOS) Server at ydyo.erciyes.edu.tr Port 80

<https://www.virustotal.com/en/file/10277bdbde086ddc7d81d56249b3bd8d50e4821967fc24fe947afecf21da989e/analysis/1366790961/>



SHA256: 10277bdbde086ddc7d81d56249b3bd8d50e4821967fc24fe947afecf21da989e

SHA1: 50f0053203b0f6b6130ff5d7512da72c849a7764

MD5: a7689cba115086de6034062af525109c

File size: 4.4 MB (4644154 bytes)

File name: TuneUpUtilities32.css


File type: DOS EXE

Detection ratio: 0 / 46

Analysis date: 2013-04-24 08:09:21 UTC (0 minutes ago)




 Less details

 Analysis

 Additional information

 Comments

 Votes

Antivirus	Result	Update
Agnitum		20130423
AhnLab-V3		20130423

ssdeep

98304:B1qP0d4q/ZuP+2RaO9Qu3fawgXmoa8l5Uo4BpoM1DPFwDgm:zqY/ZuP9RaOKuP6VaNUFBpT9/

TrID

Win32 Executable (generic) (61.9%)

Generic Win/DOS Executable (19.0%)

DOS Executable Generic (19.0%)

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

ExifTool

```
MIMEType.....: application/octet-stream
FileType.....: DOS EXE
FileCreateDate.....: 2013:04:24 09:13:54+01:00
FileAccessDate.....: 2013:04:24 09:13:54+01:00
```

First seen by VirusTotal

2013-04-24 07:49:45 UTC (57 minutes ago)

Last seen by VirusTotal

2013-04-24 08:13:57 UTC (33 minutes ago)

File names (max. 25)

1. TuneUpUtilities32 copy.exe
2. TuneUpUtilities32.css



SHA256:75abcd38c3228965ab0a3c36823ab74a7199ebbf0a97a47f08aea0e35ebdc611

SHA1:9ad497418d0781a6faf79c905250fcd3dc207252

MD5:30e02ca480716f322d1c8121beaa8c99

File size:3.4 MB (3609600 bytes)

File name:TuneUpUtilities32.gif

File type:Win32 EXE

Detection ratio:18 / 45

Analysis date:2013-04-24 08:08:01 UTC (0 minutes ago)

10

Less details

- Analysis
- Additional information
- Comments
- Votes

Antivirus	Result	Update
Agnitum	Suspicious!SA	20130423
AhnLab-V3	✓	20130423

- Analysis
- Additional information
- Comments
- Votes

ssdeep
98304:e7qM76o1dMgwK+YSQ28XKRiVfiU5nkQgU:e9vdMvYSIXKRiVHeQ7

TrID
Win32 Executable (generic) (51.7%)
Win16/32 Executable Delphi generic (16.4%)
Generic Win/DOS Executable (15.8%)
DOS Executable Generic (15.8%)
Autodesk FLIC Image File (extensions: flic, fli, cel) (0.0%)

ExifTool

```
LegalTrademarks.....:
SubsystemVersion.....: 4.0
Comments.....:
InitializedDataSize.....: 2041344
ImageVersion.....: 0.0
ProductName.....: Principal
FileVersionNumber.....: 10.1.1.1
UninitializedDataSize....: 0
LanguageCode.....: Portuguese (Brazilian)
FileFlagsMask.....: 0x003f
CharacterSet.....: Windows, Latin1
LinkerVersion.....: 2.25
OriginalFilename.....:
MIMEType.....: application/octet-stream
Subsystem.....: Windows GUI
FileVersion.....: 10.1.1.1
TimeStamp.....: 1992:06:19 23:22:17+01:00
FileType.....: Win32 EXE
PEType.....: PE32
InternalName.....:
FileAccessDate.....: 2013:04:24 09:07:58+01:00
ProductVersion.....: 10.1.1.1
FileDescription.....: Principal
OSVersion.....: 4.0
FileCreateDate.....: 2013:04:24 09:07:58+01:00
FileOS.....: Win32
LegalCopyright.....:
MachineType.....: Intel 386 or later, and compatibles
CompanyName.....: Principal

CodeSize.....: 1844224
FileSubtype.....: 0
ProductVersionNumber.....: 10.1.1.1
EntryPoint.....: 0x5b6000
ObjectFileType.....: Executable application
```

Sigcheck

```
publisher.....: Principal
product.....: Principal
description.....: Principal
file version.....: 10.1.1.1
```

Portable Executable structural information

```
Compilation timestamp.....: 1992-06-19 22:22:17
Target machine.....: Intel 386 or later processors and compatible processors
Entry point address.....: 0x00586000
```

PE Sections.....:

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
	4096	2060288	818688	7.98	c8e814905476223e0cb8280f7b98c7fd
.rsrc	2064384	1850633	1846784	7.99	e2a06a7e3f83a167a3c4cde26d0d082e
.idata	3915776	4096	512	1.28	cc05cebfd9f997cc96e0348c84c0f0ff
	3919872	1126400	512	0.26	5cd8d75ebad5f0a191ad550669128cfa
cdbfnmfy	5046272	942080	938496	7.89	454f4a9a9dab0ca3b4368f978233a611
mnpzpxyj	5988352	4096	512	4.00	7c24dd863a0243511fa9729f99061bdd

PE Imports.....:

[[kernel32.dll]]

lstrcpy

[[comctl32.dll]]

InitCommonControls

PE Resources.....:

Resource type	Number of resources
RT_STRING	40
RT_BITMAP	21
RT_GROUP_CURSOR	8
RT_RCDATA	8
RT_CURSOR	8
RT_ICON	5
RT_DIALOG	1
RT_MANIFEST	1
RT_VERSION	1
RT_GROUP_ICON	1

Resource language	Number of resources
NEUTRAL	87
PORTUGUESE BRAZILIAN	7

Symantec Reputation

[Suspicious.Insight](#)

First seen by VirusTotal

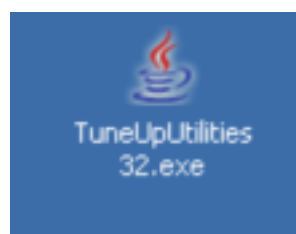
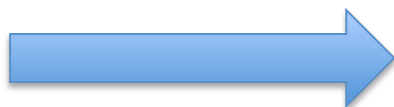
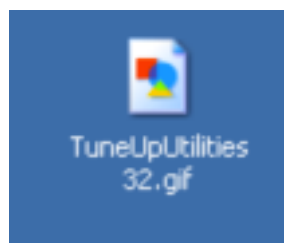
2013-04-20 11:13:39 UTC (3 days, 21 hours ago)

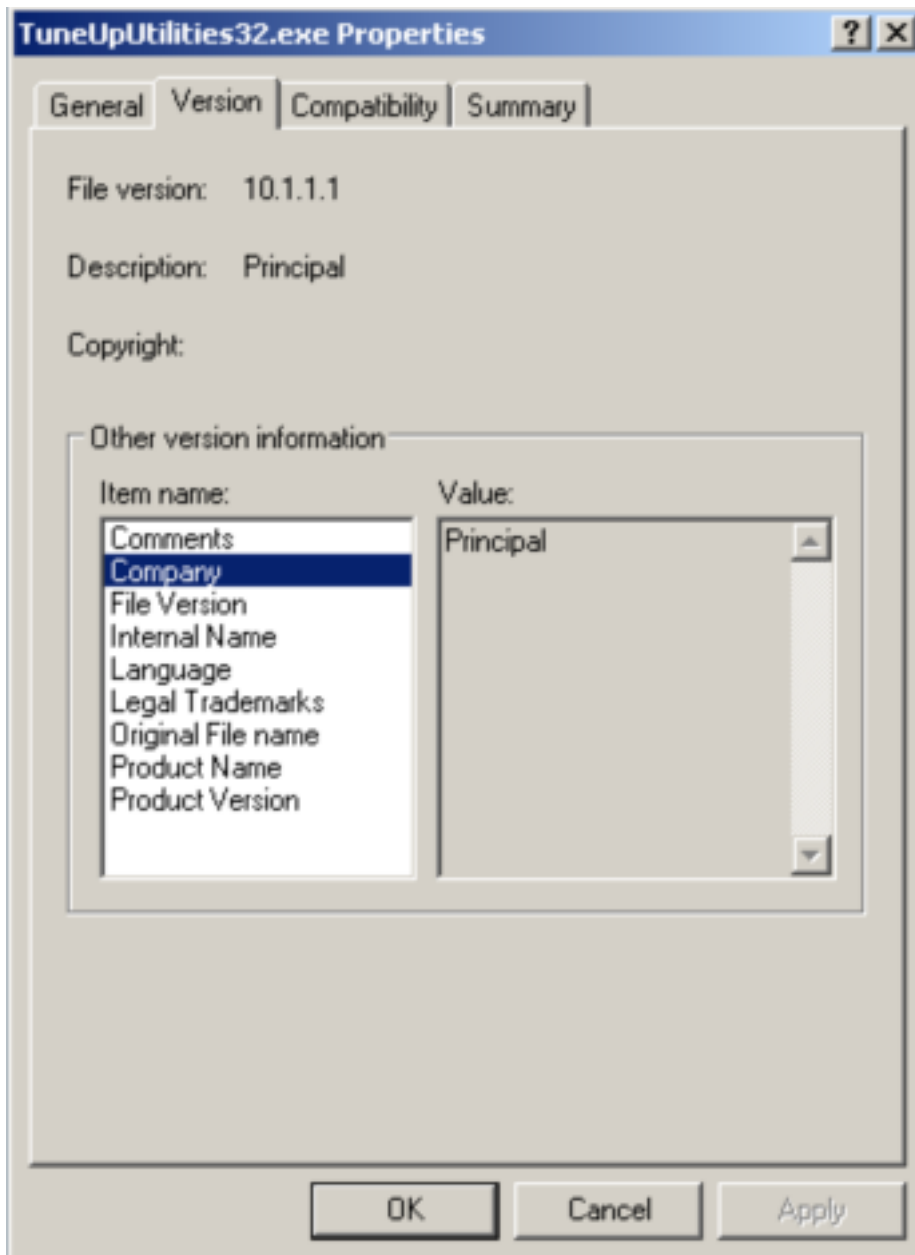
Last seen by VirusTotal

2013-04-24 08:08:01 UTC (43 minutes ago)

File names (max. 25)

1. TuneUpUtilities32.gif
2. TuneUpUtilities32.gi
3. 30e02ca480716f322d1c8121beaa8c99.9ad497418d0781a6faf79c905250fcd3dc207252
4. TuneUpUtilities32.exe





Filter: dns Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
7	15.6541940	192.168.68.134	192.168.68.2	DNS	76	Standard query 0x16e5 A navespace.com.br
8	16.0264890	192.168.68.2	192.168.68.134	DNS	92	Standard query response 0x16e5 A 200.98.197.57
15	16.5398210	192.168.68.134	192.168.68.2	DNS	74	Standard query 0x647e A azylawfirm.com
18	16.7152470	192.168.68.2	192.168.68.134	DNS	90	Standard query response 0x647e A 184.154.74.178
31	49.5897760	192.168.68.134	192.168.68.2	DNS	76	Standard query 0x7645 A navespace.com.br
32	49.6655540	192.168.68.2	192.168.68.134	DNS	92	Standard query response 0x7645 A 200.98.197.57

No.	Time	Source	Destination	Protocol	Length	Info
9	16.0275010	192.168.68.134	200.98.197.57	TCP	62	marcam-lm > http [SYN] Seq=0 win=16384 Len=0 MSS=1460 SACK
10	16.2750960	200.98.197.57	192.168.68.134	TCP	60	http > marcam-lm [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MS
11	16.2751860	192.168.68.134	200.98.197.57	TCP	54	marcam-lm > http [ACK] Seq=1 Ack=1 win=17520 Len=0
12	16.2754530	192.168.68.134	200.98.197.57	HTTP	270	GET /vw/0.inf HTTP/1.1
13	16.2756610	200.98.197.57	192.168.68.134	TCP	60	http > marcam-lm [ACK] Seq=1 Ack=217 win=64240 Len=0
14	16.5310580	200.98.197.57	192.168.68.134	HTTP	473	HTTP/1.1 200 OK (text/plain)
16	16.6315050	200.98.197.57	192.168.68.134	HTTP	473	[TCP Retransmission] HTTP/1.1 200 OK (text/plain)
17	16.6315340	192.168.68.134	200.98.197.57	TCP	54	marcam-lm > http [ACK] Seq=217 Ack=420 win=17101 Len=0
30	23.6744110	192.168.68.134	200.98.197.57	TCP	54	marcam-lm > http [RST, ACK] Seq=217 Ack=420 win=0 Len=0

Follow TCP Stream

Stream Content

```

GET /vw/0.1nf HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1;
Trident/4.0; .NET4.0C; .NET4.0E)
Host: navespace.com.br
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: wed, 24 Apr 2013 09:09:52 GMT
Content-Type: text/plain
Content-Length: 150
Connection: keep-alive
Keep-Alive: timeout=15
Server: Apache
Last-Modified: Sun, 07 Apr 2013 15:13:12 GMT
ETag: "60d8015-96-4d9c6c2375200"
Accept-Ranges: bytes

6BD8
6BD8
6BD8
FC37F122C3769545E70F30D5033A
BD71B26580AE924E81A35385AD6883BC6E16D5120521D21E1932EB
12D8150B21D10422
FC37F122C3769545E70F30D5033A

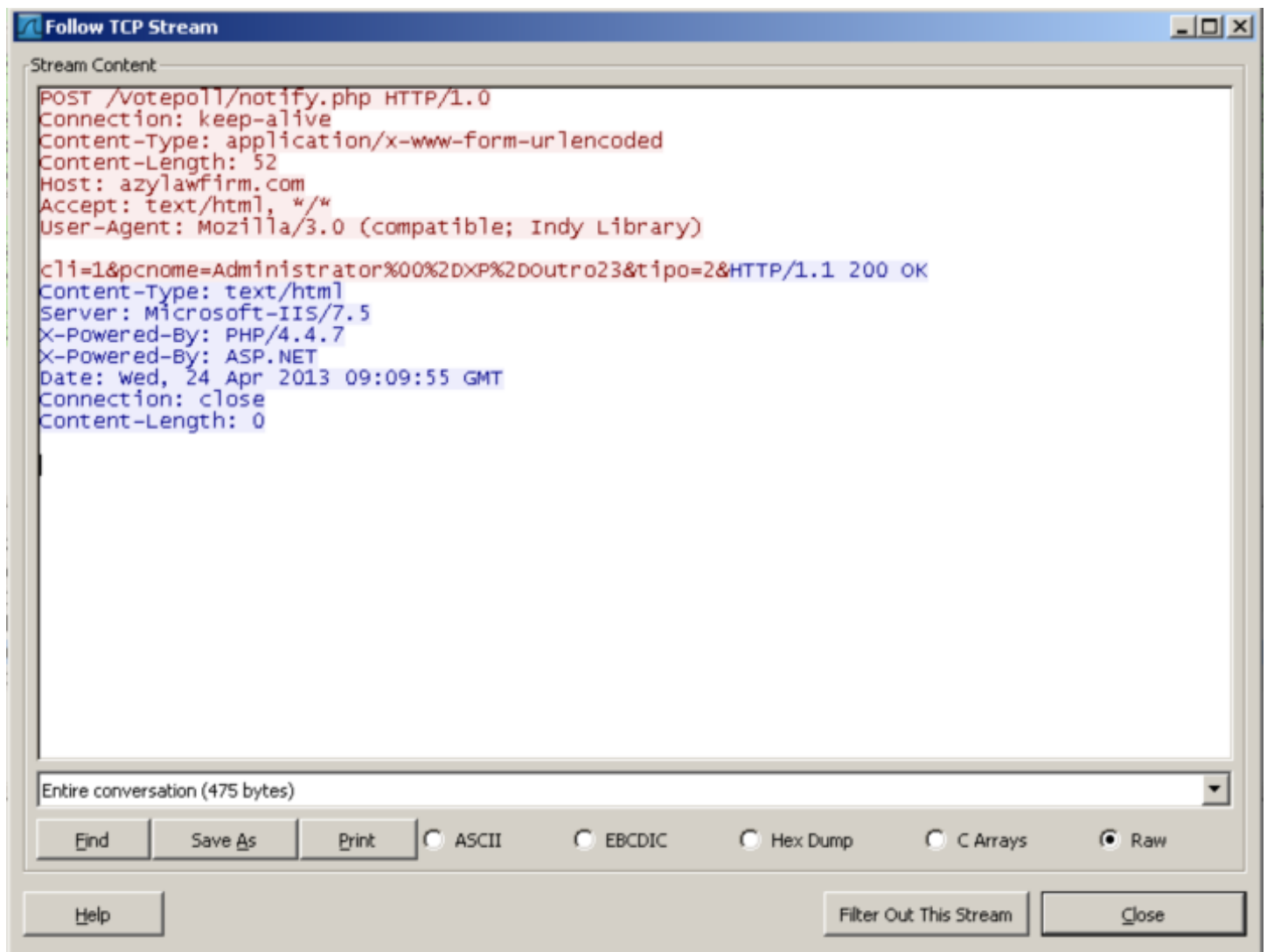
```

Entire conversation (635 bytes)

Find Save As Print ☐ ASCII ☐ EBCDIC ☐ Hex Dump ☐ C Arrays ☒ Raw

Help Filter Out This Stream Close

No.	Time	Source	Destination	Protocol	Length	Info
19	16.7156820	192.168.68.134	184.154.74.178	TCP	62	proxima-lm > http [SYN] Seq=0 win=16384 Len=0 MSS=1460 SAC
20	16.8821010	184.154.74.178	192.168.68.134	TCP	60	http > proxima-lm [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 M
21	16.8821480	192.168.68.134	184.154.74.178	TCP	54	proxima-lm > http [ACK] Seq=1 Ack=1 win=17520 Len=0
22	16.8824530	192.168.68.134	184.154.74.178	TCP	283	[TCP segment of a reassembled PDU]
23	16.8826350	184.154.74.178	192.168.68.134	TCP	60	http > proxima-lm [ACK] Seq=1 Ack=230 win=64240 Len=0
24	16.8826570	192.168.68.134	184.154.74.178	HTTP	106	POST /votepoll/notify.php HTTP/1.0 (application/x-www-for
25	16.8827510	184.154.74.178	192.168.68.134	TCP	60	http > proxima-lm [ACK] Seq=1 Ack=282 win=64240 Len=0
26	17.9856180	184.154.74.178	192.168.68.134	HTTP	248	HTTP/1.1 200 OK
27	17.9856720	192.168.68.134	184.154.74.178	TCP	54	proxima-lm > http [ACK] Seq=282 Ack=196 win=17326 Len=0
28	17.9903410	192.168.68.134	184.154.74.178	TCP	54	proxima-lm > http [FIN, ACK] Seq=282 Ack=196 win=17326 Len
29	17.9907800	184.154.74.178	192.168.68.134	TCP	60	http > proxima-lm [ACK] Seq=196 Ack=283 win=64239 Len=0



<http://navespace.com.br/>

Aviso!

Site aguardando publicação de arquivos.

Profile
Founder
Practice
Press Release
Lawyers
Clients
Contact us



نبذة
المؤسس
إختصاصا
أخبارنا
المحامون
العملاء
الإتصال بنا





Ahmed Zaki Yamani
Lawyers & Legal Consultants
since 1956
أحمد زكي يماني
محامون ومستشارون قانونيون
منذ 1956



إستشارة أون لاين

:: Webmail ::



Regulations	Academic Calendar	Activities	Exam Results	Contact	Search...	 
-------------	-------------------	------------	--------------	---------	-----------	---

- Home Page
- About Us
- Makbule Küçükçalık
- Administration
- Modern Languages Department
- Department of Basic English
- Academic Staff
- FAQ
- Hazırlık Sınıfında Uyulması Gereken Kurallar
- Information About The Proficiency Exam

