CuteCats.exe and the Arab Spring

Morgan Marquis-Boire

Disclaimer

Any views expressed in this talk are my own and not those of my employer.

This talk discusses work performed in my spare time analyzing malware I personally received. Analysis was published with the EFF and Citizen Lab, independently of Google.

Cute Cats Theories

Ethan Zuckerman - The Cute Cat Theory of Digital Activism

“Sufficiently usable read/write platforms will attract porn and activists”

(and lolcats)

Cute Cats Theories

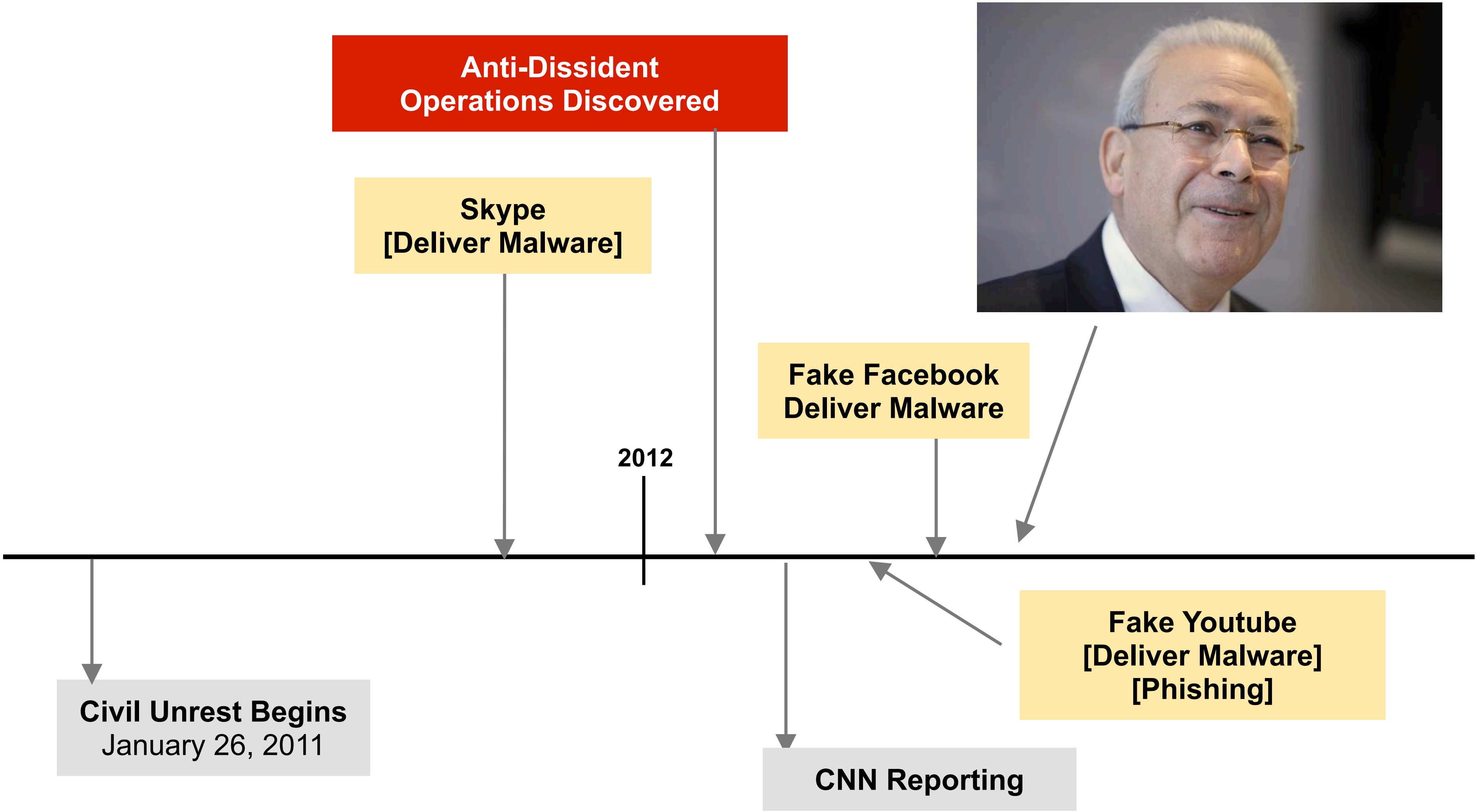
Cute Cats Theories

Morgan Marquis-Boire - The CuteCats.exe Theory of Digital Activism

“Once a platform attracts a critical mass of activists, it will be used to target them”

SYRIA

Anti-Dissident Campaign



Anti-Dissident Operations Discovered

Skype [Deliver Malware]

2012

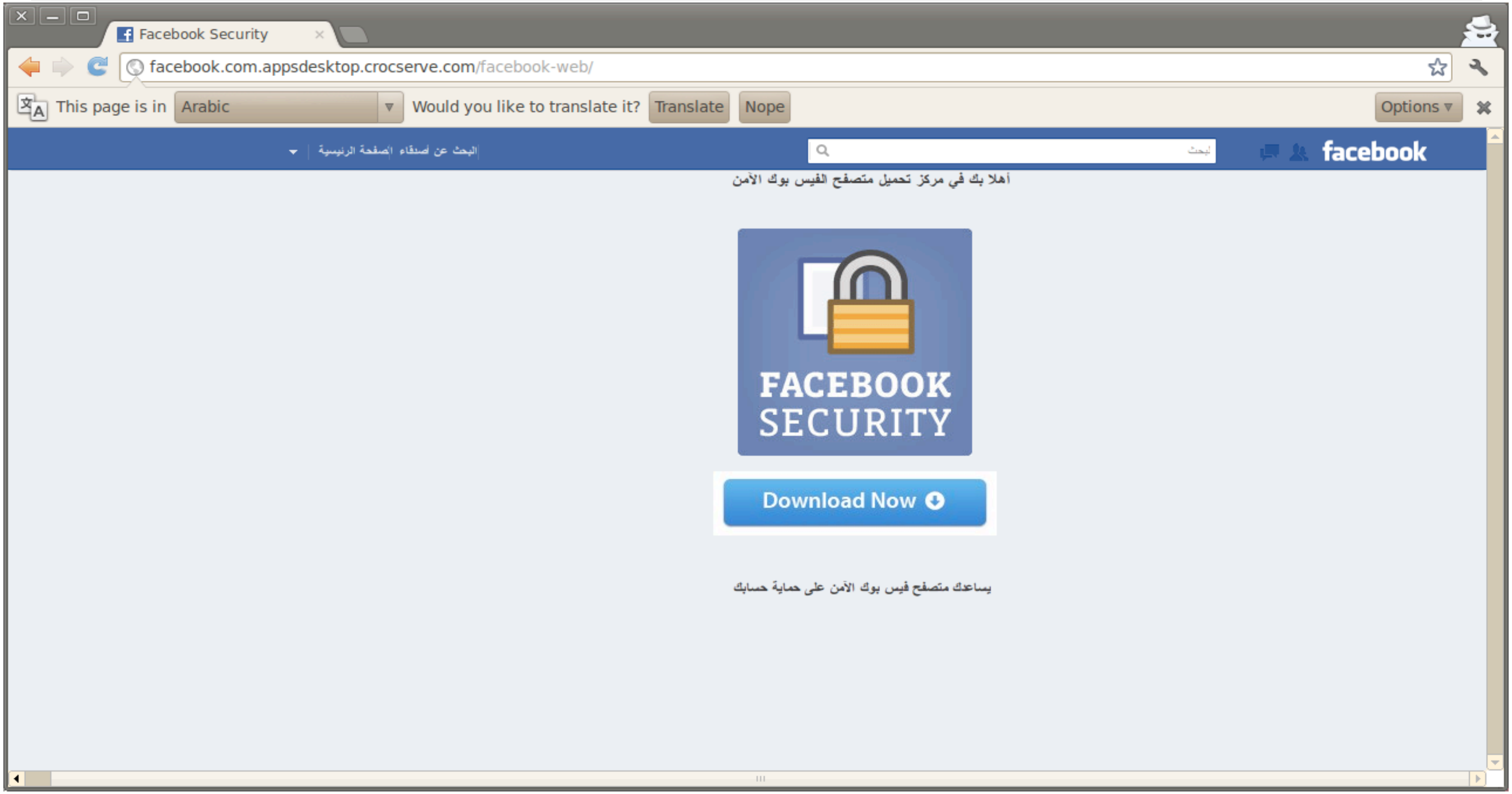
Fake Facebook Deliver Malware

Civil Unrest Begins January 26, 2011

CNN Reporting

Fake Youtube [Deliver Malware] [Phishing]

Burhan Ghalioun Facebook Hack



facebook.com.appsdesktop.crocserve.com/facebook-web/

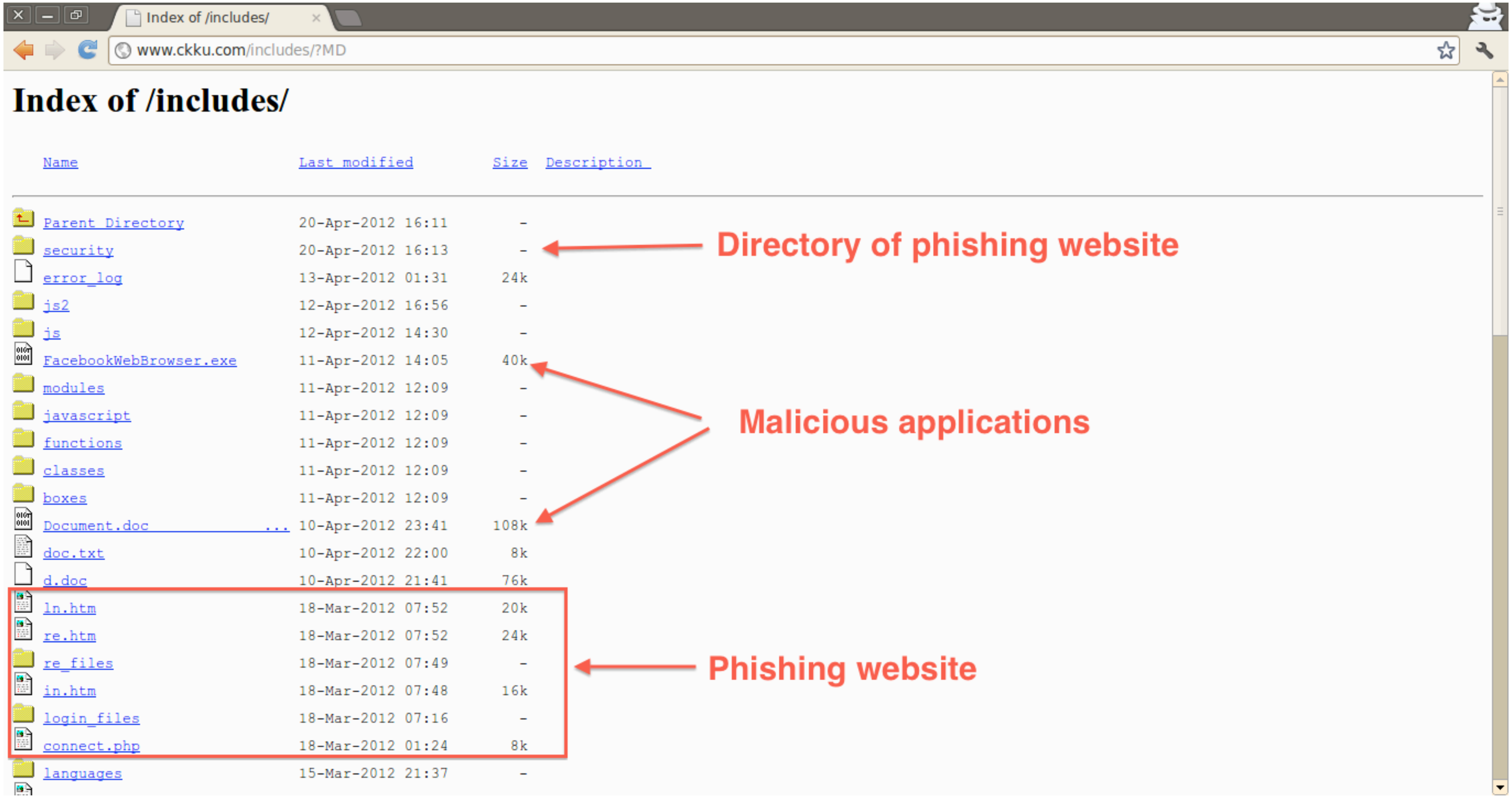
This page is in Arabic Would you like to translate it?

أهلا بك في مركز تحميل متصفح الفيس بوك الأمن

يساعدك متصفح فيس بوك الآمن على حماية حسابك

https://www.eff.org/deeplinks/2012/04/new-wave-facebook-phishing-attacks-targets-syrian-activists

Burhan Ghalioun Facebook Hack



Index of /includes/

```
     Name                            Last modified         Size  Description

     Parent Directory                20-Apr-2012 16:11        -
     security                        20-Apr-2012 16:13        -
     error_log                       13-Apr-2012 01:31      24k
     js2                             12-Apr-2012 16:56        -
     js                              12-Apr-2012 14:30        -
     FacebookWebBrowser.exe          11-Apr-2012 14:05      40k
     modules                         11-Apr-2012 12:09        -
     javascript                      11-Apr-2012 12:09        -
     functions                       11-Apr-2012 12:09        -
     classes                         11-Apr-2012 12:09        -
     boxes                           11-Apr-2012 12:09        -
     Document.doc                ... 10-Apr-2012 23:41     108k
     doc.txt                         10-Apr-2012 22:00       8k
     d.doc                           10-Apr-2012 21:41      76k
     ln.htm                          18-Mar-2012 07:52      20k
     re.htm                          18-Mar-2012 07:52      24k
     re_files                        18-Mar-2012 07:49        -
     in.htm                          18-Mar-2012 07:48      16k
     login_files                     18-Mar-2012 07:16        -
     connect.php                     18-Mar-2012 01:24       8k
     languages                       15-Mar-2012 21:37        -
```

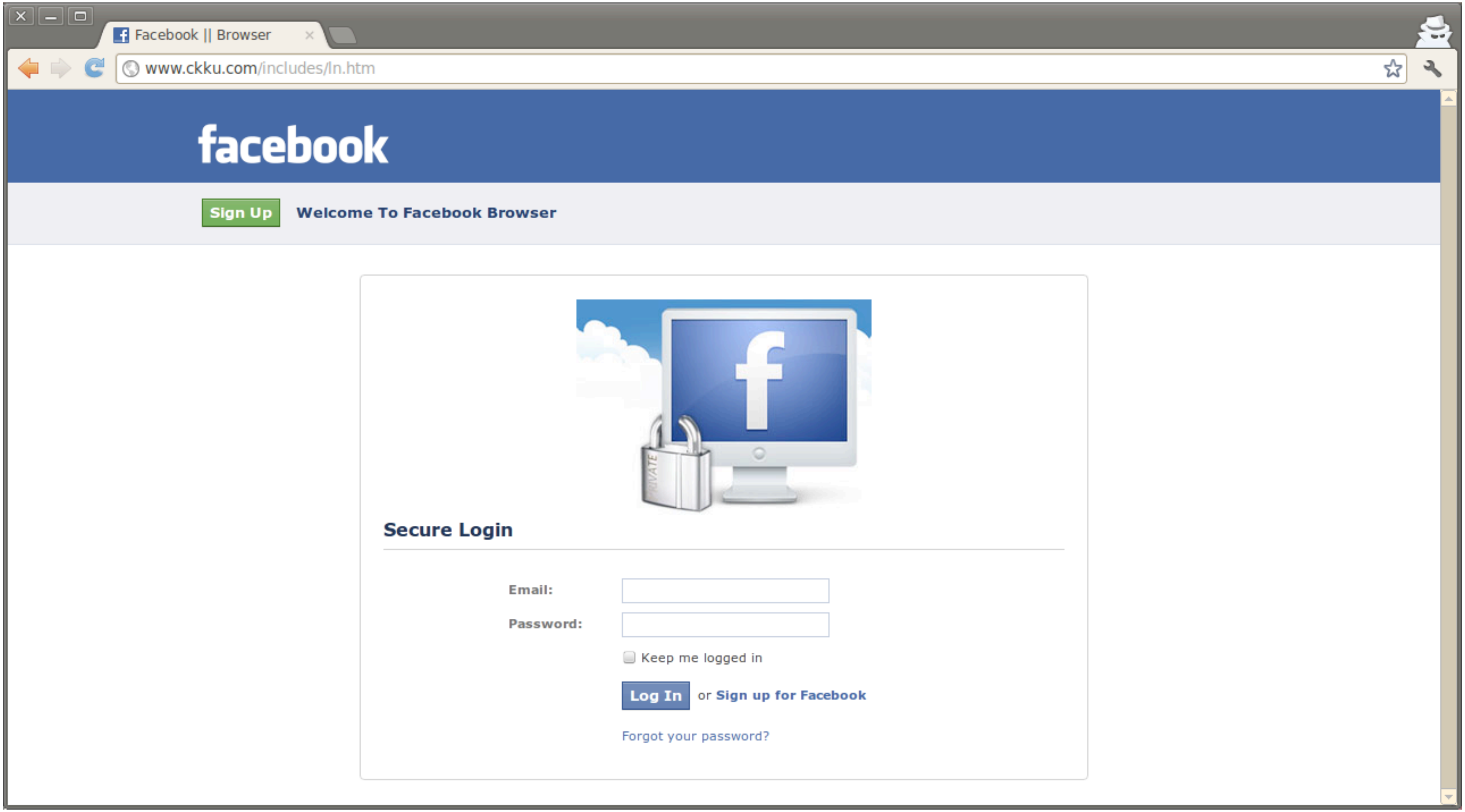
Directory of phishing website

Malicious applications

Phishing website

https://www.eff.org/deeplinks/2012/04/new-wave-facebook-phishing-attacks-targets-syrian-activists

Burhan Ghalioun Facebook Hack



Welcome To Facebook Browser

Secure Login

Email:

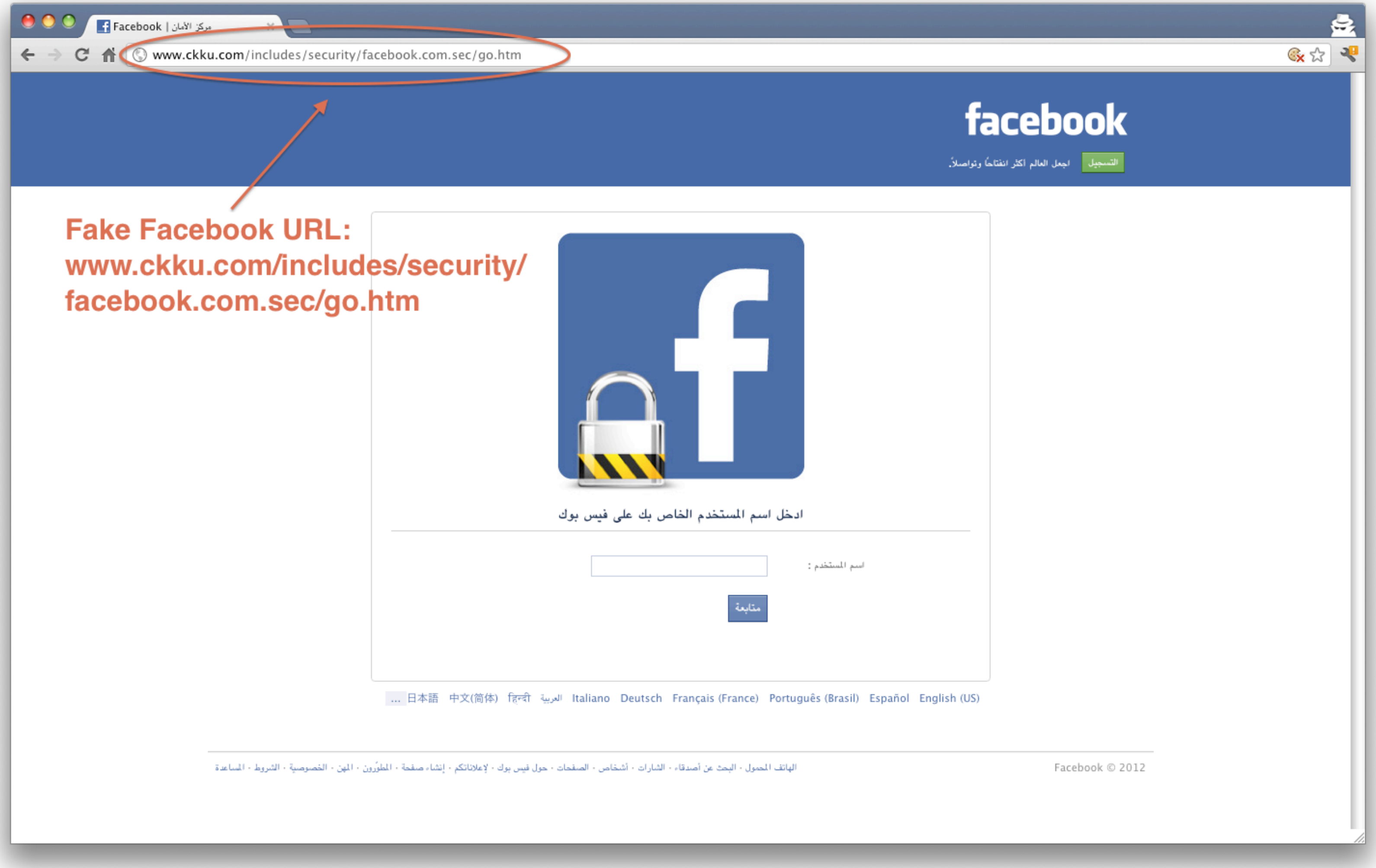
Password:

□ Keep me logged in

or Sign up for Facebook

Forgot your password?

Burhan Ghalioun Facebook Hack



Facebook | مركز الأمان

www.ckku.com/includes/security/facebook.com.sec/go.htm

facebook

التسجيل اجعل العالم اكثر انفتاحاً وتواصلاً.

Fake Facebook URL: www.ckku.com/includes/security/facebook.com.sec/go.htm

ادخل اسم المستخدم الخاص بك على فيس بوك

اسم المستخدم :

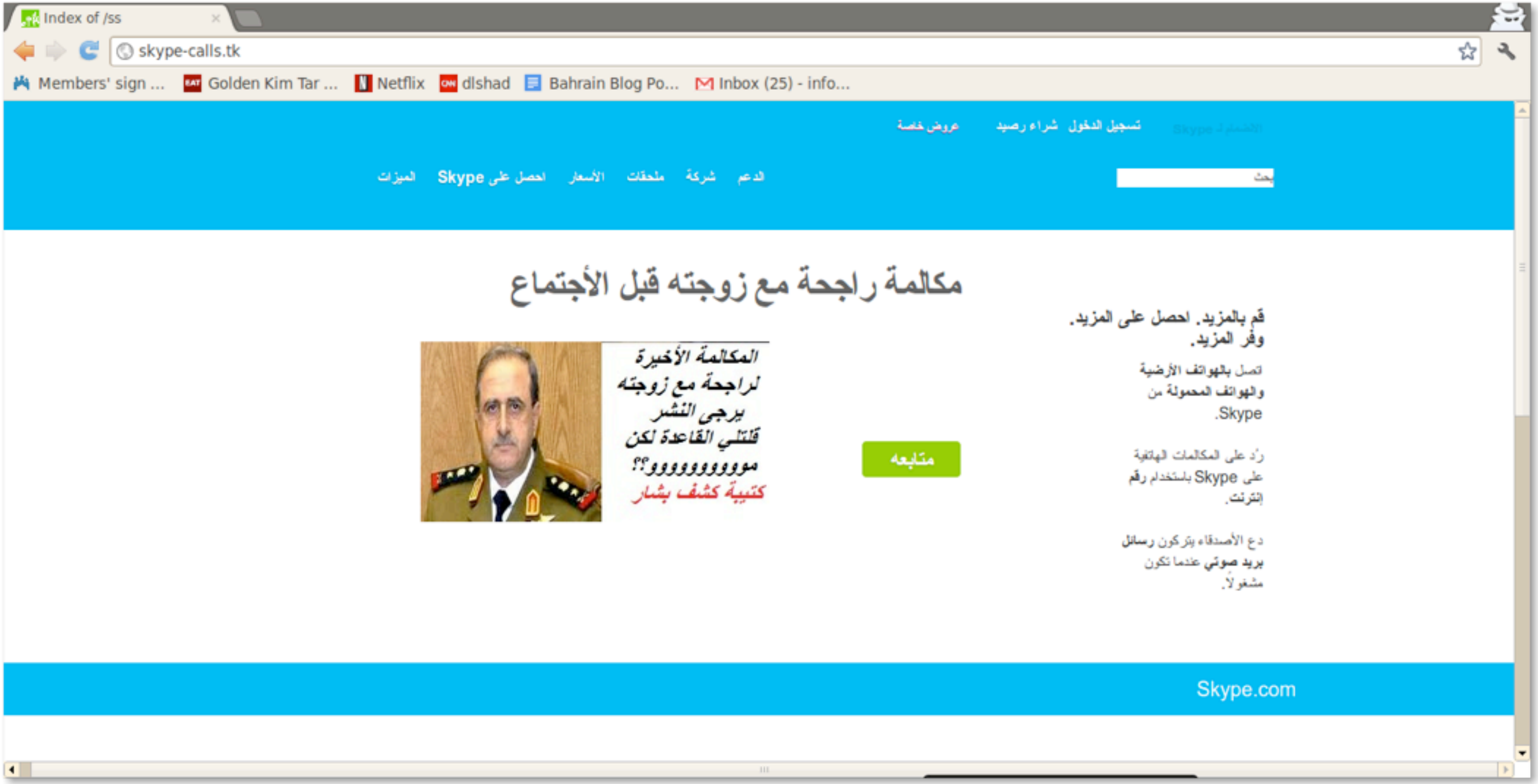
متابعة

... 日本語 中文(简体) हिन्दी العربية Italiano Deutsch Français (France) Português (Brasil) Español English (US)

الهاتف المحمول · البحث عن أصدقاء · الشارات · أشخاص · الصفحات · حول فيس بوك · لإعلاناتكم · إنشاء صفحة · المطوّرون · المهن · الخصوصية · الشروط · المساعدة

Facebook © 2012

Suicide Bombing and Phishing



مكالمة راجحة مع زوجته قبل الأجتماع

المكالمة الأخيرة
لراجحة مع زوجته
يرجى النشر
قلتلي القاعدة لكن
موووووووووو؟؟
كتيبة كشف بشار

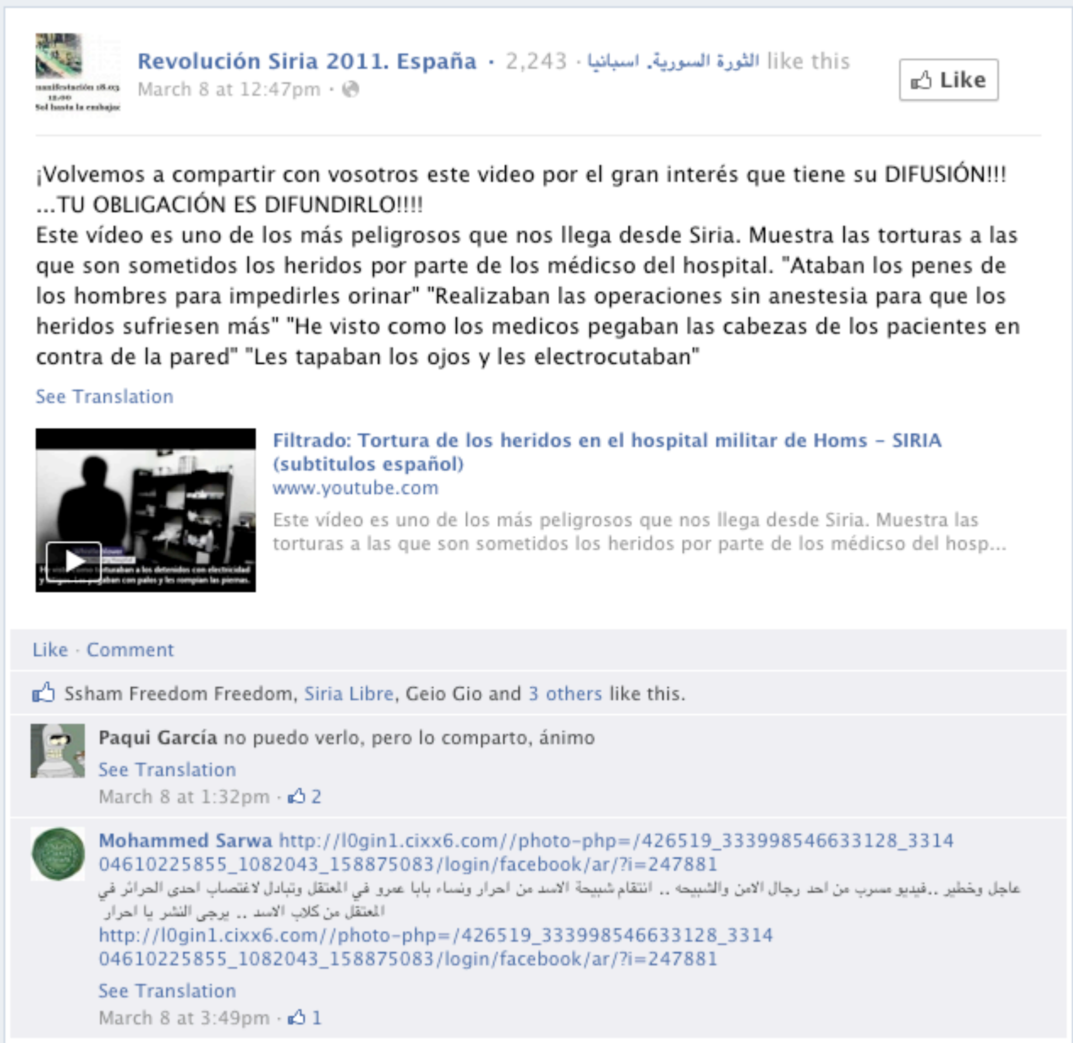
قم بالمزيد. احصل على المزيد.
وفر المزيد.

تصل بالهواتف الأرضية
والهواتف المحمولة من
.Skype

رُد على المكالمات الهاتفية
على Skype باستخدام رقم
إنترنت.

دع الأصدقاء يتركون رسائل
بريد صوتي عندما تكون
مشغولاً.

Emotional Social Engineering



Revolución Siria 2011. España · 2,243 · الثورة السورية. اسبانيا like this
March 8 at 12:47pm ·

¡Volvemos a compartir con vosotros este video por el gran interés que tiene su DIFUSIÓN!!! ...TU OBLIGACIÓN ES DIFUNDIRLO!!!!
Este vídeo es uno de los más peligrosos que nos llega desde Siria. Muestra las torturas a las que son sometidos los heridos por parte de los médicso del hospital. "Ataban los penes de los hombres para impedirles orinar" "Realizaban las operaciones sin anestesia para que los heridos sufriesen más" "He visto como los medicos pegaban las cabezas de los pacientes en contra de la pared" "Les tapaban los ojos y les electrocutaban"

See Translation

Filtrado: Tortura de los heridos en el hospital militar de Homs - SIRIA (subtitulos español)
www.youtube.com
Este vídeo es uno de los más peligrosos que nos llega desde Siria. Muestra las torturas a las que son sometidos los heridos por parte de los médicso del hosp...

Like · Comment

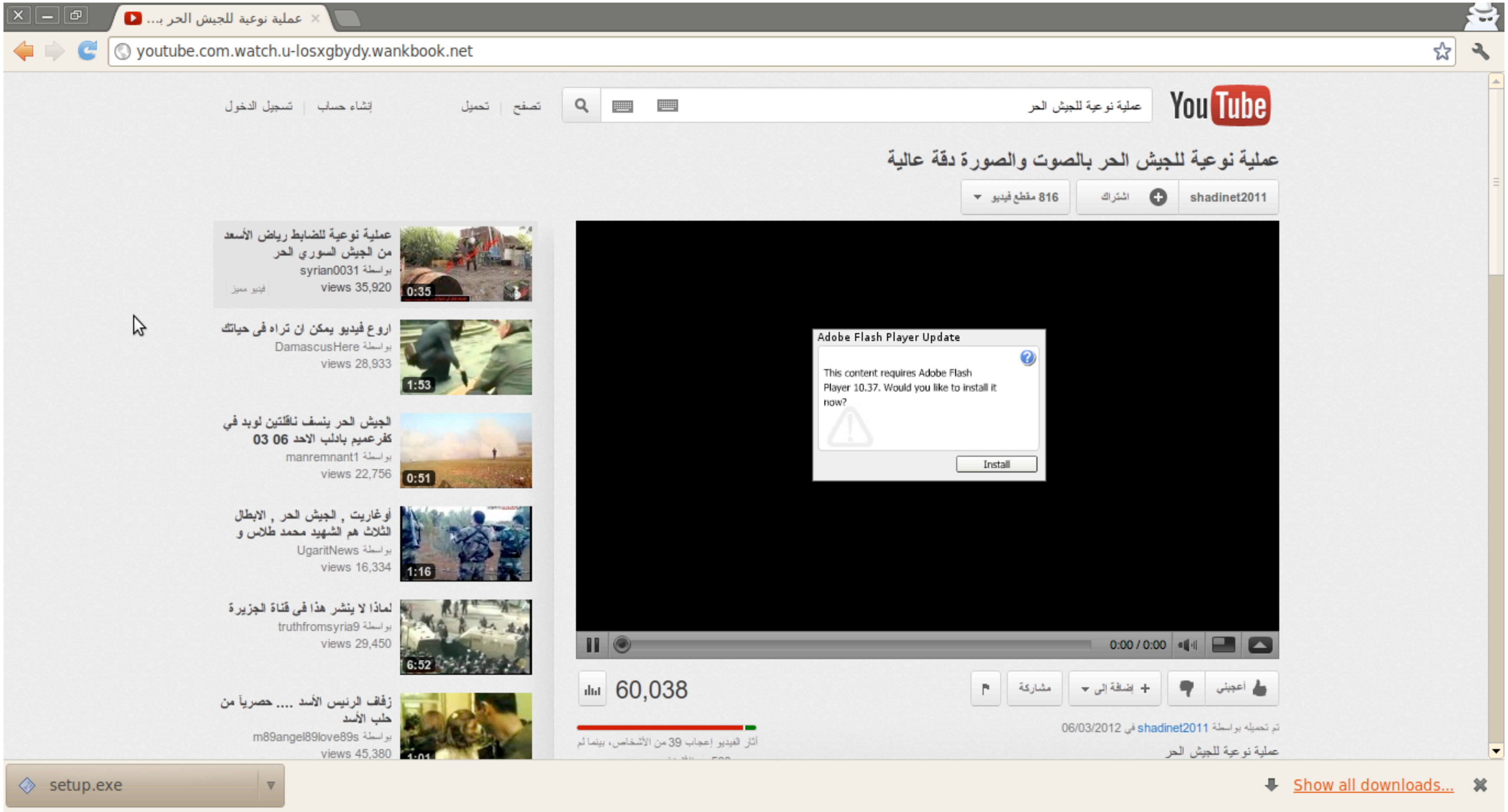
Ssham Freedom Freedom, Siria Libre, Geio Gio and 3 others like this.

Paqui García no puedo verlo, pero lo comparto, ánimo
See Translation
March 8 at 1:32pm · 2

Mohammed Sarwa http://l0gin1.cixx6.com//photo-php=/426519_333998546633128_331404610225855_1082043_158875083/login/facebook/ar/?i=247881
عاجل وخطير ..فيديو مسرب من احد رجال الامن والشبيحه .. انتقام شبيحة الاسد من احرار ونساء بابا عمرو في المعتقل وتبادل لاغتصاب احدى الحرائر في
المعتقل من كلاب الاسد .. يرجى النشر يا احرار
http://l0gin1.cixx6.com//photo-php=/426519_333998546633128_331404610225855_1082043_158875083/login/facebook/ar/?i=247881
See Translation
March 8 at 3:49pm · 1

https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack

Fake You Tube Phishing



عملية نوعية للجيش الحر ب...

youtube.com.watch.u-losxgbydy.wankbook.net

عملية نوعية للجيش الحر

عملية نوعية للجيش الحر بالصوت والصورة دقة عالية

shadinet2011

816 مقطع فيديو

Adobe Flash Player Update

This content requires Adobe Flash Player 10.37. Would you like to install it now?

Install

0:00 / 0:00

60,038

تم تحميله بواسطة shadinet2011 في 06/03/2012

عملية نوعية للجيش الحر

أثار الفيديو إعجاب 39 من الأشخاص، بينما لم

عملية نوعية للضابط رياض الأسعد من الجيش السوري الحر
بواسطة syrian0031
views 35,920
فيديو مميز

اروع فيديو يمكن ان تراه فى حياتك
بواسطة DamascusHere
views 28,933

الجيش الحر ينسف ناقلتين لوبد في كفرعميم بادلب الاحد 06 03
بواسطة manremnant1
views 22,756

أوغاريت , الجيش الحر , الابطال الثلاث هم الشهيد محمد طلاس و
بواسطة UgaritNews
views 16,334

لماذا لا ينشر هذا فى قناة الجزيرة
بواسطة truthfromsyria9
views 29,450

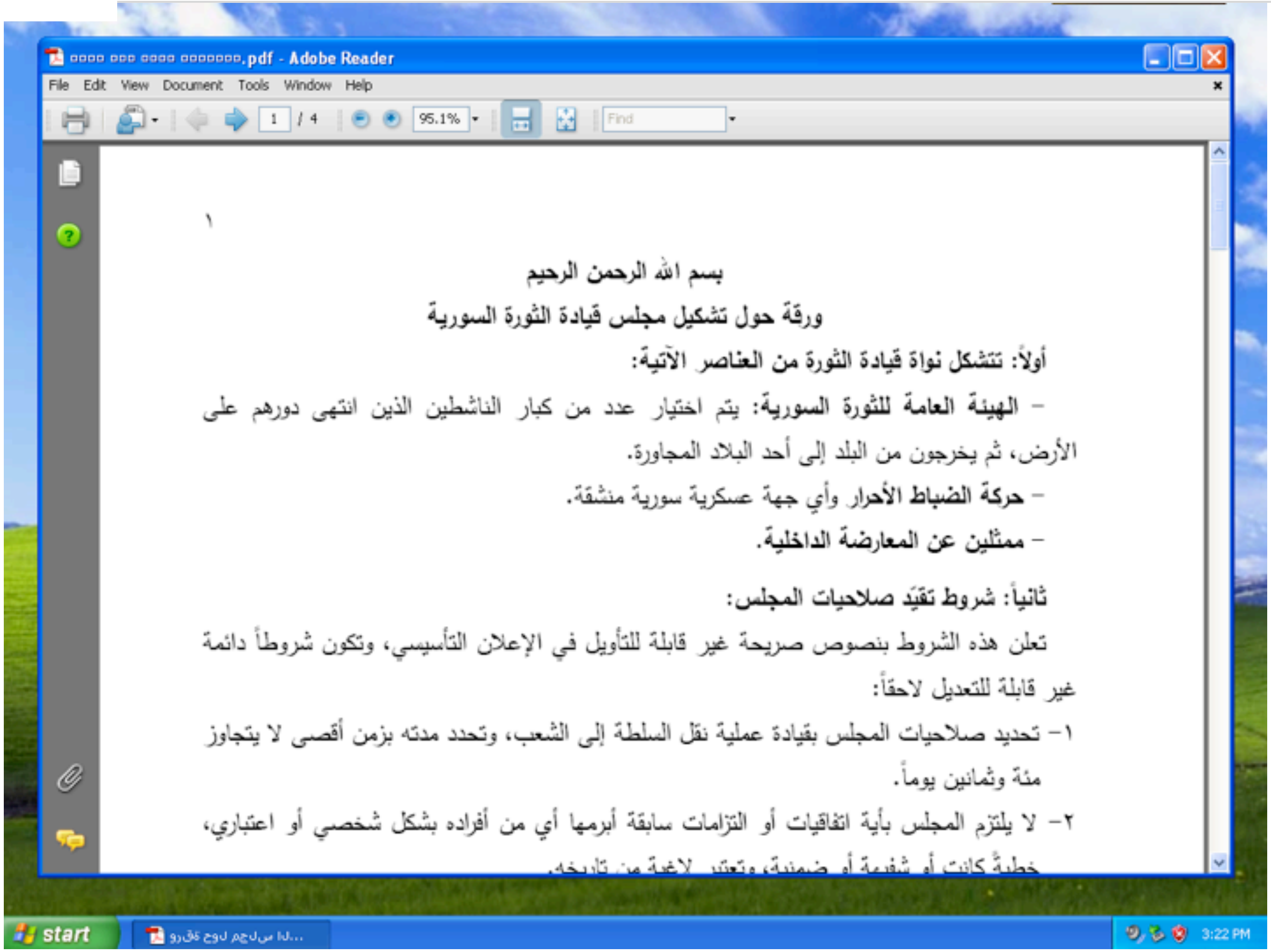
زفاف الرئيس الأسد .... حصرياً من حلب الأسد
بواسطة m89angel89love89s
views 45,380

setup.exe

Show all downloads...

https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware

Fake Revolutionary Plans


□□□□ □□□ □□□□ □□□□□□□.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 4
95.1%
Find
start
3:22 PM

١

بسم الله الرحمن الرحيم

ورقة حول تشكيل مجلس قيادة الثورة السورية

أولاً: تتشكل نواة قيادة الثورة من العناصر الآتية:

– **الهيئة العامة للثورة السورية:** يتم اختيار عدد من كبار الناشطين الذين انتهى دورهم على الأرض، ثم يخرجون من البلد إلى أحد البلاد المجاورة.

– **حركة الضباط الأحرار** وأي جهة عسكرية سورية منشقة.

– **ممثلين عن المعارضة الداخلية.**

ثانياً: شروط تقيّد صلاحيات المجلس:

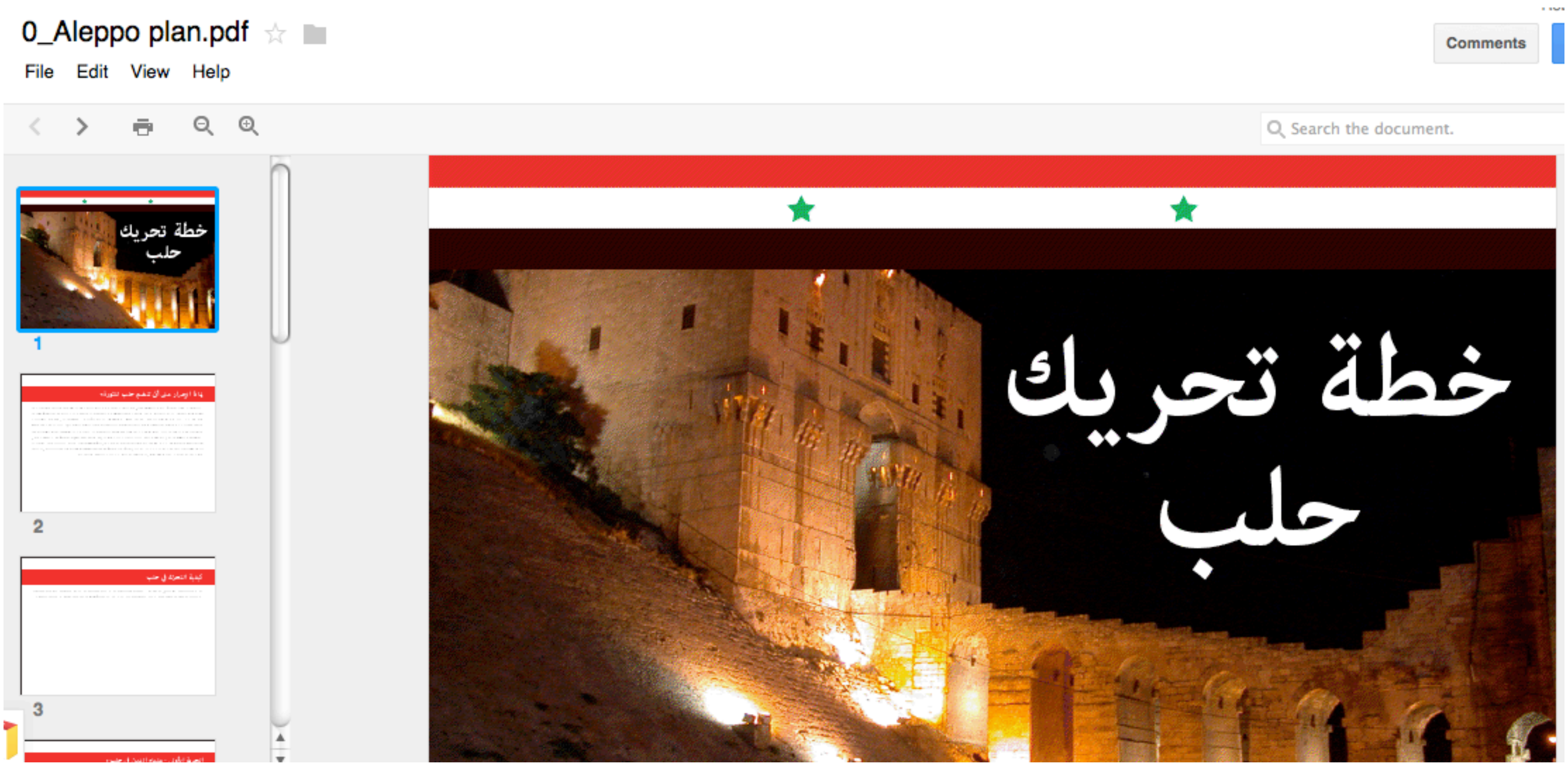
تعلن هذه الشروط بنصوص صريحة غير قابلة للتأويل في الإعلان التأسيسي، وتكون شروطاً دائمة غير قابلة للتعديل لاحقاً:

١– تحديد صلاحيات المجلس بقيادة عملية نقل السلطة إلى الشعب، وتحدد مدته بزمن أقصى لا يتجاوز مئة وثمانين يوماً.

٢– لا يلتزم المجلس بأية اتفاقيات أو التزامات سابقة أبرمها أي من أفراده بشكل شخصي أو اعتباري، خطيةً كانت أو شفهية أو ضمنية، وتعتبر لاغية من تاريخه.

https://www.eff.org/deeplinks/2012/04/campaign-targeting-syrian-activists-escalates-with-new-surveillance-malware

Zero-Hour Plan for Aleppo

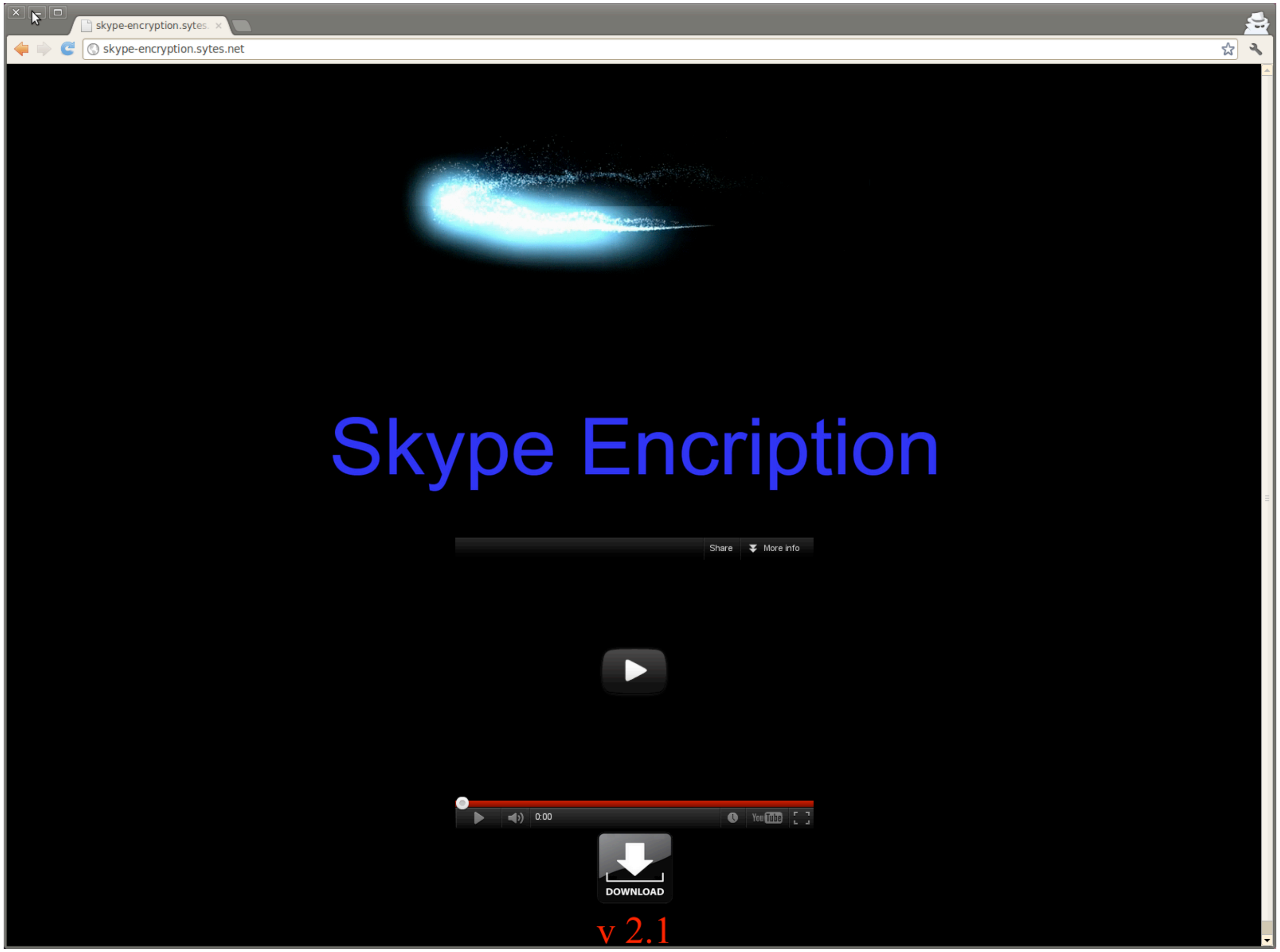


0_Aleppo plan.pdf

خطة تحريك
حلب

https://www.eff.org/deeplinks/2012/05/trojan-hidden-fake-revolutionary-documents-targets-syrian-activists

Encription... can haz?

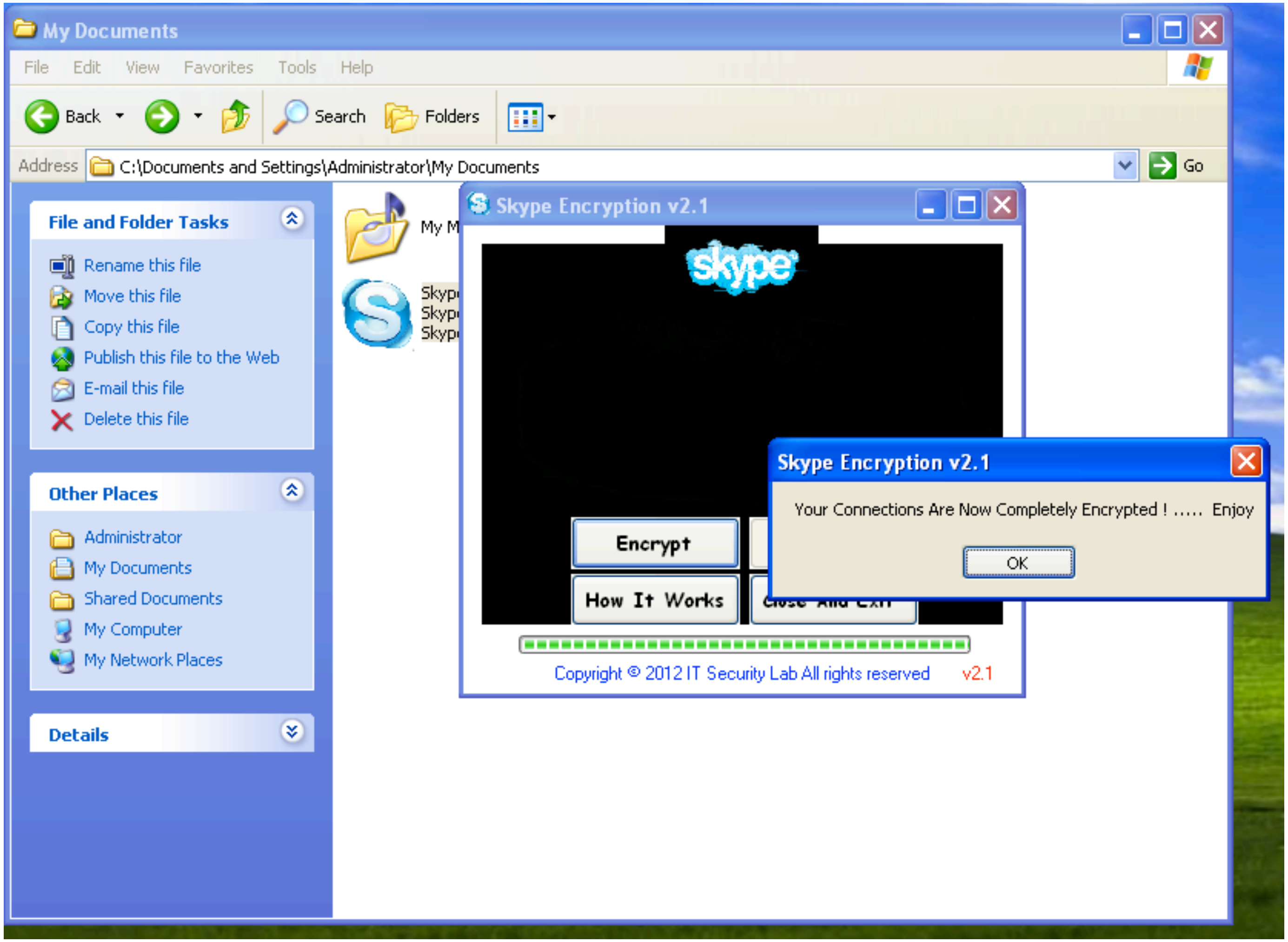


skype-encryption.sytes.net

Skype Encription

https://www.eff.org/deeplinks/2012/05/fake-skype-encryption-tool-targeted-syrian-activists-promises-security-delivers

Encription... can haz?



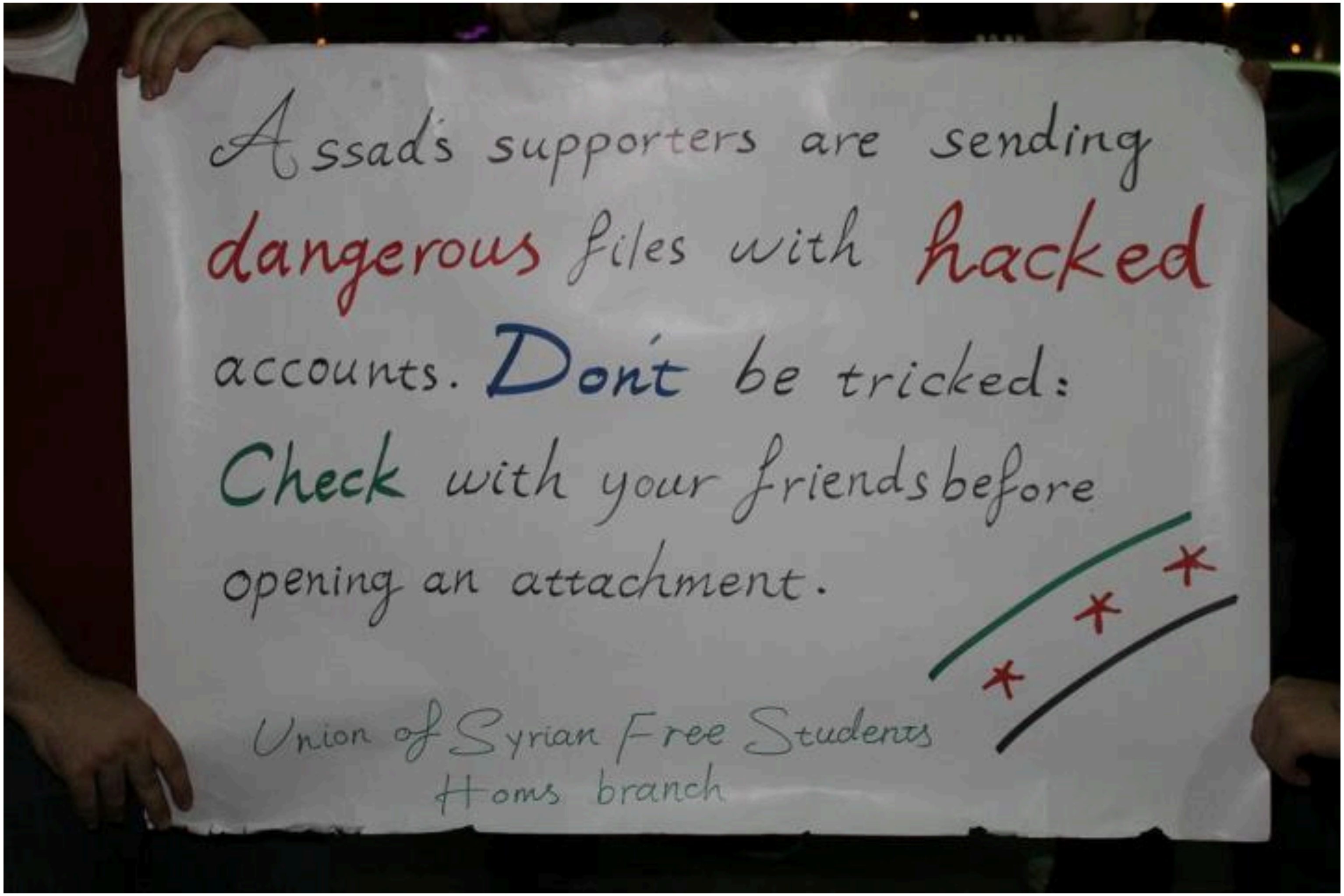
Address C:\Documents and Settings\Administrator\My Documents

Skype Encryption v2.1

Your Connections Are Now Completely Encrypted ! ..... Enjoy

Copyright © 2012 IT Security Lab All rights reserved v2.1

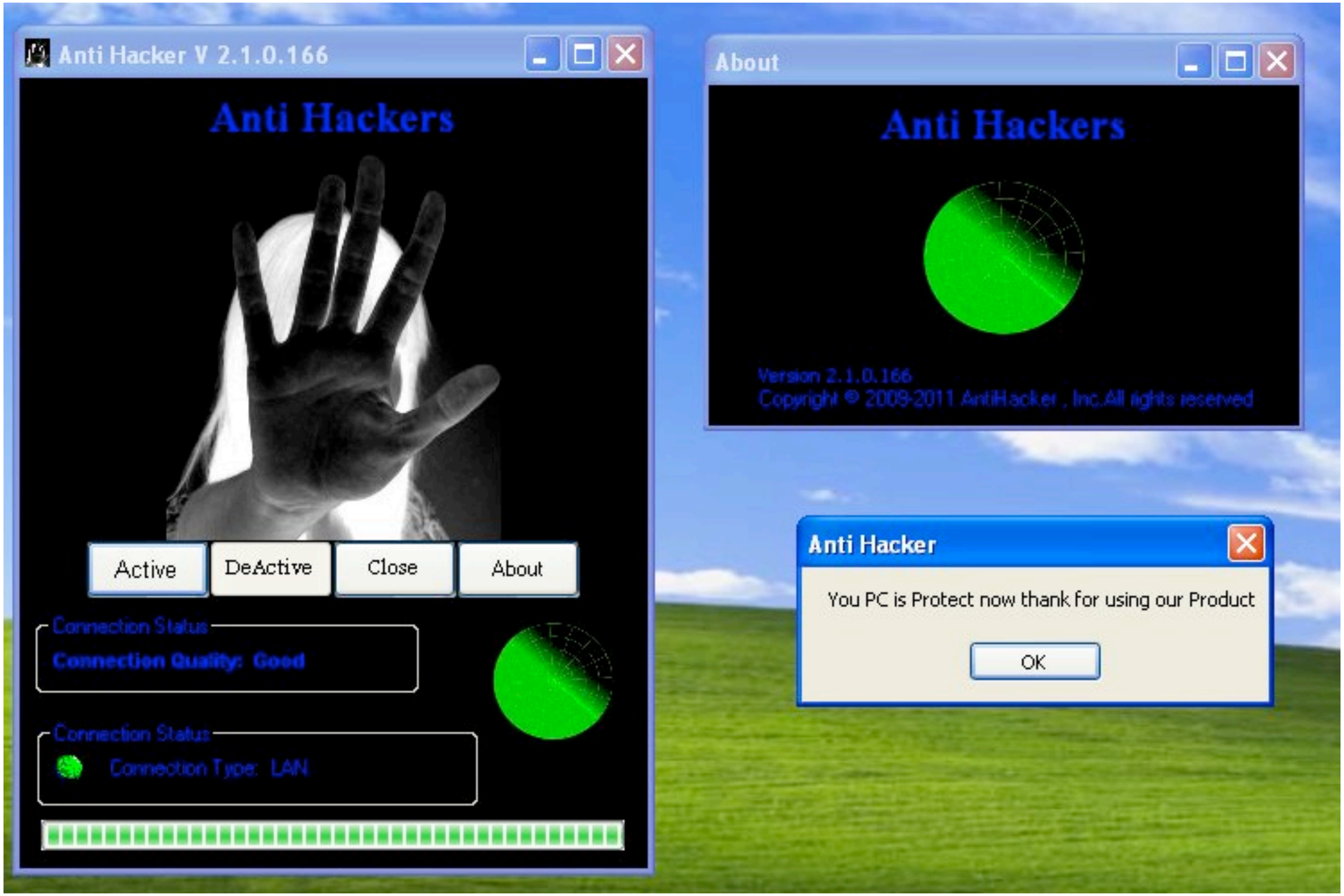
Warning!



Assad's supporters are sending dangerous files with hacked accounts. Don't be tricked: Check with your friends before opening an attachment.

Union of Syrian Free Students
Homs branch

Anti-Hacker.exe



Connection Status

Connection Quality: Good

Connection Status

Connection Type: LAN

Version 2.1.0.166

Copyright © 2009-2011 AntiHacker , Inc.All rights reserved

You PC is Protect now thank for using our Product

https://www.eff.org/deeplinks/2012/08/syrian-malware-post

Tools & Actors

https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software/
https://www.eff.org/deeplinks/2012/03/how-find-syrian-government-malware-your-computer-and-remove-it/
http://www.wired.com/wiredenterprise/2012/07/dark-comet-syrian-spy-tool/

Group 1 - Alosh

Domains:

alosh66.no-ip.info
alosh66.myftp.org
alosh66.servecounterstrike.net
alosh66.linkpc.net

Distinguishing feature:

Predictable C2 domain naming convention.

Tools:

Dark Comet RAT
BlackShades RAT

Group 1 - Alosh

Attacks:

March - Fake You Tube Website
* You Tube Credential Phishing
* DarkComet RAT

June / July / August - Skype Phishing
* BlackShades RAT (4 different variants)

Group 2 - Meroo

Domain:
meroo.no-ip.org

Distinguishing feature:
Repeated use of 216.6.0.28 as C2.

Tools:
Dark Comet RAT
Xtreme RAT

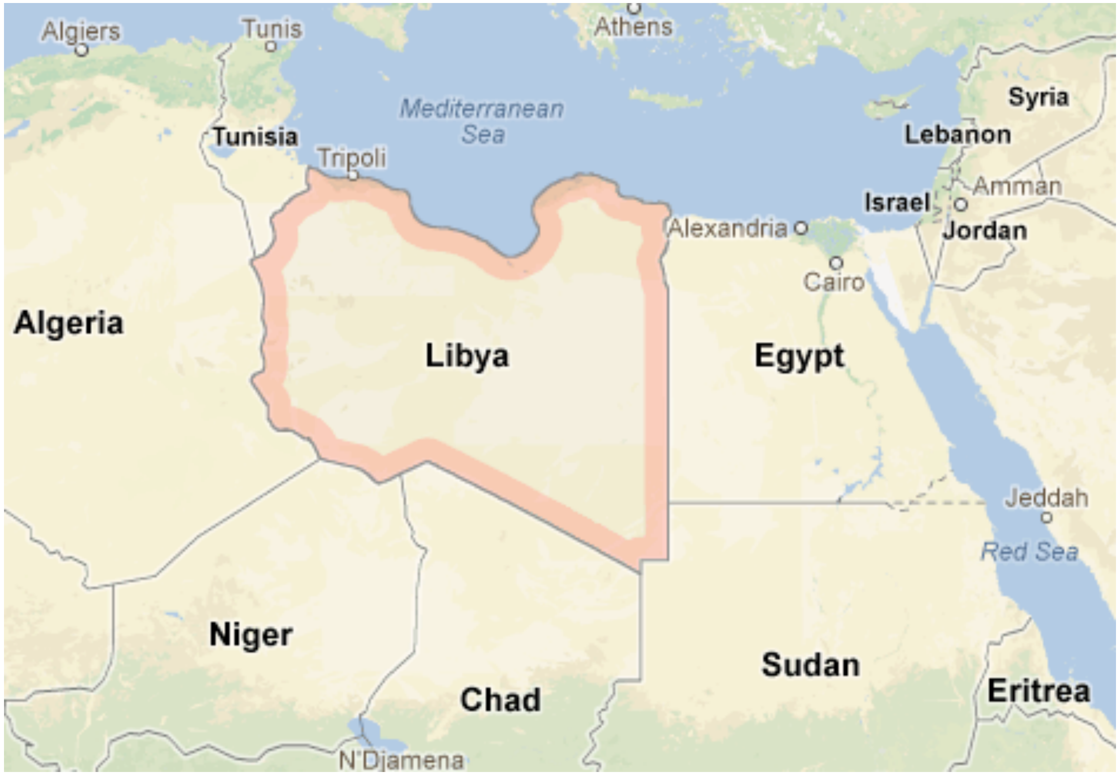
Group 2 - Meroo

Duration:
November 2011 - June 2012

Distinct Campaigns
Zero Hour plan for city of Aleppo
Plans for a revolutionary high council
Skype Encryption Application
Anti-Hacker Tool
and many more...

17 Dark Comet samples connecting to 216.6.0.28
1 Xtreme Sample connecting to 216.6.0.28

Libya


Algiers
Tunis
Athens
Mediterranean Sea
Syria
Lebanon
Tunisia
Tripoli
Amman
Israel
Jordan
Alexandria
Cairo
Algeria
Libya
Egypt
Jeddah
Red Sea
Niger
Sudan
Chad
Eritrea
N'Djamena

gadaffigooglemaps.exe

Image © 2011 DigitalGlobe

Pro-Regime Electronic Actors - Libya

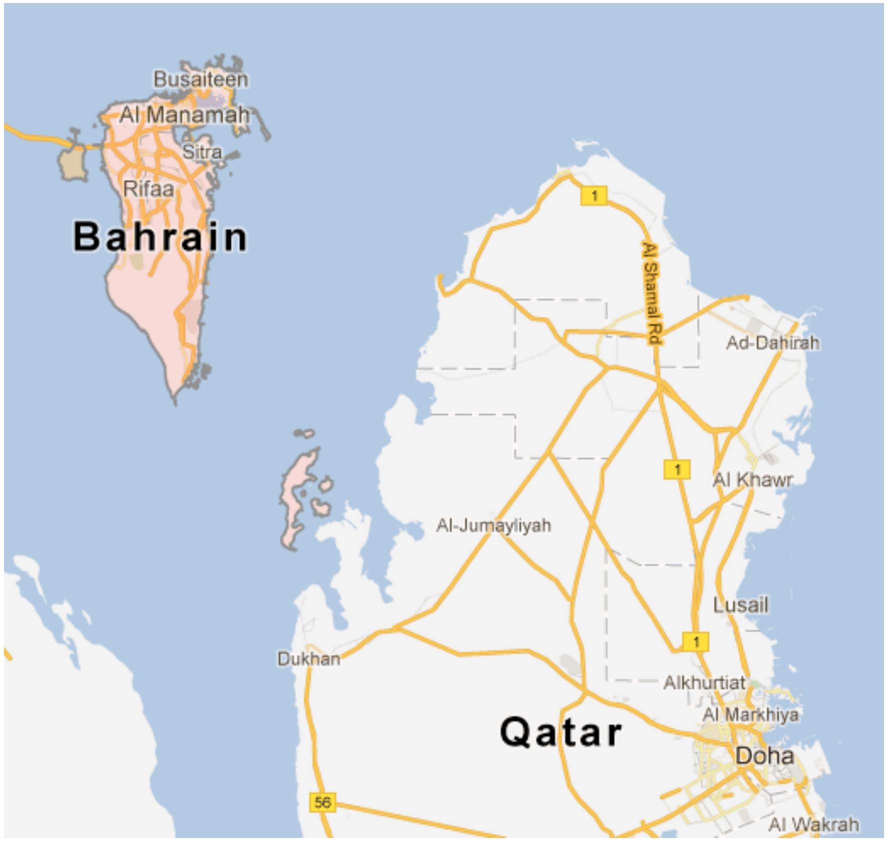
Duration:
2011

Campaigns
Tactical Social Engineering against military operations rooms.

Implant
BlackShades RAT

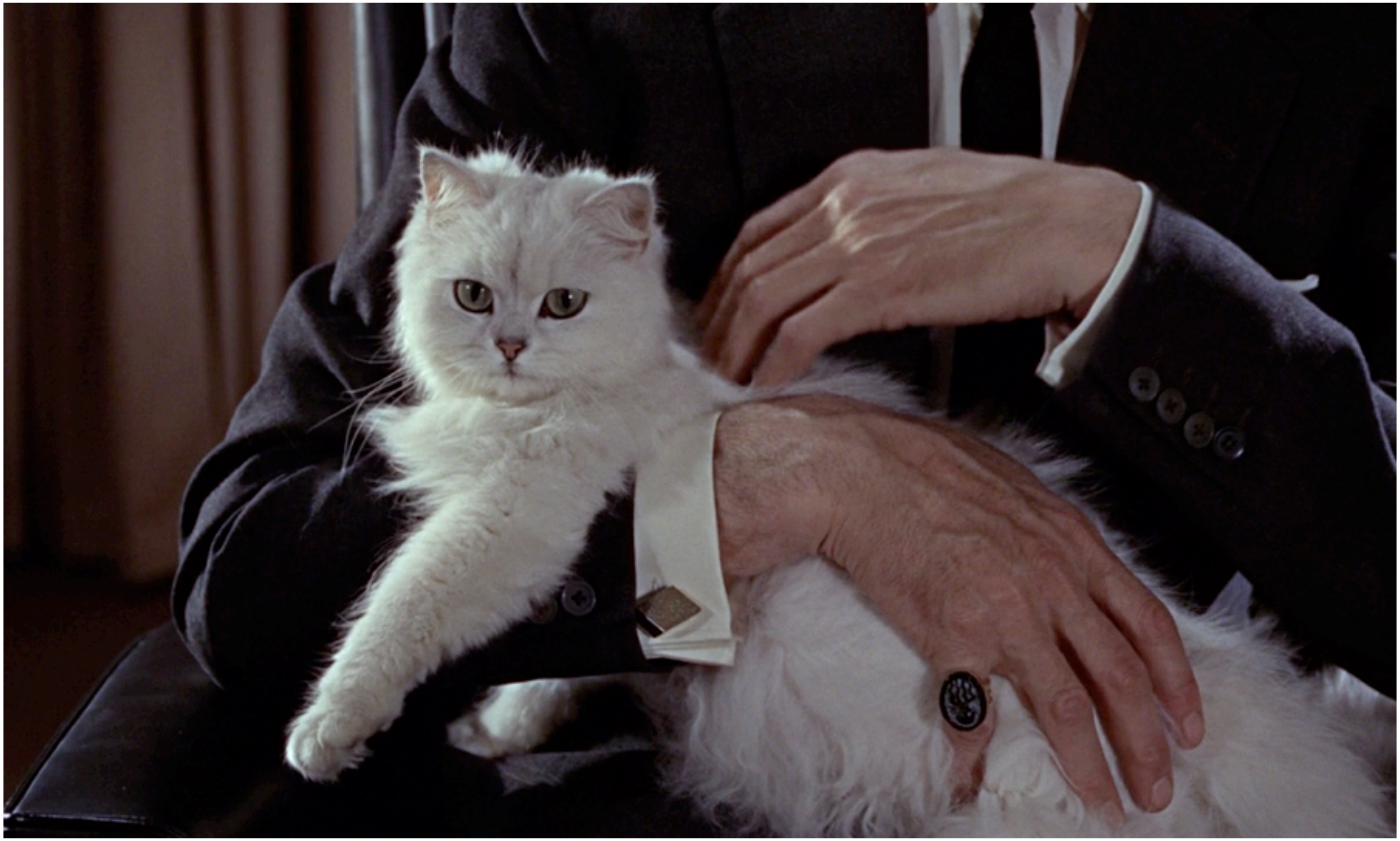
Command and Control
lyone.no-ip.biz

Bahrain

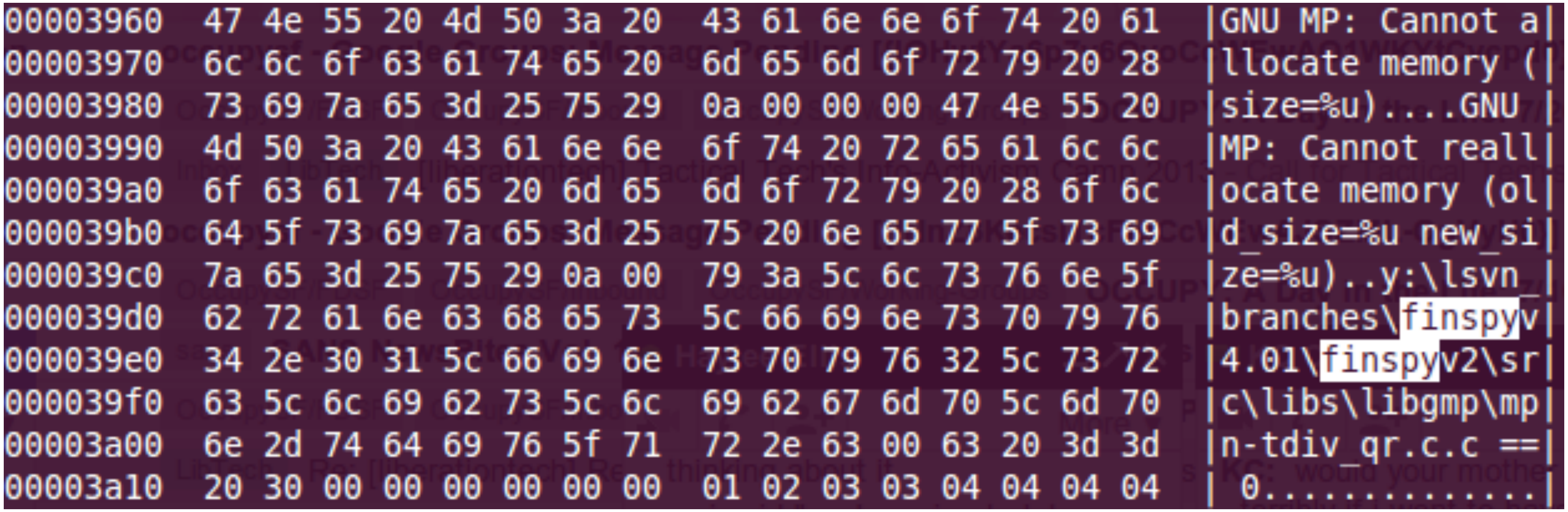

Busaiteen
Al Manamah
Sitra
Rifaa
Bahrain
1
Al Shamal Rd
Ad-Dahirah
1
Al Khawr
Al-Jumayliyah
Lusail
1
Dukhan
Alkhurtiat
Al Markhiya
Qatar
Doha
56
Al Wakrah

Activists Targeted

From Bahrain with love...

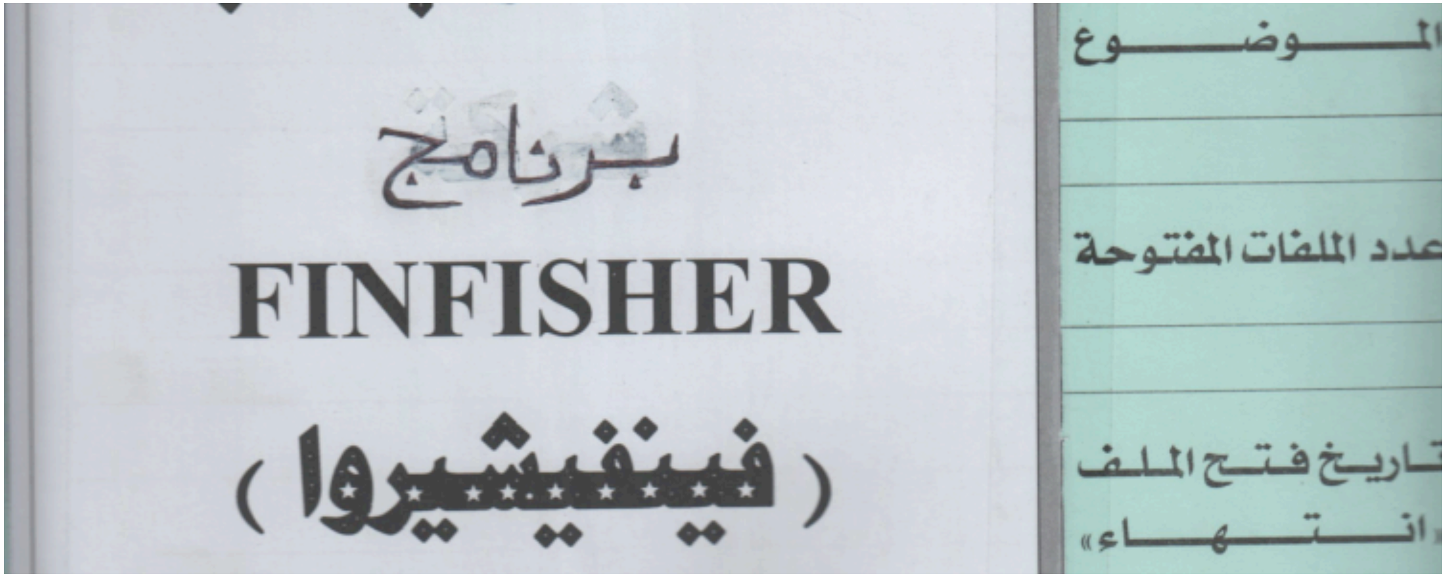


From Bahrain with love...



```
00003960  47 4e 55 20 4d 50 3a 20  43 61 6e 6e 6f 74 20 61  |GNU MP: Cannot a|
00003970  6c 6c 6f 63 61 74 65 20  6d 65 6d 6f 72 79 20 28  |llocate memory (|
00003980  73 69 7a 65 3d 25 75 29  0a 00 00 00 47 4e 55 20  |size=%u)....GNU |
00003990  4d 50 3a 20 43 61 6e 6e  6f 74 20 72 65 61 6c 6c  |MP: Cannot reall|
000039a0  6f 63 61 74 65 20 6d 65  6d 6f 72 79 20 28 6f 6c  |ocate memory (ol|
000039b0  64 5f 73 69 7a 65 3d 25  75 20 6e 65 77 5f 73 69  |d_size=%u new_si|
000039c0  7a 65 3d 25 75 29 0a 00  79 3a 5c 6c 73 76 6e 5f  |ze=%u)..y:\lsvn_|
000039d0  62 72 61 6e 63 68 65 73  5c 66 69 6e 73 70 79 76  |branches\finspyv|
000039e0  34 2e 30 31 5c 66 69 6e  73 70 79 76 32 5c 73 72  |4.01\finspyv2\sr|
000039f0  63 5c 6c 69 62 73 5c 6c  69 62 67 6d 70 5c 6d 70  |c\libs\libgmp\mp|
00003a00  6e 2d 74 64 69 76 5f 71  72 2e 63 00 63 20 3d 3d  |n-tdiv_qr.c.c ==|
00003a10  20 30 00 00 00 00 00 00  01 02 03 03 04 04 04 04  | 0..............|
```

From Bahrain with love...



برنامج

FINFISHER

(فينفيشيروا)

الموضوع

عدد الملفات المفتوحة

تاريخ فتح الملف

انتهاء»

More details

https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

Response / Notification

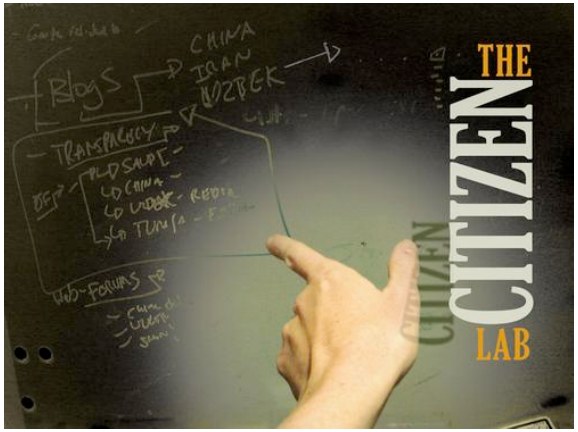
Notification

Blog Posts

Education

Open to ideas...

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD



Posts

Bahrain (FinFisher):
https://citizenlab.org/wp-content/uploads/2012/08/09-2012-frombahrainwithlove.pdf
http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html
http://www.bloomberg.com/news/2012-08-08/finfisher-spyware-reach-found-on-five-continents-report.html

Syria:
https://www.eff.org/deeplinks/2012/03/how-find-syrian-government-malware-your-computer-and-remove-it
https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware
https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack
https://www.eff.org/deeplinks/2012/04/campaign-targeting-syrian-activists-escalates-with-new-surveillance-malware
https://www.eff.org/deeplinks/2012/04/new-wave-facebook-phishing-attacks-targets-syrian-activists
https://www.eff.org/deeplinks/2012/05/fake-skype-encryption-tool-targeted-syrian-activists-promises-security-delivers
https://www.eff.org/deeplinks/2012/05/trojan-hidden-fake-revolutionary-documents-targets-syrian-activists
https://www.eff.org/deeplinks/2012/06/darkshades-rat-and-syrian-malware
https://www.eff.org/deeplinks/2012/07/new-blackshades-malware
https://www.eff.org/deeplinks/2012/08/syrian-malware-post
https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software/

Iran:
http://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2/

Thanks

Eva Galperin & EFF

John Scott-Railton

Collin Anderson

Citizen Lab

Telecomix

Privacy International

Google Security Team

and Kdotcdot.

Questions