

# **CS261N: Internet/Network Security**

Surveillance

# Who am I?

- Computer Science PhD Candidate at UC Berkeley
- Co-Founder of Bahrain Watch
- Senior Researcher at Citizen Lab



**BAHRAIN WATCH**



# **Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware**

Seth Hardy<sup>§</sup> Masashi Crete-Nishihata<sup>§</sup> Katharine Kleemola<sup>§</sup> Adam Senft<sup>§</sup>

Byron Sonne<sup>§</sup> Greg Wiseman<sup>§</sup> Phillipa Gill<sup>†</sup> Ronald J. Deibert<sup>§</sup>

*§ The Citizen Lab, Munk School of Global Affairs, University of Toronto, Canada*

*† Stony Brook University, Stony Brook, USA*

Value	Description
0	<b>Not targeted</b> , e.g. spam or financially motivated
1	<b>Targeted but not customized</b> ... obviously false
2	<b>Targeted and poorly customized.</b> Content is generally relevant ... May look questionable
3	<b>Targeted and customized.</b> May use a real person/organization ... Content is specifically relevant to the target and looks legitimate
4	<b>Targeted and well-customized.</b> Uses a real person/organization and content to convince the target the message is legitimate. Probably directly addressing the recipient ... May be sent from a hacked account.
5	<b>Targeted and highly customized using sensitive data</b> , likely using inside/sensitive information that is directly relevant to the target.



Value	Description
1	The sample contains <b>no code protection</b> such as packing, obfuscation, or anti-reversing tricks
1.25	The sample contains a <b>simple method of protection</b> , such as code protection using reversible publicly available tools, self-disabling in the presence of AV
1.5	The sample contains <b>multiple minor code protection</b> techniques (anti-reversing, packing, VM / reversing tools detection) that require some low-level knowledge.
1.75	The sample contains <b>at least one advanced protection method</b> such as rootkit functionality or a custom virtualized packer
2	The sample contains <b>multiple advanced protection Techniques</b> , and is clearly designed by a professional software engineering team



## ཟུར་སྒྲོན་(Attachment)རིགས་དང་ འོགས་སུ་སྤྲོད་།

གྲོག་འཕྲིན་བརྒྱུད་ནས་ཡིག་ཆ་བཀོ་འགྲེམས་མ་བྱེད་།  
ཡིག་ཆ་བདེ་འཇགས་ལམ་ནས་བཀོ་འགྲེམས་བྱེད་པར་།

**Dropbox.com**དང་**Ge.tt** ཡང་ན་**GoogleDocs**

སོགས་བེད་སྤྱོད་ཐོངས། ཟུར་སྒྲོན་རིགས་ཅི་ཞིག་འཕྱོར་ཡང་།

**VirusTotal.com**མཉམ་དུ་ཞིབ་བཤེར་ཐོངས།

# Hackers Target Tibetans With Malicious Google Drive Files

June 16, 2015 // 04:22 PM EST

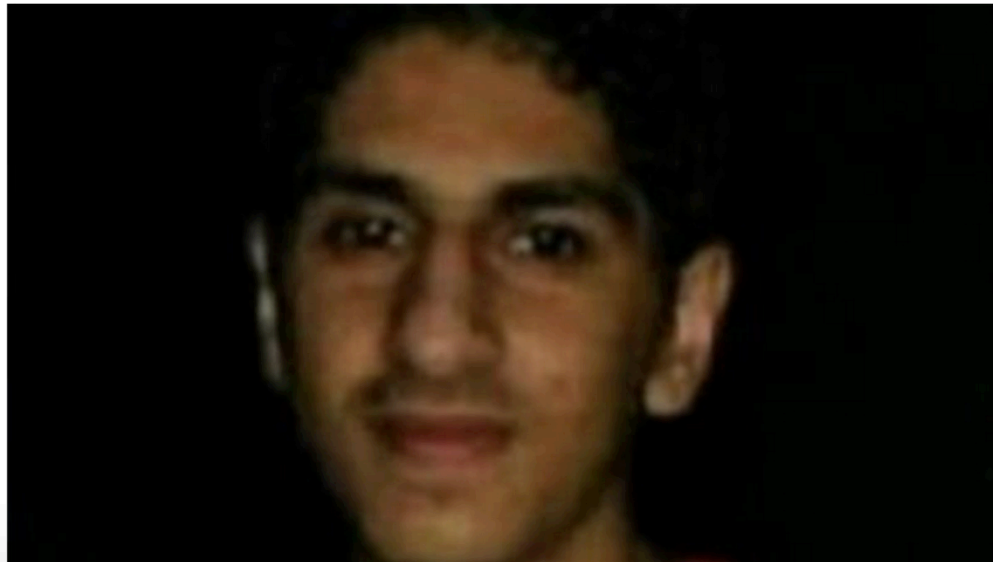
Last year, a digital security group encouraged Tibetans who are often targeted by cyberattacks not to open suspicious files sent to them via email and “[detach from attachments](#)” to avoid being hacked.

Months later, the hackers who target them seem to have adjusted, using links to Google Drive files in their latest hacking attempts, rather than simple files attached to phishing emails, according to a new report that details a series of recent attacks on Tibetan human rights activists and Hong Kong pro-democracy groups



## **Bahrain student sentenced for insulting king**

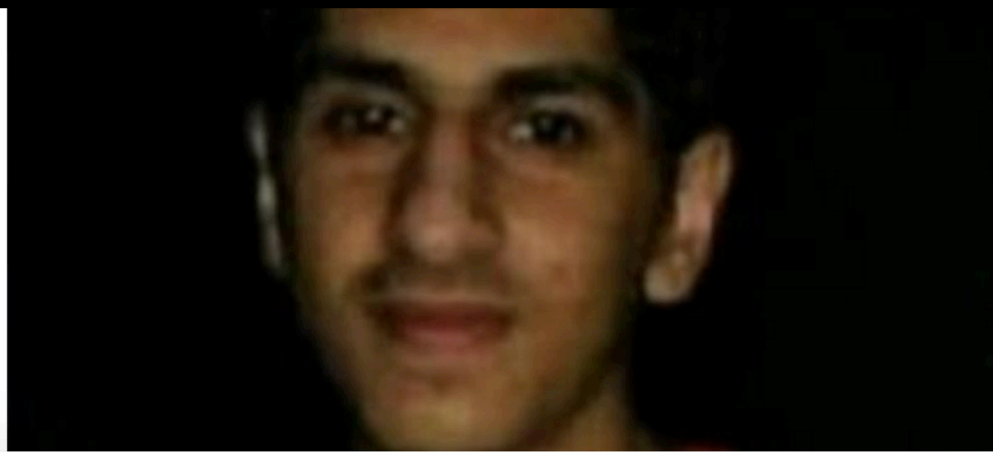
*High school pupil Ali Al Shofa sent to prison for one year for insulting Gulf island's ruler via Twitter.*





## **Bahrain student sentenced for insulting king**

Ali was accused of posting insulting comments about Sheikh Hamad Al-Khalifa using the account [@alkawarahnews](#), which he denied a relationship with. His lawyer submitted evidence that the account was still being run by other people.





شبكة الكَوْرَة الإعلامية  
@alkawahnews

#### BUSINESS INFO

Founded in July 2011

#### Biography

شبكة الكورة الاعلامية

يمكنكم متابعة على شبكات التواصل الاجتماعي التالية :-

BLACKBERRY: PIN:27604C92 |«

TWITTER: @ALKAWARAHNEWS |«

YOUTUBE: KAWARANEWS |«

:FACEBOOK |«

<http://www.facebook.com/kawaraneWS3>

#### CONTACT INFO

@alkawahnews

Message Now

kawara.news@gmail.com

<http://www.facebook.com/alkawahnews>



شبكة الكورة الإعلامية  
@alkawahnews



Follow

#تيار\_الوفاء : تظاهرات غاضبة لليوم الثاني على التوالي تعم مدن  
#البحرين وبلداتها تضامناً مع #صوت\_الحق الشيخ النمر

View translation







## **Bahrain student sentenced for insulting king**

***“It is a secret investigation  
involving private methods of  
our department that cannot  
be disclosed”***



**Col. Fawaz Alsumaim  
Cyber Crime Unit**



رقم الإشارة: ن/ع/ 4/ ٨٨٥< 2013/  
التاريخ: 2013/2/20

السيد الفاضل / مدير الإدارة العامة لمكافحة الفساد و الأمن الاقتصادي و الالكتروني المحترم،،،

بإتية طيبة وبعد،،،

الموضوع:

طلب الكشف عن مستخدم البرتوكول

@alkawarahnews

Order to uncover the  
user of an IP address of  
@alkawarahnews

الساعة	التاريخ	البروتوكول
19:57:18	2012/12/9	89.148 [REDACTED]

Batelco  
(residential ISP)

نأذن للملازم اول / قواز حسن الصميم أو لمن يندبه أو يعاونه من مخاطبة شركة مينا  
تيلكوم البحرين والمزودة بخدمة الانترنت للكشف عن اسم وعنوان صاحب البرتوكول  
المذكور أعلاه من أجل استكمال التحريات التي تجريها إدارتكم للتوصل للفاعل ومن ثم  
عمل المحاضر اللازمة وتعرض علينا في حينه لاتخاذ اللازم.

وتفضلوا سعادتكم بقبول وافر التحية والاحترام،،،

محمد صلاح  
وكيل النيابة

القائم بأعمال رئيس نيابة محافظة العاصمة

Mohammed Salah

Acting Chief Prosecutor,  
Capital Region





### محضر

فتح المحضر اليوم الاحد الموافق ٢٠١٣/٣/١٠ في تمام الساعة ١٠:٣٠ صباحا في ادارة مكافحة الجرائم الالكترونية بمعرفتي أنا الملازم أول/ فواز حسن الصميم من الإدارة سالفة الذكر وذلك بشأن التحريات التي تجريها الادارة ومن خلال ما تم رصده في الاونة الاخيرة حيال قيام عدد من الاشخاص من مستخدمي موقع التويتر بالاساءة الى جلالة الملك وإهانة والتمادي في ذلك الفعل وإزياده بشكل ملحوظ ، حيث أن هؤلاء الاشخاص يقومون بنشر هذه العبارات المسيئة علانية في حساباتهم التي يتم متابعتها من قبل عدد كبير من الاشخاص عبر موقع التويتر . وعليه من خلال التحريات الجدية التي أجريناها تم التوصل الى أحد هؤلاء الاشخاص وهو صاحب حساب تويتر (@alkawarahnews) وهو يستخدم عنوان بروتوكول مخدم من شركة بتلكو: ٨٩.١٤٨ بتاريخ ٢٠١٢/١٢/٩ م . وبعد اخذ اذن النيابة العامة لأستصدار امر بتزويدنا بمعلومات مستخدم عنوان البروتوكول تبين لنا انه مسجل باسم المدعو / فيصل علي ابراهيم محمد الشوفه -بحريني الجنسية - رقمه الشخصي [REDACTED] . ومن خلال التحريات التي أجريناها تبين لنا ان من يقوم بإدارة هذا الحساب هو أبن المذكور أعلاه المدعو/ علي فيصل علي ابراهيم محمد الشوفه - بحريني الجنسية - رقمه الشخصي [REDACTED] ، حيث يقوم المذكور من خلال هذا الحساب بنشر تغريدات تتضمن الاساءة الى جلالة الملك منها (الكورة/ احراق صورة الطاغية حمد ضمن فعالية "رجم الطاغية" لتلبية دعوه الائتلاف الان) و(مرتزقة الساقط حمد تقمع بعنف الان ..) و( تيار الوفاء / اولياء الدم في مقدمة مسيرة ختام مجلس عزاء الشهيد الجزائري مؤكدين على القصاص من السفاح حمد) وغير ذلك من الالفاظ والعبارات البذيئة والمسيئة لجلالة الملك.

KINGDOM OF BAHRAIN  
MINISTRY OF THE INTERIOR  
GENERAL DIRECTORATE OF  
ECONOMIC AND ELECTRONIC  
SECURITY AND ANTI CORRUPTION



مملكة البحرين  
وزارة الداخلية  
الإدارة العامة لمكافحة الفساد  
والامن الاقتصادي والالكتروني

محضر

فتح المحضر اليوم الاحد الموافق ٢٠١٣/٣/١٠ في تمام الساعة ١٠:٣٠ صباحا في ادارة مكافحة  
الجرائم الالكترونية بمعرفتي أنا الملازم أول/ فواز حسن الصميم من الإدارة سألته الذكر

After receiving permission from the Public Prosecutor to gain information about the user of the protocol number, we found that the user is registered under the name of Faisal Ali Ibrahim Mohammed Al Shufa. Through the investigations that we conducted it is clear that the person running the account is the named person's son Ali Faisal Ali Ibrahim Al Shufa. The individual is spreading tweets insulting His Majesty the King, such as "Al Kawarah/ Burning images of the dictator Hamad..." and "the mercenaries of the fallen Hamad are violently suppressing now..."

الان ..) و( تيار الوفاء / اولياء الدم في مقدمة مسيرة ختام مجلس عزاء الشهيد الجزائري  
مؤكدین على القصاص من السفاح حمد) وغير ذلك من الالفاظ والعبارات البذيئة والمسيئة  
لجلالة الملك.


(Arrested activist)



Red Sky 

Red Sky



السلام عليكم انا مترجم الثورة هل تحتاجون الى ترجمة موضوعكم  
<http://goo.gl/u4bZL>

كتابة رد... 

Greetings, I am a translator of the revolution. Do you need translation of this?

Analytics data for [goo.gl/u4bZL](http://goo.gl/u4bZL)

Created Dec 8, 2012

Original URL [iplogger.org/25SX](http://iplogger.org/25SX) 

(Arrested activist)

Red Sky 

سوعكم

http

## Short link

You can generate special short URL which will redirect to any website that you may indicate. Generated logger will save IP address of each user who clicked the link, date, time and other information about such clicks.

Insert your link here

Generate link

Greet  
transl

An

Crea

Original URL [iplogger.org/25SX](http://iplogger.org/25SX)


(Arrested activist)




**Red Sky** 

**Red Sky**

السلام عليكم انا مترجم الثورة هل تحتاجون الى ترجمة موضوعكم  
<http://goo.gl/u4bZL>



كتابة رد... 

Greetings, I am a translator of the revolution. Do you need translation of this?

**goo.gl analytics:**

Clicks: 1

Referrer: [www.facebook.com](http://www.facebook.com)

Country: BH

**Created: 2012-12-08T19:05:36+00:00**

**Click : 2012-12-09T19:57:18+03:00**

**Diff : 21h51m42s**



**AlBinSanad** @AlBinSanad

7 Jan

@saudi44 للتبنيہ انا لست ضد حراك الشعب في الكويت ولا في اي دولة عربية من أجل المطالبة بمزيد من الديمقراطية.. لكن لا تنهي عن امر وتأتي بمثله

Expand



**@saudi44** ابو فيصل

7 Jan

@AlBinSanad ليت تدعم التحرك بايران للتخلص من الولي الفقيه وتدعم استقلال الاهواز وتدعم ثورة السنه بالعراق وتدعم التحرك بسوريا والي قرب نصرهم

Expand



**AlBinSanad** @AlBinSanad

7 Jan

@saudi44 أنا أؤيد كل حراك شعبي ضد كل الحكومات الدكتاتورية في المنطقة.. بما فيها #سوريا.. ولكن هل لديك الرجولة كي تفعل ذلك..؟؟

Expand



**@saudi44** ابو فيصل

7 Jan

@AlBinSanad نعم املك الشجاعه ان اقول للظالم انت ظالم ولكن نحن السنه ليس عندنا عقده النقص والشعور بالمظلوميه ولا نخرج على امامنا الا اذا كفر

Expand



**AlBinSanad** @AlBinSanad

7 Jan

@saudi44 ما شاء الله عليك.. وهل كفر حسني مبارك؟ يا حبيبي الخوف من الحاكم وبطشه يتم تبريره بمثل هذه الأعذار السخيفة التي لا يقبلها العقل ☐

Expand



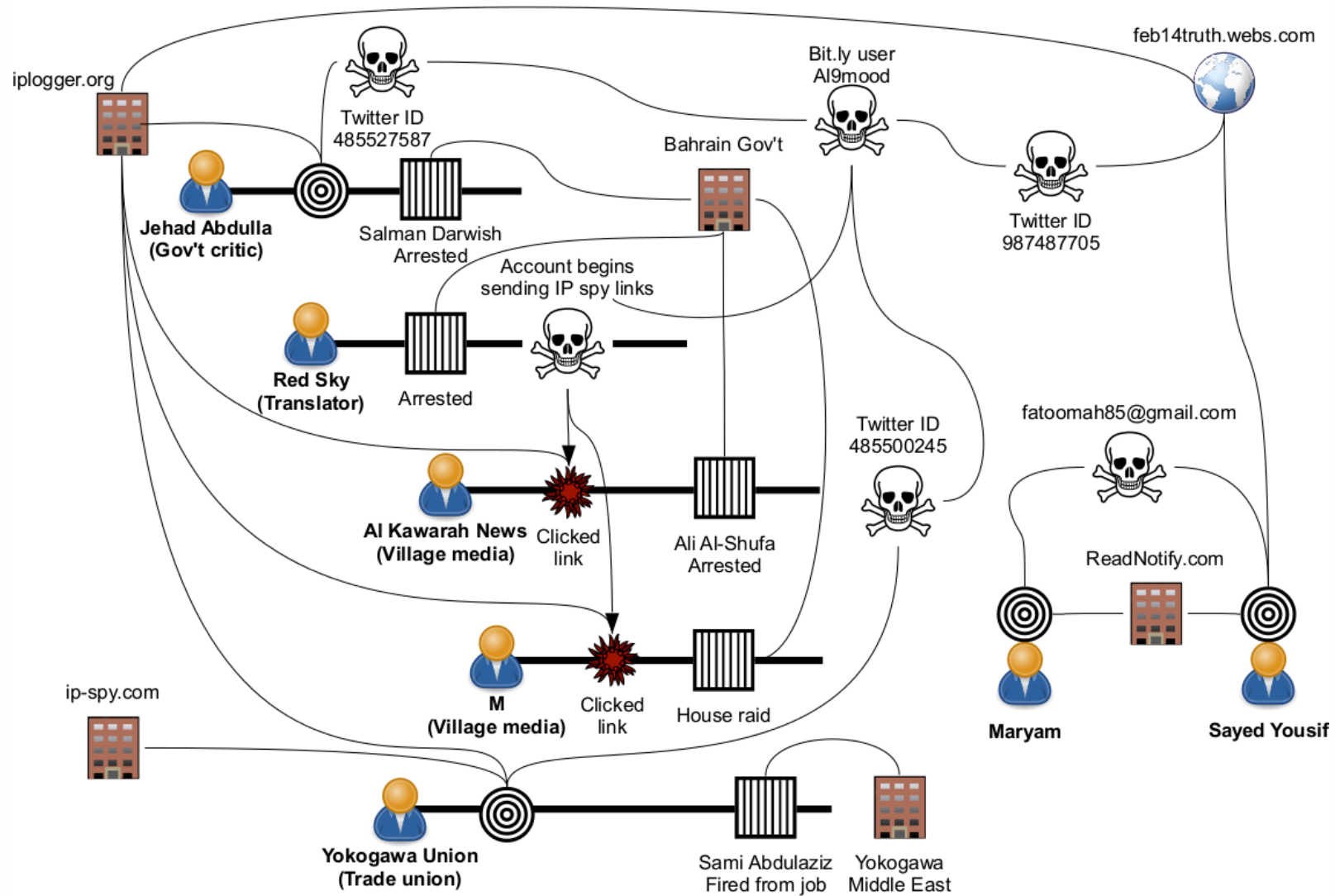
**AlBinSanad** @AlBinSanad

8h

@saudi44 @AwaiVolcano [goo.gl/WYvTs](http://goo.gl/WYvTs) حد

Hide conversation Reply Retweet Favorite More

1:09 AM - 16 Jan 13 - Details



### Legend





# Re@adNotify

Welcome to ReadNotify.com !

ReadNotify lets you know when email  
you've sent gets read



**whoreadme**  
*free email tracking service for everyone*

**Pointofmail** FEATURES SUBSCRIBE SUPPORT TESTIMONIALS

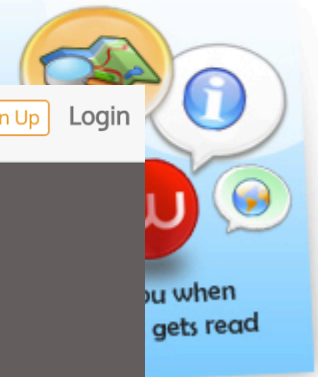
Install for Gmail

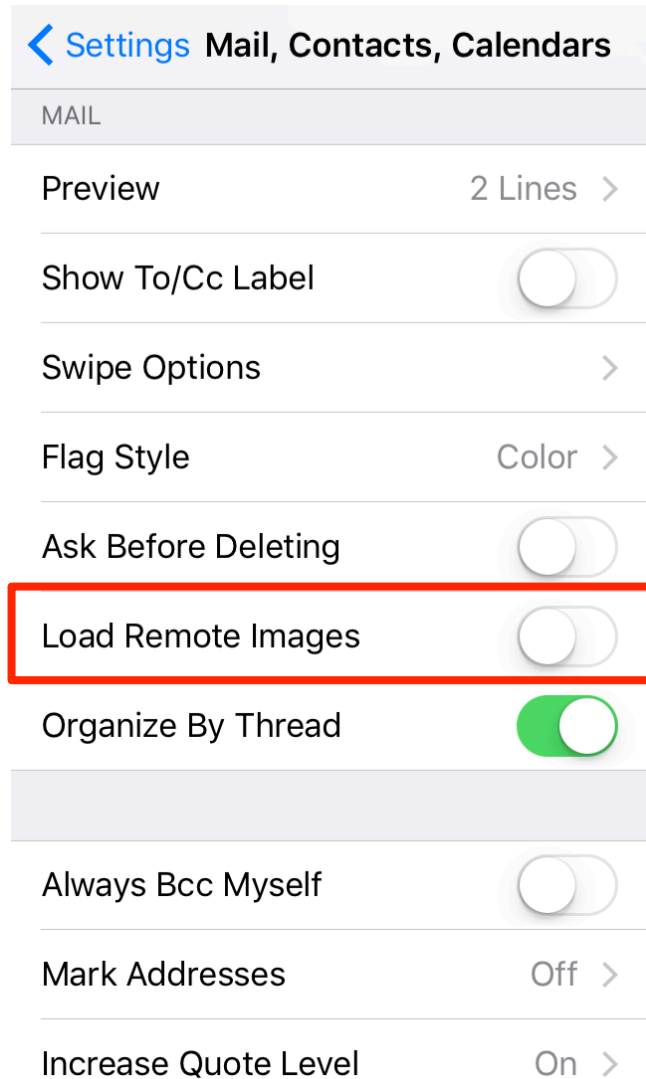
Sign Up

Login



Know Who, When and Where Read,  
Clicked and Forwarded Your Email





**Disable this option on your iPhone**



# Official Gmail Blog

News, tips and tricks from Google's Gmail team and friends.

## Images Now Showing

December 12, 2013

But thanks to new improvements in how Gmail handles images, you'll soon see all images displayed in your messages automatically across desktop, iOS and Android. Instead of serving images directly from their original external host servers, Gmail will now **serve all images** through Google's own secure proxy servers.

You have new **challenges** today

Sensitive data is transmitted over **encrypted** channels

]HackingTeam[

[About us](#)

[The Solution](#)

[Customer Policy](#)

[Careers](#)

[Contacts](#)

**Acquire  
RELEVANT  
data.**

Interesting data never gets to the Web.  
**It stays on the device.**

TeleStrategies®

# ISSWorld®

Intelligence Support Systems for Lawful  
Interception, Electronic Surveillance and  
Cyber Intelligence Gathering





TeleStrategies®



**FINFISHER**  
IT INTRUSION

**EXODUS**  
INTELLIGENCE

]HackingTeam[

zerodium®



**DARKMATTER**  
GUARDED BY GENIUS



**CYBERBIT**  
PROTECTING A NEW DIMENSION

# The "Million Dollar Dissident"



**Ahmed Mansoor:**

- Signed UAE pro-democracy petition in 2011
- UAE human rights activist



**New secrets about torture  
of Emiratis in state prisons**

# The "Million Dollar Dissident"



*iPhone Users Urged to Update Software After Security Flaws Are Found*



# The "Million Dollar Dissident"



[CVE-2016-4657](#) Visiting a maliciously crafted website may lead to arbitrary code execution

[CVE-2016-4655](#) An application may be able to disclose kernel memory

[CVE-2016-4656](#) An application may be able to execute arbitrary code with kernel privileges



# Scoring

- |   |  |
|---|--|
| 1 | The sample contains <b>no code protection</b> such as packing, obfuscation, or anti-reversing tricks |
|---|--|



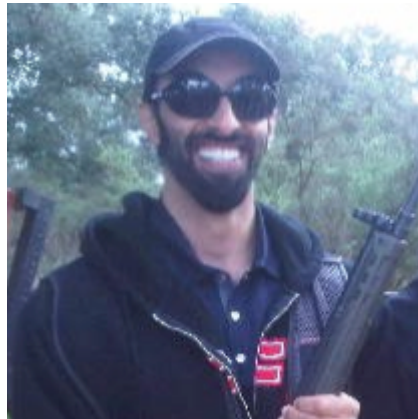
- |   |  |
|---|--|
| 2 | <b>Targeted and poorly customized.</b> Content is generally relevant ... May look questionable |
|---|--|

# Device Surveillance

- **Commercialization:** The same products are used by governments across the world



]HackingTeam[



]HackingTeam[



]HackingTeam[





# FINFISHER SPYWARE

Suspected Government Users In 2015

**Citizen Lab 2015**

Bill Marczak, John Scott-Railton,  
Adam Senft, Irene Poetranto & Sarah McKune

## Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation

October 15, 2015



# HACKING TEAM RCS

Suspected Government Users Worldwide

## Citizen Lab 2014

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire & John Scott-Railton



## 21 SUSPECTED GOVERNMENT USERS

AMERICAS	EUROPE	MIDDLE EAST	AFRICA	ASIA
Mexico Colombia Panama	Hungary Italy Poland	Oman Saudi Arabia UAE	Egypt Ethiopia Morocco Nigeria Sudan	Azerbaijan Kazakhstan Malaysia Thailand South Korea Uzbekistan

## CAUSE FOR CONCERN



**52%** (in bold) fall in the bottom 3rd of a World Bank ranking\* of freedom of expression and accountability



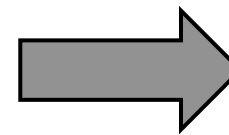
**29%** are in the bottom 3rd for Rule of Law

\*World Bank 2012 WGI

# Mapping Hacking Team's "Untraceable" Spyware

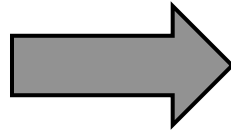
February 17, 2014

# SpyCall: Illustrated



**\*43#**  
(call waiting)

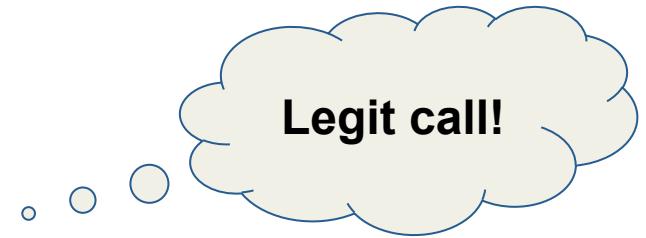
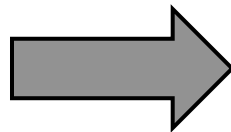
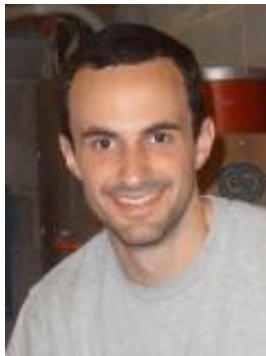
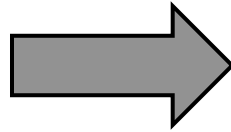
# SpyCall: Illustrated



**Special  
number!**

Cancel vibration  
Cancel ringer  
Stop backlight  
Modify call logs

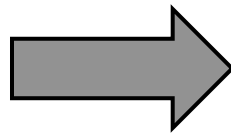
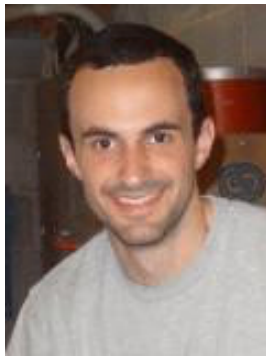
# SpyCall: Illustrated



# SpyCall: Illustrated



**Hold**



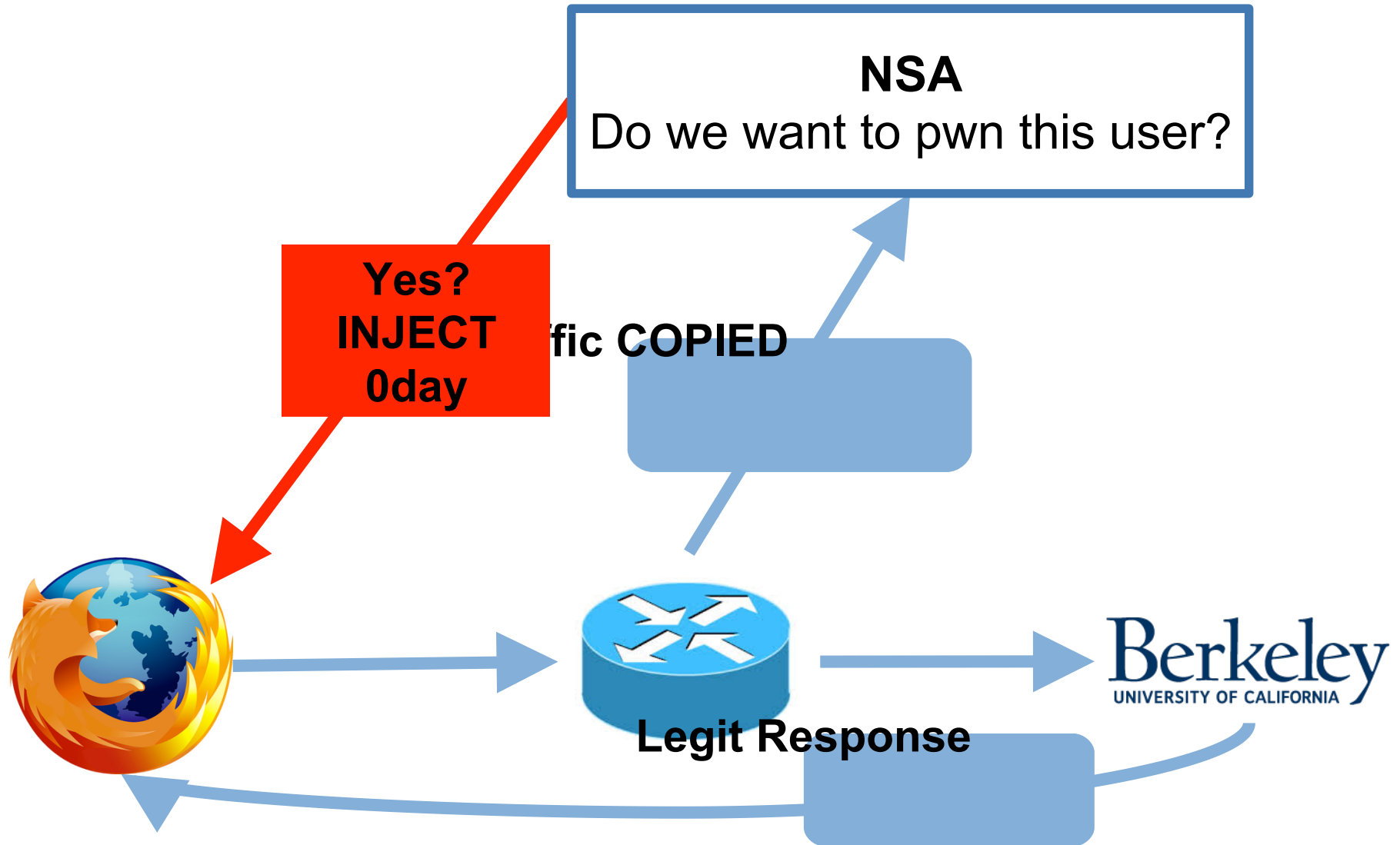
RING  
RING

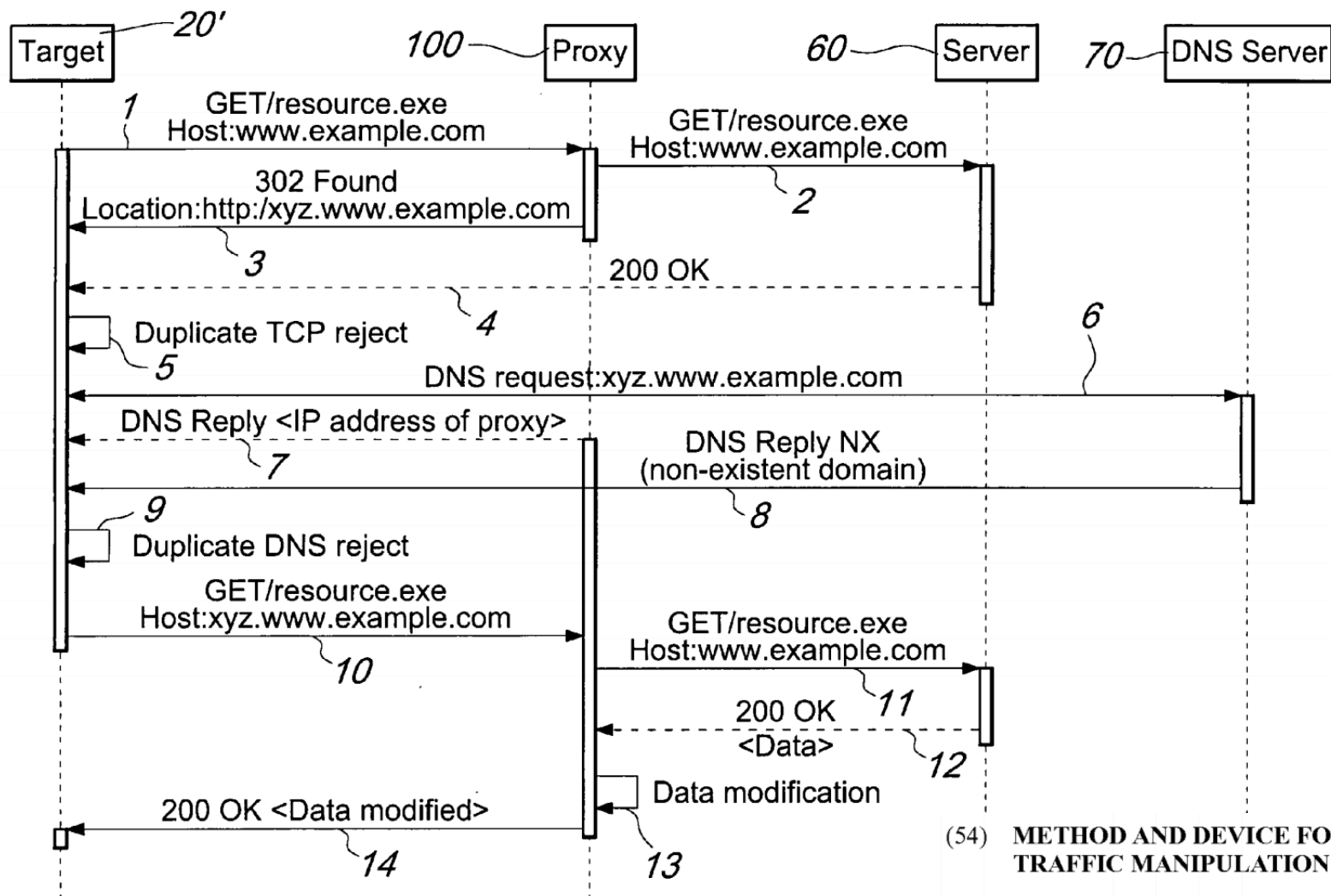
*BZZZZZZZZZZ*

FLASH  
FLASH



# The NSA's QUANTUM





(54) **METHOD AND DEVICE FOR NETWORK TRAFFIC MANIPULATION**

(75) Inventors: **Alberto Ornaghi**, Treviglio (IT); **Marco Valleri**, Lecce (IT); **Daniele Milan**, Robecchetto Con Induno (IT); **Valeriano Bedeschi**, Milano (IT)

(73) Assignee: **HT S.R.L.**, MILANO (IT)

(21) Appl. No.: **13/813,496**

(22) PCT Filed: **Aug. 3, 2010**