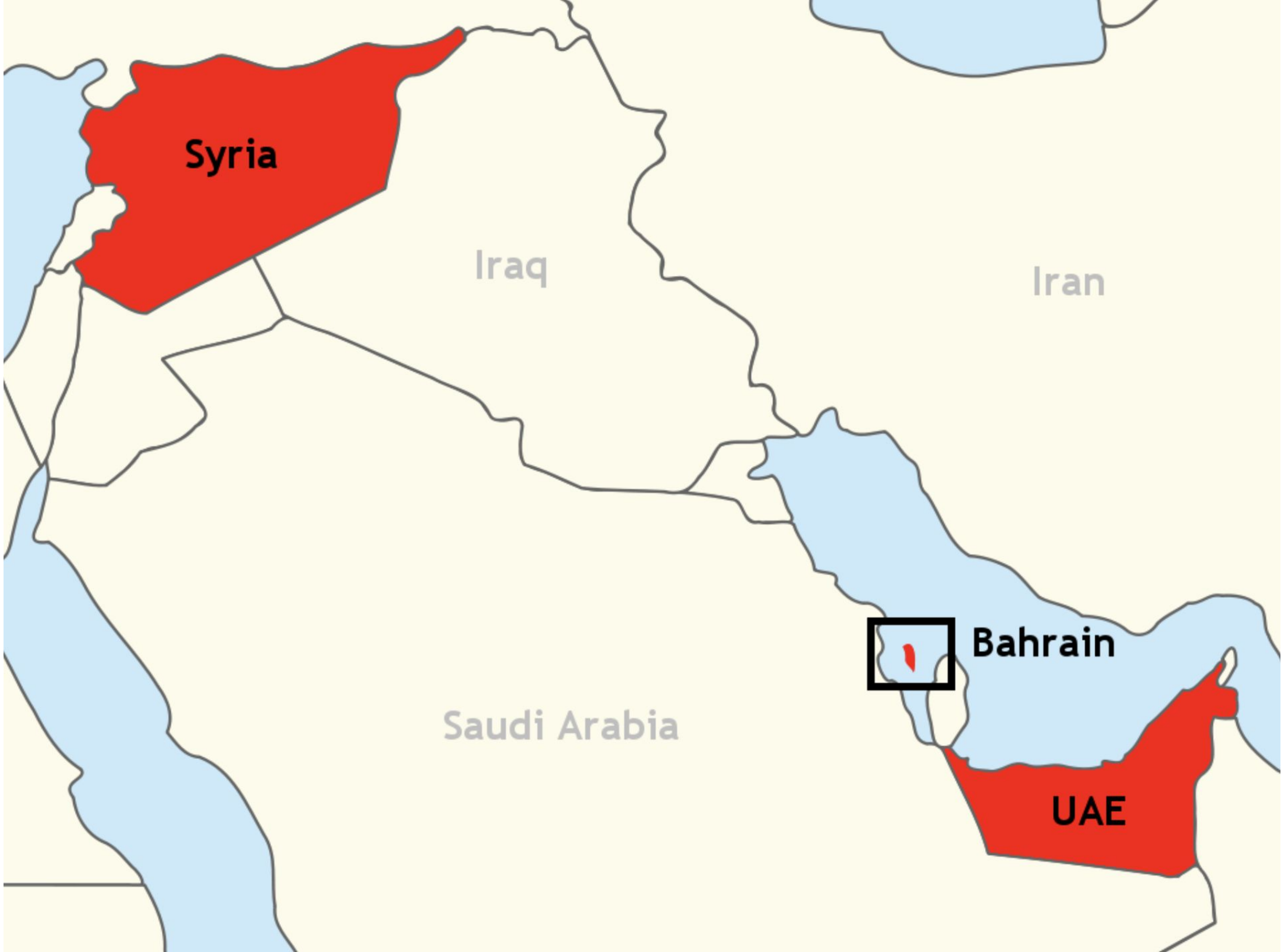
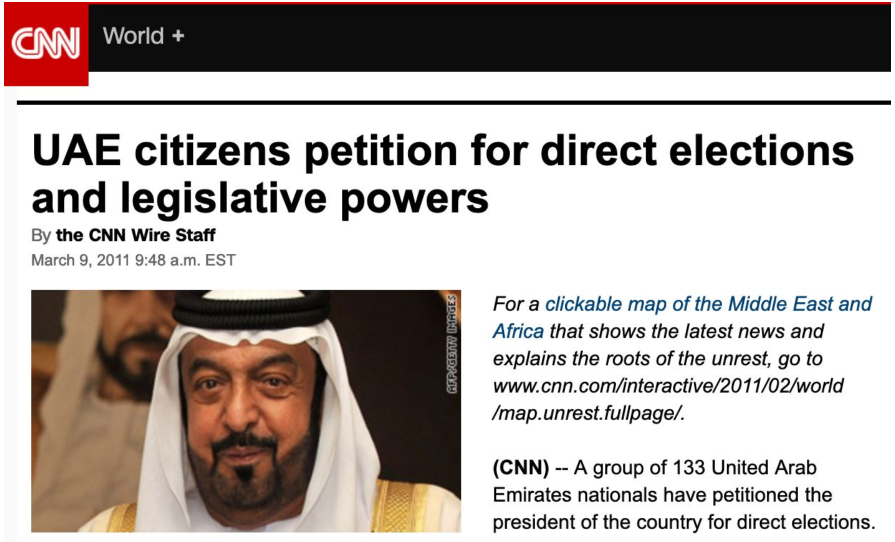
When Governments Hack Opponents

Bill Marczak

ICSI
INTERNATIONAL COMPUTER SCIENCE INSTITUTE

THE CITIZEN LAB


Syria
Iraq
Iran
Bahrain
Saudi Arabia
UAE



UAE citizens petition for direct elections and legislative powers

By **the CNN Wire Staff**

March 9, 2011 9:48 a.m. EST

For a clickable map of the Middle East and Africa that shows the latest news and explains the roots of the unrest, go to www.cnn.com/interactive/2011/02/world /map.unrest.fullpage/.

(CNN) -- A group of 133 United Arab Emirates nationals have petitioned the president of the country for direct elections.

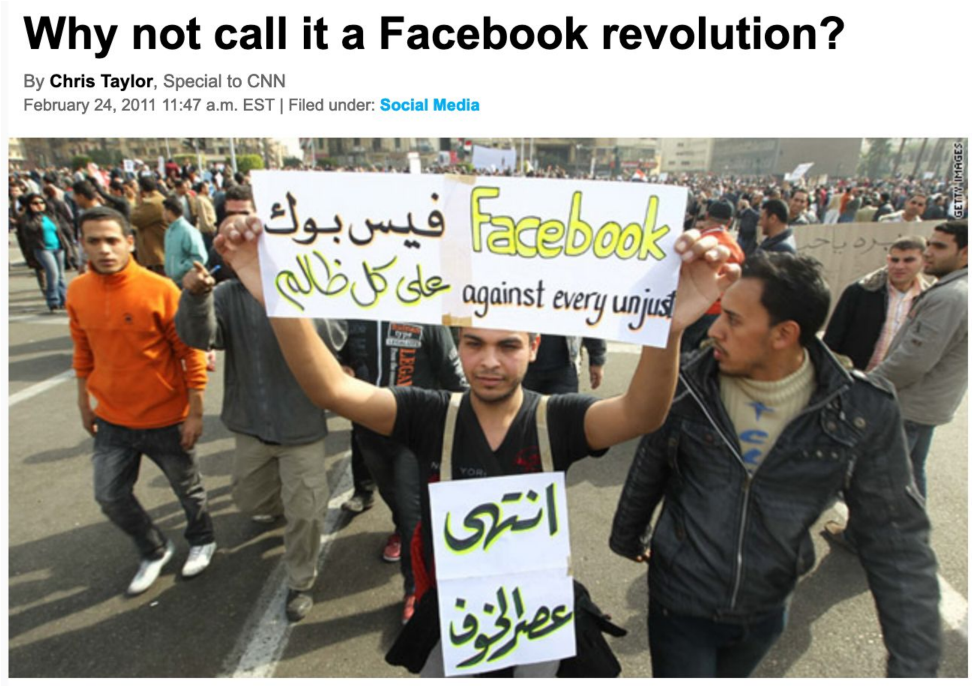
Bloomberg

Torture in Bahrain Becomes Routine With Help From Nokia Siemens

Vernon Silver and Ben Elgin
August 22, 2011, 3:01 PM PDT

Abdul Ghani al-Khanjar
Bahraini Activist

First, Bahraini jailers armed with stiff rubber hoses beat the 39-year-old school administrator and human rights activist in a windowless room… **Then, they dragged him upstairs for questioning by a uniformed officer armed with another kind of weapon: transcripts of his text messages and details from personal mobile phone conversations…**



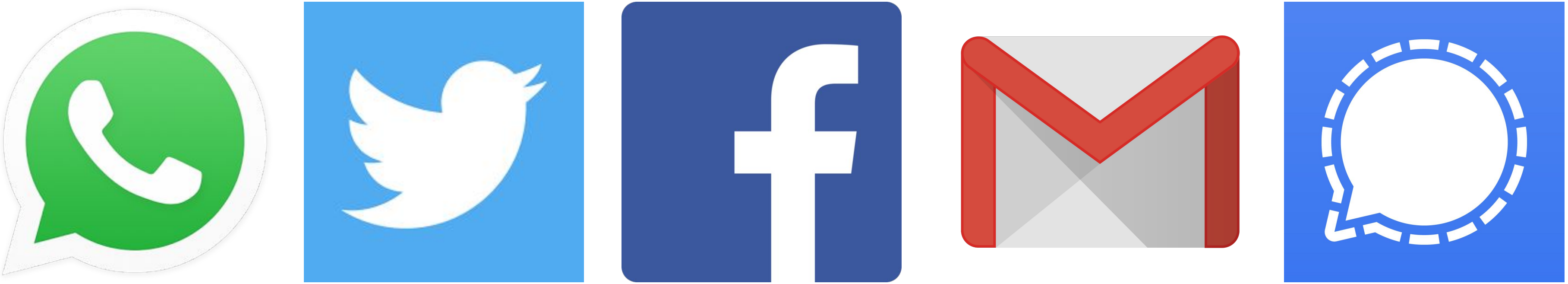
Why not call it a Facebook revolution?

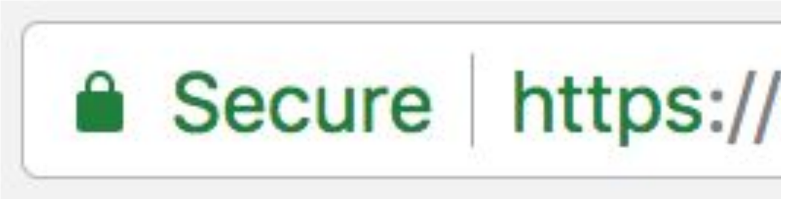
By **Chris Taylor**, Special to CNN
February 24, 2011 11:47 a.m. EST | Filed under: **Social Media**

The 'Twitter Revolution' Debate: The Egyptian Test Case

How are social networks affecting the demonstrations

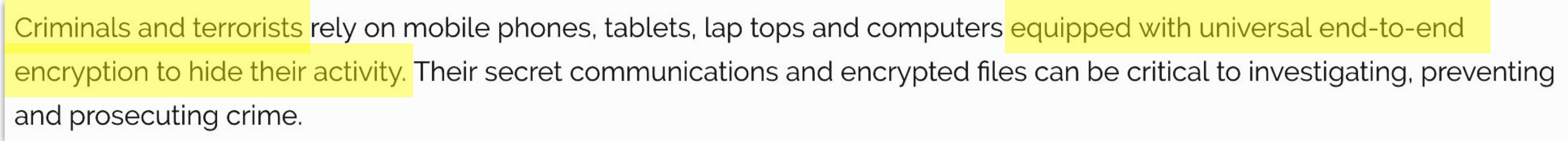
Activist communication tools...





Secure https://

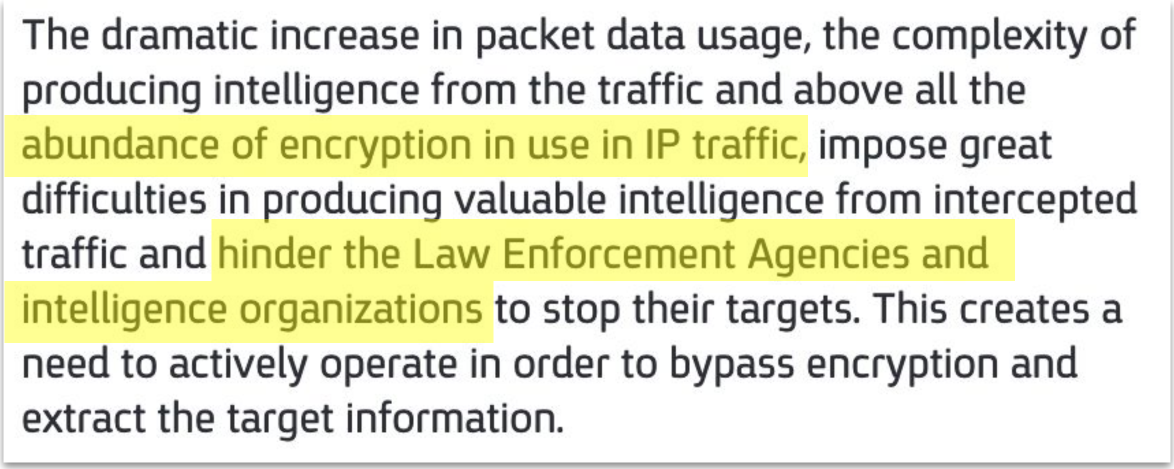
]HackingTeam[



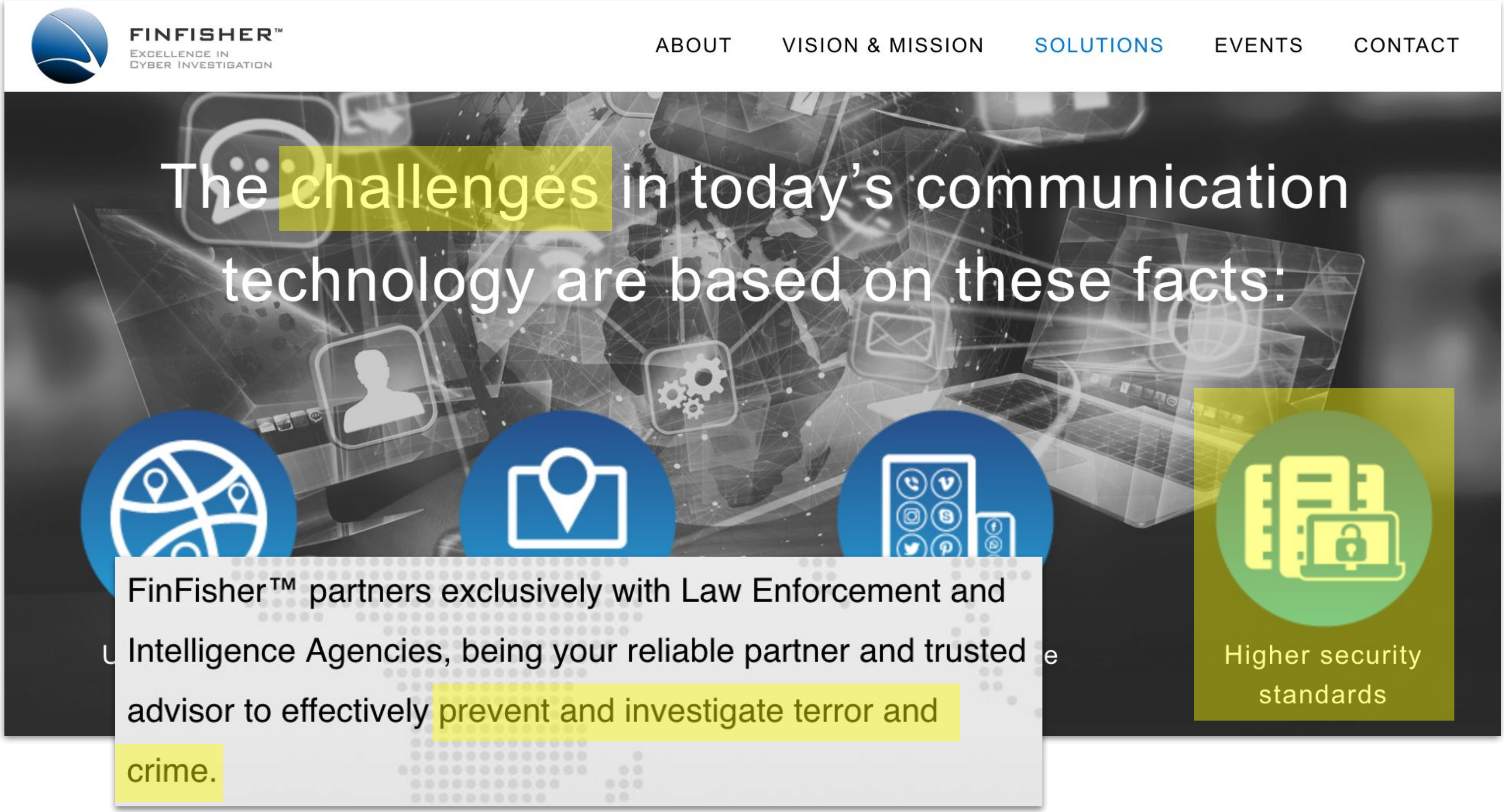
Criminals and terrorists rely on mobile phones, tablets, lap tops and computers equipped with universal end-to-end encryption to hide their activity. Their secret communications and encrypted files can be critical to investigating, preventing and prosecuting crime.

CYBERBIT

PROTECTING A NEW DIMENSION



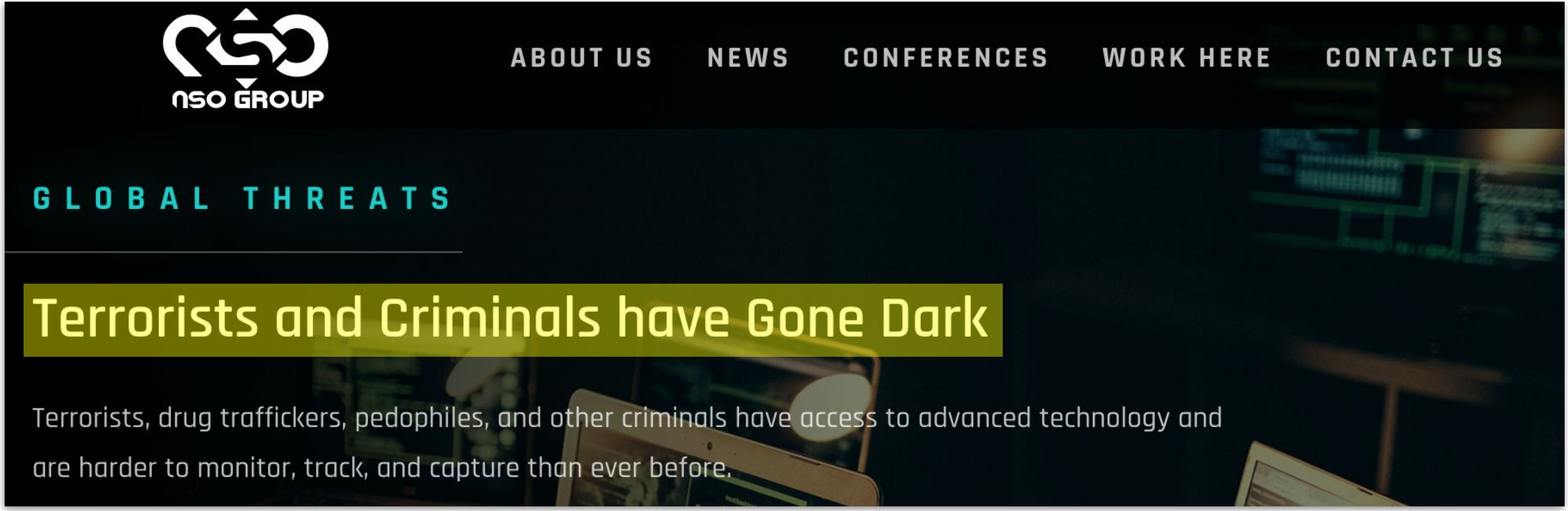
The dramatic increase in packet data usage, the complexity of producing intelligence from the traffic and above all the abundance of encryption in use in IP traffic, impose great difficulties in producing valuable intelligence from intercepted traffic and hinder the Law Enforcement Agencies and intelligence organizations to stop their targets. This creates a need to actively operate in order to bypass encryption and extract the target information.



The challenges in today's communication technology are based on these facts:

Higher security standards

FinFisher™ partners exclusively with Law Enforcement and Intelligence Agencies, being your reliable partner and trusted advisor to effectively prevent and investigate terror and crime.

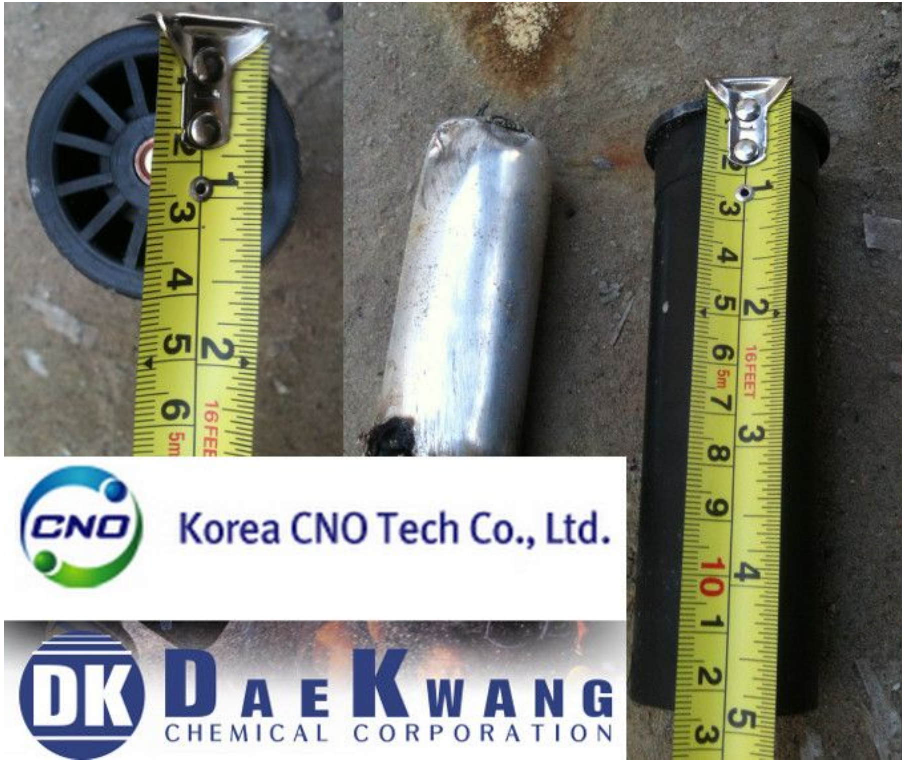


GLOBAL THREATS

Terrorists and Criminals have Gone Dark

Terrorists, drug traffickers, pedophiles, and other criminals have access to advanced technology and are harder to monitor, track, and capture than ever before.

“Cred”


Korea CNO Tech Co., Ltd.
CNO
DK
DaeKwang
CHEMICAL CORPORATION

방위사업청, 2년 연속 민원처리 최우수기관
최루탄 수출을 중단하라
STOP the Shipment

"All the News That's Fit to Print"
The New York Times
Late Edition
VOL. CLXI . . . No. 55,880
NEW YORK, FRIDAY, AUGUST 31, 2012
$2.50
NO CHARGES FILED IN TWO DEATHS INVOLVING C.I.A.
HARSH INTERROGATIONS
Not Enough Evidence to Make Case, Justice Dept. Says
Romney Vows to Deliver Country From Economic Travails
Appeal to Voters Disillusioned by Obama
NEWS ANALYSIS
A Suitor Makes the Case for Divorce
ELECTION 2012
Nuclear Report On Iran Puts Israel in a Box
Weakened Storm Still Packs a Punch
Al Jazeera, Seeking U.S. Viewers, Bets on Soccer
Software Meant to Fight Crime Is Used to Spy on Dissident
Cartier

Software Meant to Fight Crime Is Used to Spy on Dissidents

By NICOLE PERLROTH

SAN FRANCISCO — Morgan Marquis-Boire works as a Google engineer and Bill Marczak is earning a Ph.D. in computer science. But this summer, the two men have been moonlighting as detectives, chasing an elusive surveillance tool from Bahrain across five continents.

What they found was the widespread use of sophisticated, off-the-shelf computer espionage software by governments with questionable records on human rights. While the software is supposedly sold for use only in criminal investigations, the two came across evidence that it was being used to target political dissidents.

The software proved to be the stuff of a spy film: it can grab images of computer screens, record Skype chats, turn on cameras and microphones and log keystrokes. The two men said they discovered mobile versions of the spyware customized for all major mobile phones.

But what made the software especially sophisticated was how well it avoided detection. Its creators specifically engineered it to elude antivirus software made by Kaspersky Lab, Symantec, F-Secure and others.

The software has been identified as FinSpy, one of the more elusive spyware tools sold in the growing market of off-the-shelf computer surveillance technologies that give governments a sophisticated plug-in monitoring operation. Research now links it to servers in more than a dozen countries, including Turkmenistan, Brunei and Bahrain, although no government acknowledges using the software for surveillance purposes.

The market for such technologies has grown to $5 billion a year from "nothing 10 years ago," said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveil-

THOR SWIFT FOR THE NEW YORK TIMES

Morgan Marquis-Boire, left, and Bill Marczak.

Continued on Page B2

"All the News That's Fit to Print"
The New York Times
Late Edition
VOL. CLXI . . No. 55,880
NEW YORK, FRIDAY, AUGUST 31, 2012
$2.50
NO CHARGES FILED IN TWO DEATHS INVOLVING C.I.A.
Romney Vows to Deliver Country From Economic Travails
Appeal to Voters Disillusioned by Obama
A Suitor Makes the Case for Divorce
Nuclear Report On Iran Puts Israel in a Box
Weakened Storm Still Packs a Punch
Al Jazeera, Seeking U.S. Viewers, Bets on Soccer
Software Meant to Fight Crime Is Used to Spy on Dissidents
Cartier

Software Meant to Fight Crime Is Used to Spy on Dissidents

By NICOLE PERLROTH

SAN FRANCISCO — Morgan Marquis-Boire works as a Google engineer and Bill Marczak is earning a Ph.D. in computer science. But this summer, the two men have been moonlighting as detectives, chasing an elusive surveillance tool from Bahrain across five continents.

What they found was the widespread use of sophisticated, off-the-shelf computer espionage software by governments with questionable records on human rights. While the software is supposedly sold for use only in criminal investigations, the two came across evidence that it was being used to target political dissidents.

The software proved to be the stuff of a spy film: it can grab images of computer screens, record Skype chats, turn on cameras and microphones and log keystrokes. The two men said they discovered mobile versions of the spyware customized for all major mobile phones.

But what made the software especially sophisticated was how well it avoided detection. Its creators specifically engineered it to elude antivirus software made by Kaspersky Lab, Symantec, F-Secure and others.

The software has been identified as FinSpy, one of the more elusive spyware tools sold in the growing market of off-the-shelf computer surveillance technologies that give governments a sophisticated plug-in monitoring operation. Research now links it to servers in more than a dozen countries, including Turkmenistan, Brunei and Bahrain, although no government acknowledges using the software for surveillance purposes.

The market for such technologies has grown to $5 billion a year from "nothing 10 years ago," said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveil-

THOR SWIFT FOR THE NEW YORK TIMES

Morgan Marquis-Boire, left, and Bill Marczak.

Continued on Page B2

IF YOU GET A SUSPICIOUS EMAIL OR MESSAGE, SEND IT TO ME!

"All the News That's Fit to Print"

The New York Times

Late Edition

VOL. CLXI . . No. 55,880

NEW YORK, FRIDAY, AUGUST 31, 2012

$2.50

NO CHARGES FILED IN TWO DEATHS INVOLVING C.I.A.

HARSH INTERROGATIONS

Not Enough Evidence to Make Case, Justice Dept. Says

Romney Vows to Deliver Country From Economic Travails

Appeal to Voters Disillusioned by Obama

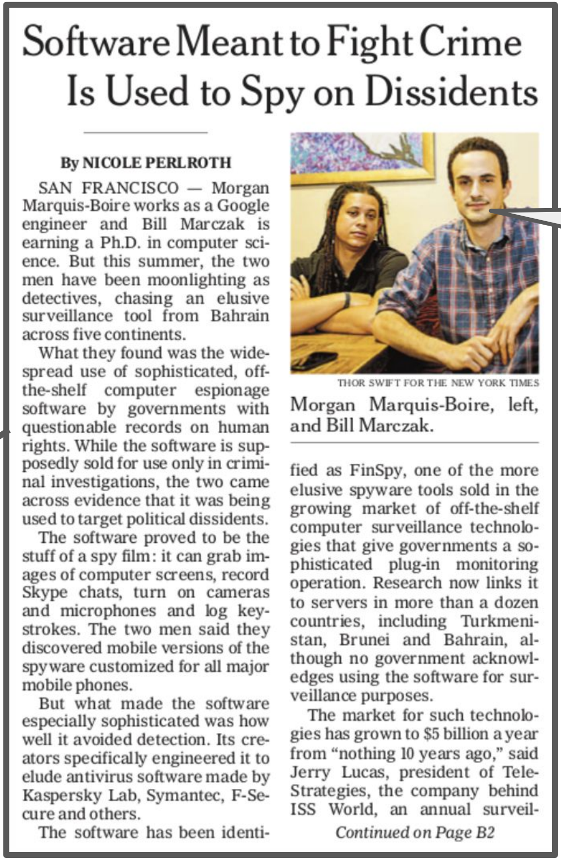
A Suitor Makes the Case for Divorce

Nuclear Report On Iran Puts Israel in a Box

Weakened Storm Still Packs a Punch

Al Jazeera, Seeking U.S. Viewers, Bets on Soccer

Software Meant to Fight Crime Is Used to Spy on Dissidents



Software Meant to Fight Crime Is Used to Spy on Dissidents

By NICOLE PERLROTH

SAN FRANCISCO — Morgan Marquis-Boire works as a Google engineer and Bill Marczak is earning a Ph.D. in computer science. But this summer, the two men have been moonlighting as detectives, chasing an elusive surveillance tool from Bahrain across five continents.

What they found was the widespread use of sophisticated, off-the-shelf computer espionage software by governments with questionable records on human rights. While the software is supposedly sold for use only in criminal investigations, the two came across evidence that it was being used to target political dissidents.

The software proved to be the stuff of a spy film: it can grab images of computer screens, record Skype chats, turn on cameras and microphones and log keystrokes. The two men said they discovered mobile versions of the spyware customized for all major mobile phones.

But what made the software especially sophisticated was how well it avoided detection. Its creators specifically engineered it to elude antivirus software made by Kaspersky Lab, Symantec, F-Secure and others.

The software has been identified as FinSpy, one of the more elusive spyware tools sold in the growing market of off-the-shelf computer surveillance technologies that give governments a sophisticated plug-in monitoring operation. Research now links it to servers in more than a dozen countries, including Turkmenistan, Brunei and Bahrain, although no government acknowledges using the software for surveillance purposes.

The market for such technologies has grown to $5 billion a year from "nothing 10 years ago," said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveil-

Continued on Page B2

THOR SWIFT FOR THE NEW YORK TIMES

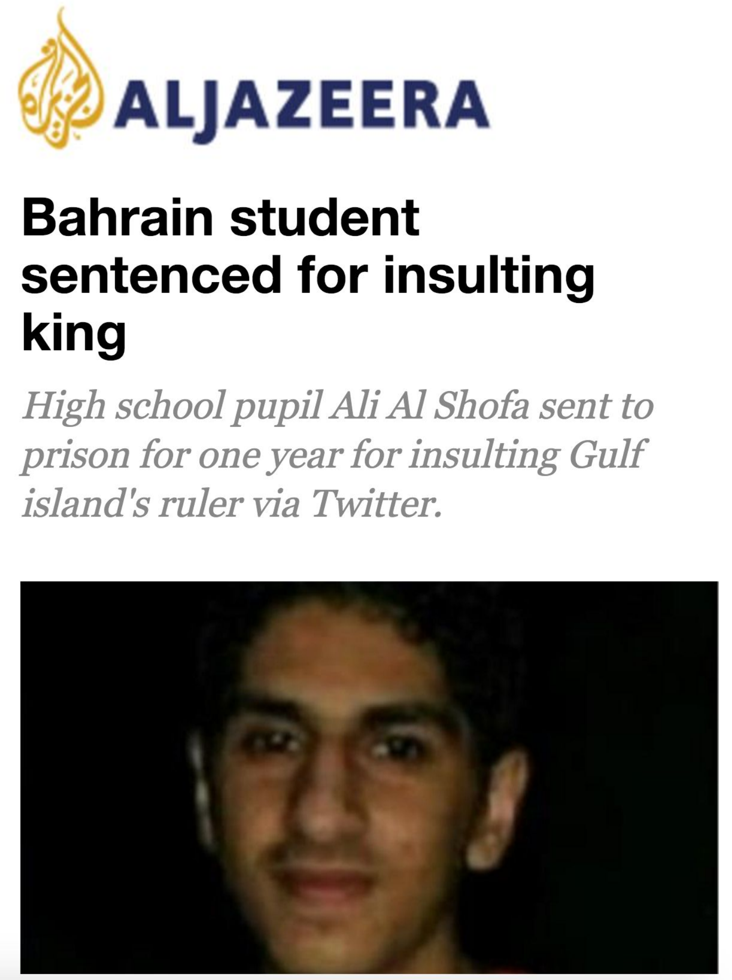
Morgan Marquis-Boire, left, and Bill Marczak.

IF YOU GET A SUSPICIOUS EMAIL OR MESSAGE, SEND IT TO ME!

HEY BILL, I GOT A WEIRD EMAIL!

Ahmed Mansoor
UAE Activist

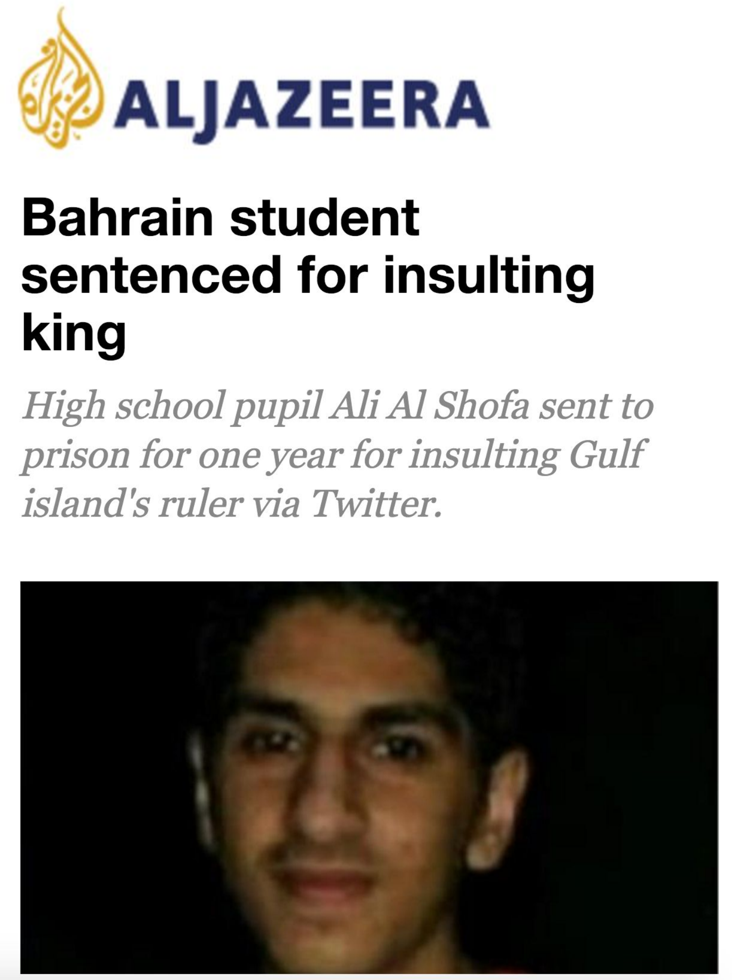
The Data



ALJAZEERA

Bahrain student sentenced for insulting king

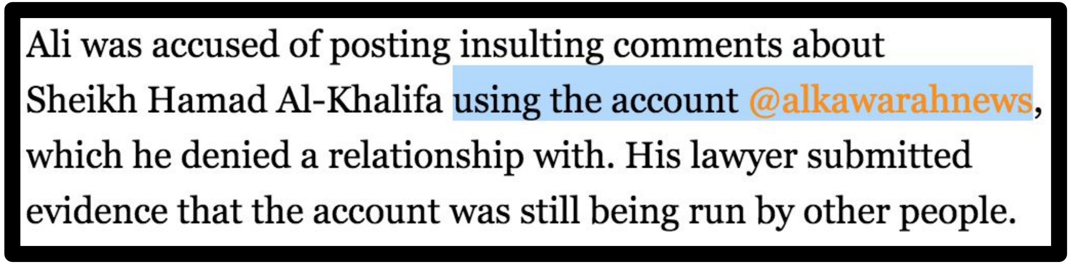
High school pupil Ali Al Shofa sent to prison for one year for insulting Gulf island's ruler via Twitter.



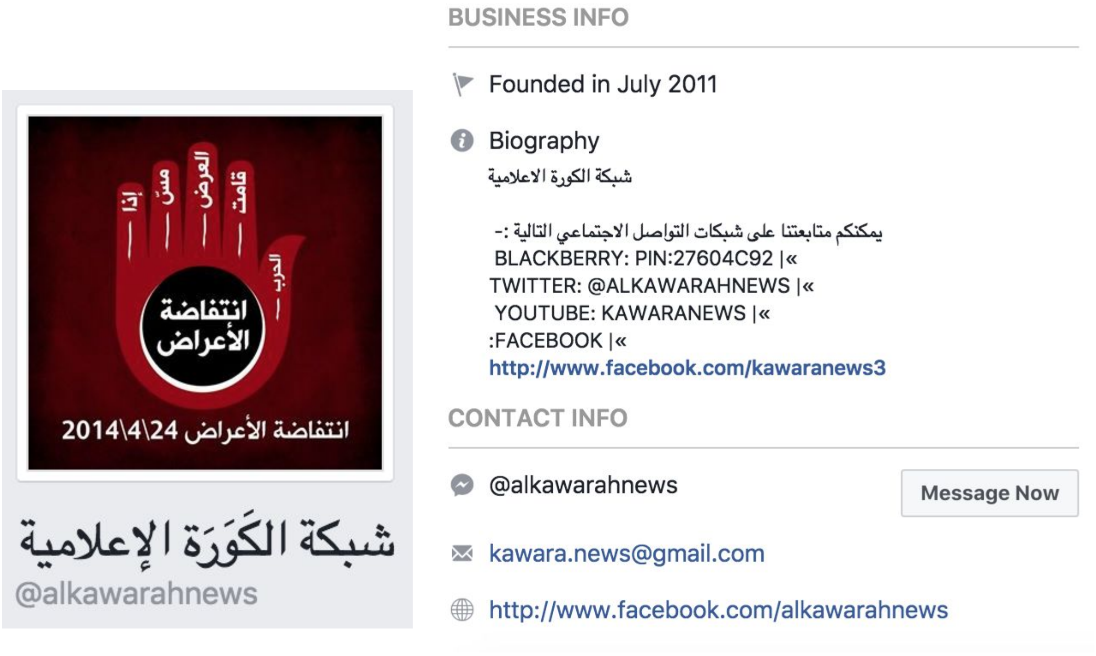
ALJAZEERA

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.



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 الكَوَرَة الإعلامية

@alkawarahnews

BUSINESS INFO

Founded in July 2011

Biography

شبكة الكورة الاعلامية

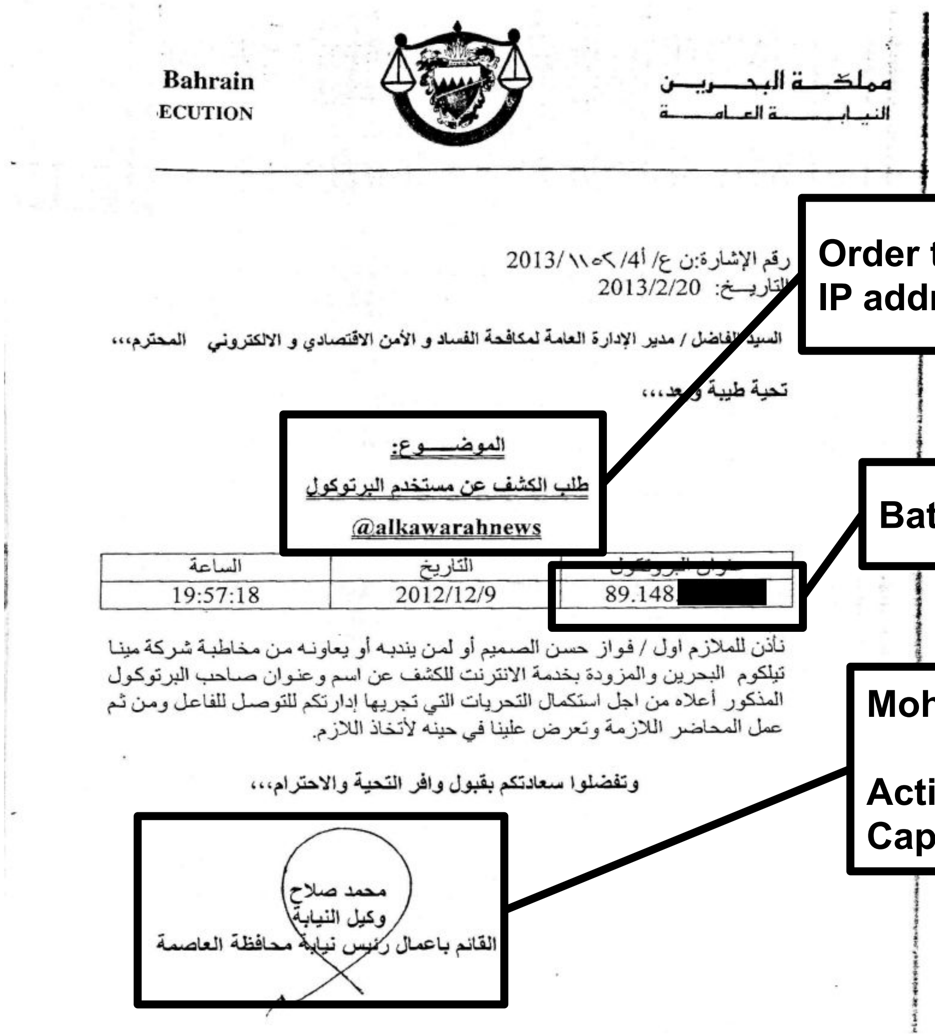
يمكنكم متابعتنا على شبكات التواصل الاجتماعي التالية :-
BLACKBERRY: PIN:27604C92 |«
TWITTER: @ALKAWARAHNEWS |«
YOUTUBE: KAWARANEWS |«
:FACEBOOK |«
http://www.facebook.com/kawaranews3

CONTACT INFO

@alkawarahnews

kawara.news@gmail.com

http://www.facebook.com/alkawarahnews



Bahrain
ECUTION

مملكـــة البحـــريـــن
النيابـــــة العامــــة

رقم الإشارة:ن ع/ أ/4/ ١١٥٧/ 2013
التاريـــخ: 2013/2/20

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

تحية طيبة وبعد،،،

الموضـــــوع:
طلب الكشف عن مستخدم البرتوكول
@alkawarahnews

عنوان البرتوكول	التاريخ	الساعة
89.148.[redacted]	2012/12/9	19:57:18

نأذن للملازم اول / فواز 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 اجل استكمال التحريات التي تجريها إدارتكم للتوصل للفاعل ومن ثم عمل المحاضر اللازمة وتعرض علينا في حينه لأتخاذ اللازم.

وتفضلوا سعادتكم بقبول وافر التحية والاحترام،،،

محمد صلاح
وكيل النيابة
القائم باعمال رئيس نيابة محافظة العاصمة

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

Batelco (residential ISP)

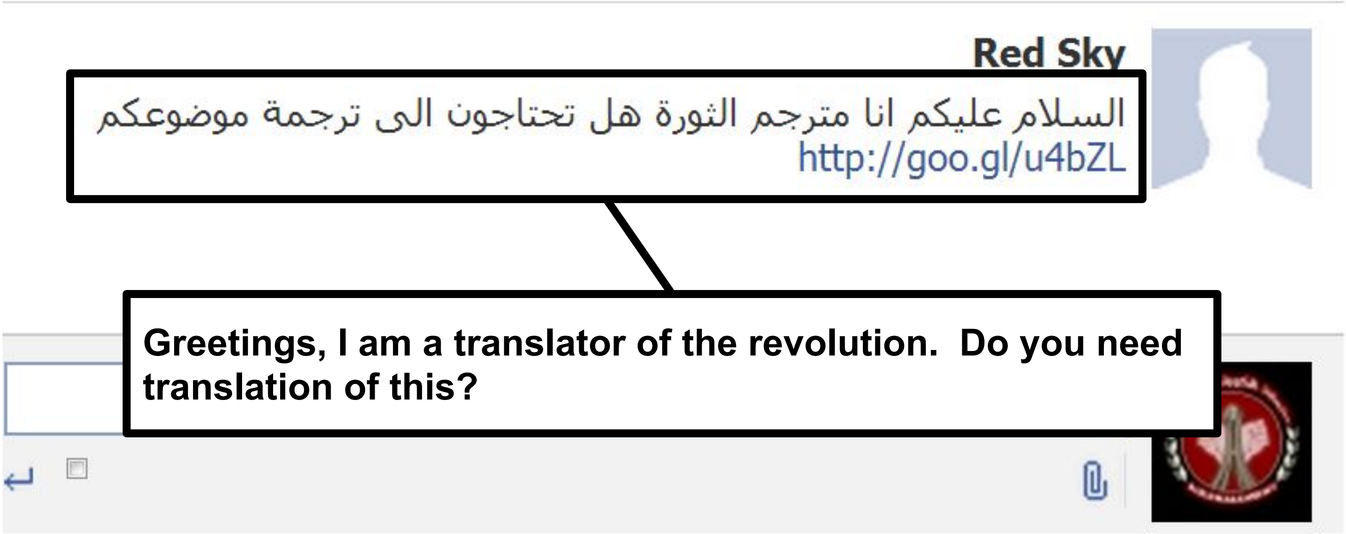
Mohammed Salah

Acting Chief Prosecutor, Capital Region

"IT IS A SECRET INVESTIGATION INVOLVING PRIVATE METHODS OF OUR DEPARTMENT THAT CANNOT BE DISCLOSED"

Col. Fawaz al-Sumaim
Bahrain Cyber Crime Unit

(Arrested activist) **Red Sky**

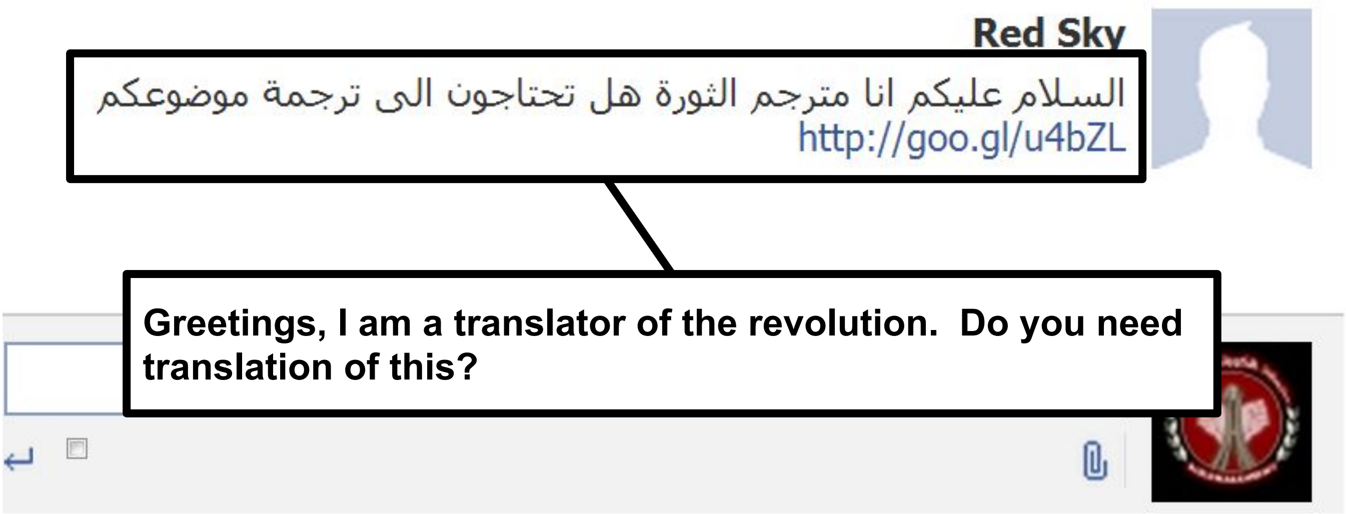


Red Sky

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

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

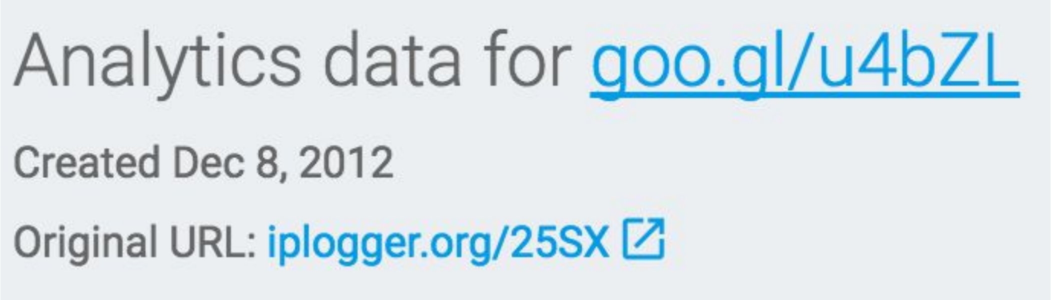
(Arrested activist) **Red Sky**



Red Sky

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

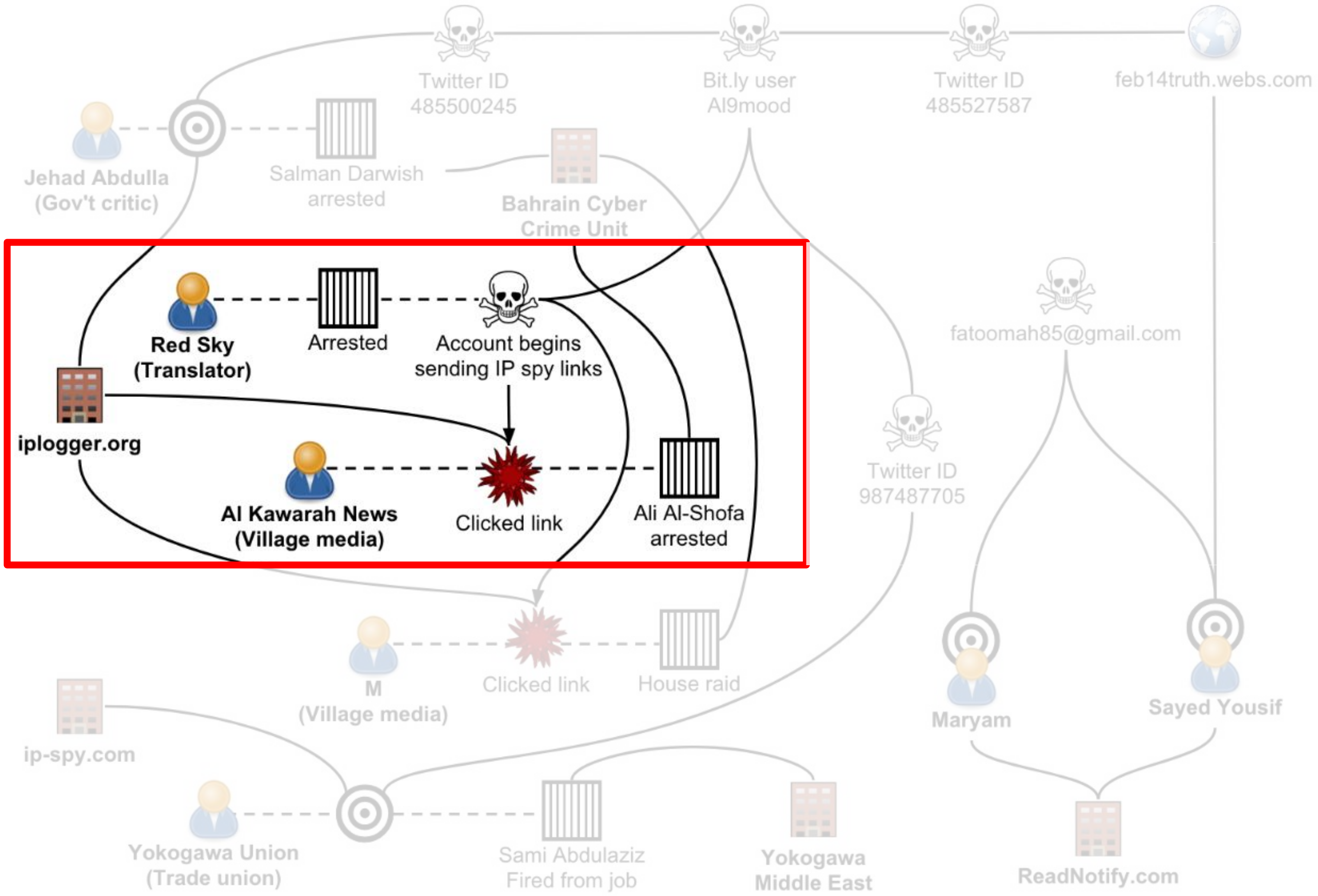
Greetings, I am a translator of the revolution. Do you need translation of this?

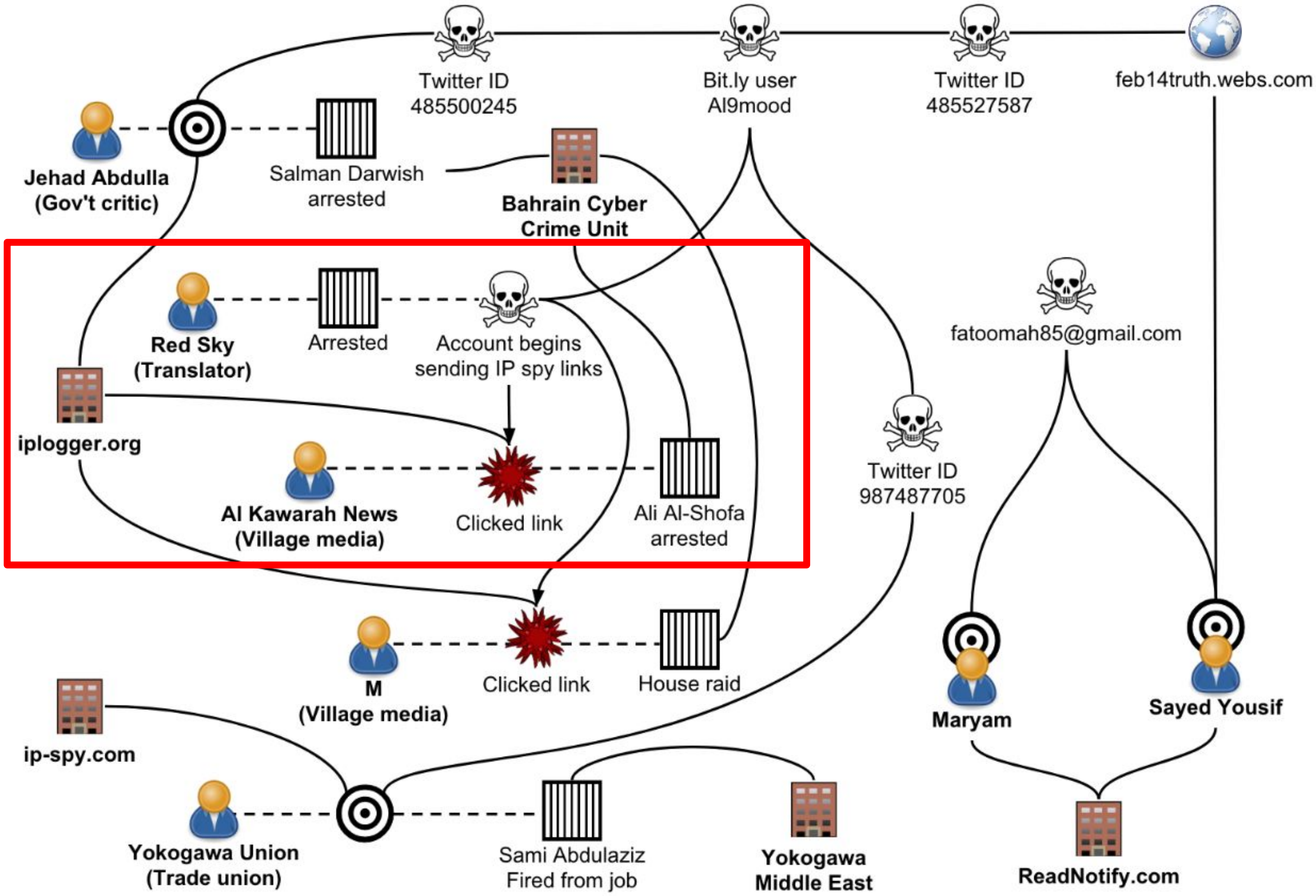


Analytics data for goo.gl/u4bZL

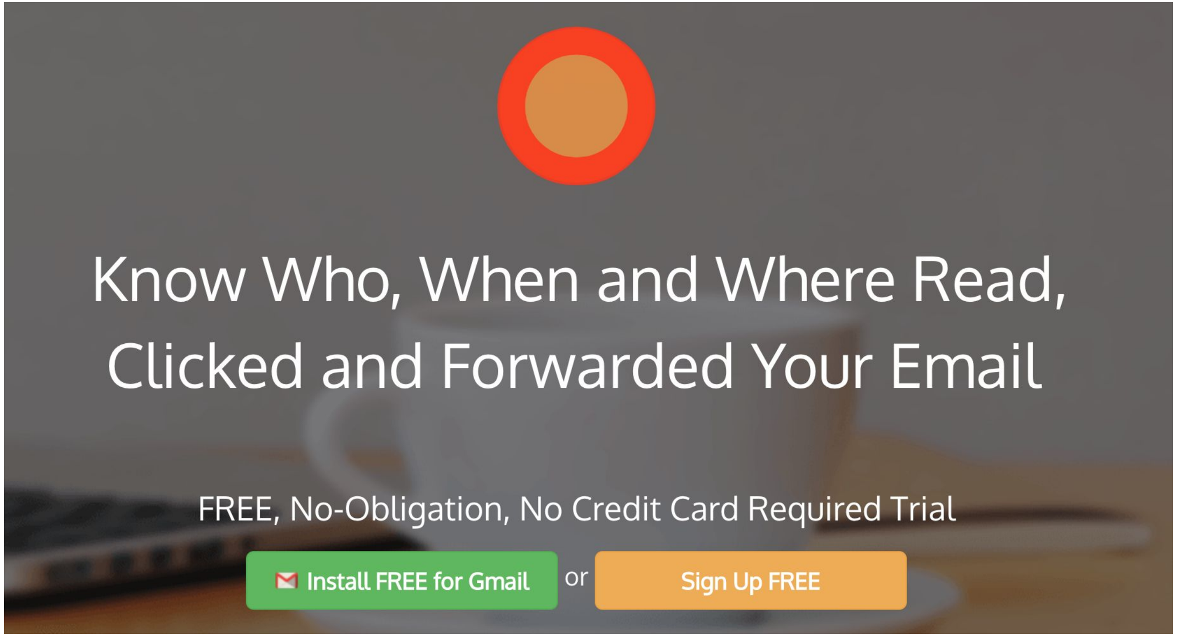
Created Dec 8, 2012

Original URL: iplogger.org/25SX


Twitter ID 485500245
Bit.ly user Al9mood
Twitter ID 485527587
feb14truth.webs.com
Jehad Abdulla (Gov't critic)
Salman Darwish arrested
Bahrain Cyber Crime Unit
Red Sky (Translator)
Arrested
Account begins sending IP spy links
fatoomah85@gmail.com
iplogger.org
Twitter ID 987487705
Al Kawarah News (Village media)
Clicked link
Ali Al-Shofa arrested
M (Village media)
Clicked link
House raid
Maryam
Sayed Yousif
ip-spy.com
Yokogawa Union (Trade union)
Sami Abdulaziz Fired from job
Yokogawa Middle East
ReadNotify.com

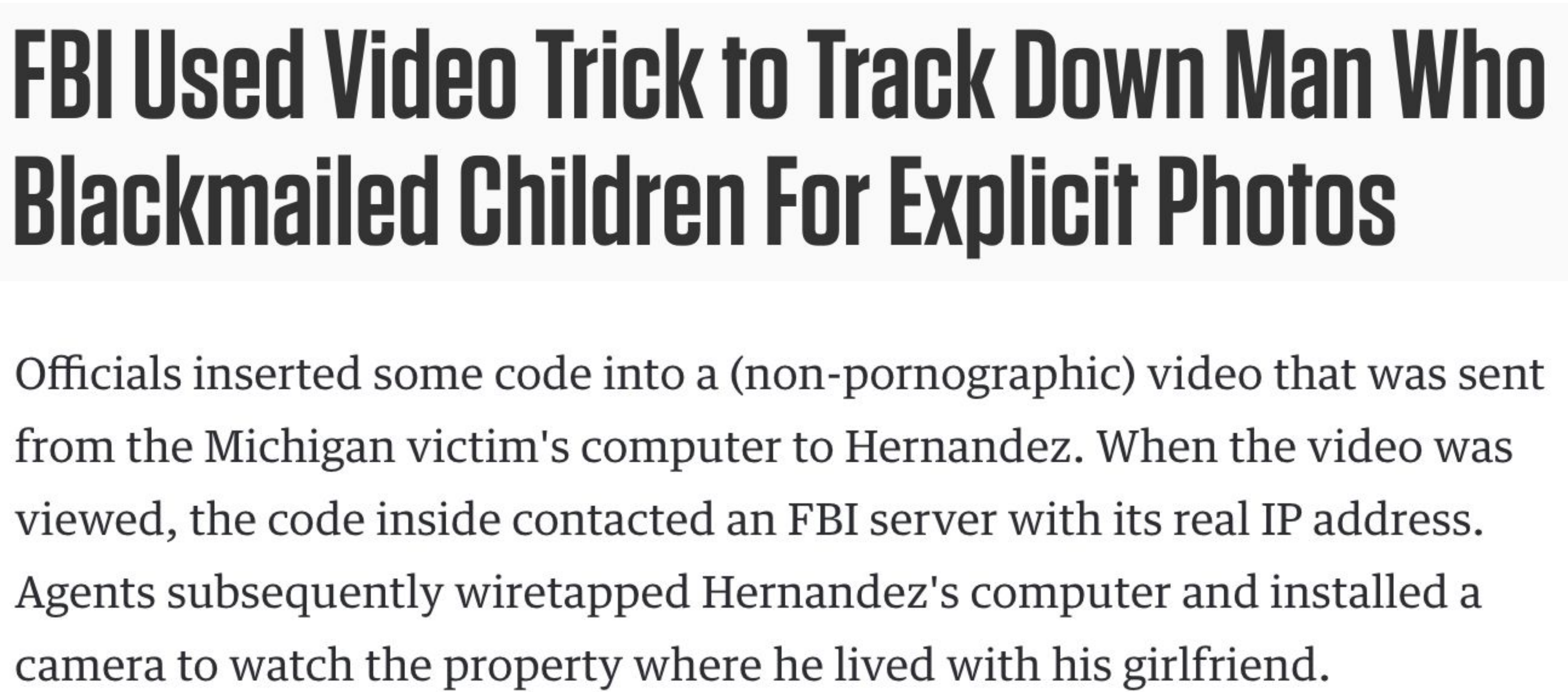


Twitter ID 485500245
Bit.ly user Al9mood
Twitter ID 485527587
feb14truth.webs.com
Jehad Abdulla (Gov't critic)
Salman Darwish arrested
Bahrain Cyber Crime Unit
Red Sky (Translator)
Arrested
Account begins sending IP spy links
fatoomah85@gmail.com
iplogger.org
Al Kawarah News (Village media)
Clicked link
Ali Al-Shofa arrested
Twitter ID 987487705
M (Village media)
Clicked link
House raid
Maryam
Sayed Yousif
ip-spy.com
Yokogawa Union (Trade union)
Sami Abdulaziz Fired from job
Yokogawa Middle East
ReadNotify.com



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

FREE, No-Obligation, No Credit Card Required Trial

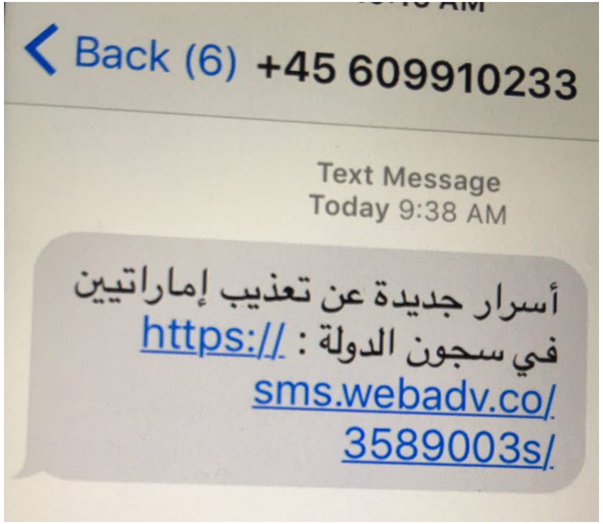


FBI Used Video Trick to Track Down Man Who Blackmailed Children For Explicit Photos

Officials inserted some code into a (non-pornographic) video that was sent from the Michigan victim's computer to Hernandez. When the video was viewed, the code inside contacted an FBI server with its real IP address. Agents subsequently wiretapped Hernandez's computer and installed a camera to watch the property where he lived with his girlfriend.

Sketch: Social Engineering

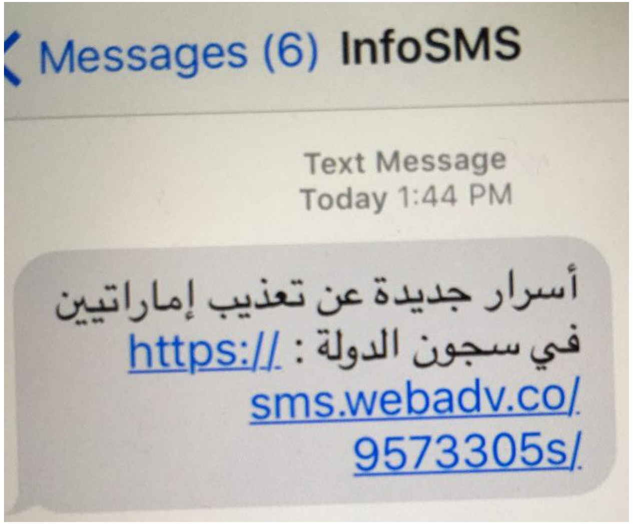
Ahmed Mansoor
UAE Activist



< Back (6) +45 609910233

Text Message
Today 9:38 AM

أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
3589003s/



< Messages (6) InfoSMS

Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
9573305s/

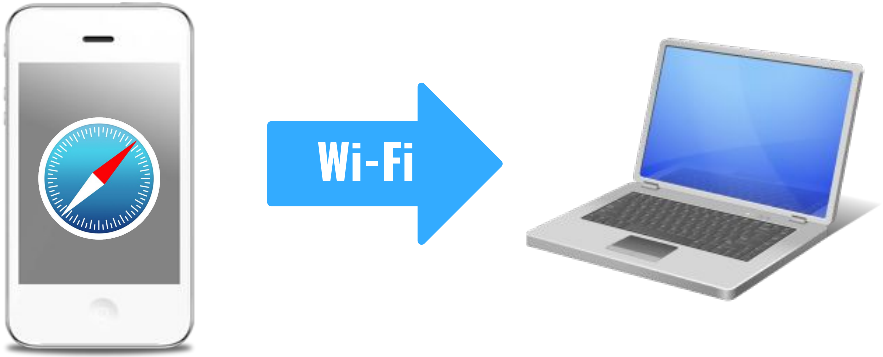
"NEW SECRETS ABOUT TORTURE OF EMIRATIS IN STATE PRISONS"

Nice Bait, we’ll take it!

Nice Bait, we'll take it!

Factory-Reset iPhone (Wi-Fi Only)

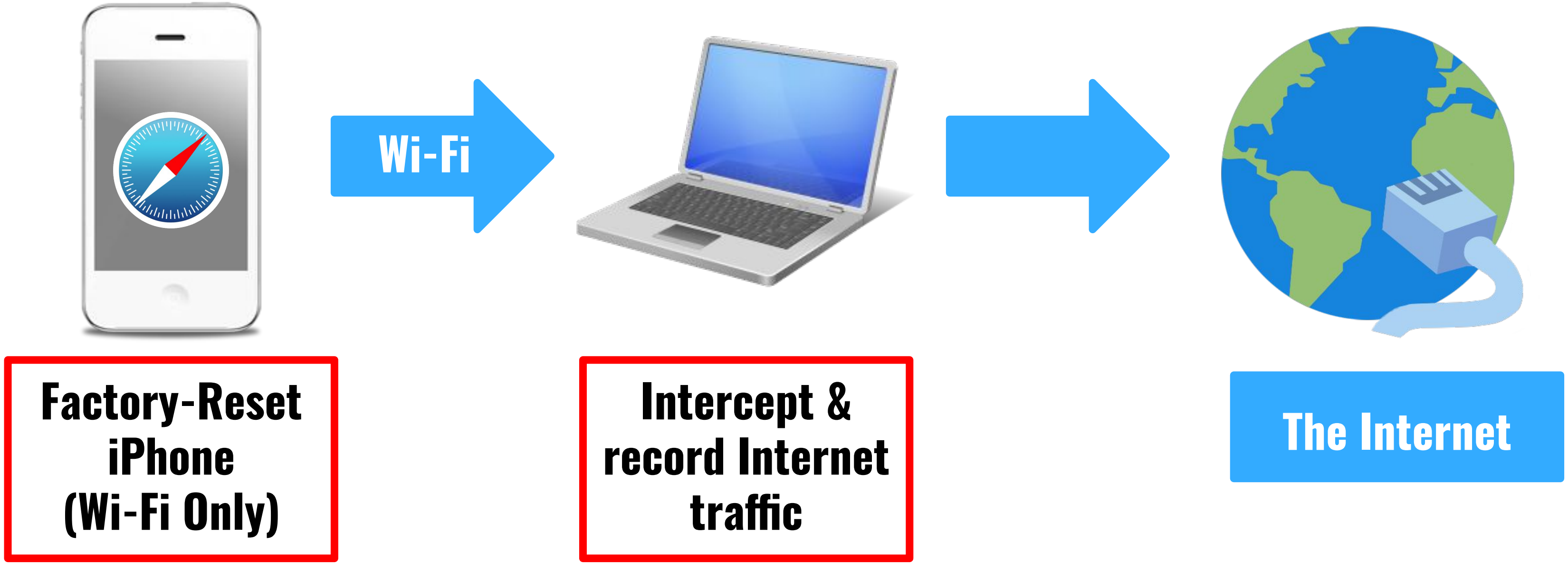
Nice Bait, we’ll take it!



Factory-Reset
iPhone
(Wi-Fi Only)

Intercept &
record Internet
traffic

Nice Bait, we'll take it!



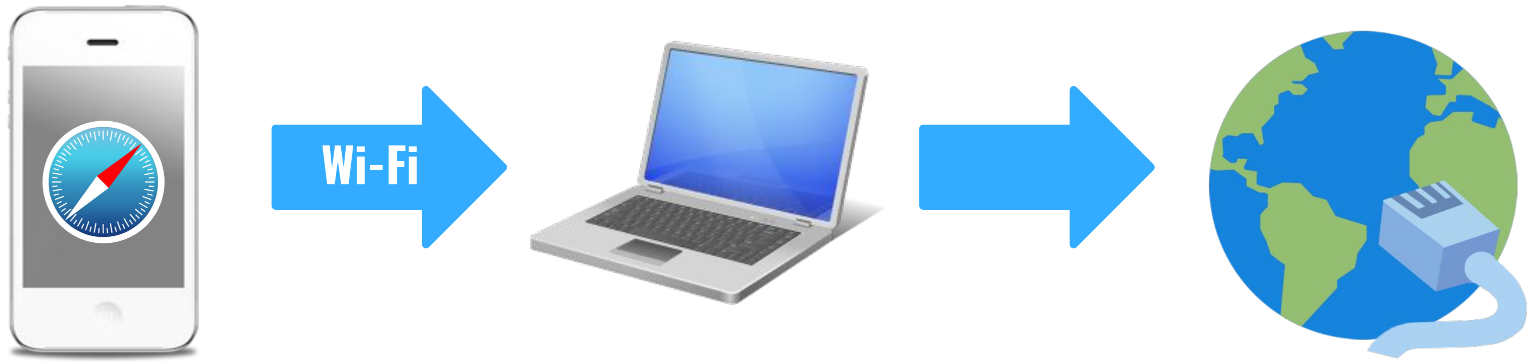
Wi-Fi

Factory-Reset iPhone (Wi-Fi Only)

Intercept & record Internet traffic

The Internet

Nice Bait, we'll take it!



Factory-Reset iPhone (Wi-Fi Only)

Intercept & record Internet traffic

The Internet

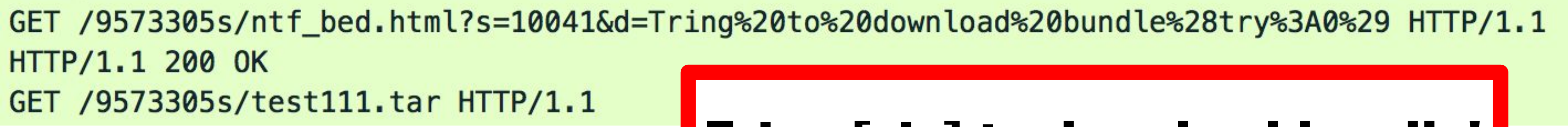
Type in the link from Mansoor...

… and what happens next will SHOCK YOU!

Safari window closes!

… and what happens next will SHOCK YOU!

Safari window closes!



```
GET /9573305s/ntf_bed.html?s=10041&d=Tring%20to%20download%20bundle%28try%3A0%29 HTTP/1.1
HTTP/1.1 200 OK
GET /9573305s/test111.tar HTTP/1.1
```

Tring [sic] to download bundle!

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

CVE-2016-4657

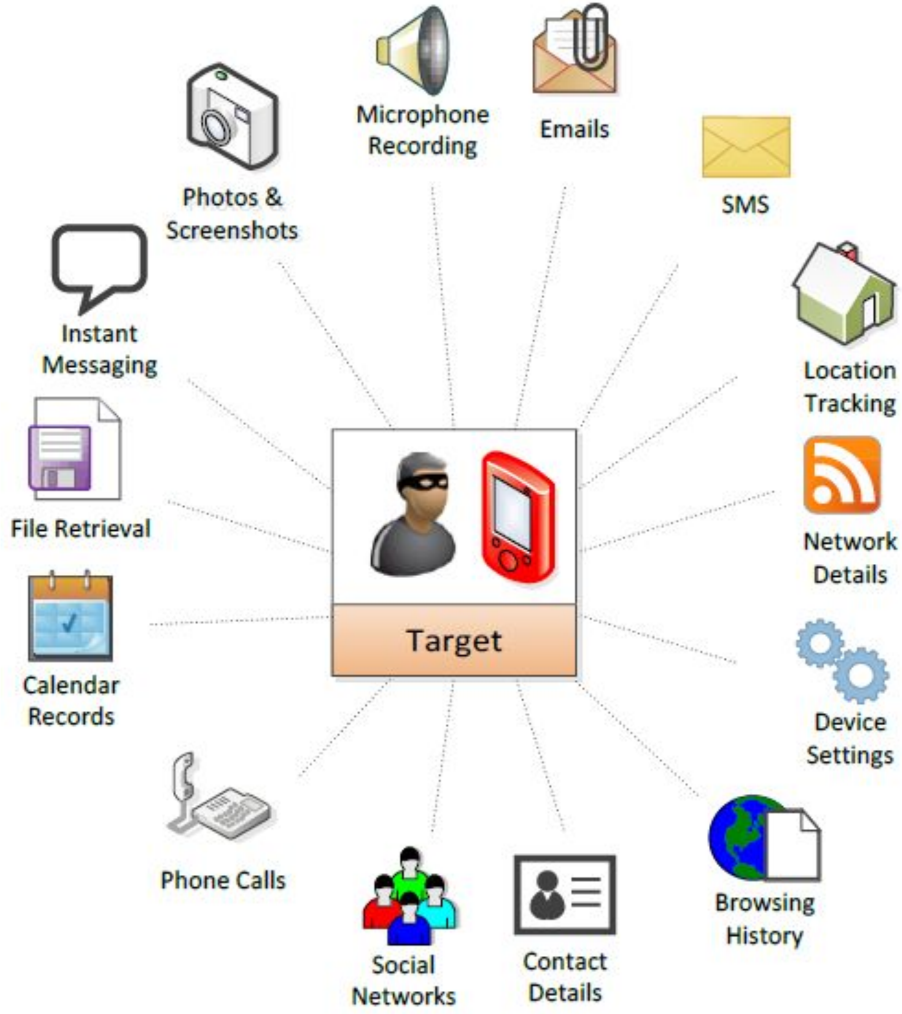
Visiting a maliciously crafted website may lead to arbitrary code execution

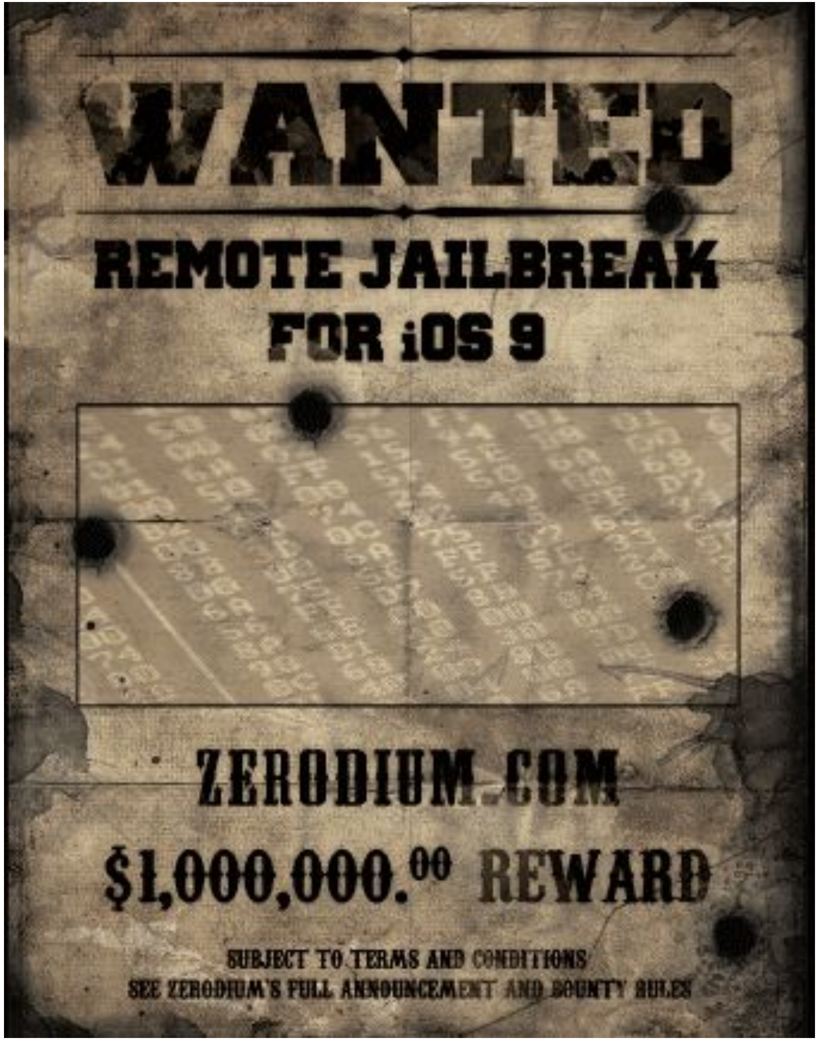
CVE-2016-4655

An application may be able to disclose kernel memory

CVE-2016-4656

An application may be able to execute arbitrary code with kernel privileges





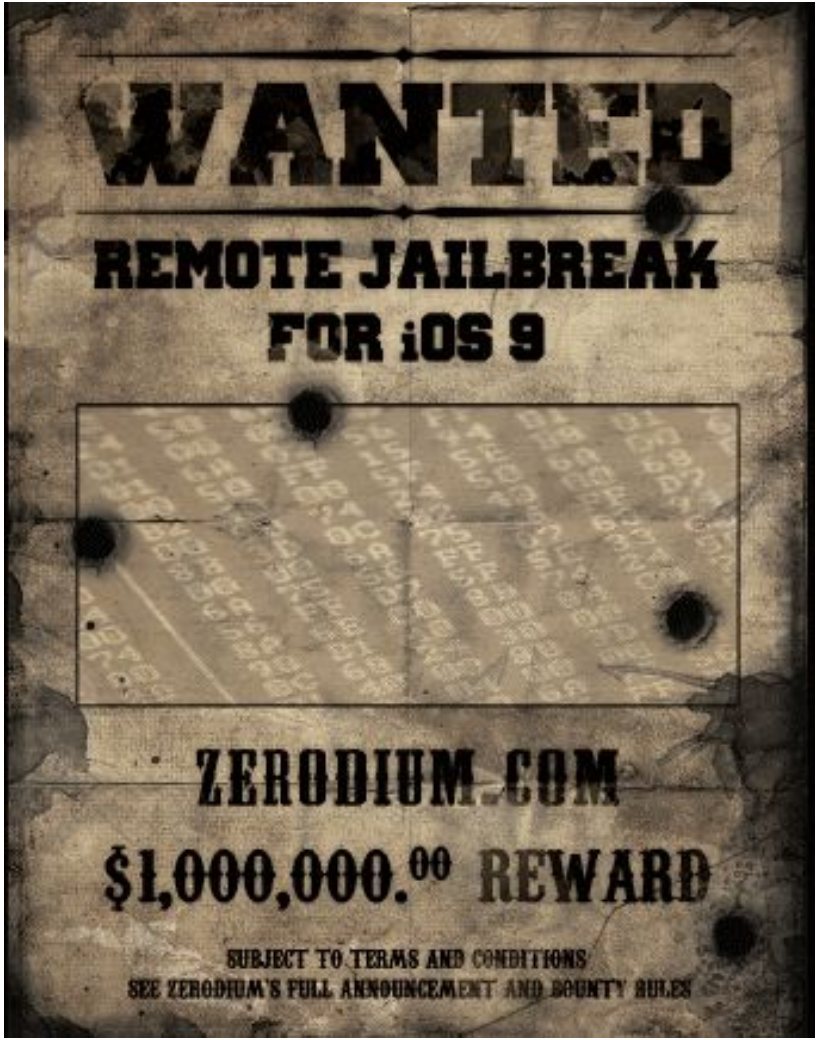
WANTED

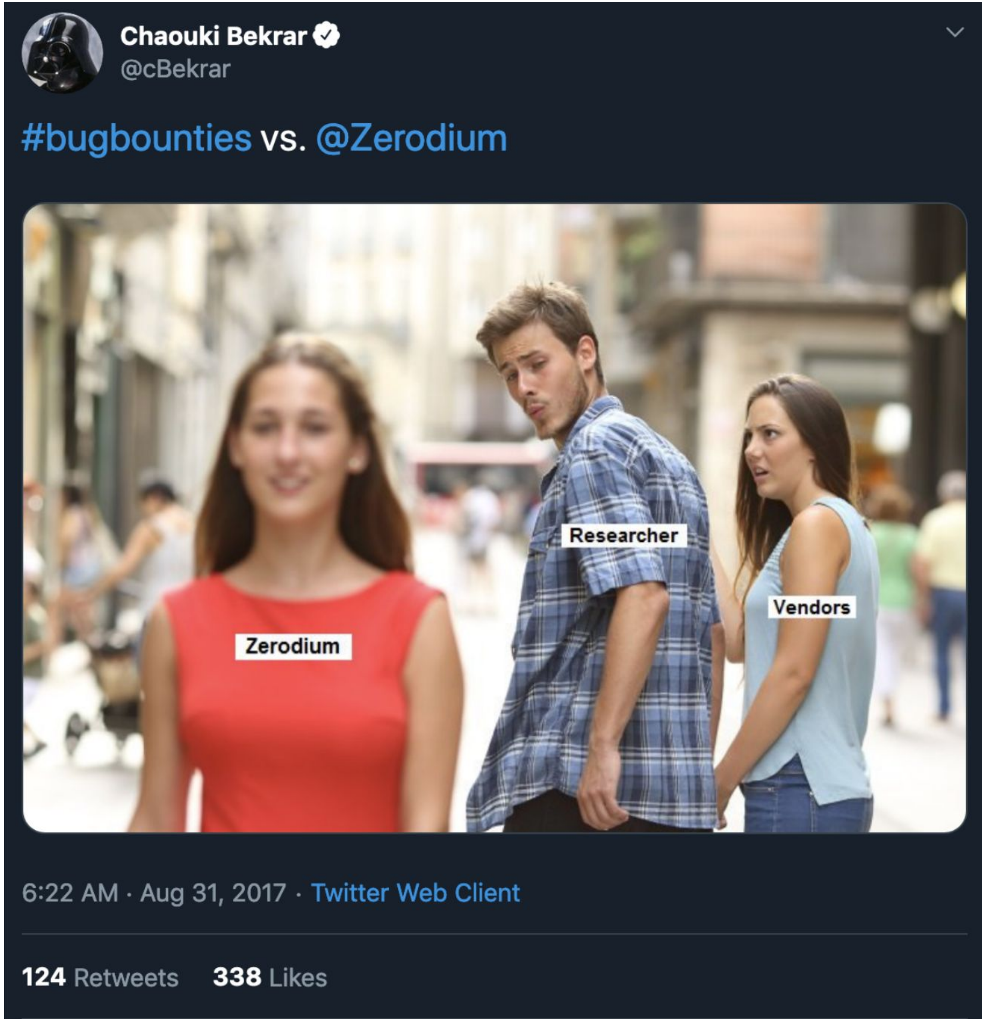
REMOTE JAILBREAK FOR iOS 9

ZERODIUM.COM

$1,000,000.00 REWARD

SUBJECT TO TERMS AND CONDITIONS
SEE ZERODIUM'S FULL ANNOUNCEMENT AND BOUNTY RULES


WANTED
REMOTE JAILBREAK
FOR iOS 9
ZERODIUM.COM
$1,000,000.00 REWARD
SUBJECT TO TERMS AND CONDITIONS
SEE ZERODIUM'S FULL ANNOUNCEMENT AND BOUNTY RULES



Chaouki Bekrar
@cBekrar

#bugbounties vs. @Zerodium

6:22 AM · Aug 31, 2017 · Twitter Web Client

124 Retweets 338 Likes

KARDASHIAN PARIS HOTEL HEIST! By MARK SEAL

CARTER

The 2016 Holiday GIFT GUIDE

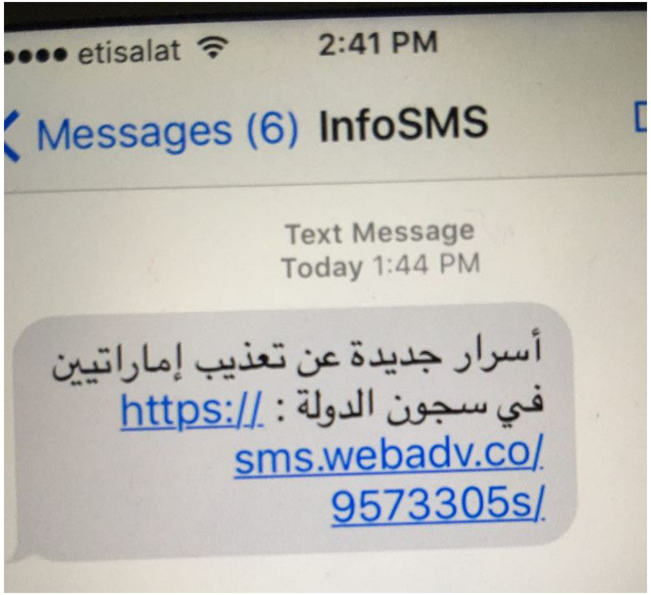
BIGGER! BETTER! NO NUTCRACKERS!

PLUS

WHO HACKED SILICON VALLEY'S CROWN JEWEL?

By BRYAN BURROUGH

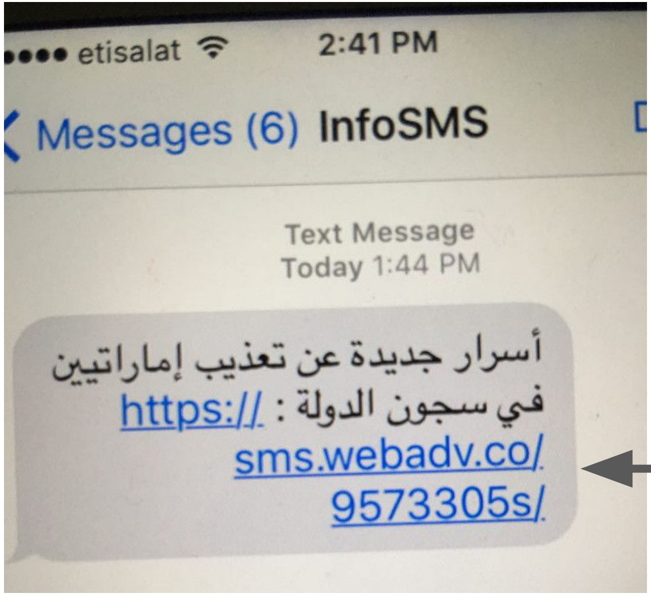
Attribution



InfoSMS

Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين في سجون الدولة : https://sms.webadv.co/9573305s/

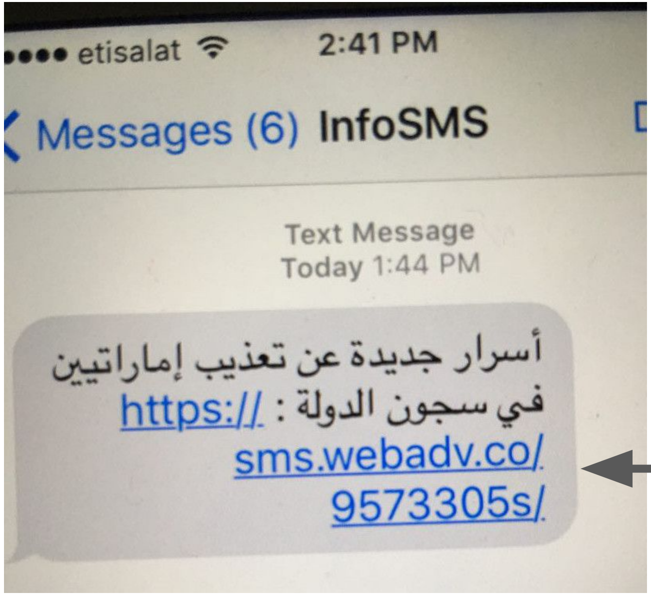


Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين في سجون الدولة : https://sms.webadv.co/9573305s/

When we clicked again, redirect to:

`https://sms.webadv.co/redirect.aspx`



etisalat 2:41 PM

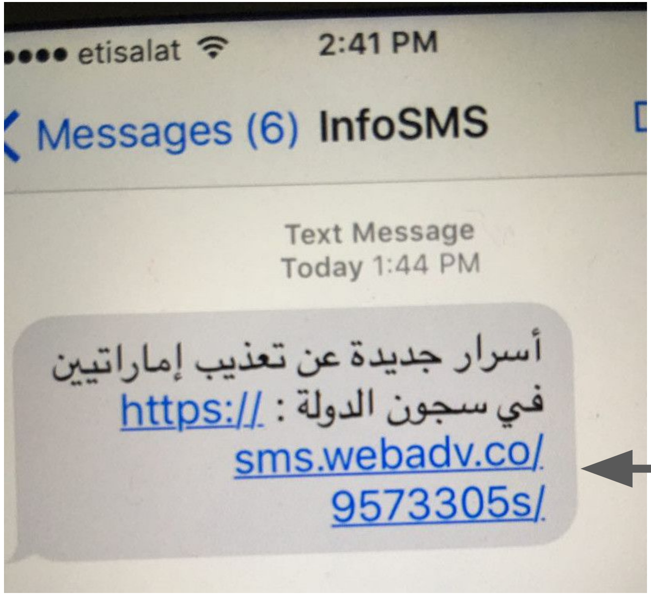
Messages (6) InfoSMS

Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
9573305s/

When we clicked again, redirect to:
`https://sms.webadv.co/redirect.aspx`

```
<html><head><meta http-equiv='refresh'
content='0;url=http://www.google.com' /><meta http-equiv='refresh'
content='1;url=http://www.google.com'
/><title></title></head><body></body></html>
```



InfoSMS

Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
9573305s/

When we clicked again, redirect to:

`https://sms.webadv.co/redirect.aspx`

```
<html><head><meta http-equiv='refresh'
content='0;url=http://www.google.com' /><meta http-equiv='refresh'
content='1;url=http://www.google.com'
/><title></title></head><body></body></html>
```

WOW, THAT'S WEIRD!

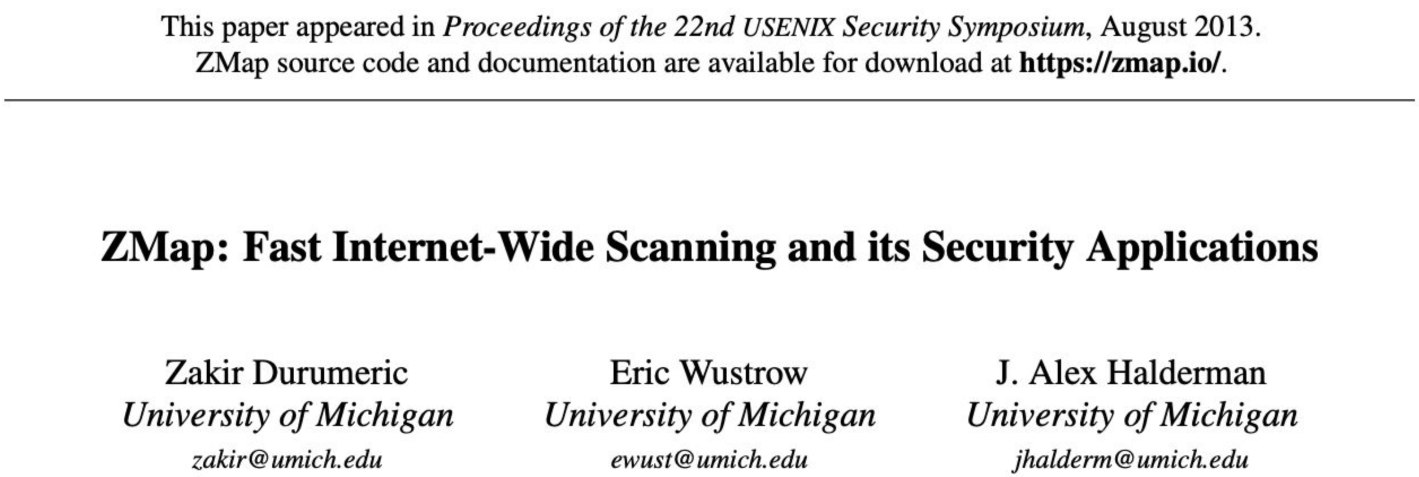
This paper appeared in *Proceedings of the 22nd USENIX Security Symposium*, August 2013.
ZMap source code and documentation are available for download at **https://zmap.io/**.

ZMap: Fast Internet-Wide Scanning and its Security Applications

Zakir Durumeric
University of Michigan
zakir@umich.edu

Eric Wustrow
University of Michigan
ewust@umich.edu

J. Alex Halderman
University of Michigan
jhalderm@umich.edu



This paper appeared in *Proceedings of the 22nd USENIX Security Symposium*, August 2013.
ZMap source code and documentation are available for download at **https://zmap.io/**.

ZMap: Fast Internet-Wide Scanning and its Security Applications

Zakir Durumeric
University of Michigan
zakir@umich.edu

Eric Wustrow
University of Michigan
ewust@umich.edu

J. Alex Halderman
University of Michigan
jhalderm@umich.edu

PLAN:

1. USE ZMAP TO FETCH /REDIRECT.ASPX FROM EVERY IPV4 ADDRESS (2^{32} = 4,294,967,296)
2. CHECK WHICH RESPONSES ARE THE SAME AS OUR FINGERPRINT:

```
<html><head><meta http-equiv='refresh'
content='0;url=http://www.google.com' /><meta http-equiv='refresh'
content='1;url=http://www.google.com'
/><title></title></head><body></body></html>
```

Result: 149 IP addresses

New plan: Look at historical internet scanning data for the 149 IP addresses

SHODAN

https://shodan.io/

Censys

https://censys.io/

RAPID7

https://opendata.rapid7.com/

RESULT: 19 IP ADDRESSES RETURNED IN RESPONSE TO A FETCH FOR /

```
\xef\xbb\xbf<HTML><HEAD><META HTTP-EQUIV="refresh"
CONTENT="0;URL=http://www.google.com/">
<TITLE></TITLE></HEAD><BODY>
</BODY></HTML>
```

RESULT: 19 IP ADDRESSES RETURNED IN RESPONSE TO A FETCH FOR /

```
\xef\xbb\xbf<HTML><HEAD><META HTTP-EQUIV="refresh"
CONTENT="0;URL=http://www.google.com/">
<TITLE></TITLE></HEAD><BODY>
</BODY></HTML>
```

NEW PLAN: WHAT ELSE RETURNED THIS?

RESULT: 19 IP ADDRESSES RETURNED IN RESPONSE TO A FETCH FOR /

```
\xef\xbb\xbf<HTML><HEAD><META HTTP-EQUIV="refresh"
CONTENT="0;URL=http://www.google.com/">
<TITLE></TITLE></HEAD><BODY>
</BODY></HTML>
```

NEW PLAN: WHAT ELSE RETURNED THIS?

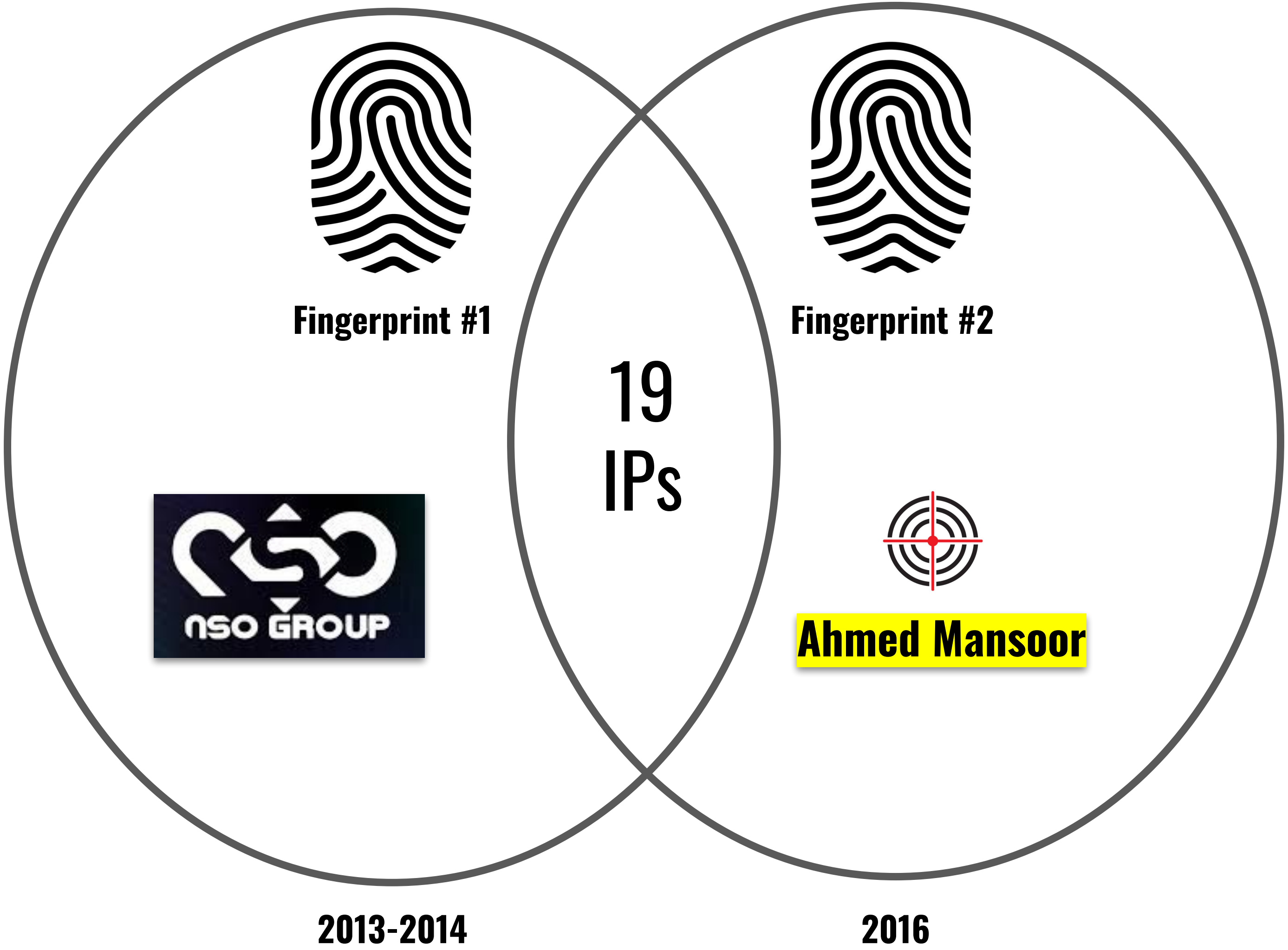
RESULT: 89 IP ADDRESSES INCLUDING:

```
Admin Organization: Nso Group
Admin Street: P.O Box 4166
Admin City: Hertzelia
Admin Country: IL
Admin Email: IT@nsogroup.com
```

"NSO Group is a leader in the field of Cyber warfare."

"… a powerful and unique monitoring tool, called **Pegasus**, which allows remote and stealth monitoring and full data extraction from remote targets devices via untraceable commands."

"…exclusively for the use of Government, Law Enforcement and Intelligence Agencies."



Fingerprint #1

Fingerprint #2

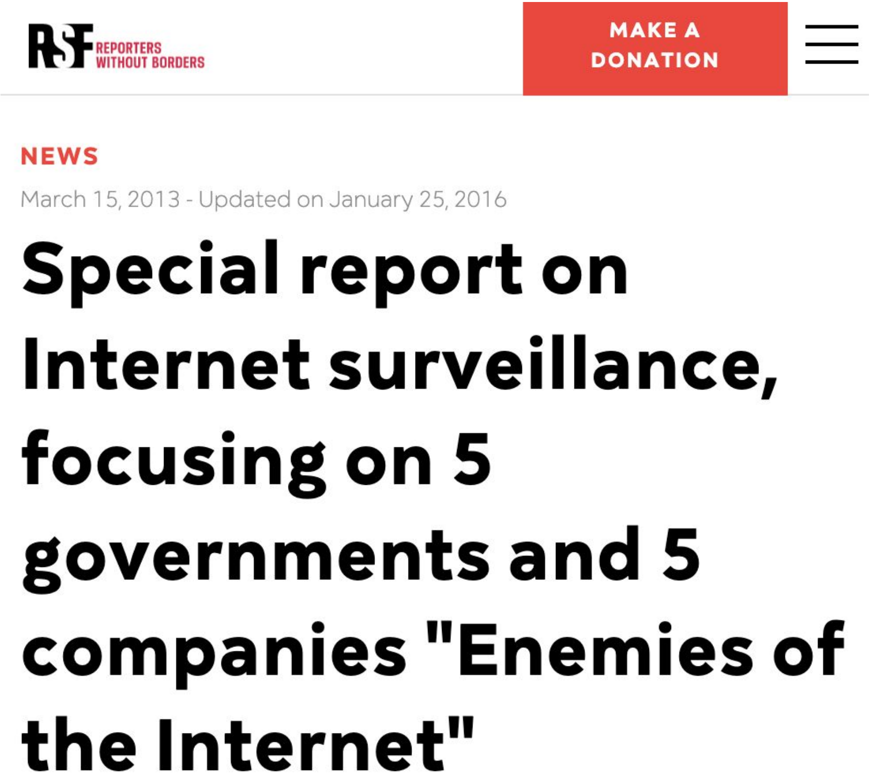
19 IPs

NSO GROUP

Ahmed Mansoor

2013-2014

2016



RSF REPORTERS WITHOUT BORDERS

MAKE A DONATION

NEWS

March 15, 2013 - Updated on January 25, 2016

Special report on Internet surveillance, focusing on 5 governments and 5 companies "Enemies of the Internet"

Why do NSO servers return Google redirects?

```
<html><head><meta http-equiv='refresh'
content='0;url=http://www.google.com' /><meta http-equiv='refresh'
content='1;url=http://www.google.com'
/><title></title></head><body></body></html>
```

```
\xef\xbb\xbf<HTML><HEAD><META HTTP-EQUIV="refresh"
CONTENT="0;URL=http://www.google.com/">
<TITLE></TITLE></HEAD><BODY>
</BODY></HTML>
```

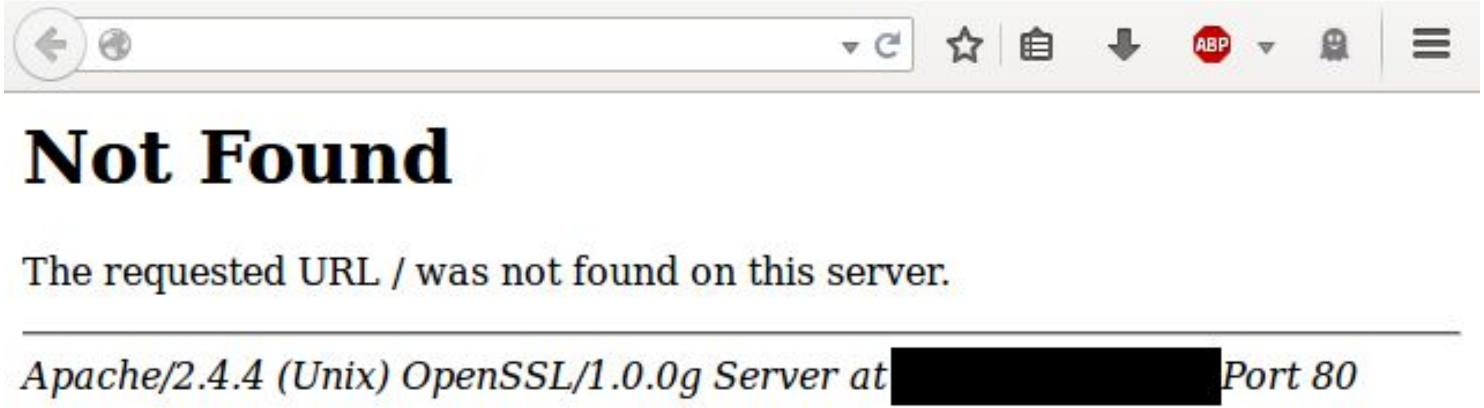
Why do NSO servers return Google redirects?

```
<html><head><meta http-equiv='refresh'
content='0;url=http://www.google.com' /><meta http-equiv='refresh'
content='1;url=http://www.google.com'
/><title></title></head><body></body></html>
```

```
\xef\xbb\xbf<HTML><HEAD><META HTTP-EQUIV="refresh"
CONTENT="0;URL=http://www.google.com/">
<TITLE></TITLE></HEAD><BODY>
</BODY></HTML>
```

DECOY PAGE: "REDIRECT OR CUSTOMIZE UNDESIRED REMOTE ... LANDING ON THE SERVER"

Fake Apache Decoy Pages (Hacking Team)

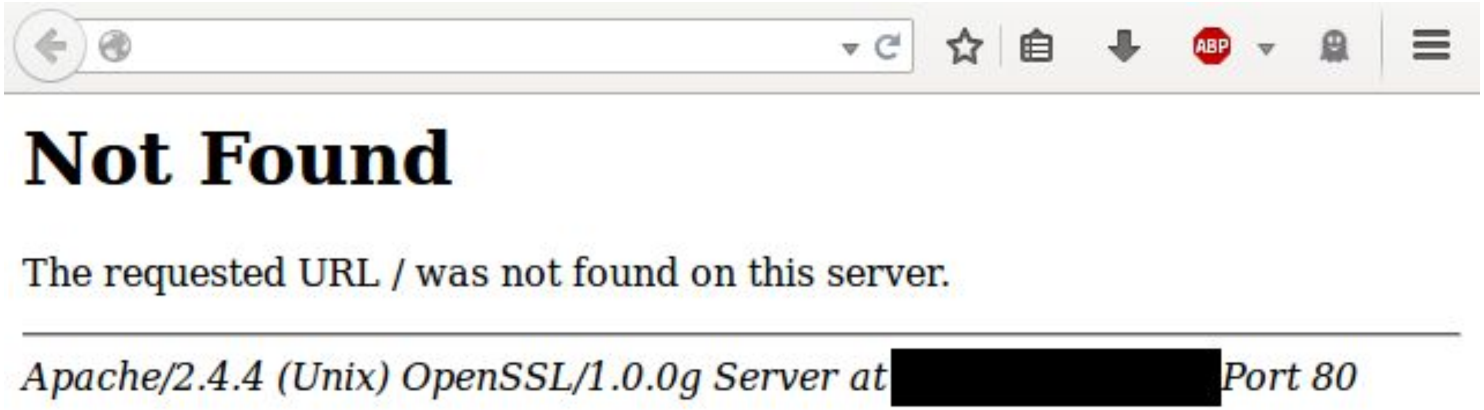


Not Found

The requested URL / was not found on this server.

Apache/2.4.4 (Unix) OpenSSL/1.0.0g Server at [redacted] Port 80

Fake Apache Decoy Pages (Hacking Team)



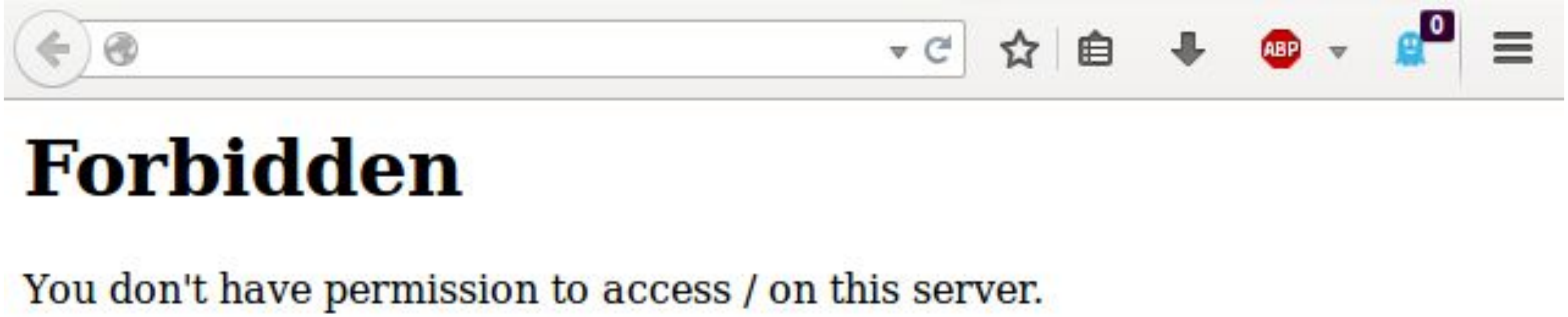
Not Found

The requested URL / was not found on this server.

Apache/2.4.4 (Unix) OpenSSL/1.0.0g Server at [redacted] *Port 80*

Apache	Hacking Team
HTTP/1.1 404 Not Found **Date: $DATE** Server: $SERVER Content-Length: $LENGTH Connection:close Content-Type: text/html**; charset=$CHARSET**	HTTP/1.1 404 **NotFound** **Connection: close** **Content-Type: text/html** **Content-length: $LENGTH** **Server: Apache/2.4.4 (Unix) OpenSSL/1.0.0g**

Fake Apache Decoy Pages (FinFisher)

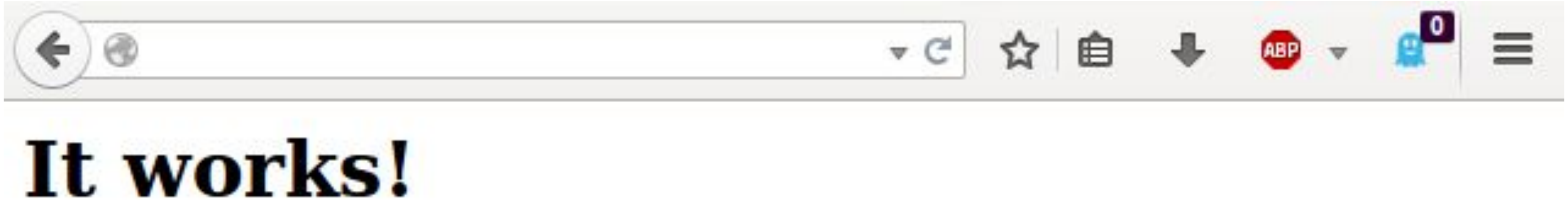


Forbidden

You don't have permission to access / on this server.

Apache	FinFisher
HTTP/1.1 403 Forbidden Date: $DATE GMT Server: Apache Vary: Accept-Encoding Content-Length: 321 Content-Type: text/html; charset=iso-8859-1	HTTP/1.1 403 Forbidden Date: $DATE **UTC** Server: Apache Vary: Accept-Encoding Content-Length: 321 Content-Type: text/html; charset=iso-8859-1

Fake Apache Decoy Pages (FinFisher)



It works!

Apache	FinFisher
<html><body><h1>It works!</h1></body></html>	**<!DOCTYPE HTML PUBLIC ``-//IETF//DTD HTML 2.0//EN''>** <html>**<head>** **<title>200 OK</title>** **</head>**<body> <h1>It works!</h1> </body></html>

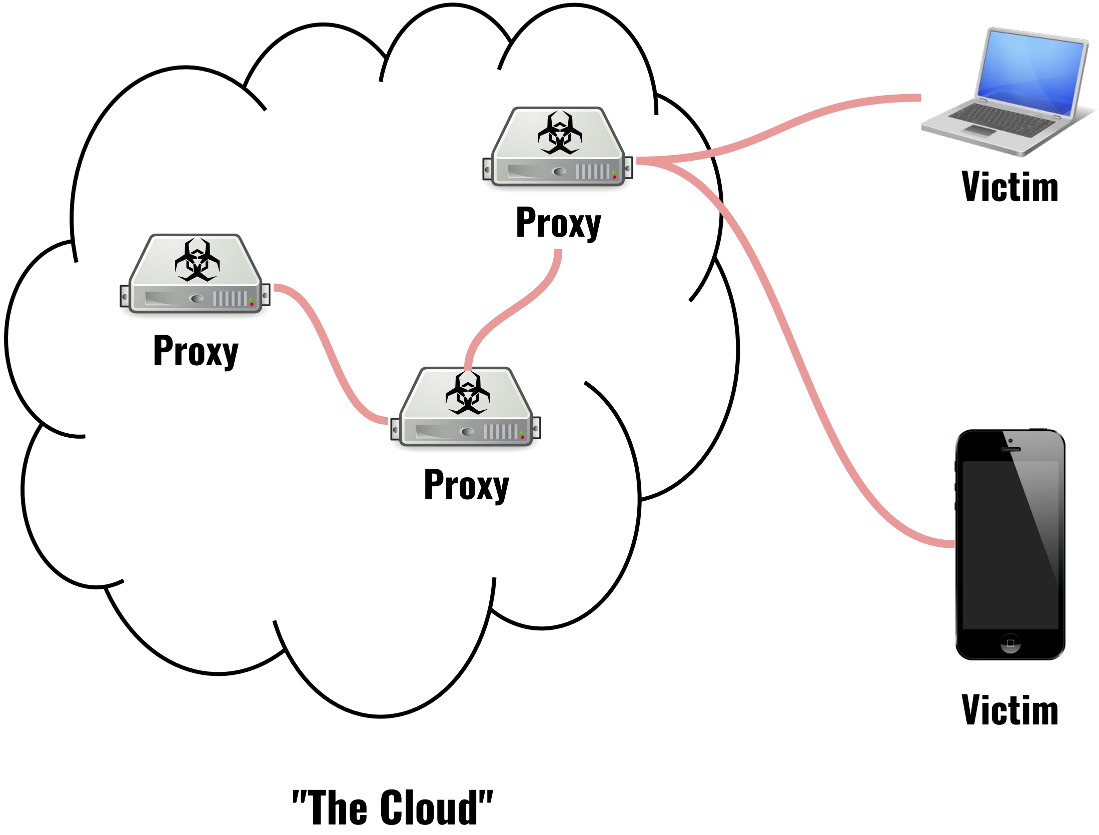
Spyware Command-and-Control

Command and Control

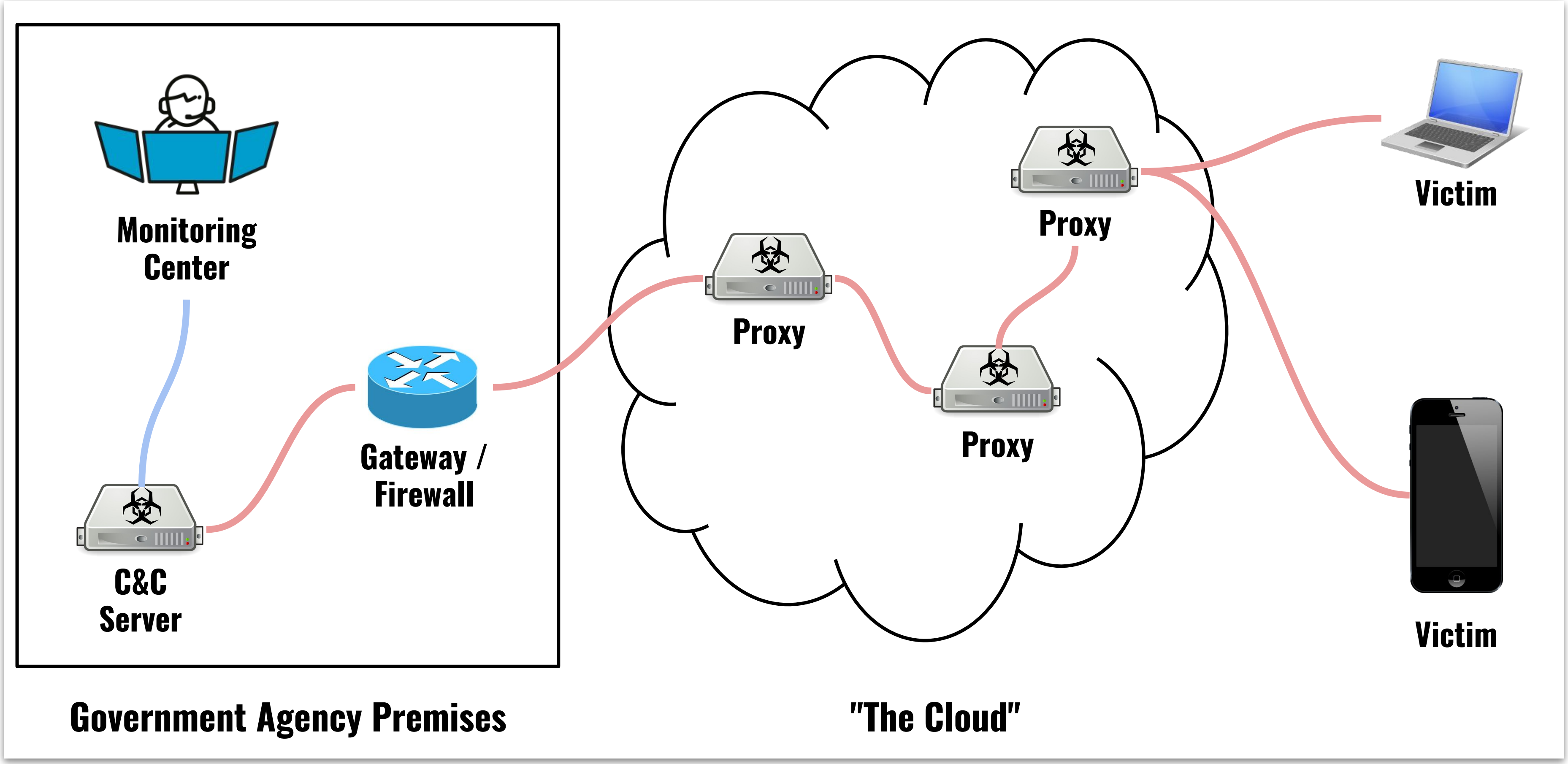
Victim

Victim

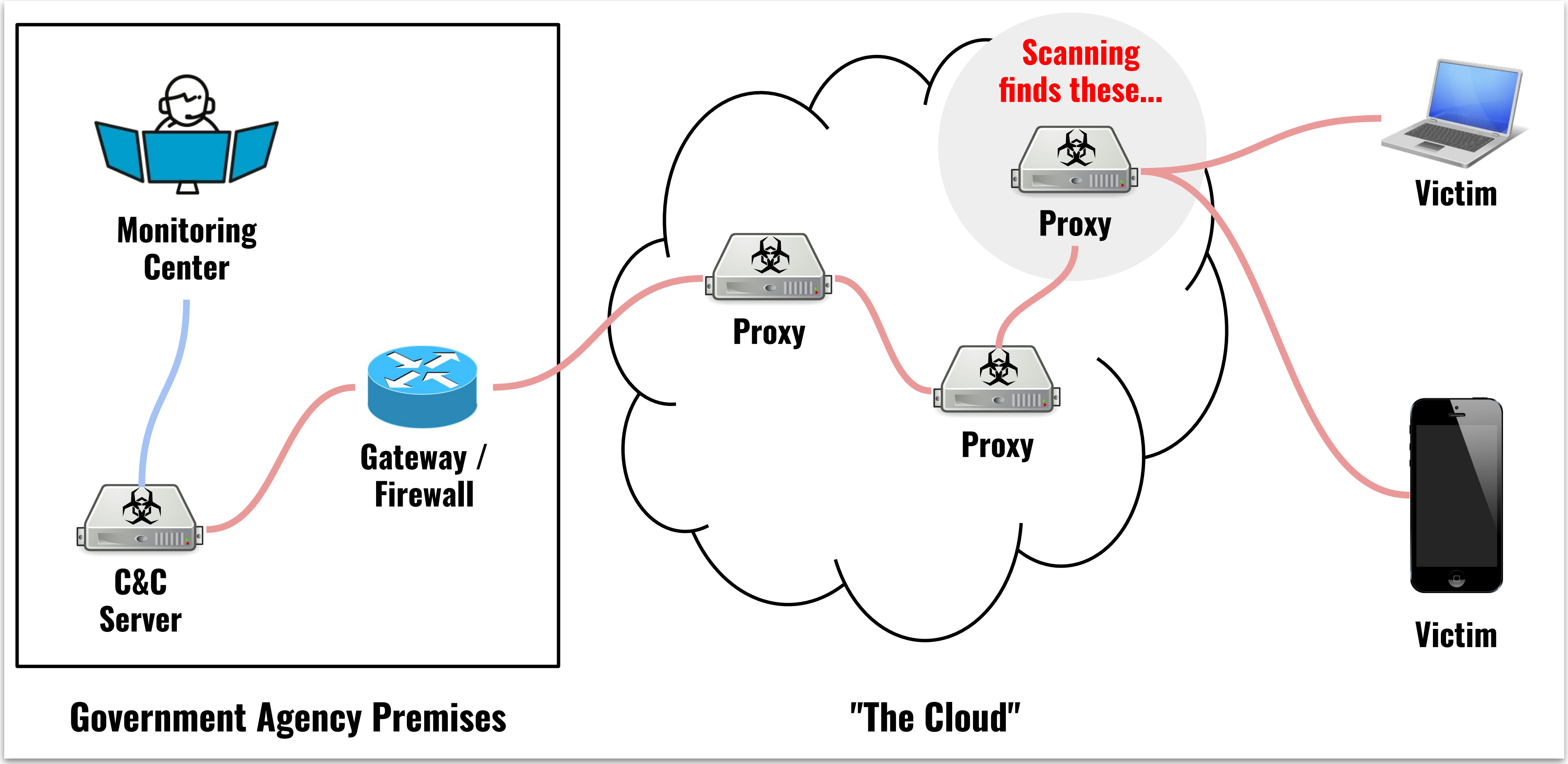
Command and Control



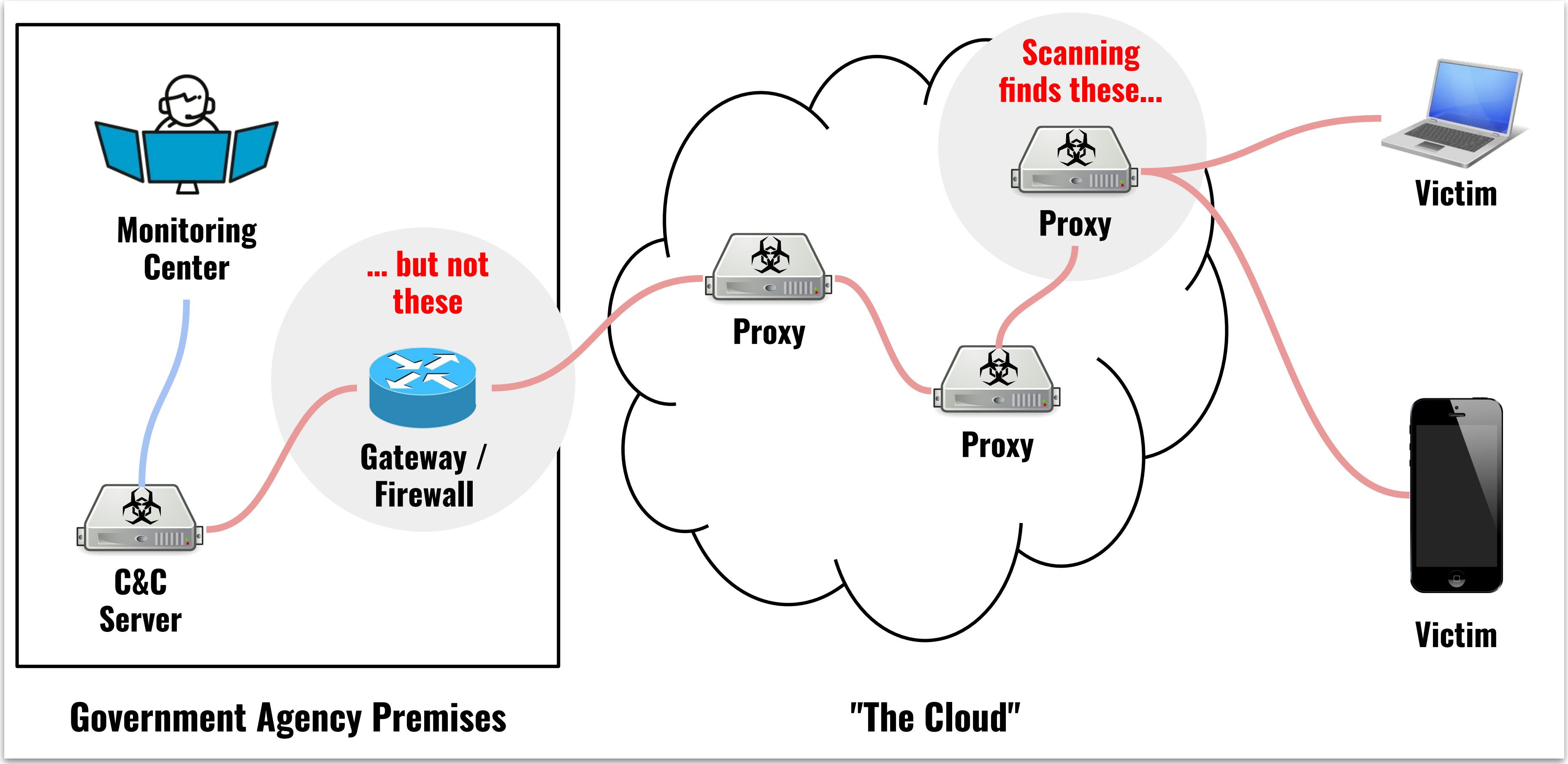
Command and Control



Command and Control



Command and Control



Monitoring Center
... but not these
Gateway / Firewall
C&C Server
Government Agency Premises
Scanning finds these...
Proxy
Proxy
Proxy
"The Cloud"
Victim
Victim