Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents

May 29, 2016

Categories: Bill Marczak, John Scott-Railton, Reports and Briefings, Research News

Media Coverage: New York Times, Foreign Policy, International Business Times, Chicago Tribune, VICE Motherboard, Taipei Times, Forbes, Techworm, Sputnik News, Network World, BoingBoing.

Authors: Bill Marczak, John Scott-Railton

1. Executive Summary

This report describes a campaign of targeted spyware attacks carried out by a sophisticated operator, which we call **Stealth Falcon**. The attacks have been conducted from 2012 until the present, against Emirati journalists, activists, and dissidents. We discovered this campaign when an individual purporting to be from an apparently fictitious organization called "The Right to Fight" contacted Rori Donaghy. Donaghy, a UK-based journalist and founder of the Emirates Center for Human Rights, received a spyware-laden email in November 2015, purporting to offer him a position on a human rights panel. Donaghy has written critically of the United Arab Emirates (UAE) government in the past,[1] and had recently published a series of articles based on leaked emails involving members of the UAE government.[2]

Circumstantial evidence suggests a link between Stealth Falcon and the UAE government. We traced digital artifacts used in this campaign to links sent from an activist's Twitter account in December 2012, a period when it appears to have been under government control. We also identified other bait content employed by this threat actor. We found 31 public tweets sent by Stealth Falcon, 30 of which were directly targeted at one of 27 victims. Of the 27 targets, 24 were obviously linked to the UAE, based on their profile information (e.g., photos, "UAE" in account name, location), and at least six targets appeared to be operated by people who were arrested, sought for arrest, or convicted in absentia by the UAE government, in relation to their Twitter activity.

The attack on Donaghy — and the Twitter attacks — involved a malicious URL shortening site. When a user clicks on a URL shortened by Stealth Falcon operators, the site profiles the software on a user's computer, perhaps for future exploitation, before redirecting the user to a benign website containing bait content. We queried the URL shortener with every possible short URL, and identified 402 instances of bait content which we believe were sent by Stealth Falcon, 73% of which obviously referenced UAE issues. Of these URLs, only the one sent to Donaghy definitively contained spyware. However, we were able to trace the spyware Donaghy received to a network of 67 active command and control (C2) servers, suggesting broader use of the spyware, perhaps by the same or other operators.

Figure 1: Tag cloud of bait content topics used by Stealth Falcon showing a strong emphasis on political topics and narratives critical of the UAE government

2. Background

Rori Donaghy[3] is a London-based journalist who currently works for UK news organization *Middle East Eye*, a website that covers news in the Middle East.[4] *Middle East Eye* has recently published a series of articles about UAE foreign policy, based on leaked emails involving members of the UAE government. Previously, Donaghy led the Emirates Center for Human Rights,[5] an organization he founded to *"promote the defence of human rights in the United Arab Emirates … through building strong relationships with the media, parliaments and other relevant organisations outside the UAE"*.[6]

2.1. Political and Human Rights Situation in the UAE

In its most recent (2015) Freedom in the World ranking, Freedom House classified the UAE as *"not free,"* and noted that the UAE continues to *"suppress dissent"*.[7] Human Rights Watch stated in its most recent (2016) country report, that the UAE has *"continued … to arbitrarily detain and in some cases forcibly disappear individuals who criticized the authorities"*.[8] Amnesty International says that UAE courts have *"accepted evidence allegedly obtained through torture"*.[9]

Specifically in the online realm, there is evidence that the UAE government has previously conducted malware attacks against civil society. At least three dissidents[10] including a journalist, and UAE human rights activist Ahmed Mansoor, were targeted in 2012 with Hacking Team spyware[11] by a Hacking Team customer in the UAE, apparently operating under the auspices of the office of Sheikh Tahnoon bin Zayed al-Nahyan,[12] a son of the founder of the UAE, and now the UAE Deputy National Security Advisor.[13] The UAE client had a license from Hacking Team to concurrently infect and monitor 1100 devices.[14]

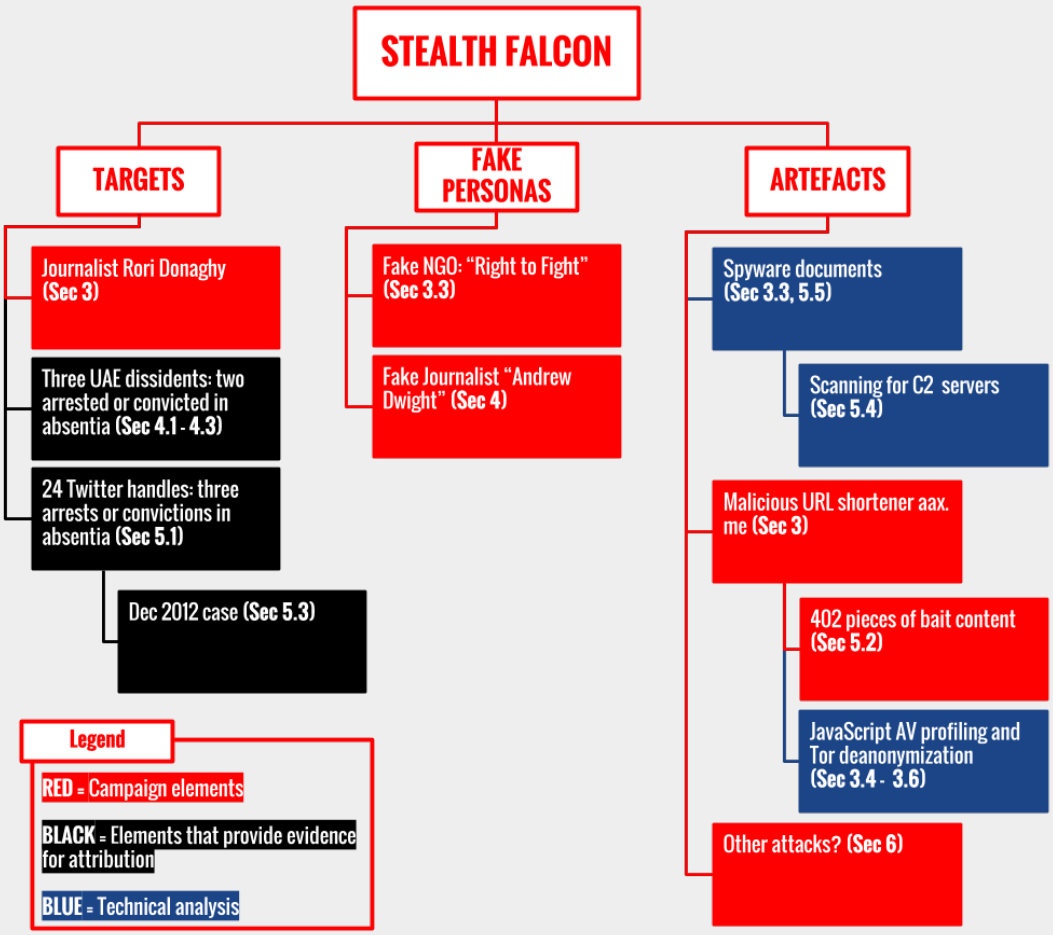

Figure 2: Diagram of Stealth Falcon's known Targets, Fake Personas, and campaign Artefacts, along with relevant sections of the report. The document paints a picture of a large-scale campaign with a focus on critics of the UAE Government

3. The November 2015 Attack: An "Invitation"

This section describes an email attack against journalist Rori Donaghy. The operators used a Microsoft Word macro that installs a custom backdoor allowing operators to execute arbitrary commands on a compromised machine.

3.1 Initial Attack Email

In November 2015, the journalist Donaghy received the following email message, purportedly offering him a position on a panel of human rights experts:

> **From**: the_right_to_fight@openmailbox.org
> **Subject**: Current Situation of Human Rights in the Middle East
>
> Mr. Donaghy,
>
> We are currently organizing a panel of experts on Human Rights in the Middle East.
>
> We would like to formally invite you to apply to be a member of the panel by responding to this email.
>
> You should include your thoughts and opinions in response to the following article about what more David Cameron can be doing to help aid the Middle East.
>
> **http://aax.me/d0dde**
> Thank you.
>
> We look forward to hearing back from you,
>
> Human Rights: The Right to Fight

Donaghy was suspicious of the email, and forwarded it to us for analysis. We found that the link in the email (**http://aax.me/d0dde**) loaded a page containing a redirect to the website of *Al Jazeera*. Before completing the redirect, it invoked JavaScript to profile the target's computer. We describe the profiling in detail in **Section 3.1-3.3** below.

3.2 Communication with the Operator

On our instruction, Donaghy responded to the email, asking for further information. The operators responded with the following message:

> **From**: the_right_to_fight@openmailbox.org
> **Subject**: RE: Current Situation of Human Rights in the Middle East
>
> Mr. Donaghy,
>
> Thank you for getting back to us. We are very interested in you joining our panel.
>
> The information you requested is in the attached document.
>
> In order to protect the content of the attachment we had to add macro enabled security.
>
> Please enable macros in order to read the provided information about our organization.
>
> We hope you will consider joining us.
> Thank you.
>
> We look forward to hearing back from you,
>
> Human Rights: The Right to Fight

By chance, the attachment was identified as malicious and blocked by a program running in Donaghy's email account. We instructed him to follow up and request that the operators forward the attachment via another method. Donaghy received the following reply:

> **From**: the_right_to_fight@openmailbox.org
> **Subject**: RE: Current Situation of Human Rights in the Middle East
>
> Mr. Donaghy,
>
> We apologize for having problems with our attachment.
>
> Please follow this link to download our organizational information.
>
> **http://aax.me/a6faa**
>
> The link has been password protected. The password is: right2fight
>
> In order to protect the content of the attachment we also had to add macro enabled security.
>
> Please enable macros in order to read the provided information about our organization.
>
> We hope you will consider joining us.
> Thank you.
>
> We look forward to hearing back from you,
>
> Human Rights: The Right to Fight

This second link (**http://aax.me/a6faa)** redirects to the following URL using an HTTP 302 redirect:

> **https://cloud.openmailbox.org/index.php/s/ujDNWMmg8pdG3AL/authenticate**

This is a password-protected link to a file shared on an ownCloud[15] instance. We obtained this file, and found it to be a Microsoft Word document.

3.3 The Malicious Document

The document is:

```
Filename:   right2fight.docm
MD5:        80e8ef78b9e28015cde4205aaa65da97
SHA1:       f25466e4820404c817eaf75818b7177891735886
SHA256:     5a372b45285fe6f3df3ba277ee2de55d4a30fc8ef05de729cf464103632db40f
```

When opened, the target is greeted with the following image, purporting to be a message from "proofpoint," a legitimate provider of security solutions for Office 365.[16] The image claims that *"This Document Is Secured"* and requests that the user *"Please enable macros to continue."*

Figure 3: Fake Proofpoint image in the malicious document sent to Donaghy

If the target enables macros, they are presented with the following document:

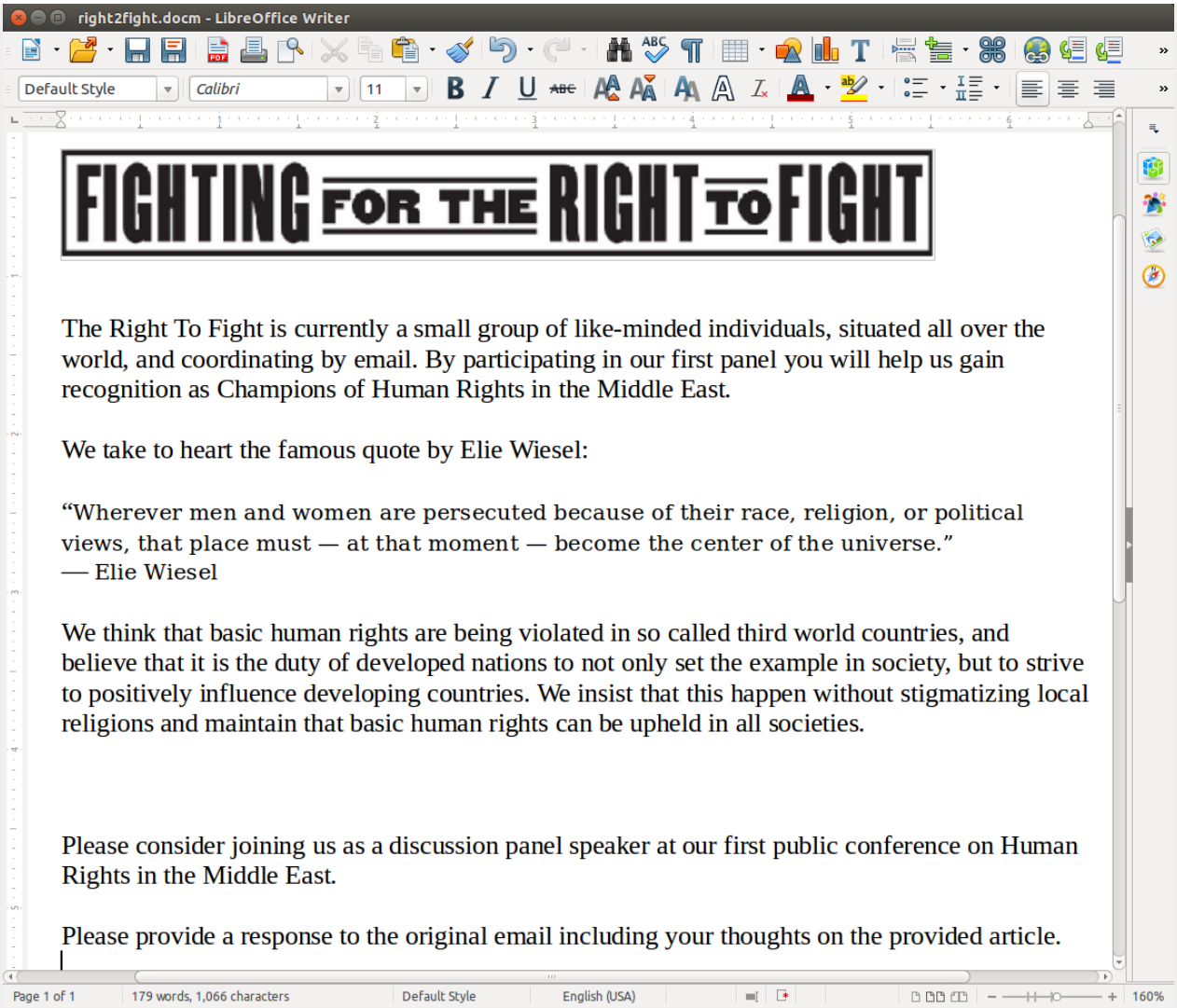

Figure 4: Document that Donaghy would have seen, had he enabled macros

The document purports to be from an organization called “The Right To Fight,” and asks the target Donaghy to open the link in the original email he received (the email containing the profiling URL). We believe that “The Right To Fight” is a fictitious organization, as their logo appears to be copied from an exhibition about *“African American Experiences in WWII”*.[17] Further, “The Right to Fight” has no discernable web presence.

Figure 5: Logo from exhibition about African American experiences in WWII.

3.3.1 Profiling

The document attempts to execute code on the recipient’s computer, using a macro. The macro passes a Base64-encoded command to Windows PowerShell, which gathers system information via Windows Management Instrumentation (WMI), and attempts to determine the installed version of .NET by querying the registry (full script available in **Appendix A: Stage One PowerShell Command**).

3.3.2 Communication & Obtaining a Shell

Gathered information is returned to **http://adhostingcache.com/ehhe/eh4g4/adcache.txt**, and the server’s response is executed as a PowerShell command. At the time, **adhostingcache.com** resolved to **95.215.44.37**. The domain was apparently deleted on November 30th 2015 (Donaghy received the malicious Word Document on November 24th 2015). A new domain, **adhostingcaches.com**, was registered on December 3rd, which points to the same IP address. The deletion of **adhostingcache.com** may reflect operator suspicion that the file received by Donaghy had been sent to security researchers.

The server response is a PowerShell command that decodes and materializes an invocation of a Base64-encoded PowerShell command to disk as **IEWebCache.vbs**, and creates a scheduled task entitled *"IE Web Cache"* that executes the file hourly (full script available in **Appendix B: Stage Two PowerShell Command**).

IEWebCache.vbs runs a Base64-encoded PowerShell command, which periodically POSTs a unique identifier to **https://incapsulawebcache.com/cache/cache.nfo** (via HTTPS without verifying the server certificate, and with a hardcoded user-agent header matching Internet Explorer 10.6). The script executes server responses as PowerShell commands, responding back to the server with the exit status of, output of, or any exceptions generated by the commands.

This gives the operator control over the victim's computer, and allows the operator to install additional spyware or perform other activities. All commands and responses are encrypted using RC4 with a hardcoded key, and the encrypted message is prefixed with a hardcoded value.

Despite some similarities in functionality to the Empire backdoor,[18] we were unable to identify any shared code, and we suspect that the backdoor is custom-made.

3.4. Technical Analysis: aax.me Browser Profiling

While aax.me has a public interface where anyone may shorten a link, aax.me only conducts browser profiling of individuals who click on links that are specially shortened by Stealth Falcon operators.

In November 2015, when we accessed the link in the second email that Donaghy received, **http://aax.me/a6faa**, we found that it redirected directly to **https://cloud.openmailbox.org/index.php/s/ujDNWMmg8pdG3AL/authenticate** via an HTTP 302 redirect. When we accessed the link in the first email that Donaghy received, **http://aax.me/d0dde**, the server responded with the following page:

```
<iframe src='redirect.php' height='1' width='1' border='0' scrolling='no' frameborder='0'
unselectable='yes' marginheight='0' marginwidth='0' onload='setTimeout("document.location
=\"http://www.aljazeera.com/indepth/opinion/2015/11/british-pm-middle-east-human-rights-
151103070038237.html\"", 20000)'></iframe><br><br><br><center><img src='loading.gif'><br>Loading the
website:<br><b>http://www.aljazeera.com/indepth/opinion/2015/11/british-pm-middle-east-human-rights-
151103070038237.html</b>.<br>This may take a few seconds.</center>
```

The page is apparently designed to redirect to an *Al Jazeera* op-ed after twenty seconds.[19] However, the URL is incorrect: the last character of the filename should be a "1" instead of a "7". Therefore, an *Al Jazeera* 404 page is returned instead of the op-ed. It is possible that the use of "7" instead of "1" represents a transcription error on the part of the operators. When we accessed this same **aax.me** URL in March 2016, it redirected directly to the *Al Jazeera* URL (with typo) via an HTTP 302 redirect.

The iframe, **http://aax.me/redirect.php**, reloads itself with a parameter "inFr" in its query string, to indicate whether the page has been opened up inside a frame.

```
<html><body><script type="text/javascript">if(window!=window.top)
{inFr="1"}else{inFr="0"}document.location=document.location+"?inFr="+inFr;</script><noscript><img
src="?jSc=0"/></noscript></body></html>
```

If the page has not been opened up inside a frame (inFr=0), then a blank page is returned. If the page is opened inside a frame (inFr=1), as is the case here, then the following page is returned (we ommitted the PHPSESSID value):

```
<html><head></head><body><div id='display' height='1' style='display:none;'></div><form
id='statsPost' action='?stats=1' method='POST'><input type="hidden" name="PHPSESSID" value="" />
<input id='theData' name='theData' type='hidden' value='' /></form><script type='text/javascript'
src='redirect.js'></script></body></html>
```

We examined the referenced JavaScript file, **http://aax.me/redirect.js**. The file is designed to profile a user's system, perhaps to gather intelligence about potentially exploitable vulnerabilities. The file has apparently not been updated since 7 May 2013,[20] rendering some of the probing obsolete. We enclose the file's full contents in **Appendix C: JavaScript Profiling File**. The profiling performs the following actions:

- For Internet Explorer, it attempts to create several instances of ActiveXObject to get the versions of Flash, Shockwave, Java, RealPlayer, Windows Media Player, and Microsoft Office (classified as either *2003*, *2007*, or *2010*).
- For non-Internet Explorer browsers, it attempts to get a list of enabled plugins from navigator.mimeTypes.

- For all browsers, it captures the user agent, whether cookies are enabled, the OS, the size of the browser window, and the timezone. It classifies browsers into different versions, denoted by letters, based on the existence and behavior of certain JavaScript methods.
- The script attempts to exploit an information leak in older versions of Tor Browser. We explore the technique used in **Section 3.5**.
- For Windows browsers (except Opera, and versions of Internet Explorer before IE9), it sends a series of XMLHttpRequests to 127.0.0.1, which we believe are designed to deduce if the computer is running any one of several specific antivirus programs. The code for this appears to be borrowed from the **JS-Recon** port scanning tool.[21] The creator of JS-Recon presented the tool at BlackHat Abu Dhabi in 2010.[22] We explore such techniques in more detail in **Section 3.6**.

We were unfamiliar with the website **aax.me**, so we investigated it further. We found that the main page of **aax.me** purported to be a public URL shortening service, powered by YOURLS,[23] an open source PHP framework allowing anyone to set up their own URL shortening service. We are unable to ascertain whether the site actually uses any YOURLS code. We also noted that the homepage contains a typo ("Shortend [sic] URL").

Figure 6: Homepage of aax.me

We shortened a URL using the homepage, but found that clicking on the shortened URL did not trigger the loading of the intermediate page, **http://aax.me/redirect.php**. We also did not find the code for **redirect.php** or **redirect.js** in the public code repository for YOURLS.[24] Thus, we deduced that this code was likely specially written by the operators, and the link sent to Donaghy was likely created by someone with administrator access to **aax.me**.

3.5. Technical Analysis: aax.me Tor Deanonymization Attempt

The aax.me site appears to attempt to deanonymize users of Tor Browser. While the technique the operators used was out-of-date at the time we observed the attack, the attempted Tor deanonymization speaks to their motivations and potential targets.

The script first detects Tor Browsers by checking whether **navigator.buildID** is set to zero (all testing was conducted on English, Windows builds of Tor Browser). Versions of Tor Browser before 2.3.25-12 (released on 13 August 2013) had their buildID set to zero. This behavior was originally introduced in TorButton,[25] in support of the goal of making Tor users appear homogenous.[26] Current Tor Browser versions have navigator.buildID set to a different distinctive value, 20000101000000.

When the script detects a Tor Browser, it attempts to deduce the version of Tor Browser by checking for the existence and behavior of certain JavaScript methods. Once a browser is determined to be *older* than a certain version of Tor Browser, the script exploits a now-fixed bug to get the disk path of the browser installation.[27] The disk path may contain the target's username, which may include the target's real name.

The bug in Tor Browser was first disclosed at Defcon 17, which took place in August 2009.[28] The bug was first fixed on on 25 May 2012 in Tor Browser release 2.2.35-13.[29] The bug was, however, later reintroduced into Tor Browser on 18 December 2013 with the release of Tor Browser 3.5, and subsequently fixed again in Tor Browser 3.6 on 29 April 2014.[30] However, unfortunately for the operators, they failed to update their profiling script to reflect Tor Browser's **navigator.buildID** change (before the bug was reintroduced). Thus, the profiling script did not detect Tor Browsers with the reintroduced bug as Tor Browsers, so it did not try to exploit them. Even if it had been updated to reflect the navigator.buildID change, the version check in the Tor Browser exploitation code would also have to be updated to select the versions with the reintroduced bug for exploitation.

The version of Tor Browser (as determined by JavaScript checks) is submitted back to the server, along with the value of *navigator.oscpu* ~~(which reveals the version of the OS on which Tor Browser is running — e.g., the latest version of Tor Browser on OSX El Capitan reveals: *"Intel Mac OS X 10.11"*)~~ which is set to "Windows NT 6.1" in the latest Tor browser, *navigator.vendor* (which appears blank in the latest Tor Browser), and any data gathered about the installation path.

3.6. Technical Analysis: aax.me Antivirus Profiling

Interestingly, aax.me also attempts to determine the presence of various antivirus products on a target's machine.

We expand on the probing of antivirus programs which we observed on **aax.me**, as we were unfamiliar with this technique. The technique appears to work on any modern version of Windows, with the latest versions of Chrome, Firefox, and IE/Edge (though, the profiling script excludes IE versions less than IE9 from the profiling, using the *vertical tab test*).[31] Specifically, the script conducts GET XMLHttpRequests (one at a time) to 127.0.0.1/ on the following ports: 12993, 44080, 24961, 1110, 6646, 6999, 30606. The script stops conducting these requests if it finds one request whose **readyState** is set to 4 less than 20ms after the request was initiated (200ms for port 6646), and submits the number of this port to the server.

The latest versions of Internet Explorer/Edge, Chrome, and Firefox (except Tor Browser) will all perform these XMLHttpRequests to 127.0.0.1 on behalf of any site. Of course, the *result* of such a request will most likely not be available to the script, due to the same-origin policy, and likely absence of a CORS[32] header in the response. Indeed, the script does not attempt to read the results of its requests. Rather, it leverages the fact that the web browser makes the *status* of the request sent available, via the **readyState** parameter of an XMLHttpRequest instance (*1* approximately represents TCP SYN sent, and *4* represents HTTP response received or TCP connection terminated). For a closed port, Windows will issue an RST/ACK for each SYN sent. However, it appears that Windows' TCP stack will not consider an outgoing connection it is initiating to be terminated until it has sent 3 SYNs, and received three corresponding RST/ACKs (or timeouts).

1	0.000000	127.0.0.1	127.0.0.1	TCP	66 49868 → 2000 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=2
2	0.000014	127.0.0.1	127.0.0.1	TCP	54 2000 → 49868 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.508806	127.0.0.1	127.0.0.1	TCP	66 [TCP Spurious Retransmission] 49868 → 2000 [SYN] Seq=0
6	0.508823	127.0.0.1	127.0.0.1	TCP	54 2000 → 49868 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	1.008816	127.0.0.1	127.0.0.1	TCP	62 [TCP Spurious Retransmission] 49868 → 2000 [SYN] Seq=0
10	1.008832	127.0.0.1	127.0.0.1	TCP	54 2000 → 49868 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 7: Three RST/ACKs required until Windows considers outgoing TCP connection terminated

When testing with a TCP connection from Windows to a remote host, we can clearly see that Windows transmits the second SYN ~500ms after the first RST/ACK, and the third SYN ~500ms after the second RST/ACK.

1	0.000000	10.0.2.15	75.126.24.80	TCP	66 49201 → 2000 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
2	0.162371	75.126.24.80	10.0.2.15	TCP	60 2000 → 49201 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.666735	10.0.2.15	75.126.24.80	TCP	66 [TCP Spurious Retransmission] 49201 → 2000 [SYN] Seq=0
4	0.828057	75.126.24.80	10.0.2.15	TCP	60 2000 → 49201 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	1.338741	10.0.2.15	75.126.24.80	TCP	62 [TCP Spurious Retransmission] 49201 → 2000 [SYN] Seq=0
6	1.494261	75.126.24.80	10.0.2.15	TCP	60 2000 → 49201 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 8: Windows sends the next SYN 500ms after the latest RST/ACK

Thus, the **readyState** value for a request to a closed port on 127.0.0.1 will not be set equal to 4 until approximately 1000ms after the request is issued. In summary, one can use this technique to distinguish between a closed port (**readyState** set to 4 at around 1000ms), an open port (**readyState** set to 4 before 1000ms), and a filtered port (**readyState** set to 4 long after 1000ms).

This script was apparently designed to detect the presence of certain components of Avast, Avira, ESET, Kaspersky, and Trend Micro antivirus products. We were not able to determine which program the probing of port 24961 was designed to detect. We verified that the latest version of Avast can be detected by this script, as it opens TCP port 12993, which is associated with its *Mail Shield* component for scanning email traffic; port 6999 is opened by Trend Micro's *tmproxy*[33] which scans web and email traffic; port 1110 is used by Kaspersky[34] to scan web and email traffic; it appears that Avira's *Web Protection* component for scanning web traffic used to open port 44080,[35] though we observed it opening 44081 instead; port 30606 appears to have been used by ESET to scan web and email traffic,[36] but we did not observe this port open while testing the latest version of ESET; port 6646 may be used by McAfee, though we did not test this.[37]

The code for the port scanning appears to be adapted from the **JS-Recon** port scanning tool.[38] JS-Recon is a generic tool that enumerates all open ports on 127.0.0.1 in a range; it does not specifically target anti-virus programs. The **scan_xhr** and **check_ps_xhr** functions in the **aax.me** profiling script are similar to the **scan_ports_xhr** and **check_ps_xhr** functions in JS-Recon. The creator of JS-Recon seems to have first presented the tool at BlackHat Abu Dhabi in 2010.[39]

Behavior based on port status:

Port Status	WebSocket (ReadyState 0)	COR (ReadyState 1)
Open (application type 1&2)	< 100 ms	< 100 ms
Closed	~1000 ms	~1000 ms
Filtered	> 30000 ms	> 30000 ms

Figure 9: Image from the author of JS-Recon showing how long WebSocket and XMLHttpRequest ("COR") connections remain in their initial readyState on Windows.[40]

Note that this technique can be generalized to any remote content timing side channel (e.g, the **onerror** event for an **Image**). Additionally, one can identify the presence of an open port on 127.0.0.1 that speaks HTTP without using timing information, and thus without the Windows TCP behavior assumption (e.g., by handling the **onerror** and **oncomplete** events of certain types of **link** elements).

We are unsure whether the purpose of the antivirus profiling is to identify potentially exploitable antivirus software running on a target's computer, or for evasion of antivirus products. In December 2015, Google Security discovered a critical vulnerability in Avast's antivirus product, which involved a webpage sending HTTP requests to a port that Avast opens on 127.0.0.1. Google Security demonstrated that the vulnerability allowed exfiltration of arbitrary files from a victim's disk.[41] In January 2016, Google Security discovered a critical vulnerability in Trend Micro's antivirus product, which similarly involved a web page sending HTTP requests to a port that Trend Micro opens on 127.0.0.1. Google Security demonstrated that the vulnerability allowed arbitrary command execution.

4. The Case of the Fake Journalist

In the course of our investigation we scanned the e-mail of journalist Donaghy and found evidence that he had been contacted by a fictitious journalist, whom we linked to Stealth Falcon.

We scanned Donaghy's GMail account for any previous messages featuring links that redirected through **aax.me**. We identified the following message from December 2013, purporting to be from a UK journalist named Andrew Dwight:

> **From:** andrew.dwight389@outlook.com
> **Subject:** FW: Correspondence Request
>
> Greetings Mr. Donaghy,
>
> I have been trying to reach you for comment and I am hoping that this e-mail reaches the intended recipient. My name is Andrew Dwight and I am currently writing a book about my experiences in the Middle East. My focus is on human factors and rights issues in seemingly non-authoritarian regimes (that are, in reality, anything but). I was hoping that I might correspond with you and reference some of your work, specifically this piece (**http://goo.gl/60HAqJ**), for the book. I'm quite impressed with the way you articulate this complex issue for the masses, and hope to have a similar impact with my book.
>
> Happy New Year,
>
> Andrew

The link in the email, **http://goo.gl/60HAqJ**, redirects to **http://aax.me/0b152**, which, as of December 2015, redirected to a 2013 Huffington Post blog post authored by Donaghy.[42] We did not observe any **redirect.php** behavior with this link; as of December 2015, the **aax.me** link directly served an HTTP 302 redirect to the Huffington Post (we omitted the **date** header below). However, it is possible that the link formerly exhibited **redirect.php** behavior:

```
HTTP/1.1 302 Moved Temporarily
Date:
Server: Apache/2.2.9 (Debian) mod_ssl/2.2.9 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.6-1+lenny13
Location: http://www.huffingtonpost.co.uk/rori-donaghy/uae-94_b_3549671.html
Vary: Accept-Encoding
Content-Type: text/html
```

We found that Donaghy had responded to this message shortly after receiving it, offering to meet in-person with Andrew in the UK.

Andrew responded several weeks later with the following:

> **From:** andrew.dwight389@outlook.com
> **Subject:** RE: Correspondence Request
>
> Hello Rori,
>
> Happy New Year! I apologize for the delay in getting back to you. I was on a ski holiday in upstate New York for the New Year and just returned to my current accommodations in the city. I was due back sooner, but as you may know, the weather has not been agreeable here in the Eastern United States!
>
> I am currently situated in the US. while I complete my book to be closer to my publisher and editor. The book focuses on the various guises used by Middle Eastern countries to demonstrate that they are providing equal and fair treatment with concern to human rights. I am working with several organizations in identifying cases that reveal their true lack of concern for liberty and personal freedoms. I'm using these cases as testimony about this under reported issue. Have you heard of a Swedish organization named Al Karama?
>
> There website: **http://en.alkarama.org/index.php?option=com_content&view=article&id=1005&Itemid=74&slid=102**
>
> I have spoken to one of their junior editors and I am hoping to obtain input from some of their sources as well.
>
> This issue never gets any smaller does it? I hope that a few loud voices (and a well received book) can make a difference.
>
> Cheers,
>
> Andrew

While attempting to determine whether "Andrew Dwight" was a real person, we we found a Twitter profile, **@Dwight389** for the same persona, and that mentions the same address from which Donaghy received the email.

Figure 10: Andrew Dwight's Twitter profile, @Dwight389, mentioning the email address that corresponded with Donaghy in 2013, andrew.dwight389@outlook.com

We found that this account messaged three UAE dissident accounts via Twitter mentions. While we were unable to establish if **@Dwight389** successfully attacked any of these individuals, we profile the targets below.

4.1. Another Target: Obaid Yousef Al-Zaabi

This section describes how the fake journalist persona contacted Obaid Yousef Al-Zaabi, a blogger who was arrested for criticising the UAE.

Figure 11: @Dwight389 contacted @bukhaledobaid on 24 April 2013

Obaid Yousef Al-Zaabi was arrested on 2 July 2013[43] for Tweeting about the UAE94 detainees (94 defendants prosecuted in a mass trial on charges of attempting to overthrow the government)[44] on his **@bukhaledobaid** account, which displays his real name.[45] He was released due to health problems a month later, but was arrested again on 12 December 2013,[46] a day after talking to CNN[47] about the condition of US citizen Shezanne Cassim, imprisoned for making a parody video[48] about "youth culture in Dubai".[49] Al-Zaabi and Cassim were imprisoned in the same cellblock. Al-Zaabi was acquitted on 23 June 2014 of all charges including "slander concerning the rulers of the UAE using phrases that lower their status, and accusing them of oppression" and "disseminating ideas and news meant to mock and damage the reputation of a governmental institution," but, according to information received from two UAE sources, Al-Zaabi is still imprisoned in the prisoners ward of a hospital. A coalition of 13 human rights organizations including Amnesty International consider Al-Zaabi's ongoing detention to be arbitrary, and without legal basis.[50] Amnesty International reported that "a senior State Security Prosecution official" told Al-Zaabi he would continue to be detained even if acquitted.[51]

Al-Zaabi's brother, Dr. Ahmed Al-Zaabi, is one of the UAE94 detainees and is currently serving a 10 year prison sentence. According to a report by the Gulf Center for Human Rights, Ahmed was tortured in prison: his fingernails were pulled out, and he was *"beaten to the point he was left swollen, covered in bruises all over his body and with large amounts of blood in his urine".*[52]

4.2. Another Target:Professor Abdullah Al-Shamsi

This section describes how the fake journalist persona contacted professor Abdullah Al-Shamsi, Vice Chancellor of the British University in Dubai.

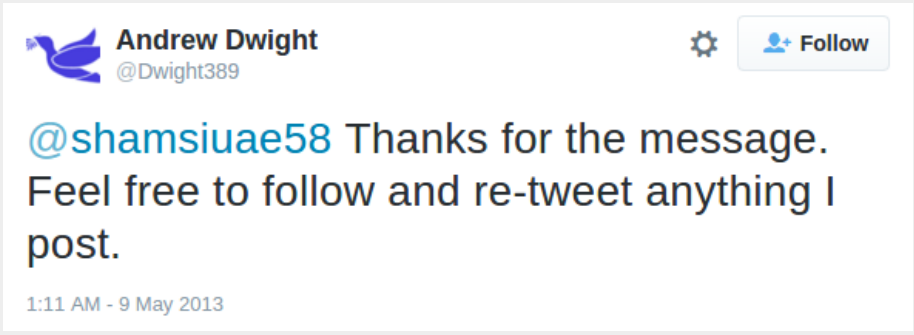

Figure 12: @Dwight389 sent a message on 9 May 2013 suggesting he had targeted @shamsiuae58

Professor Abdullah Al-Shamsi (**@shamsiuae58**) is the Vice Chancellor of the British University in Dubai.[53] He (Arabic name: أ.د.عبدالله محمد رحمة الشامسي)[54] is signatory #79 (out of 133) to a March 2011 petition to the UAE government[55] for direct elections[56] (UAE activist Ahmed Mansoor was arrested after signing the same petition).[57] Al-Shamsi's father (محمد بن رحمة العامري الشامسي) was appointed to, and chaired the first sessions of, the Federal National Council (FNC), a legislative advisory council that is now an elected body. He called for more powers to be given to the FNC.[58]

4.3. Additional Targets: Qatari Citizens Sentenced to Prison

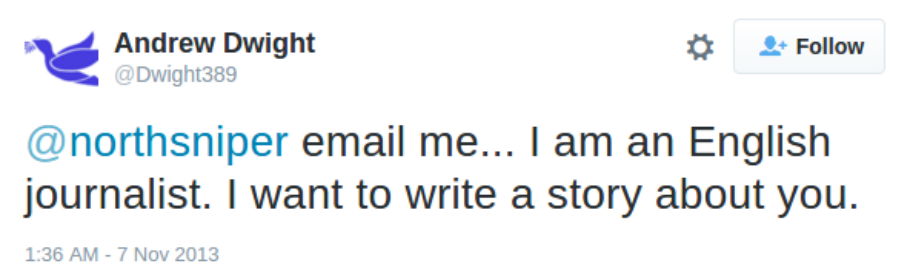

Figure 13: @Dwight389 contacted @northsniper on 7 November 2013

In May 2015, five Qataris were sentenced (one present in the UAE to 10 years in prison, and four in absentia to life in prison), for posting allegedly offensive pictures of the UAE Royal Family on three Twitter accounts and two Instagram accounts,[59] including **@northsniper**.[60] At trial, the prosecution accused the five of being agents of Qatar's State Security, and posting the allegedly offensive pictures as part of a "military mission" to "show that Emiratis had offended their own leaders".[61] The **@northsniper** account is currently suspended. One Instagram account allegedly used by defendants in this case (**@9ip**) is still active, and still appears to display unflattering photoshopped images of the President, Crown Prince, and Founder of the UAE.[62]

5. Stealth Falcon's Widespread Targeting of UAE Figures

This section describes how we identified additional Stealth Falcon victims and bait content, and traced Stealth Falcon's spyware to additional C2 servers.

Given Stealh Falcon's use of public Twitter mentions to contact individuals, we searched Google and Twitter for instances of **aax.me** links. The links we found indicated that we could easily probe **aax.me** to get a comprehensive list of all currently active short URLs, and their corresponding long URLs. Our findings point to a UAE-focused operator, whose bait content and targets are linked to the Emirates. Furthermore, we were able to connect this attack to case from December 2012, where an anonymous UAE activist contacted us and claimed to have received a suspicious link from a Twitter account that was purportedly under government control.

5.1. Public Targets and Links to Arrests

This section describes 24 Stealth Falcon Twitter targets we identified on the basis of them receiving an aax.me link in a Twitter mention.

We found aax.me links targeting 24 accounts, each of whom was mentioned in a tweet that also contained an aax.me shortened link. We were unable to get details about 17 of the accounts. **Of the accounts we have been able to identify, several individuals were subsequently arrested or convicted in absentia by the UAE Government in relation to their online activities**.

The following table outlines these cases, and notes arrests. For completeness, the table includes the cases from Section 4.1-4.3:

Handle	Targeting	Related Arrests / Convictions	Note
@omran83	14 January 2012[63]	16 July 2012[64] (arrested)	UAE94 prisoner; serving 7 years in prison.[65]
@weldbudhabi	5 August 2012;[66] 20 October 2012[67]	14 December 2012[68] (arrested)	
@intihakat	5 August 2012[69]	25 December 2013[70] (convicted)	Qatari convicted in absentia; sentenced to 5 years in prison.
@bukhaledobaid (Sec 4.1)	24 April 2013[71]	2 July 2013;[72] 12 December 2013[73] (arrested)	Brother of UAE94 prisoner; acquitted of charges; indefinitely detained in prisoners ward of hospital.
@northsniper		18 May 2015[75]	Five Qataris convicted; sentences ranged from 10

(Sec 4.3)	7 November 2013[74]	(convicted)	years to life in prison.
@71UAE	9 January 2012[76]		Last tweeted 1 July 2013, a day before arrest of @bukhaledobaid.
@kh_oz	10 January 2012[77]		Likely son of @bukhaledobaid.[78]
@shamsiuae58 (Sec 4.2)	9 May 2013[79]		Signed 2011 pro-democracy petition that Ahmed Mansoor was arrested after signing.
@newbedon	9 January 2012[80]		Donaghy describes the account as "ensur[ing that] details of mistreatment [by security forces] are readily available".[81]
@bomsabih	9 January 2012[82]		Inactive since 8 October 2014. Owner claimed affiliation with State Security Apparatus.

We list additional details in **Appendix D: Public Stealth Falcon Tweets**.

5.2. Ennumerating aax.me for Bait Content

This section describes how we probed every conceivable short URL on aax.me, and found 402 pieces of bait content that we believe were sent by Stealth Falcon.

All of the public **aax.me** links we found, as well as the links sent to Donaghy, matched the regular expression /aax\.me\/[0-9a-f]{5}/. Assuming all links shortened via **aax.me** match this regular expression, there are only 165 (1,048,576) possible short URLs. We sent a request to **aax.me** for each possible URL, and observed the returned page or redirect. We found 57 URLs that exhibited the **redirect.php** profiling behavior, and 524 URLs that returned an HTTP 302 redirect to an expanded URL. The other 1,047,995 **aax.me** links returned a HTTP 302 redirect to the **aax.me** homepage; we assume these short URLs were unassigned to an expanded URL, as of the time of our scan.

We coded the long URLs where the URLs were still active, or where we could find an archived copy of, or some information about, the URL. We were able to code 535 URLs, and failed to code 46 URLs as the corresponding websites were down, and we could not find reliable information about what content the URLs contained. See **Appendix E: Results of aax.me Scan** for details. We coded 133 URLs as "advertisement" (25% of all coded URLs), as they appeared to represent an advertisement for a product. The vast majority of these advertisements seemed to be products typically marketed via spam (e.g., "dietary supplement" or "green coffee"). We suspect that these links may have been shortened by spammers, as the **aax.me** URL shortening page is pubilcly accessible and indexed by Google, and YOURLS advises that publicly accessible URL shorteners will receive spam.[83] All "advertisement" links were 302 redirects, and none were **redirect.php** links. This is consistent with our observation that the **aax.me** public interface only permits visitors to shorten links using the 302 redirect method.

We filtered out the short URLs classified as "advertisement." There were 402 non-advertisement short URLs that we tagged. We display a summary of the top ten tags below:

Tag	Number of Short URLs	% of non-advertisement URLs
UAE	292	73%
Torture	57	14%
Security Forces	49	12%
Denaturalization	46	11%
Isa bin Zayed	42	10%
Rule of Law	40	10%
Criticism	40	10%
ABC News	40	10%
Violations	33	8%

Islam	29	7%

We noted that a number of long URLs had multiple corresponding short URLs. We display the top ten long URLs below.

Long URL	# Short URLs	Description
http://www.youtube.com/watch?v=F6NU4pc378k	40	ABC News report featuring video of Abu Dhabi Crown Prince's brother, Sheikh Isa bin Zayed al-Nahyan, torturing an Afghani grain salesman.
http://mohaamoon.com/uae/17.htm	40	Personal website criticizing rule of law and human rights issues in the UAE, including torture, slavery, and imprisonment for debts.
https://r7aluae2.wordpress.com/2012/01/09/اتحاد-المنظمات-الإسلامية-في-أوروبا-يس/	19	Copied statement from the Federation of Islamic Organizations in Europe (FIOE), criticizing the UAE's denaturalization of citizens.
https://www.a7rarelemarat.com/vb	10	Purported to be an opposition web forum for discussing Emirati issues, and providing proxy tools. The site is now down, so we cannot inspect the specific forum posting.
http://google.com	9	Google.
https://www.a7rarelemarat.com/vb/showthread.php?p=3423#post3423	6	(see a7rarelemarat above)
http://www.youtube.com/watch?v=Xcc9Tdc_Hxg&feature=player_embedded#!	5	Video montage talking about torture by UAE security forces.
http://www.youtube.com/watch?v=izeSn9Am6us&list=UU2wwG6r1J_GRgXuMGi9m8FQ&index=1&feature=plcp	5	Video unavailable.
https://www.youtube.com/watch?feature=player_embedded&v=Q3aQpfyXSrg	5	Video published by Al Islah, which appears to be a montage of UAE political detainees.
https://www.a7rarelemarat.com/vb/forumdisplay.php?f=3	5	(see a7rarelemarat above)

5.3. A Connection to an Account Potentially Under UAE Government Control

This section describes a case from December 2012 where an Emirati activist said he received links connected to aax.me from an account that may have been under UAE government control.

In December 2012, an author of this report was contacted by an Emirati activist, who reported that an account, **@WeldBudhabi**, had sent him a link on 14 December 2012 via Twitter direct message that took him to a page on **a7rarelemarat.com**. A report by BBC notes that UAE authorities on 14 December 2012 arrested an individual who they believed to be associated with **@WeldBudhabi**, and that the account was *"reportedly hacked by the authorities"* on the same day.[84] The Emirati activist told us that he later contacted **@WeldBudhabi**, who reported that he did not send the link.

This link provides the strongest connection between Stealth Falcon and the UAE Authorities that we are aware of.

a7rarelemarat.com is a now-defunct website that purported to be an opposition web forum for discussing Emirati issues, and providing proxy tools for *"hiding from the thugs"* (presumably a reference to the UAE State Security Apparatus). We found four links involving **aax.me** posted by the site's Twitter account, **@a7rarelemarat**. We display two Tweets below, as the rest of the Tweets had the same links:

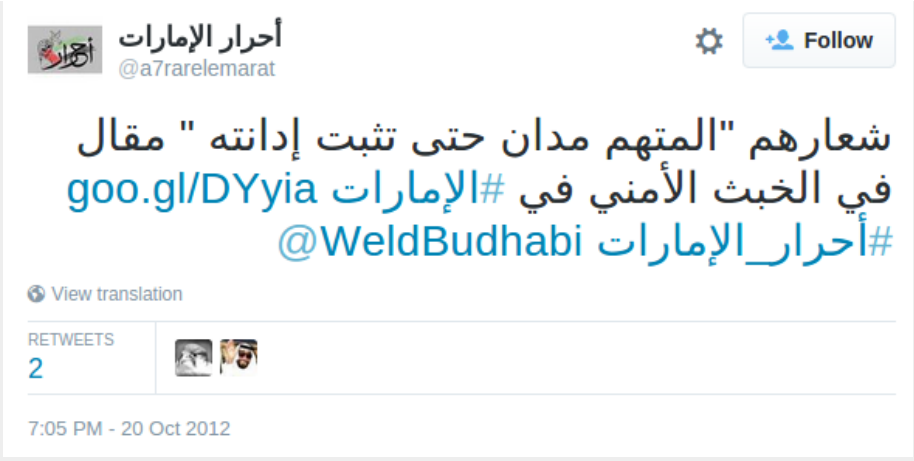

Figure 14: @a7rarelemarat targeted @WeldBudhabi with a malicious link on 20 October 2012

Twitter's API records the date of the tweet's creation:

```
Sun Oct 21 05:05:41 +0000 2012
```

We also accessed the **goo.gl** link statistics, and found that the **goo.gl** link in the tweet was created less than two minutes prior to the tweet:

```
2012-10-21T05:03:45.585+00:00
```

The second tweet exhibited a similar pattern:

Figure 15: @a7rarelemarat publicly sent a malicious link on 2 October 2012

Twitter's API records the date of the tweet's creation:

```
Wed Oct 03 06:54:33 +0000 2012
```

We again accessed the **goo.gl** link statistics, and found that the **goo.gl** link in the tweet was created less than one minute prior to the tweet:

```
2012-10-03T06:53:45.151+00:00
```

The link redirects to **https://www.a7rarelemarat.com/vb/showthread.php?p=3423#post3423** via **http://aax.me/d910a**.

The use of both **goo.gl** and **aax.me** in these cases suggests that the **goo.gl** link may have been designed to conceal the **aax.me** domain. Also, the proximity in creation time between the Tweet and the **goo.gl** link suggests that the person who posted the Tweet through **@a7rarelemarat** was likely the same person who created the **goo.gl** link.

We suspect that the **aax.me** operator had some control over **@a7rarelemarat** at the time, and may have had control of **a7rarelemarat.com** as well.

5.4. Infrastructure Analysis of Stealth Falcon Command & Control

This section describes how we traced Stealth Falcon's spyware to live C2 servers and domain names.

We fingerprinted the behavior of **adhostingcache.com** (the C2 server for the Stage One spyware that Donaghy received) and traced it to a series of 14 active IP adresses and 11 domains (using PassiveTotal[85]). Nine domains are named like generic Internet backend servers (e.g., **simpleadbanners.com**, **clickstatistic.com**), whereas two appear to be thematically related to travel (**bestairlinepricetags.com**, **fasttravelclearance.com**), perhaps indicative of travel-themed targeting or targets.

We fingerprinted the behavior of **incapsulawebcache.com** (the C2 server for the Stage Two spyware that Donaghy receied) and scanned the Internet (including historical scanning results[86]) for servers that matched our fingerprint. We also used Passive DNS to correlate IP addresses to domains. In total, we associated 67 active (and 30 historical) IP addresses with the Stage Two spyware. Using PassiveTotal, we linked 69 domain names to these IP addresses, the earliest registered on 28 January 2013, and the most recent registered on 19 April 2016. The vast majority of the domains are named like generic Internet backend servers. One domain name appears to be travel-themed (**airlineadverts.com**), and two appear to be news and/or government themed (**ministrynewschannel.com**, **ministrynewsinfo.com**).

The earliest date we found an IP addresses matching our Stage Two fingerprint was 21 July 2014, as recorded by *sonar-ssl* scans. It is possible that the operator used a different configuration of spyware between January 2013 and July 2014.

We traced several additional domains to Stealth Falcon using WHOIS information, or Passive DNS. Of these, one was designed to impersonate a China-based provider of VoIP solutions (**yeastarr.com**), and two appeared to perhaps contain the Arabic word for security, "amn," (**amnkeysvc.com**, **amnkeysvcs.com**). Full scan results and other indicators of targeting can be found in **Appendix F: Indicators of Targeting**.

The domain names we found were typically registered with WHOIS privacy providers. Although, in some cases, we were able to obtain the true registration email through historical WHOIS. Typically, the operators practiced disciplined operational security: we rarely found an email address that was used to register two domains, and we rarely found two domains linked to the same IP address.

5.5. May 2016: New Stealth Falcon Document

In May 2016, the following document was submitted to VirusTotal:

```
Filename:  message_032456944343.docm
MD5:       87e1df6f36b96b56186444e37e2a1ef5
SHA1:      1c3757006f972ca957d925accf8bbb3023550d1b
SHA256:    4320204d577ef8b939115d16110e97ff04cb4f7d1e77ba5ce011d43f74abc7be
```

The document was similar to the one sent to Donaghy, except that it purported to be encrypted with WordSecure, *"a simple, HIPAA .. business-grade software for sharing encrypted files and secure messages with anyone"*.[87] The bait content was a single line of text reading:

```
MESSAGE_ERROR: 0E684AD042_(LANGUAGE NOT SUPPORTED)
```

The document's macro was identical to the one sent to Donaghy, except it reported back to, and downloaded Stage Two from a different URL: **http://optimizedimghosting.com/wddf/hrrw/ggrr.txt**. The server **optimizedimghosting.com** matched our Stage One fingerprint for **adhostingcache.com**.

We obtained Stage Two, which appeared to be a newer version of the Stage Two than in Donaghy's case. The Stage Two in this case reported back to **https://edgecacheimagehosting.com/images/image.nfo**. The server **edgecacheimagehosting.com** matched our Stage Two fingerprint for **incapsulawebcache.com**.

When we connected, the Stage Two server sent us additional commands (which we were unable to obtain in Donaghy's case). The Stage Two C2 sent us a bundle of 7 commands, that did the following:

1. Gathered system info from WMI
2. Gathered the ARP table
3. Gathered a list of running processes
4. Materialized a file "OracleJavaUpdater.ps1" to disk. This file gathers passwords and web browser data from a variety of sources: Windows Credential Vault, Internet Explorer, Firefox, Chrome, Outlook. In general, the file appears to be bespoke attacker code, though some routines are copied from other sources (e.g., some Internet Explorer password gathering code

appears to be lifted from the GPLv3-licensed QuasarRAT[88])

5. Executed “OracleJavaUpdater.ps1”
6. Deleted “OracleJavaUpdater.ps1”
7. Gathered a list of running processes again

After command execution, results were returned to the Stage Two C2.

6. Tip of the Iceberg: Possibly Related Attacks

We suspect that the activity we have observed is simply the tip of the iceberg in ongoing attacks against dissidents in the UAE. Reuse of tactics, techniques and procedures and general carelessness by operators can often lead to discovery of links between campaigns. We briefly discuss some instances of potentially related attacks below.

6.1. An Instagram attack?

We noticed that one of the Twitter accounts that sent out **aax.me** links, **@um_zainab123**, solicited followers for an Instagram account **@al7ruae2014**.

Figure 16: @um_zainab123 soliciting followers for Instagram account @al7ruae2014 on 26 April 2014

Figure 17: The @al7ruae2014 Instagram account

We contacted an activist with knowledge of the UAE94 case, who told us that the @al7ruae2014 Instagram account got in touch with several family members of detainees involved in the case, and was soliciting information from them via Instagram private message. The domain name **al7ruae2014.com** has the same name as the Instagram account, so we suspect it may also be related to the operator.

6.2. A fake file sharing site?

We identified one **aax.me** link (**http://aax.me/4b708**) that points to **http://velocityfiles.com/download.php?id=a81abdd8a0c0cd1d5d3b6baadcc9eb18**. We visited this link in February 2016, and were served a blank page. VelocityFiles appears to have been disabled in March 2016.

We found that the site purported to be a file hosting site, where users could register and upload files. However, the registration and signup pages are currently blank, and were blank as of the Internet Archive’s oldest capture of the pages in December 2013.[89] We were unable to identify any links to velocityfiles.com from Twitter, or any pages indexed by Google.

The design of VelocityFiles appeared to be a loosely modified version of a public website design template.[90] Given that the site appears to be designed to pose as a public file sharing service, has no obvious public functionality, and was linked to through aax.me, we suspect that it may have been an attack site.

Figure 18: Comparison between web design template image (left) and VelocityFiles website (right).

Given VelocityFiles' reference to "**FREE** MD5 HASHING" (their emphasis), it is possible that the value of the *id* parameter in the URL, a81abdd8a0c0cd1d5d3b6baadcc9eb18, represents the MD5 hash of a file. We were, however, unable to locate any file with this MD5 hash.

6.3. Fake web forums?

We found an **aax.me** link[91] that pointed to https://call4uaefreedom.com/vb. The domain was registered on 5/15/2013 and expired on 5/15/2015. We were unable to find any webpages or tweets linking to this website. A Google search for "call4uaefreedom" reveals a blog, containing five posts, all within a 30 minute span on 4 June 2013, and an empty Twitter account @call4uaefreedom, created in May 2013. Given the suspicious activity associated with the alias "call4uaefreedom," this may have been created by operators.

While searching for domains with similar domain names, we came across **uaefreedom.com**. The domain name was first registered on 11 June 2010 by the administrators of UAE Hewar,[92] an online discussion forum founded in 2009 that was a frequent government target. The domain name expired on 11 June 2011, but was re-registered by a different registrant on 7 October 2012.

On 16 October 2012, we find the only tweet linking to **uaefreedom.com**. A Google search yields no links to the site and we found no passive DNS data available for this domain. The tweet was sent from account **@FreeUAE2012**, directed at @uaemot. An individual based in Qatar was convicted in absentia on 25 December 2013 for running @uaemot.[93]

Figure 19: @FreeUAE2012 contacts @uaemot with a suspicious link on 16 October 2012

Other public tweets involving **@FreeUAE2012** included two responses[94] from Ahmed Mansoor to **@FreeUAE2012** on 10 October 2012, regarding the 10 October 2012 Citizen Lab report about how Ahmed Mansoor was targeted with Hacking Team spyware. The tweets from @FreeUAE2012 to which Ahmed Mansoor was responding appear to have been deleted.

Three days later, **@FreeUAE2012** attempted to convince Ahmed Mansoor that Tor Browser logged private information of its users, posting a screenshot of the Tor Metrics page, which provides non-sensitive data for researchers.[95]

Figure 20: @FreeUAE2012 attempts to convince Ahmed Mansoor that Tor logs private information of its users

7. Attribution

In this section, we analyze two competing hypotheses about the identity of Stealth Falcon, and conclude that the balance of evidence suggests Stealth Falcon may be linked to the UAE government.

Hypothesis 1: Stealth Falcon is State Sponsored

Stealth Falcon is a sophisticated threat actor, capable of deploying a wide range of technical and social engineering techniques against a potential target. The operations targeting Donaghy are linked to a series of primarily UAE-focused campaigns against UAE dissidents, starting in January 2012. While there is no "smoking gun," several pieces of evidence suggest a connection between Stealth Falcon and the UAE Government.

UAE Focused Targeting, Links to Arrests

The majority (73%) of bait content on aax.me was focused on UAE-related political issues (**Section 5.2**). Furthermore, of the 27 victim Twitter accounts we linked to public Stealth Falcon targeting, 24 **primarily engaged in political activities, or were otherwise critical of the UAE government** (**Section 5.1**). Of these 24, we were able to find a subsequent arrest or a conviction in absentia by the UAE government.

Tweets During a Period of Government Control

A reported case in which a Twitter account apparently under UAE Government control shared a Stealth Falcon link also suggests a connection.

In December 2012, an activist contacted us and asserted that an **a7rarelemarat.com** link was sent to him in a private message from the **@WeldBudhabi** account the same day that an individual accused of operating the account was arrested, and while the account was *"reportedly hacked by authorities"*.[96] The activist asserted that he contacted an owner of the account, who claimed he did not send that link. The Twitter account associated with **a7rarelemarat.com**, **@a7rarelemarat**, appears to have been under the control of Stealth Falcon at some point during October 2012 (and possibly before and after), as the account sent several **aax.me** links in October 2012.

Sophisticated Target Knowledge and Operational Security

Stealth Falcon demonstrates some familiarity with the patterns of behavior, interests, and activities of its targets, suggesting that the operators may have been working with other sources of information about their targets' behaviors. In addition, Stealth Falcon

displayed above-average operational security throughout the campaign. Some of the social engineering was highly intricate, particularly the email from Andrew Dwight about his ski holiday. Stealth Falcon also shows familiarity with creating and maintaining a range of fictitious personas, and registering and managing a significant amount of attack and C2 infrastructure with concern for operational security.

The infrastructure behind the malware attacks showed good compartmentalization of identities. We rarely found the same (fake) registration information used for more than one C2 domain. Stealth Falcon operators also appear to have deleted one of their attack domains, **adhostingcache.com** when they realized their attempt to target Donaghy had failed. We also noted that the (self-signed) SSL certificates on the C2 domains were changed several times as we monitored the infrastructure, perhaps in an attempt to thwart fingerprinting of their infrastructure via SSL certificates.

This level of sophistication is consistent with a state sponsored attacker. Importantly, we found little evidence that indicate criminal or other motivation for the attack, with no evidence of financial or industry targeting.

We also note that while some Stealth Falcon domains were registered on anonymousbitcoindomains.com, which is linked to APT28 activities, we found no evidence to support such a connection. See **Appendix G: No Evidence of APT28 Connection** for more details.

Hypothesis 2: Stealth Falcon is Not State Sponsored

We have considered the possibility that Stealth Falcon's operators are not state sponsored, but ultimately find little evidence to support this possibility.

Stealth Falcon's attacks show no evidence of cyber criminal motivations, like financial theft or fraud, nor is there any evidence of attempts to steal intellectual property or conduct other forms of economic espionage. Instead, the targets are politically engaged individuals and public figures. Furthermore, the activity of targets we have been able to identify often concerns domestic UAE issues. Therefore, we would need to posit an operator with an interest in individuals known for their engagement in domestic UAE issues.

Other potential motivations might include blackmail or extortion. If this were the case, however, we might expect follow-up interactions between attackers and successful victims, and we would also expect attackers to use off-the-shelf Remote Access Tools (RATs), rather than apparently coding a general-purpose RAT from scratch. This would save them the trouble of needing to load additional malware to exfiltrate files or other material. We are aware of no evidence of follow-up interactions between the operators and successful victims as part of any extortion attempts. Furthermore, Stealth Falcon's use of JavaScript to profile and de-anonymize victims seems inconsistent with a primary motivation of collecting information that could be used for blackmail.

The strongest scenario for a non-state sponsored attacker is thus a politically motivated group. Stealth Falcon targets are primarily individuals known for their criticism of the UAE government. It is perhaps conceivable that a group of pro-government hackers might, without coordination, target these individuals.

There are, however, several features of Stealth Falcon's activities that tell against this possibility. First, there is limited existing evidence that such autonomous groups exist and are active in the UAE. Given what is known about this kind of group, we might expect such a group to have engaged in defacements, public boasting, or other public-facing activities related to Stealth Falcon's campaign. Furthermore, it seems unlikely that a previously unknown political group would have the resources to develop and maintain Stealth Falcon's fictitious personas and compartmentalized infrastructure.

Evaluation of Hypotheses

We evaluated both hypotheses and found **Hypothesis 1: Stealth Falcon is State Sponsored** to be the best at explaining the many elements that we have observed. Stealth Falcon's tactics, resources, and targets all fit with the profile of a state sponsored attacker. Furthermore, the circumstantial evidence we have presented in this report is suggestive of a link between Stealth Falcon and an entity within the UAE Government.

8. Conclusion: The Big Picture

Stealth Falcon appears to be a new, state sponsored threat actor. As an operator, Stealth Falcon is distinguished by well informed and sophisticated social engineering, combined with moderately sophisticated[97] technical attempts to deanonymize and monitor political targets working on the UAE, and relatively simple malcode.[98]

Social Engineering and the Achilles Heel of Civil Society

Stealth Falcon's technical approach may not be cutting edge, but the operators are neither unsophisticated or ineffective. Analyzed

holistically as an operation, Stealth Falcon is a logical and multi-pronged approach to compromising and unmasking a class of targets. Stealth Falcon's campaign highlights the power of social engineering, once a technical bar has been met, in conducting a large scale campaign.

Contemporary social movements and civil society groups rely heavily on the internet for both their core operations, as well as advocacy activities. Yet these groups are often operating outside a centrally managed IT environment. The constant sharing of links and materials, as well as regular communications with journalists makes them especially vulnerable to targeting with social engineering.

However, the emphasis on social engineering can also cut in the other direction. Many modern attack techniques require an attacker to interact with a target. When operators like Stealth Falcon send malicious e-mails and tweets, there are a range of opportunities for retrospective investigation. As this report shows, the inboxes of targets, for example, are often a more efficient object of investigation than computers themselves, especially once features of a particular campaign are recognized.

The Growing Trend of Impersonating Journalists

Stealth Falcon is only the latest example of civil society-focused threat actors impersonating NGOs and journalists to conduct espionage operations. The tactic has been used by a wide range of actors, including Bahrain's government,[99] Packrat in Latin America,[100] Iranian groups,[101] and China related groups,[102] among others. Threat actors seem to gravitate towards this tactic because interacting with journalists is an essential part of civil society activity. It is common for journalists to send unsolicited messages to activists and civil society organizations asking for information, and there is typically a strong incentive for the organization to engage. Indeed, even Western law enforcement agencies have occasionally adopted the approach.[103] The reporter-source relationship is protected in many jurisdictions, based on the understanding that protecting this trust is important to a healthy and vibrant civil society. Tactics that play on this trust are risky, and can quickly contribute to eroding the trust on which civil society is based.

Final Note: A Plea for More Research

Importantly, while we were unable to identify evidence of a conclusive link between Stealth Falcon and a particular sponsor, we have assembled a body of circumstantial evidence that points to an alignment of interests between Stealth Falcon and the UAE Security Forces. We hope that other researchers will draw from our findings and work to identify additional cases. Finally, we urge anyone who recalls receiving a link to "aax.me," or an email from "Andrew Dwight" to contact the authors of this report for further investigation.

Acknowledgements

Special thanks to PassiveTotal and Rori Donaghy. Thanks to Jeffrey Knockel, Sarah McKune, Chris Doman, Mansoureh Mills.

Footnotes

[1] http://www.youthdiplomaticservice.com/zzold-business-blog/category/business

[2] See for example: http://www.middleeasteye.net/news/leaks-show-uae-shipped-weapons-libya-violated-un-resolution-1712843977; http://www.middleeasteye.net/news/uae-paid-pr-firm-millions-brief-uk-journalists-qatar-muslim-brotherhood-attacks-1058875159; http://www.middleeasteye.net/news/leaks-show-uae-shipped-weapons-libya-violated-un-resolution-1712843977; http://www.middleeasteye.net/news/exclusive-emirati-plan-ruling-egypt-2084590756

[3] http://www.middleeasteye.net/users/rori-donaghy

[4] http://www.middleeasteye.net/about-middle-east-eye-1798743352

[5] http://www.echr.org.uk/

[6] http://www.echr.org.uk/?page_id=25

[7] https://freedomhouse.org/report/freedom-world/2015/united-arab-emirates

[8] https://www.hrw.org/world-report/2016/country-chapters/united-arab-emirates

[9] https://www.amnesty.org/en/countries/middle-east-and-north-africa/united-arab-emirates/

[10] https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-marczak.pdf

[11] https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

[12] https://wikileaks.org/hackingteam/emails/emailid/585453

[13] http://www.uae-embassy.org/news-media/sheikh-mohamed-bin-zayed-al-nahyan-meets-congressional-leaders-and-senior-us-government

[14] https://ht.transparencytoolkit.org/rcs-dev%5Cshare/HOME/cristian/9.4%20lic/UAEAF/LICENSE-1262004202-v9.4.lic

[15] https://owncloud.org/

[16] https://www.proofpoint.com/us/office365

[17] http://righttofightexhibit.org/home/

[18] http://www.powershellempire.com/

[19] http://www.aljazeera.com/indepth/opinion/2015/11/british-pm-middle-east-human-rights-151103070038231.html

[20] Based on *last-modified* header

[21] http://www.andlabs.org/tools/jsrecon.html

[22] https://media.blackhat.com/bh-ad-10/Kuppan/Blackhat-AD-2010-Kuppan-Attacking-with-HTML5-slides.pdf

[23] https://yourls.org/

[24] https://github.com/YOURLS/YOURLS

[25] A Firefox extension to be used in conjunction with Tor, before the introduction of Tor Browser

[26] Importantly, making Tor users appear similar to non-Tor users was a not a goal

[27] https://trac.torproject.org/projects/tor/ticket/5922

[28] https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-gregory_fleischer-attacking_tor.pdf

[29] https://blog.torproject.org/blog/new-tor-browser-bundles-windows

[30] https://blog.torproject.org/blog/tor-browser-36-released

[31] https://msdn.microsoft.com/en-us/library/2yfce773(v=vs.94).aspx#s-e6f6a65cf14f462597b64ac058dbe1d0-system-media-system-caps-note

[32] https://en.wikipedia.org/wiki/Cross-origin_resource_sharing

[33] https://esupport.trendmicro.com/en-us/home/pages/technical-support/1057722.aspx

[34] http://support.kaspersky.com/us/11255

[35] http://ssj100.fullsubject.com/t446-avira-antivir-premium-allows-all-outbound

[36] http://www.wilderssecurity.com/threads/port-80-is-redirected-to-30606-and-no-webpage-is-opened.212599/

[37] https://community.mcafee.com/thread/21790?tstart=0

[38] The tool is available at: http://www.andlabs.org/tools/jsrecon.html. The JavaScript source code may be viewed by viewing the source of jsrecon.html

[39] https://media.blackhat.com/bh-ad-10/Kuppan/Blackhat-AD-2010-Kuppan-Attacking-with-HTML5-slides.pdf

[40] http://www.andlabs.org/tools/jsrecon/jsrecon.html

[41] https://code.google.com/p/google-security-research/issues/detail?id=679

[42] http://www.huffingtonpost.co.uk/rori-donaghy/uae-94-verdict_b_3549671.html

[43] http://en.rsf.org/emirats-arabes-unis-journalist-held-incommunicado-02-08-2013,45013.html

[44] https://www.indexoncensorship.org/2015/03/united-arab-emirates-stop-the-charade-and-release-activists-convicted-at-the-mass-uae-94-trial/

[45] http://blogs.voanews.com/repressed/2014/01/14/update-shez-cassim-back-home-after-months-in-uae-jail/

[46] http://www.al-monitor.com/pulse/originals/2014/07/uae-twitter-imprisoned-not-guilty-activist-cyber-crime.html

[47] http://newday.blogs.cnn.com/2013/12/11/u-s-man-in-jail-in-dubai-over-parody-video/

[48] https://www.youtube.com/watch?v=IUk5CB9kaBY

[49] http://www.nydailynews.com/news/national/shezanne-cassim-sentenced-year-united-arab-emirates-parody-video-article-1.1556327

[50] https://www.article19.org/resources.php/resource/37279/en/united-arab-emirates:-stop-the-charade-and-release-activists-convicted-at-the-mass-uae-94-trial

[51] https://www.amnesty.org/en/documents/mde25/015/2014/en/

[52] http://www.gc4hr.org/report/view/33

[53] http://www.buid.ac.ae/vc

[54] http://www.wam.ae/ar/news/emirates/1395239973989.html

[55] http://emarati.katib.org/2011/03/09/%D8%A5%D9%85%D8%A7%D8%B1%D8%A7%D8%AA%D9%8A%D9%88%D9%86-%D9%8A%D8%B1%D9%81%D8%B9%D9%88%D9%86-%D8%B1%D8%B3%D8%A7%D9%84%D8%A9-%D9%84%D8%AD%D9%83%D8%A7%D9%85-%D8%A7%D9%84%D8%A5%D9%85%D8%A7%D8%B1%D8%A7/

[56] http://www.cnn.com/2011/WORLD/meast/03/09/uae.petition/

[57] http://www.bbc.com/news/world-middle-east-13043270

[58] http://www.alittihad.ae/details.php?id=8416&y=2005

[59] http://www.thenational.ae/uae/courts/defendant-denies-insulting-leaders-of-uae-on-social-media

[60] http://dohanews.co/uae-court-convicts-qataris-for-insulting-royals-on-social-media/

[61] http://www.thenational.ae/uae/foreign-agent-ordered-to-spread-false-information-about-uae

[62] https://www.instagram.com/9ip/

[63] https://twitter.com/Bu_saeed2/status/158267593269063680

[64] http://www.gc4hr.org/news/view/198

[65] http://www.echr.org.uk/?page_id=207

[66] https://twitter.com/islam_way_2030/status/232392466760863744

[67] https://twitter.com/a7rarelemarat/status/259883131807621120

[68] http://www.bbc.com/news/world-middle-east-20768205

[69] https://twitter.com/islam_way_2030/status/232393358243401728

[70] http://www.echr.org.uk/?p=1104

[71] https://twitter.com/Dwight389/status/327033672979079168

[72] http://en.rsf.org/emirats-arabes-unis-journalist-held-incommunicado-02-08-2013,45013.html

[73] http://www.al-monitor.com/pulse/originals/2014/07/uae-twitter-imprisoned-not-guilty-activist-cyber-crime.html

[74] https://twitter.com/Dwight389/status/398413653315031041

[75] http://www.thenational.ae/uae/courts/20150518/five-qataris-found-guilty-of-insulting-uae-royals

[76] https://twitter.com/MiriamKhaled/status/156625204280434688

[77] https://twitter.com/Bu_saeed2/status/156781983983349760

[78] https://twitter.com/kh_oz/status/351828658371039233

[79] https://twitter.com/Dwight389/status/332452681325088768

[80] https://twitter.com/r7aluae2/status/156418043424157696

[81] http://www.huffingtonpost.co.uk/rori-donaghy/uae-94-verdict_b_3549671.html

[82] https://twitter.com/Bu_saeed2/status/156406670866653184

[83] https://github.com/YOURLS/YOURLS/wiki/Spam

[84] http://www.bbc.com/news/world-middle-east-20768205

[85] https://www.passivetotal.org/

[86] *sonar-ssl*

[87] https://wordsecure.com/

[88] https://github.com/quasar/QuasarRAT/blob/master/Client/Core/Recovery/Browsers/InternetExplorer.cs

[89] See https://web.archive.org/web/20131207060523/https://velocityfiles.com/login.php and https://web.archive.org/web/20131207054158/https://velocityfiles.com/register.php

[90] http://templates.entheosweb.com/template_number/live_demo.asp?TemplateID=54257

[91] http://aax.me/1a732

[92] https://en.wikipedia.org/wiki/Emirates_Discussion_Forum

[93] http://www.echr.org.uk/?p=1104

[94] https://twitter.com/Ahmed_Mansoor/status/256142870896054273 and https://twitter.com/Ahmed_Mansoor/status/256144504116109312

[95] https://metrics.torproject.org/

[96] http://www.bbc.com/news/world-middle-east-20768205

[97] e.g., local portscanning from webpages with JS-Recon, determining web browser versions by testing JavaScript functionality, Tor Browser profiling bug, macro infection.

[98] e.g., Powershell remote shell.

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

[100] https://citizenlab.org/2015/12/packrat-report/

[101] https://citizenlab.org/2015/08/iran_two_factor_phishing/

[102] https://targetedthreats.net/

[103] http://www.latimes.com/nation/la-na-associated-press-lawsuit-20150827-story.html

One Comment

1.  Ken Nickerson
   Posted June 3, 2016 at 8:11 am | Permalink

   One of the best reads this year. Brilliant analysis, I am printing for a second “snail read” with a trusty highlighter. Thank you!