IntelCrawler

Syrian Electronic Army - Hacktivision to Cyber Espionage?

FOR PUBLIC RELEASE

March 20, 2014




IntelCrawler, info@intelcrawler.com (PGP), 13636 Ventura Blvd. #421 Sherman Oaks, CA 91423, www.intelcrawler.com

Table of Contents

Disclaimer

The research, findings, and analysis in this report are based on a combination of open and operative sources. To protect some victims and open cases, the non-disclosure of operative sources may leave some gaps in the linkage of some parts of the analysis. This report is solely the opinion of IntelCrawler LLC.

Executive Summary

IntelCrawler, a cyber-threat intelligence company based in Los Angeles, has been investigating the activities of the Syrian Electronic Army (SEA) since they first surfaced in 2011. In the beginning they seemed only interested in hacking to make political statements. But over time, as they gained notoriety and picked up technical resources and support, the SEA has evolved into the realm of global espionage, where some of their targets are “C” level executives at technology and media companies, allied military procurement officers, United States defense contractors, and foreign attaches and embassies.

Although the Syrian Electronic Army has used malware and sophisticated hacking tools, their standard method of operation is usually spear phishing, a craft they have perfected very well. In this report, you will see some high level technical people who may have fallen victim and had their email compromised. With this type of breach to email contacts and content, the SEA can send trusted emails from one company CEO to another or move laterally within the now compromised organization.

Many modern businesses’ spend millions of dollars on network security, protecting against emerging Advanced Persistent Threats (APT’s), new exploits, malicious code, and zero-day vulnerabilities, only to have a key executive compromised via spear phishing and essentially expose potential keys to the kingdom.

This report will show the speed and efficiently at which the SEA operates. Also outlined are their probable profiles, conquests, tools, tactics, and procedures and some indicators of compromise. We’ve laid out the hacktivision attacks chronologically and then moved to the cyber espionage attacks where the SEA has a specific agenda to acquire sensitive documents.

Many of the Syrian Electronic Army’s exploits and successes have gone unreported. There’s really no way to know exactly what they may have downloaded. But it’s clear when viewing the totality of their successful attacks, their reach and access is unparalleled.

In a public interview[1], the Syrian Electronic Army has noted that they are the most famous hacking organization in the world.

[1] Interview With The Syrian Electronic Army (https://www.youtube.com/watch?v=n8e2DIoQSwI)

Key Findings

The SEA hosted most of the stolen information on Syrian Telecommunication Operators hosting platforms, and also placed there malicious code and fake spear phishing pages for targeted attacks.

- On these servers were found gigabytes of stolen information, including their own SEA WEB-site backups;

- Having limited geopolitical relations, the bad actors started to organize bulletproof hosting platforms in anti-west jurisdictions such as Syria and Lebanon;

- Even in cases when the bad actors had some difficulties with placing malicious content, they used hacked WEB-resources of their own country in order to avoid any possible issues with other ISPs;

- Some of the hosting platforms they used were ordered virtually and paid for via bank transfers by people from other countries;

The lifecycle of some targeted cyber-attacks organized by the SEA was sometimes less than 1 hour, which confirms a high degree of sophistication and co-ordination.

- The preparation period for some attacks was approximately 3-5 days with deep surveillance of potential victim's employees and contacts;

- In order to arrange spear phishing campaigns, which were used in approximately 65% of the attacks done by SEA, there were clear defined roles of an intelligence officer and an offensive officer, which confirms a chain of command mentality;

- Their army-like battalion structure acting with a designated leader points to possible relationships with special services or intelligence agencies. After analysis of some of their actions, it was found that some of them didn't know each other personally and they interchanged nicknames during different periods.

- After the first compromised data was received by SEA, their members spent more than 7-12 days monitoring intercepted communications of the victims, in order to disseminate all data, which in turn was used against other victims.

The SEA seems focused only on US and specific geographical regions in the Middle East.

- More than 80 famous US corporations were hacked, with just approximately 30% of them revealed in the press by the bad actors. This selective reporting lends credence to their cyber espionage campaigns;

- The dynamics of interests of SEA have slowly changed to governments from the private sector;

- SEA has also targeted embassies, government, military and law enforcement communications, again which were not published by them because of potential state sponsorship and ongoing intelligence operation;

- Some of the past hacks and intrusions were explained from a political point of view, but in reality some provided deep access to sensitive intelligence data, such as the Viber and Tango mobile messengers hacks.

Besides sophisticated cyber-attacks, they engaged in a large scale social media campaign for promoting their cause.

- During 2013/2014 they have engaged more than 200 Facebook accounts and more than 20 Twitter accounts for their public page, which confirms their interest and need to cover and to promote own activities;

- Syrian Electronic Army became a brand supported by professional designers, hidden ideologists and social network marketing teams, replacing current Anonymous hacking activities across the world;

- Each of SEA members knows English, besides Arabic, which was used by some of them as the main language of communications.

Most of the instruments they have used are self-written and targeted on long-term cyber intelligence and offensive client-side vulnerabilities exploitation.

- Most of compromised e-mail accounts by them were forwarded to specially prepared registered e-mail accounts automatically alerting them of the new e-mails and encrypting them and transferring to other secure storages.

Why We Are Exposing It?

As IntelCrawler's' intimate investigation of the SEA pierced their veil of hacktivision, revealing compromised civilian and military personnel in charge of procuring sniper pads, night vision goggles, and WMD defense systems, it became apparent that the world might need to know.

By profiling the SEA members and exposing their cyber prints, indicators of compromise, tools, tactics, and procedures, we felt the report might help security researchers, MSSP's, and government investigators to mitigate attacks and plan future defenses.

As talented as these young hackers apparently are, they seem to have left some digital bread crumbs as clues. The collection of these crumbs i.e. cyber prints, narrows the probability of identifications, and more importantly, they may follow them the rest of their technology lives and career. The exposure and the databasing of these cyber prints, that never go away, may have long term consequences. Those concerns or consequences like traveling and working outside Syria were alluded to by the SEA in their TV interview.

Since the SEA has shaped facts in their press postings, we felt exposing how they selectively report for political reasons but hold back compromised intelligence or data related to cyber espionage shows their true motives.

The SEA has attacked Syrian websites and peaceful companies and organizations incurring significant reputational and economic losses, without any direct relation to the armed conflicts in Syria. So again their motivations are inconsistent with only a policy of hacktivision.

Spending more than a year of deep research, IntelCrawler released this report in hopes of exposing one of the most sophisticated cyber espionage campaigns of 21st century, targeting 18 different countries and 110 corporations.

SEA: Bad Actors Profiles

The Syrian Electronic Army consists primarily of 8 key technical leaders and various hidden supporters who have defined roster functions. These are their probable profiles.

“The Pro”

The Pro or Th3Pr0 is one of the most aggressive and experienced members in SEA, responsible for the majority of past hacks - the Leader of Special Operations Department of Syrian Electronic Army. He is also one of the more stealth members.

This bad actor first surfaced with the hack of the University of California Los Angeles (UCLA) website, which was defaced by him in July 2011. This date is the unofficial starting point of all SEA activities.

According to our analysis, the following person used various nicknames comingled with his name - The Pr0, Saqer Syria, Sy Team and al3rab. The last one is also associated with Arab Attack and Syrian Arab Army, which will be used in some of the projects by the SEA, which points to some collaboration between several groups.

№	Contact	Information
1	WEB-site	http://about.me/Th3Pr0 http://th3pro.pro
2	Twitter	http://twitter.com/Th3Pro_SEA https://twitter.com/ThePro_Sy https://twitter.com/SEATh3Pr0
3	LinkedIn	http://www.linkedin.com/pub/th3pr0-sea/[2]
4	Google Plus	https://plus.google.com/116471187595315237633/posts
5	Flickr	http://www.flickr.com/photos/th3pr0/
6	Foursquare	http://foursquare.com/user/29524714
7	Emails	syrian.es.sy@gmail.com syrianessy@gmail.com sea.wr4th@gmail.com th3pr0123@gmail.com pr0@hotmail.nl

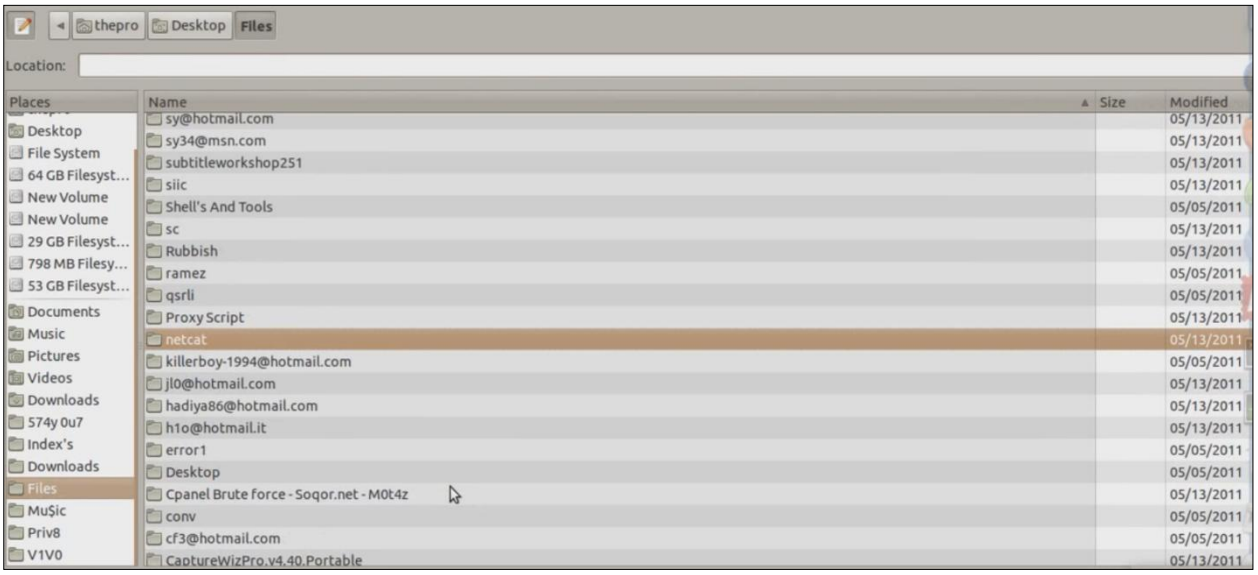
It is important to note that “The Pro” unknowingly and carelessly mentioned on his Google Plus page that he worked at the Syrian Electronic Army.

In one of his videos he disclosed several other e-mails, such as:

- sy@hotmail.com;
- sy34@msn.com (“Alammer Naser”);
- killerboy-1994@hotmail.com (“Ahmad”);
- jl0@hotmail.com;

[2] http://webcache.googleusercontent.com/search?q=cache:ZcyZ_5Up420J:www.linkedin.com/pub/th3pr0-sea/73/819/271+&cd=1&hl=en&ct=clnk&gl=ru

- cf3@hotmail.com (“koteba”)



The above e-mails will be used within the SEA by several team members in order to cloud their profiles.

“SyRiAn_34G13”

For example, with “sy34@msn.com” we will see this email in early defacements by “The Pro” and so called “SyRiAn_34G13″ (leet-speak for Syrian Eagle).

The e-mail was registered on “Alammer Nasser”, as well as Skype account “sy34-sy34” with “Naser” in details were linked with it. A bit later, a Romanian Security Team discloses the profile details of “SyRiAn_34G13” from their own community:

BONUS from the staff: After hunting for his "sy34@msn.com" e-mail in the grep pile, this turned up:

(507395, 'SyRiAn_34G13', 'd897913c95e6ac5d439c219db363fa57', 'VqygBQl4', 'FYKxfPqMZnuFDYFIJKWAVbWMIvegXJ77HJiyB1BgGHpblWuYaI', 'sy34@msn.com', 26, 0, 0.00, NULL, NULL, NULL, 2, NULL, 0, NULL, 1286748398, 1295553662, 1295406585, 1289771038, NULL, 0, NULL, NULL, NULL, '3-4-1991', 'all', NULL, NULL, 1, 0, 0, 0, 1, 0, 0, 'linear', 1, 1, 1, 1, 0, 0, 0, NULL, NULL, -5, 0, 2, NULL, NULL, 0, 0, 0, 0, NULL, '1**Inbox$%%$2**Sent Items$%%$3**Drafts$%%$4**Trash Can', NULL, 0, 0, 0, '82.137.200.5', '82.137.200.5', 1384761349, 1384761349, NULL, 16171, 1, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, NULL)

View Profile: SyRiAn_34G13 - Romanian Security Team
rstforums.com
SyRiAn_34G13 is a Registered user in the Romanian Security Team. View SyRiAn_34G13's profile.

Published IP address will refer to Halab in Aleppo, the largest city in Syria and serves as the capital of Aleppo Governorate, the most populous Syrian governorate. It is located in northwestern Syria 310 kilometers from Damascus.

IP Address	82.137.200.5
Location	SYRIAN ARAB REPUBLIC, HALAB, ALEPPO
Latitude & Longitude	36.201240, 37.161170 (36°12'4N 37°9'40E)
Connection	SYRIAN TELECOMMUNICATIONS ESTABLISHMENT
Local Time	10 Mar, 2014 12:30 PM (UTC +02:00)
Domain	STE.GOV.SY
Net Speed	(COMP) Company/T1

The Pro will release three more nicknames associated with his hacking activities.

SyRiAn Sh3ll V7[3] - http://pastebin.com/0X98Xuy0	
# Coders : # SyRiAn_34G13 : sy34@msn.com [Main Coder] . # SyRiAn_SnIpEr : zq9@hotmail.it [Metasploit RC] . # Darkness Caesar : doom.caesar@gmail.com [Finding 3 Bugs] . #// kinG oF coNTroL : y8p@hotmail.com [Translating Shell To Arabic] .	Syrian Hackers Team[4] SyRiAn GhOsT & SyRiAn SnIpEr i5e@Hotmail.Com & Zq9@Hotmail.iT

This is a new gang which will become a part of the SEA, adding two three members – “Syrian Gh0st”, “Syrian_Sniper” and “Darkness Caesar”. Before the SEA and Syrian Hackers Team, he was a member of so called “Team-SQL”[5].

[3] http://packetstormsecurity.com/files/author/9015/
[4] webcache.googleusercontent.com/search?q=cache:bOxUh4k-lVYJ:www.allmudugnews.com/index.php+&cd=1&hl=en&ct=clnk&gl=ru
[5] http://webcache.googleusercontent.com/search?q=cache:GDo7LeC7JaEJ:americandigest.org/archives/+&cd=2&hl=en&ct=clnk&gl=ru

Palestine Terrorist
Mahmoud SQL
SQL@Live.se

You Got Owned By Team SQL
There Is No Mercy In This Life
When Children Killed Every Day In Palestine Then No Mercy
We Have No Mercy 2 Now After See This Things
Jihad for the sake of Allah Even In Internet world
We Have To Kill 2 But By Other Way Because We Are Not Animals
I Will Back H3r3 Soon To Your System Again
Your System Has Been Bypassed Now
Make Your Security Sure Next Time
 # Then Wait Me To Hack Your System Again

#	Special Great For My Team	#
#	Team SQL	#
#	Mr. Sohayl	#
#	Mr. Danger	#
#	TNT HACKER	#
#	SyRiAn_34G13	#

Title: Joomla Component com_radio SQL injection vulnerability
Date: 27-4-2010
Author: Mahmoud SQL
Tested on: Linux
Email : SQL[at]Live[dot]Se

```
#####       ######    #
#           #      #   #
#  Mahmoud #      #    #
#####       #      #   #
 S     #      # Q    #    #   L
       #      #      #   #
#####       ######    #######
            #
           #
```

Dork : inurl:index.php?option=com_radio

Exploit :/index.php?option=com_radio&task=exibi_descricao&id=-289+uNiOn+SeLeCt+1,2,3,group_concat(login,0x3e,password,0x3e,email),5,6,7,8+from+chat_user--

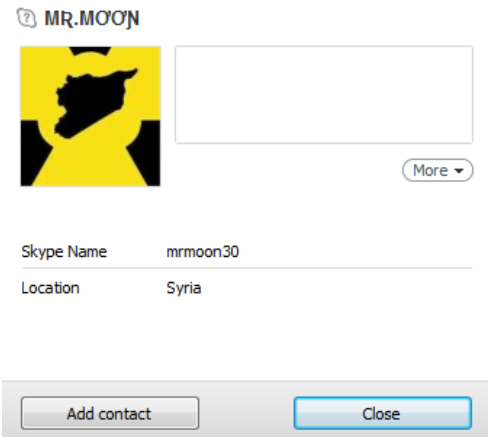
My Hom3 : www.team-sql.com/cc
Special Thanks For SyRiAn 34G13
Greats For : Team SQL [Mr SohayL ~ Mr Danger ~**SyRiAn 34G13** ~ Tnt HACKER] My Team & My Brothers
& Every Member In our Website & Net Own3r & Ma3sTr0-Dz & SHNKOOH & Harth

[www.arhack.net] & GoLdeN-z3r0 [www.sec-center]

Besides “Team SQL” and “Syrian Hackers Team”, some roots of the future SEA will be detected in so called “Sy Team” in one of the very old videos[6]. Another interesting fact is an e-mail cf3@hotmail.com from Th3Pr0 hard-drive will point at Mr.MooN.

HaCkEd By Sy-Team

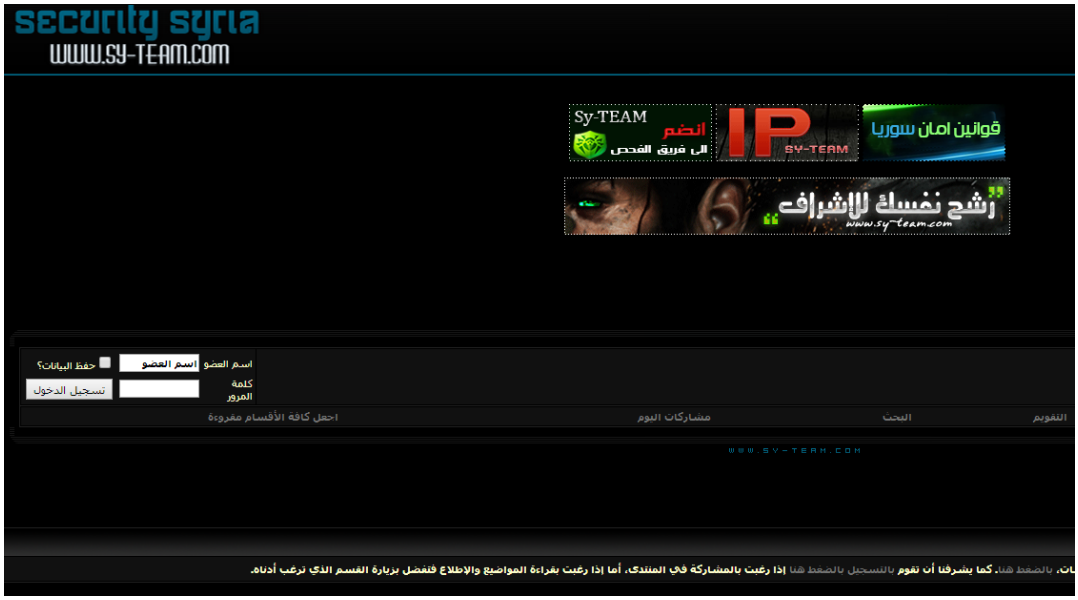
Mr.VeNuS
iji@HotmaiL.com
~!
Mr.MooN
Rg1@Hotmail.com



№	Contact	Information
1	E-mail	rg1@hotmail.com cf3@hotmail.com
2	Facebook	https://www.facebook.com/syria.sec
3	Skype	syria.sec koteba63

Together they will create their own underground hacking community for Syrian hackers which will be named “Security Syria” - http://www.sy-team.com/cc/index.php

[6] http://www.youtube.com/watch?v=q8oG5U47xVc&list=PL980BB3F7B74B349B



1,093	138	3 نقرات مدفوعة مسربة من طرف... بواسطة AnGeL HaCkeR Of SyRiA PM 04:55 03-24-2013
1,148	160	Sy-Team Sh3ll v1.0 بواسطة aboud-alshami اليوم AM 03:46
282	35	wordpress slovemedia بواسطة الاسطوره هنو اليوم AM 07:56
142	8	مسابقة اجمل اندكس اسلامي „|... بواسطة آلولد آلشرير PM 09:24 03-13-2013
187	20	23 فيروس !!! بواسطة زيزو الملكي اليوم AM 10:12
242	34	مشكلة دخول ضروري :(بواسطة ALMUTEM ALSyRiE اليوم AM 06:20
37	4	طرق مهاجمة العقول ... بواسطة alaasade PM 03:11 03-21-2013
14	2	تعريف الهندسة العكسية بواسطة تسر سوريا || SyRiAn EaGLE AM 09:44 03-13-2013

On March 12, 2014 the SEA website will move to another hosting ISP and will update own content, especially on the SEA team. “SyRiAn_34G13” will be named as Official Email Manager, “Young Syrian man who loved the SEA work and joined it, now he manages the official email of the SEA”, as announced on their website.

Through several of his emails he will reveal one new Syrian IP addresses:

IP Address	94.252.249.94
Location	SYRIAN ARAB REPUBLIC, DIMASHQ, DAMASCUS
Latitude & Longitude	33.510200, 36.291280 (33°30'37N 36°17'29E)
Connection	SYRIATEL MOBILE TELECOM
Local Time	10 Mar, 2014 06:35 PM (UTC +02:00)
Domain	SYRIATEL.COM.SY
Net Speed	(DSL) Broadband/Cable
IDD & Area Code	(963) 011
ZIP Code	-
Weather Station	DAMASCUS (SYXX0004)

Right after this leak “SyRiAn_34G13” will disappear from any press, social media and SEA related websites.

This fact helped to define that his identity is very important in the whole structure of SEA. In the leaked database from SEA there were also found several profiles with the same status field “realmann”, registered as the first 5 users:

- Admin2 (sy34@msn.com);
- Test (sy34@msn.com);
- 31 (wassemkortab@yahoo.com);
- ckjacketsthe (sf0725zq0330@dressmall.com) – two times;
- Adam MaqdiSsi (adam.maqdissi@hotmail.com).

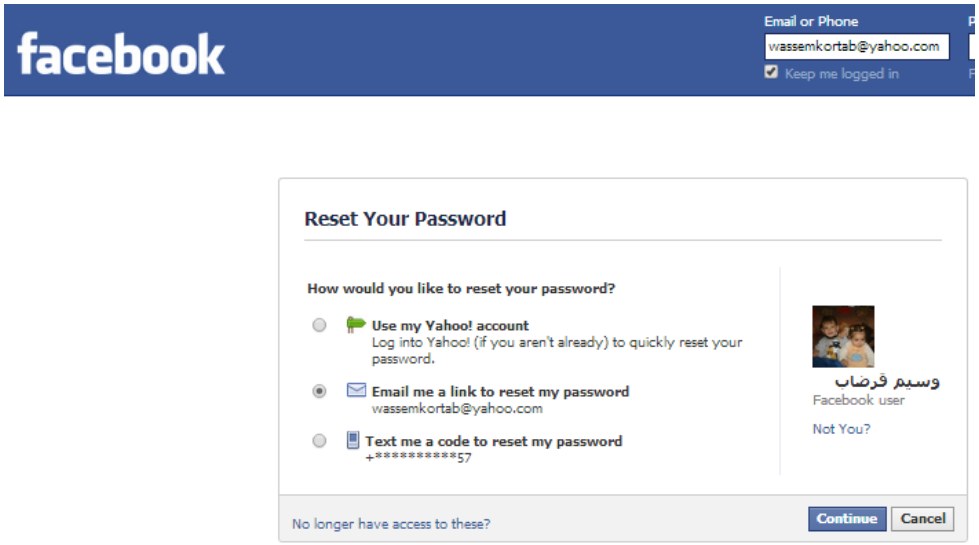
URL: http://pastebin.com/XScJzyRE

```
26. LOCK TABLES `users` WRITE;
27. /*!40000 ALTER TABLE `users` DISABLE KEYS */;
28. INSERT INTO `users` VALUES
29. (1,'admin','eafab3af77996160577b434e0d6adf7f','admin','male','2012-12-
    12','syria','b6f@hotmail.es','','','','jpg'),
30. (4,'admin2','31fd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
    00','','sy34@msn.com','','','not_published',''),
31. (18,'test','31fd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
    00','','sy34@msn.com','','','not_published',''),
32. (19,'31','وسيمfd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
    00','','wassemkortab@yahoo.com','','','not_published',''),
33. (3,'ThePro','33d5cbc6755c127cc7251932d0ec03d1','1','male','0000-00-
    00','Syria','admin@thepro.sy','','','not_published','jpg'),
34. (21,'ckjacketsthe','f35364bc808b079853de5a1e343e7159','super123','male','0000-00-
    00','','sf0725zq0330@dresssmall.com','','','not_published',''),
35. (22,'ckjacketsthe','31fd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
    00','','sf0725zq0330@dresssmall.com','','','not_published',''),
36. (23,'Adam MaqdiSsi','31fd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
    00','','Adam.MaqdiSsi@Hotmail.Com','','','not_published',''),
37. (24,'Adam MaqdiSsi','31fd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
    00','','Adam.MaqdiSsi@Hotmail.Com','','','not_published',''),
```

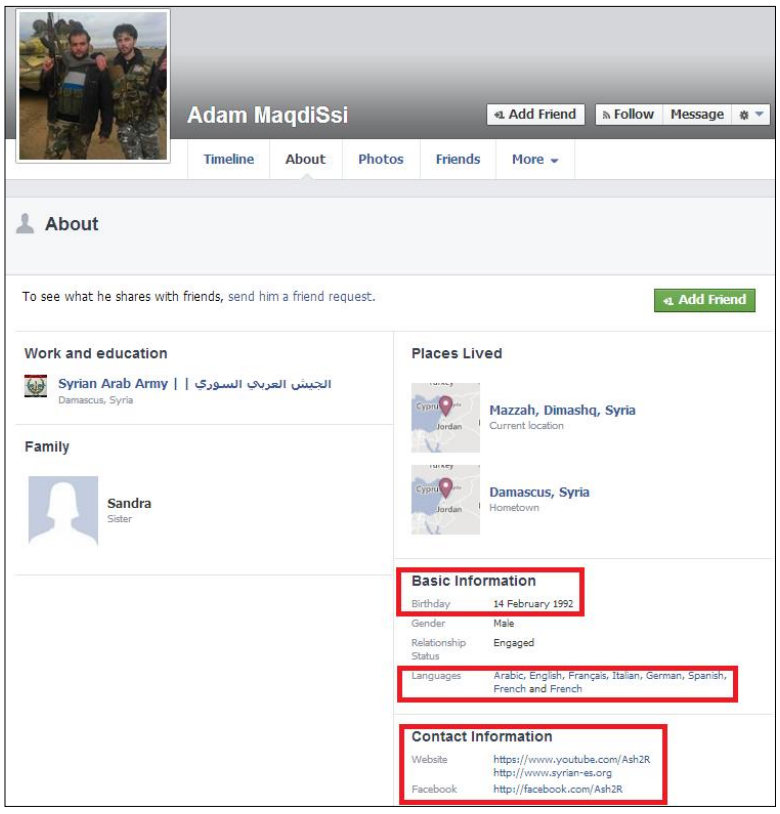
It means that the same person or a team tried to test web-application using different accounts placing quite similar details.

```
71. (1,'sy34@msn.com','realman','2012-06-22 15:05:18'),
72. (4,'sy34@msn.com','realman','2012-06-22 15:05:35'),
73. (18,'sy34@msn.com','realman','2012-06-22 15:05:46'),
74. (19,'wassemkortab@yahoo.com','2009929','2012-06-22 15:05:57'),
75. (3,'admin@thepro.sy','thepro4ever','2012-06-22 15:06:09'),
76. (22,'sf0725zq0330@dresssmall.com','super123','2012-06-22 15:06:38'),
77. (23,'Adam.MaqdiSsi@Hotmail.Com','7777777','2012-06-22 15:07:02'),
78. (24,'Adam.MaqdiSsi@Hotmail.Com','7777777','2012-06-22 15:07:24'),
```

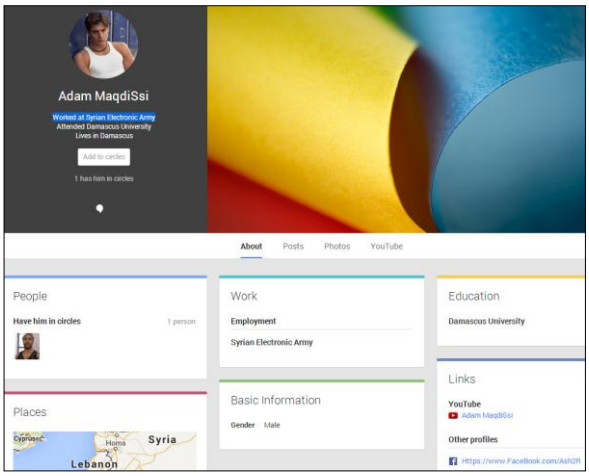
Using Facebook password recovery on this e-mail - wassemkortab@yahoo.com, was found a profile. The received information pointed to http://facebook.com/wassemkortab.

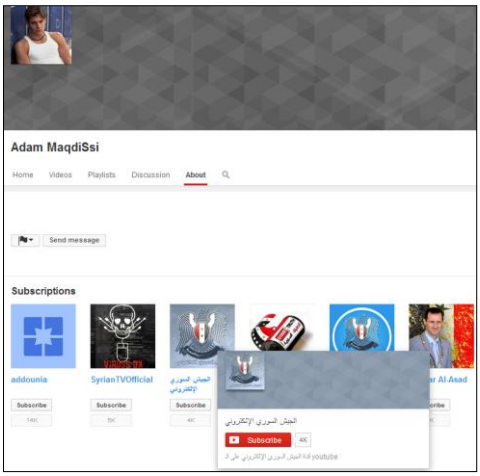


Adam Maqdissi has a profile on Facebook - https://www.facebook.com/Ash2R/about with a link to the old website of SEA – http://syrian-es.org.



Google Profile (https://plus.google.com/101992324227017134298/about) also points to this person referring to Employment in Syrian Electronic Army and education in Damascus University.





Both profiles are not supported anymore and were quite hidden from SEA.

The Pro may have been misidentified by the press, possibly confusing him with his friends – Ali Fahra[7] and another one from Syria,Habib Deeb. The first version seemed off base because of the age issues. Ali was mentioned in the first SEA domain "syrian-es.org" as registrant name, along with Mouhamed Shabaan, which was confirmed by WHOIS history:

SYRIAN-ES.ORG
Domain ID:D162194543-LROR
Domain Name:SYRIAN-ES.ORG
Created On:05-May-2011 05:09:33 UTC
Last Updated On:12-Nov-2012 11:55:37 UTC
Expiration Date:05-May-2013 05:09:33 UTC
Sponsoring Registrar:Network Solutions, LLC (R63-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:52904778-NSIV
Registrant Name:Ali Farha
Registrant Organization:Ali Farha
Registrant Street1:ATTN insert domain name here
Registrant Street2:care of Network Solutions
Registrant Street3:PO Box 459
Registrant City:Drums
Registrant State/Province:PA
Registrant Postal Code:18222
Registrant Country:US
Registrant Phone:+1.5707088780
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:c37pr3ny5tt@networksolutionsprivateregistration.com
Admin ID:53094902-NSIV
Admin Name:Mouhamed Shabaan
Admin Organization:Mouhamed Shabaan

[7] http://pastebin.com/GcPVz4S4

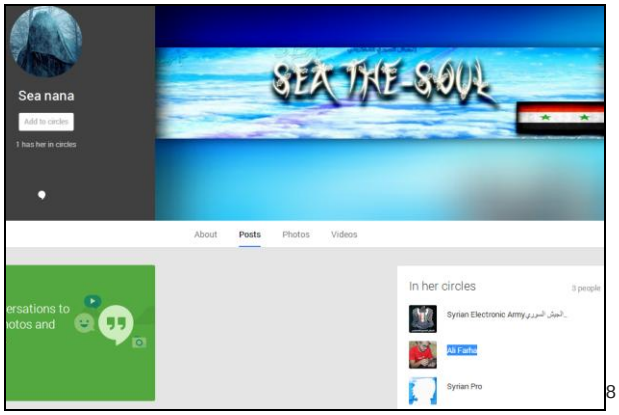
Admin Street1:ATTN insert domain name here
Admin Street2:care of Network Solutions
Admin Street3:PO Box 459
Admin City:Drums
Admin State/Province:PA
Admin Postal Code:18222
Admin Country:US

Later his identity will be covered using sanitized name “Syrian ES” and contact e-mail “sea.the.shadow@gmail.com” which refers to member of SEA – “Shadow”.

SYRIAN-ES.ORG

Domain Name:SYRIAN-ES.ORG
Created On:05-May-2011 05:09:33 UTC
Last Updated On:21-Mar-2013 06:21:10 UTC
Expiration Date:05-May-2013 05:09:33 UTC
Sponsoring Registrar:Network Solutions, LLC (R63-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:53557724-NSI
Registrant Name:Syrian ES
Registrant Street1:Damascus
Registrant Street2:
Registrant Street3:
Registrant City:Damascus
Registrant State/Province:
Registrant Postal Code:963
Registrant Country:SY
Registrant Phone:+963.0119955
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:sea.the.shadow@gmail.com
Admin ID:53557724-NSI
Admin Name:Syrian ES
Admin Street1:Damascus
Admin Street2:
Admin Street3:
Admin City:Damascus
Admin State/Province:
Admin Postal Code:963
Admin Country:SY
Admin Phone:+963.0119955
Admin Phone Ext.:
Admin FAX:
Admin FAX Ext.:
Admin Email:sea.the.shadow@gmail.com

Ali Farha is pretty well connected with the SEA in social networks and has pretty similar content of their ideology in his Twitter account and could act as a system administrator.



[8]

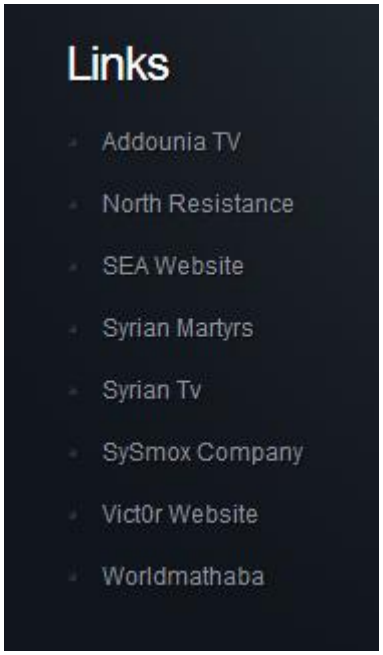
№	Contact	Information
1	VK	http://vk.com/id223151924
2	Twitter	https://twitter.com/ali_farha
3	Facebook	https://www.facebook.com/Ally.farha
4	About.me	http://about.me/Ali.Farha
5	Google Plus	https://plus.google.com/111097291456761184036/about

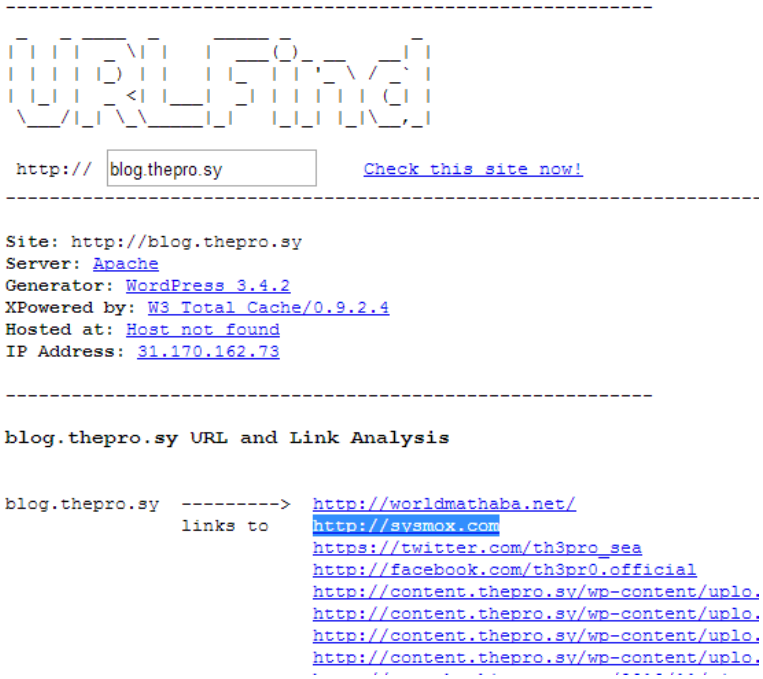
The second will be denied by “The Pro” in the press, explaining that it is his friend, but not him, and he doesn't want his name to be mentioned as an SEA member.

Another version will name Ammara Reda[9] as “The Pro” in the press and seems to be wrong once again, but it will uncover an interesting fact. Reda is from Morocco, from where “The Pro” apparently is too. He is working for a Moroccan penetration testing company known as “Sysmox”.

For some time, this company will have a direct link on the SEA and Vikt0r websites, as well as “The Pro” will create a mutual link[10] on them too:

[8] https://plus.google.com/118380274973539505251/posts
[9] http://pastebin.com/YFSEatW6
[10] http://webcache.googleusercontent.com/search?q=cache:OxIo-FP15QIJ:urlfind.org/?site%3Dblog.thepro.sy+&cd=10&hl=en&ct=clnk&gl=ru





Sysmox Twitter and Facebook will cover the SEA activities with rather remarkable speed. For example, right after Aljazeera will be hacked by The Pro[11] - 2012-01-29 20:40:32 Sysmox will publish it right after 9 minutes in own blog - http://sysmox.com/blog/hacked/syria-hackers-take-down-al-jazeera-english-website - 2012-01-29 20:49:00.

"The Shadow"

The second main nickname which was very visible on most of the defacements is "Shadow".

This person was involved in the first correlation between the SEA and some other hackers. For example, http://aaddejong.nl/r.htm was defaced by Iranian hacker Reza_0o0, and then by the Syrian Electronic Army.

[11] http://zone-h.com/mirror/id/16809132

№	Contact	Information
1	Twitter	https://twitter.com/3144_7 https://twitter.com/Th3Shad0w_SEA
2	Email	b-6f@hotmail.com b6f@hotmail.es sea.the.shadow@gmail.com

"Reza_0o0" reported and uploaded screenshots of the affected websites to zone-h.org, an online archive of defaced websites, on May 13, 2011. As of June 25, 2011 Reza_0o0 had reported a total of 945 defaced websites, of which 773 were mass defacements, since December 11, 2010.

The fact that these pages were defaced by both an Iranian entity and the SEA may indicate some kind of collaboration. The Shadow also left a link to the Arabic underground hacking forum http://www.aljyyosh.com .

Correlation between «Reza» (Iranian Hackers) and «The Shad0w» (SEA)

2010

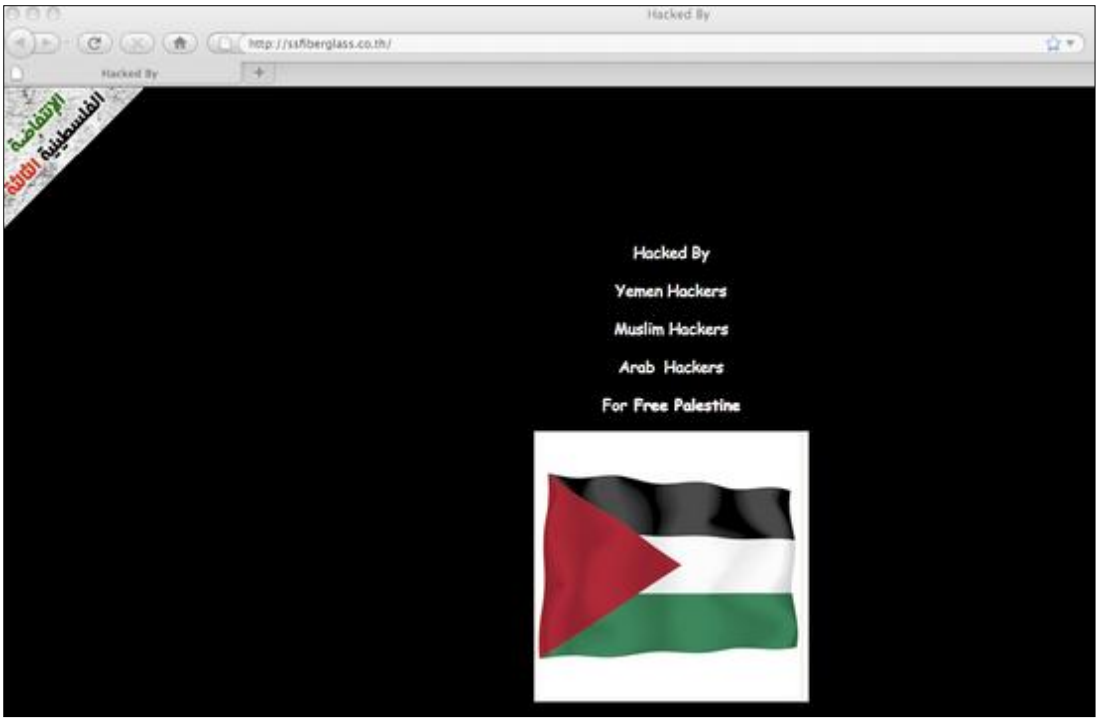
2011

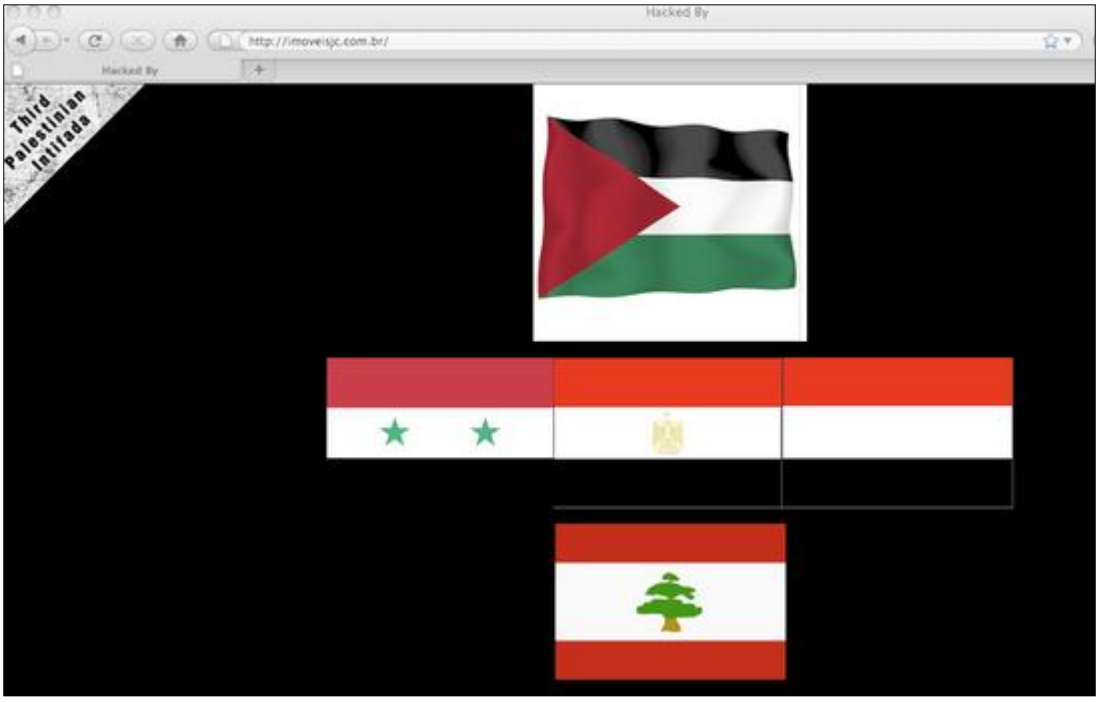
Following a specific signature, the Syrian Arab Army demonstrates a correlation between SEA and so called Arab Attack hacker and by the similar logo used in attacks on Israeli websites, which then had the signature “Hacked by SEA”.

In some hacks there was also a detected signature “Arab Attack” under the Brigade of the Syrian Electronic Army to commemorate the Naksa Day.

On June 12, 2011, the SEA claimed responsibility for compromising two more Israeli websites and said these targets were chosen as part of an operation to cleanse up the web from Israeli websites that promote hatred towards the Palestinian people. These and previous facts are pointing at multi-national linkage of the SEA with the Arabian World, Palestine, and Iran.

In June 2011 there was also detected a defacement page with quite specific Alliance of Palestine, Syria, Egypt, Yemen, and Lebanon hackers, and a banner that read Third Palestinian Intifada. According to IntelCrawler, these people will form a core for the future of the SEA.

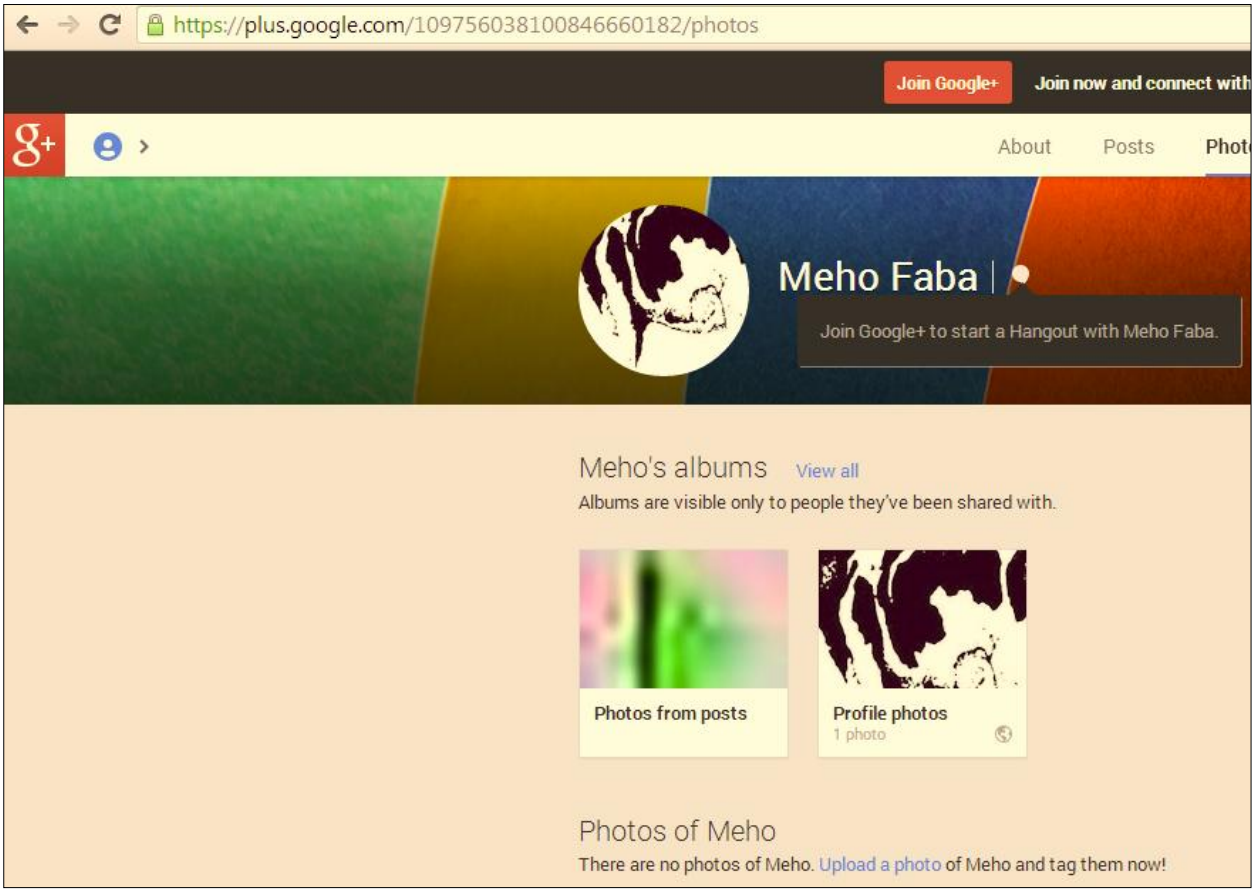

Hacked By
http://ssfiberglass.co.th/
Hacked By
Hacked By
Yemen Hackers
Muslim Hackers
Arab Hackers
For Free Palestine


Hacked By
http://moveisjc.com.br/
Hacked By
Third Palestinian Intifada

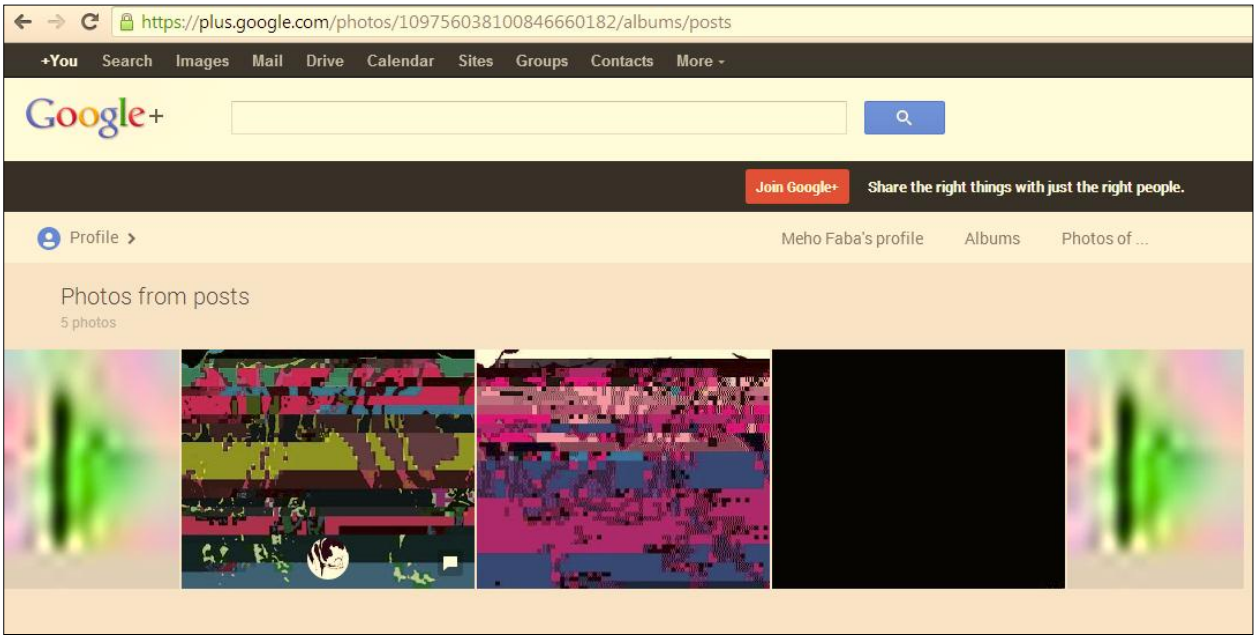
“Shadow” mentions current powers in the SEA, including Iranian hackers:

Using operatives, an e-mail from “Meho Faba” contains a specific encrypted attachment looking like steganography which was forwarded to the SEA and various embassies of Iran.

“Meho Faba” as outlined at Google Profile, has absolutely the identical encrypted pictures uploaded to one of the albums.



It seems to be that it was one of the secure covert channels to transfer information between specific contacts close to the SEA.



Right after the SEA resources will be hacked by Anonymous, the leak will also explain the links between several of contacts of SEA key members, including “The Shadow”:

URL: http://archive.is/dPIs6#selection-9.7810-9.7814

```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES
(1,'admin','eafab3af77996160577b434e0d6adf7f','admin','male','2012-12-
12','syria','b6f@hotmail.es','','','','jpg'),
(4,'admin2','31fd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
00','','sy34@msn.com','','','not_published',''),
(18,'test','31fd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
00','','sy34@msn.com','','','not_published',''),
(19,'وسيم','31fd0156202830c37a5d8c7f445e7084','realmanm','male','0000-00-
00','','wassemkortab@yahoo.com','','','not_published',''),
(3,'ThePro','33d5cbc6755c127cc7251932d0ec03d1','1','male','0000-00-
00','Syria','admin@thepro.sy','','','not_published','jpg'),
```

```
(46,'The
Shadow','ae653896176d10c9be6e58feceb07505','123qwe123qwe','male','0000-00-
00','syria','b-6f@hotmail.com','','','not_published',''),
(47,'ailaemead
ailsyria','2cfcb659ce80505c6b614182c77c58e7','hkrsyria14789','male','0000-00-
00','','hkrsyria000@hotmail.com','','','not_published',''),
(48,'احمد','81a71d15e0e7f88eab5ad63522c9115e','algerie','male','0000-00-
00','','videocam@live.fr','','','not_published',''),
(49,'SYrain
EAgje','92ba1a120b3210e180fe1e0ea83f9f44','abcdef_9toy','male','0000-00-
00','','s.syrianeagle@hotmail.com','','','not_published',''),
(50,'الليث1992','0a7c32f6b341995170b6921e0cba21da','1992011','male','0000-00-
00','','ali19921953@hotmail.com','','','not_published',''),
(51,'ThE SyRIaN
EaGle','0f5f92e30ec593b0e99add3dcaaf0ea9','ab12cd34_ef567','male','1995-01-
03','aleppo','zd.hammodah@hotmail.com','','','not_published',''),
```

Having very similar e-mails “b6f@hotmail.es” and “b-6f@hotmail.com” it becomes clear that the “The Shadow” was one of administrators of the SEA resources. Two Skype accounts will refer to “b-6f@hotmail.com”:

- Sea.shadow3 (Anderson, USA);
- The.shadow21 (Homs, Syria).

This e-mail will also disclose the links of “The Shadow” with hackers from Yemen, Saudi Arabia and Palestine within the hacking crew called “Aliyyosh Team”: lightspringspilates.com (deface).

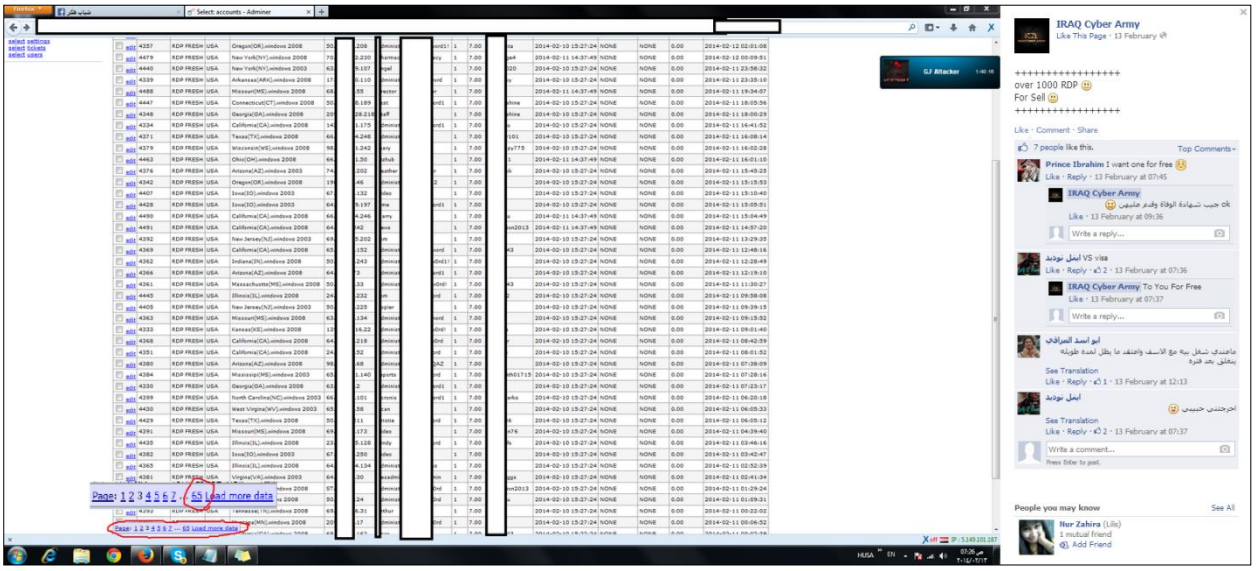
№	Bad Actor	Contact	Country
1	Black.Jaguar	bg_@hotmail.com	Yemen
2	Adsdely-Scorpion	asdelylord@hotmail.com	Palestine
3	She!! Access	i-8u@hotmail.com	Palestine
4	Mr.Snake	b-8g@hotmail.com	Saudi Arabia
5	The Shadow	b-6f@hotmail.com	Syria

The group was founded around May 16th 2013, which explains that possibly “The Shadow” was engaged by the older SEA.

This newer hacking team has very close relations to Iraq and links with so called “Iraq Cyber Army”, which looks very similar to “Syrian Electronic Army”.

https://www.facebook.com/AljyyoshTeam	https://www.facebook.com/IraqCyberArmy
	

The commonality of the attacks is also similar to the SEA – the US and Israel.



One of the detected posts[12] of selling of 1 000 US hacked dedicated servers in various States, including California and Oregon, disclosed the real IP address of one of the leaders, confirming their physical location in Iraq:

IP Address	5.149.101.187
Location	IRAQ, BAGHDAD, BAGHDAD
Latitude & Longitude	33.340580, 44.400880 (33°20'26N 44°24'3E)
Connection	PURE LINE CO. FOR TELECOMMUNICATIONS & INTERNET LTD.
Local Time	10 Mar, 2014 03:40 PM (UTC +03:00)
Domain	PLCIQ.COM
Net Speed	(DSL) Broadband/Cable
IDD & Area Code	(964) 0770

Such close affiliation explains the ranges of attacks by the SEA as they could be done with the help of other hackers from Eastern countries hired by the SEA or using shared resources. The

12

https://www.facebook.com/IraqCyberArmy/photos/a.479670008820300.1073741827.479172488870052/516109325176368/?type=1&theater

possible linkage here shows that ideological “Electronic Armies”, when successfully organized for hacktivision, may escalate to other motives and receive state sponsored support for various cyber intelligence and espionage operations.

“Tiger”

“Tiger” is one of the more stealth and hidden members of the SEA.

№	Contact	Information
1	Google Plus	https://plus.google.com/116330048991143322272/about
2	Gmail	tiger.tiger248@gmail.com
3	Skype	tiger.white20

His Skype location will point to Tartus. After the Reuters hack, he will release the following post on The Verge: “It’s the one army that I feel I’m more productive than”[13].

On Thursday July 5, 2012, WikiLeaks began publishing the Syria Files – more than two million emails from Syrian political figures, ministries and associated companies, dating from August 2006 to March 2012.

This extraordinary data set derives from 680 Syria-related entities or domain names, including those of the Ministries of Presidential Affairs, Foreign Affairs, Finance, Information, Transport and Culture.

Email-ID	2101305
Date	2011-04-16 09:13:09
From	gk005@hotmail.com
To	imfarhat@gmail.com, br280@mail.sy, tiger.tiger248@gmail.com, n.kabibo@mopa.gov.sy, raghadmah@yahoo.com, ibrahimmousawi@gmail.com, reem.haddad@gmail.com, ghassanshami1@hotmail.com, sdc@net.sy, gassanabdellah@yahoo.com

G.KANDIL

[13] Thomson Reuters Twitter account flooded with pro-Assad cartoons in Syrian Electronic Army hack - http://www.theverge.com/2013/7/29/4569776/thomson-reuters-twitter-account-hacked-syrian-electronic-army#175725745

Email-ID	2071072
Date	2011-07-13 11:34:00
From	gk005@hotmail.com
To	minister@moi.gov.sy, tiger.tiger248@gmail.com, abdulrahimad@yahoo.com, mfsamaha33@hotmail.com, ibrahimmousawi@gmail.com, mafif2@hotmail.com, buthainak1@hotmail.co.uk

مع تحيات غالب قنديل
009611366969 : هاتف المكتب
00961-3-535371: هاتف خليوي

Attached Files

#	Filename	Size
323583	323583_موضوعان عن سوريا ولبنان.doc	47.5KiB

One of published e-mails from gk005@hotmail.com will be sent to several e-mails, including Tiger and contacts in MOI of Syria and Ministry of Presidential Affairs (mopa.gov.sy). Does it mean that a member of the SEA has some type of relationship to government entities of Syria?

Both e-mails were sent from Ghaleb Kandil, a Lebanese journalist, discussing in press and TV some anti-US topics.

№	Contact	Information
1	Twitter	https://twitter.com/ghalebkandil
2	Gmail	gk005@hotmail.com
3	Skype	ghaleb.kandil
4	Facebook	https://www.facebook.com/gkandil

It may also possibly explain why the interview of the SEA was done on Lebanon TV channel Al Mayadeen (Arabic: الميادين; English: The Squares), which is a pan-Arabist satellite television channel launched on June 11, 2012 in Lebanon.

Another contact in copy - Ibrahim Mousawi (also spelled Moussawi, El-Moussaoui, ar: إبـ راهيم الـمو سوي) may be a Lebanese journalist and Hezbollah media relations officer. Why is a possible SEA member linked via email with a possible Hezbollah member?

One new Lebanese contact seems to have appeared in the copy – "Mfsamaha33@hotmail.com", possibly related to Michel Samaha (aka Mishal Fuad Samahah

and Saadah Al Naib Mishal Fuad Samahah; born September 9, 1948) might be a former Lebanese intelligence operative, deputy, and former minister of information and tourism. Samaha is known for his pro-Assad regime views. and is described as silver-tongued politician. He was one of the pro-Syrian Lebanese officials who were sanctioned in 2007 by the United States for alleged contributing to political and economic instability in Lebanon. Subsequently confessing to the aforementioned terrorist actively, Samaha was on 17 December 2012 listed by the United States as a global terrorist under section 1(b) of Executive Order 13224.

Does it mean that "Tiger", a SEA member was connected with Lebanon special services?

The last cc'd email address seems interesting – "Buthainak1@hotmail.co.uk" - Dr Bouthaina Shaaban Special Advisor to President Bashar al Asad President of the Syrian Arab Republic.

A similar situation with emails in copy exists with "Mr.MooN" and the e-mail "cf3@hotmail.com", which was on "Th3Pr0's" hard-drive, also found in the Syrian WikiLeaks Files along with embassy contacts of Syria in various countries and people from the Syrian government.

Date	2011-10-03 05:34:08
From	af5149@gmail.com
	capt.jawhar68@gmail.com, eissa_alleji@yahoo.com, careerme7000@yahoo.com, dmcus@dfait-maeci.gc.ca, dianajabbour@yahoo.com, dagher@net.sy, chawki@scs-net.org, damamb@um.dk, damascene@mail.sy, damascus@embassy.mzv.cz, churbaji_hashem@hotmail.com, camiranex-52@hotmail.com, central@alalmiah-ex.com, durrat-alsham@mail.sy, eden1@mail.sy, daadouche@net.sy, contract@mhe.gov.sy, chadan.naji@gmail.com, dr.ihabalzarrad@hotmail.com, dmloubani@yahoo.fr, chihabi@gmail.com, dr.j.massoud@hotmail.com, dror@scs-net.org, eiadsyr@yahoo.com, contact@cshs-syria.eu, cairoembassy@dfa.ie, chinaemb_sy@mfa.gov.cn, dpoison13@hotmail.com, easir1@yahoo.com, diplobel@net.sy, echilesy@scs-net.org, chrei-ah@scs-net.org, dr.abedyakan@gmail.com, dawwouds@scs-net.org, Damascuseca@state.gov, droubihassan@hotmail.com, cyrrhus@net.sy, classic.group@hotmail.com, chairman@GeminiGrp.net, dgam@dgam.gov.sy, dream_love2040@yahoo.com, chinaconsul_ax_eg@mfa.gov.cn, drengsattar@yahoo.com, dralkhalil@hotmail.com, chihadeve@hotmail.com, dunia@net.sy, ecvacationsy@ureach.com, elitetour@net.sy, chamitravel@net.sy, damascusman@hotmail.com, drsabdeen@hotmail.com, eidou84@hotmail.com, dr.h.jawish@mail.sy, elc.top@gmail.com, Eah@mail2007.com, easirl@yahoo.com, dakconsultant@yahoo.com, cmlc@bcs.gov.sy, claire@scs-net.org, director@lite-tech.co.uk, dlyakout@hotmail.com, dmhali@hotmail.com, doaamisr@yahoo.com, dolle@iamm.fr, d23@mhc.gov.sy, egypt_sbes@hotmail.com, drsamiram@hotmail.com, drsamiram@asu.edu.jo, ecosalex@yahoo.com, drtalibali_1947@yahoo.com, drtalib_ali@yahoo.com, Coop-fo@rd.gov.sy, d23@mho.gov.sy, dr.s.saadi@hotmail.com, chouiaseif2@yahoo.fr, councilhe@mhe.gov.sy, cnt@defense.tn, eghanem@aec.org.sy, elfadel@us.ibm.com, campbell@cubrc.org, derradjidal@yahoo.fr, connell@ncl.ac.uk, Dr_kismat56@yahoo.com, dr-m-gha@scs-net.org, dr.m.gha@scs-net.org, Chouia_mld@yahoo.fr, damaziz@yahoo.fr, drnabilssharif@yahoo.com, chabbi_chemrouk@yahoo.fr, cheri-ah@scs-net.org, cairo2000cairo@yahoo.com, cairo-cs@international.gc.ca, cairoparep@yahoo.com, cairope@tedata.net.eg, casanovas_x@hotmail.com, casio@yahoo.com, cassilas.khalil@gmail.com, cat_cozma@hotmail.com, catelolo86@yahoo.com, cavalirtravel3@hotmail.com, cccooo@hotmail.com, ccrssrigat@yahoo.com, cdicenter@hotmail.com, cdjaroueh@yahoo.com, cell2shop@gmail.com, cell2shop@hotmail.com, cell2shop47@yahoo.com, cellularcitycompany@gmail.com, cena.saeed@gmail.com, center@embjapan.org.eg, centre4444@gmail.com, cepnihasan@gmail.com, cerato.323@yahoo.com, cesalamica@gmail.com, cf3@hotmail.com, cgfcaire@link.net, cgspalejandria@mail.mae.es, ch.abou@scs-net.org, chaimahakam@hotmail.com, chakkam@gmail.com, chamecoptour@hotmail.com,

“Soul”

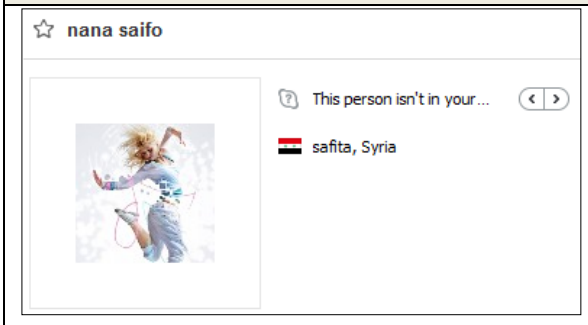
A quite popular member, but seemingly not a leading member.

THE SOUL

1	Twitter	https://twitter.com/sea_the_soul
2	Email	nagham_saifo@hotmail.com
3	Skype	nana.saifo1 nana.saifo
4	Google Plus	https://plus.google.com/118380274973539505251/posts

After a created profile on VK.com, it seems that this profile might be a female. But the SEA website explains that it is male in some texts. Soul’s functions were mainly targeted on graphical design and social media support, possibly maintaining the activity of SEA in blogs, Twitter and FB.

The Soul seems to be an original member of the SEA. She may manage the official SEA Facebook page.

Skype Profile	VK Profile
	

“Vikt0r”

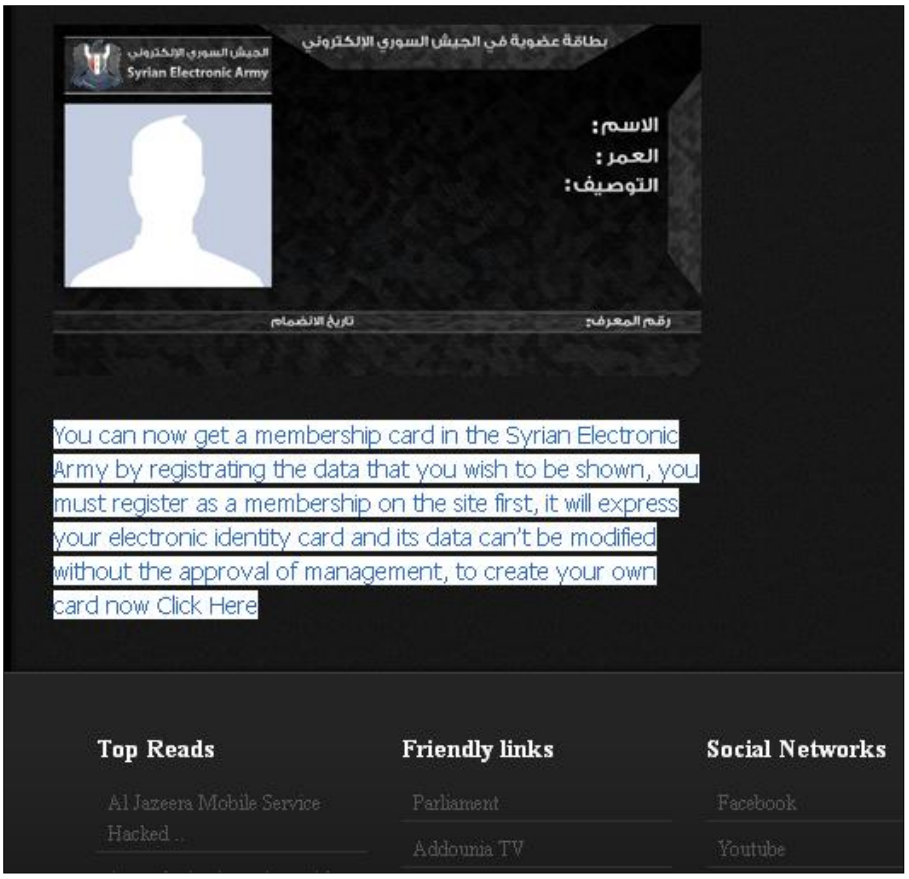
In the honor of this person, SEA has named one of their battalions. He is also a Member of Special Operations Department (SOD) in Syrian Electronic Army Team.

№	Contact	Information
1	Facebook	https://www.facebook.com/SEA.Vict0r.5 https://fb.com/SEA.Vict0r
2	Twitter	https://twitter.com/Vict0rSEA https://twitter.com/Vict0r_Fans
3	Email	victor@thepro.sy
4	Website	http://victor.thepro.sy

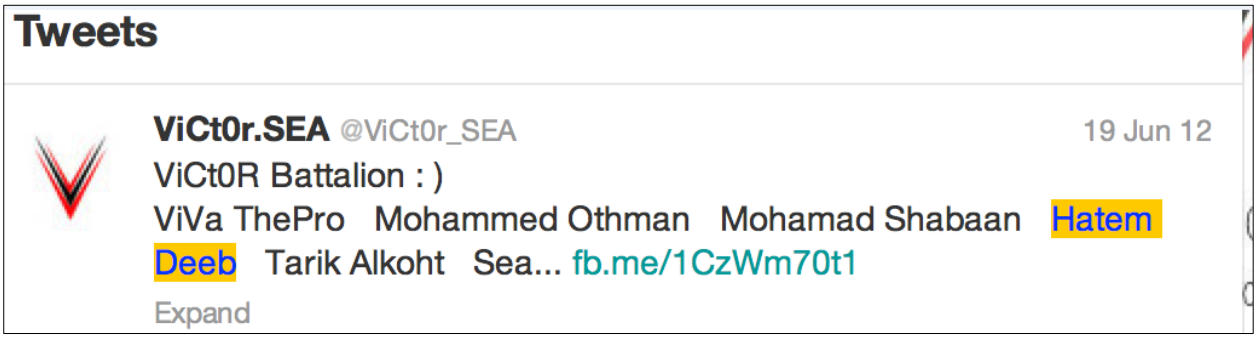
In June 2012 he revealed an interesting fact about the SEA offering special membership cards for SEA members.

It is not clear for the motive behind this offering, but it was well promoted through one of the first SEA websites – Syrian-es.org[14]. Of note, the original name of the future of the SEA might be “Syrian Electronic Soldiers” (Syrian-ES).

[14] http://web.archive.org/web/20130114222745/http://syrian-es.org/



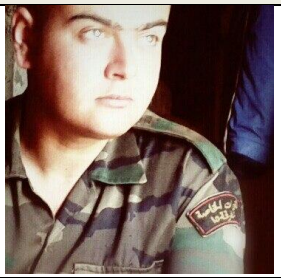
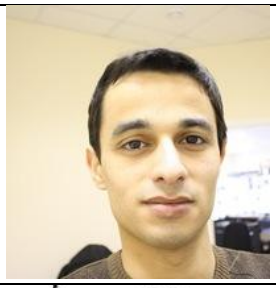
In one of the posts in 2013 he has published some of the nicknames and possibly the real people related to the SEA activities of his "Battalion".



Besides "The Pro" these names appeared:

- Mohammed Othman;
- Mohamad Shabaan;
- Hatem Deeb;
- Tarik Alkoht.

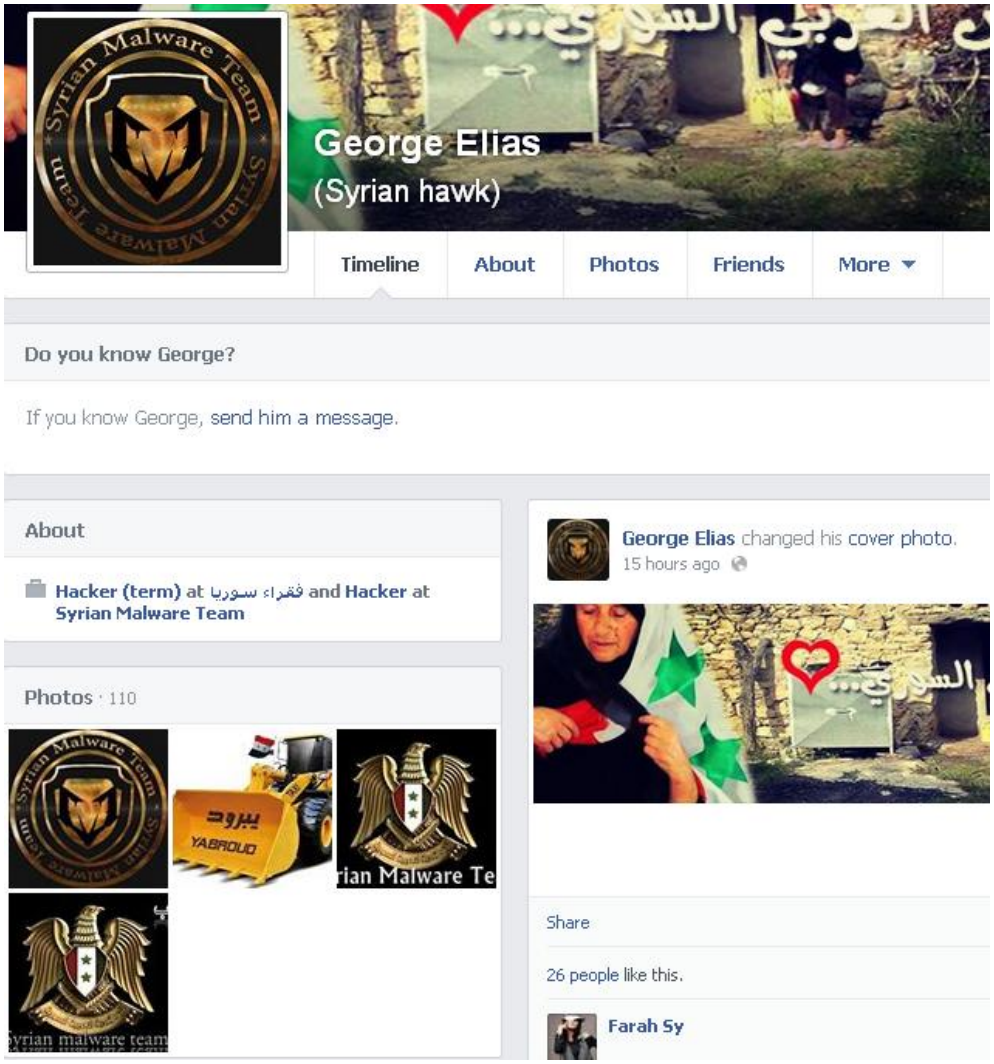
Most of them will be identified in the social network VK.COM (Vkontakte), linked between each other as friends. September 2013 will create own group - http://vk.com/syrianelectronicarmy.

№	Name	VK Profile	Foto
1	Abo Ziad (Tarik Alkoht)[15] http://www.tarikalkoht.com/	http://vk.com/id241738508	
2	“Sea The-Soul”	http://vk.com/sea.th3.soul	
3	Hatem Deeb	http://vk.com/hatemdeeb	
4	“Sea The-Shadow”	http://vk.com/sea.theshadow	

“Syrian Hawk”

One of the persons “liked” at - http://www.tarikalkoht.com/ is George Elias, having the nickname “Syrian Hawk” (https://www.facebook.com/moony.elias).

[15] Friend of Pr0 on https://plus.google.com/108581697608639774074/posts



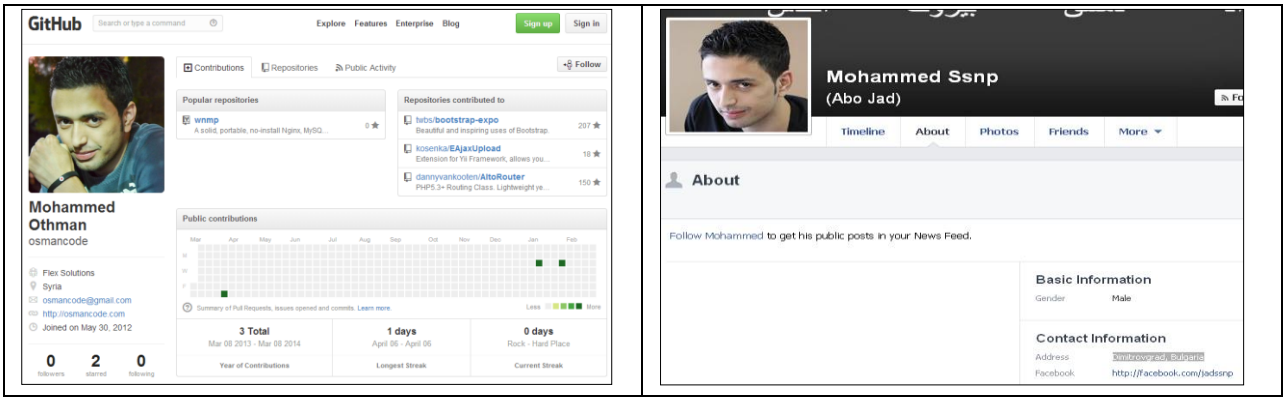
Then this person will join the Syrian Electronic Army: https://twitter.com/Hawk_syr

For some personal reason he will withdrawal from it in 2012. It seems to be that this person would love to develop their own beginning with the Syrian Malware Team - https://www.facebook.com/malwareteam.gov.org.sy, which is also naming themselves as “Syrian Hawks”. Some of their members (https://www.facebook.com/syrian.malware1/about) are also linked with INDIAN HACKERS.

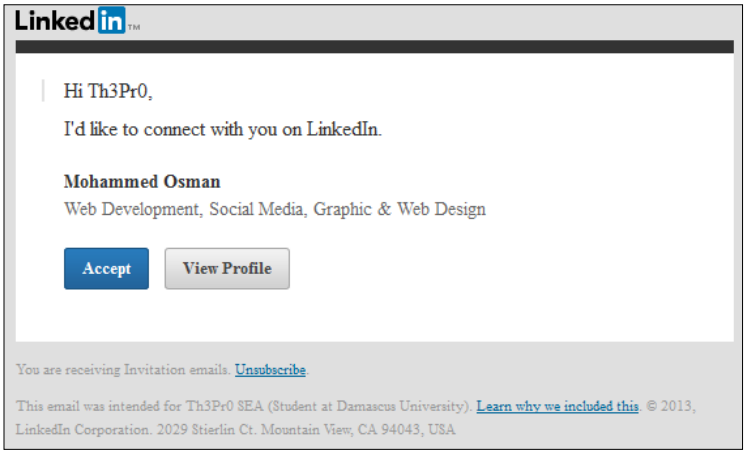
He also seems to have some relationship to the person “Tiger” - https://www.facebook.com/syrian.tiger.161?fref=pb&hc_location=profile_browser. One of the possible common denominators among some SEA members is a connection to Tartus, with some having education later in University at Damaskus.

“Osmancode”

Mohammed Osman (Othman) or “Osmancode” is allegedly a professional WEB-master and designer, who possibly managed all the design and WEB-applications programmed for SEA. “I am a virtuoso web designer looking around for unique palettes of life. My efforts depict an amalgamation of creativity with sheer hard work poised by my portfolio” - osmancode.com.



A bit later, he will rename his own Facebook account to https://www.facebook.com/jadssnp naming himself as Mohammed Ssnp (Abo Jad), living in Dimitrovgrad, Bulgaria. According to some operative information Mohammed was possibly hired by SEA for some graphical works and coding.



Besides evolving and co-mingled nicknames, it seems that the structure and members of the SEA has changed several times. They also modified their website and have added additional resources, including social media communities and pages.

In order to bolster new power and add energy to the SEA, they started what constitutes a virtual academy to recruit and educate sympathizers on how to use Denial of Service (DoS) software and computer exploitation and infiltration techniques.

The group posted an announcement on Facebook seeking recruits who speak different languages, and provided an email address for interested individuals to send details and times of availability.

One of the Facebook pages that demonstrate resources for computer exploitation and infiltration techniques belongs to a group calling them the Syrian Hackers School.

An interesting coincidence during this period of time is that National Agency for Network Services of Syrian Government[16] will publish a post that they are interested in hiring full-time and part-time experts and specialists in the field of information security and ethical hacking.

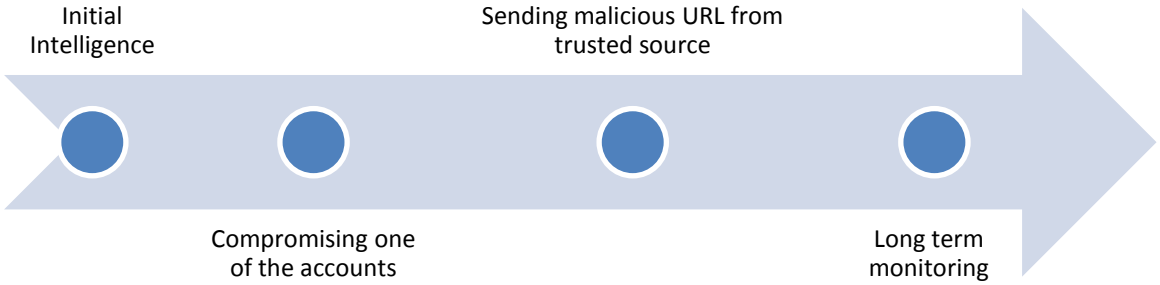
[17]

[16] http://nans.gov.sy/
[17] http://translate.google.com/translate?sl=ar&tl=en&js=n&prev=_t&hl=en&ie=UTF-8&u=http%3A%2F%2Fwww.moct.gov.sy%2Fmoct%2F%3Fq%3Dar

SEA: Attacks Timeline

SEA: The Style of the Attacks

The SEA will base the majority of their attacks on various spear phishing techniques. Besides corporate and government e-mail accounts, they will also actively attack Gmail.com and Hotmail.com of interested persons.



One of the most interesting attack vectors was used against Gmail 2-Step Verification by doubled spear phishing attack, when the user received the fake URL to Gmail authentication password page.

Then the attacker filled in the intercepted password to Gmail, waiting for the sent SMS code. The same phishing page redirected user to fake SMS Authentication page, where user placed received SMS code to his telephone and it was immediately intercepted by the bad actor.

Gmail account interception Template 1
X-PHP-Script: **accounts.igoogle.hostoi.com/AuthLogin.Service** for 66.37.35.162 Message-Id: <20140210173937.7A45115FD70@srv34.000webhost.com> Date: Mon, 10 Feb 2014 12:39:37 -0500 (EST) From: a7779409@srv34.000webhost.com X-Spam: Not detected X-Mras: Ok X-DMARC-Policy: no

X-Mru-AVCheck: false
X-Mru-Authenticated-Sender: uid:7779409@srv34.000webhost.com

Gmail account interception Template 2

X-PHP-Script: **accounts.googlecom.comyr.com/Service.Login** for 173.212.194.82
Message-Id: <20131228092101.D33A69A0F9@srv24.000webhost.com>
Date: Sat, 28 Dec 2013 04:21:01 -0500 (EST)
From: a5712017@srv24.000webhost.com
X-Spam: Not detected
X-Mras: Ok
X-DMARC-Policy: no
X-Mru-AVCheck: false
X-Mru-Authenticated-Sender: uid:5712017@srv24.000webhost.com

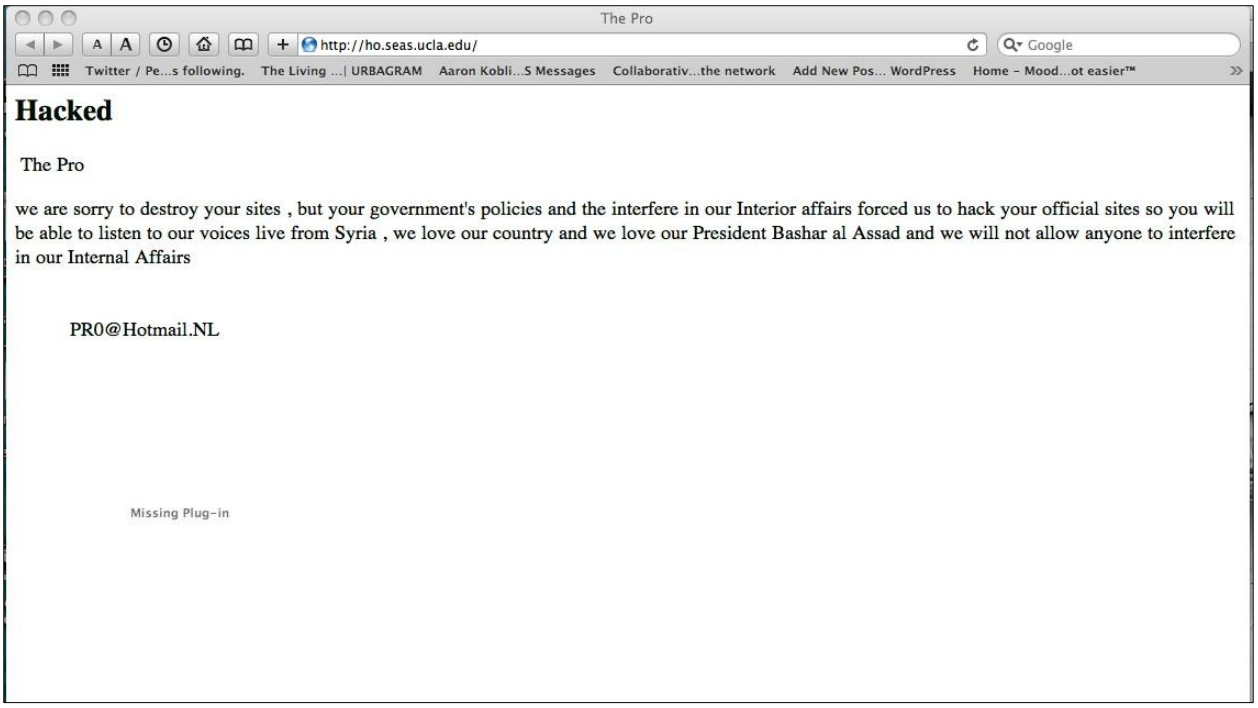
Gmail SMS interception

X-PHP-Script: **accounts.igoogle.hostoi.com/SMSAuth.Service** for 50.193.119.6
Message-Id: <20140210173948.DC34B15FE23@srv34.000webhost.com>
Date: Mon, 10 Feb 2014 12:39:48 -0500 (EST)
From: a7779409@srv34.000webhost.com
X-Spam: Not detected
X-Mras: Ok
X-DMARC-Policy: no
X-Mru-AVCheck: false
X-Mru-Authenticated-Sender: uid:7779409@srv34.000webhost.com

Some of the compromised e-mail servers were linked with Google Mail, which provided to bad actors high level of efficiency.

July 6, 2011 - UCLA

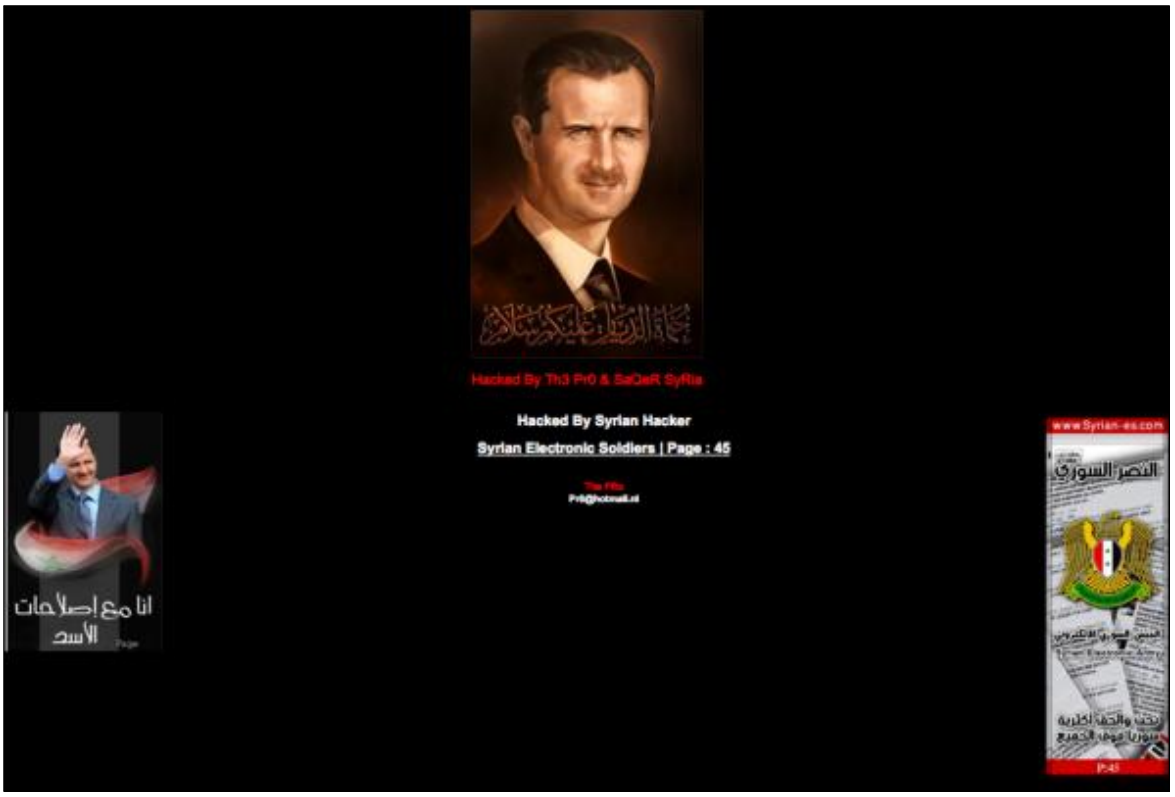
At the beginning of July 2011 the first successful cyber-attack was organized by the SEA. The ideologists of the SEA have chosen a quite famous American University - UCLA, which was the first step for promoting their activities.



For that time, the press and other officials couldn't foresee future attacks and intrusions. The group didn't use any of SEA official symbols, and "The Pro" positioned himself as a single hacker.

July 24, 2011 – Anonplus

The alternative social network established by famous hacking group Anonymous was hacked by SEA. According to SEA leaders, it was the first follow up to defacement of the Syrian Ministry of Defense by Anonymous as a sign of support of rioters.



Although previously hacked by the SEA, one of the new hacks was done in August of 2011. It's the first time when the SEA used the official abbreviation Syrian Electronic Army in public.

Besides The Pro, the bad actor with nickname "SaQer" Syria has also taken responsibility for the attack, but the used slogan Hacked by Syrian Hacker was still evidence of a single person. It is possible that the SEA was searching for new members to show an official group of coordinated people, but had no resources for it, which may explain why that named person disappeared from SEA activities after some time.

September 26, 2011 – Harvard University

Along with a picture of Syrian president, Bashar al-Assad, the hacked home page showed a message saying the "Syrian Electronic Army Were Here". A further message made terror threats against the United States and criticized its opposition to the Assad regime.

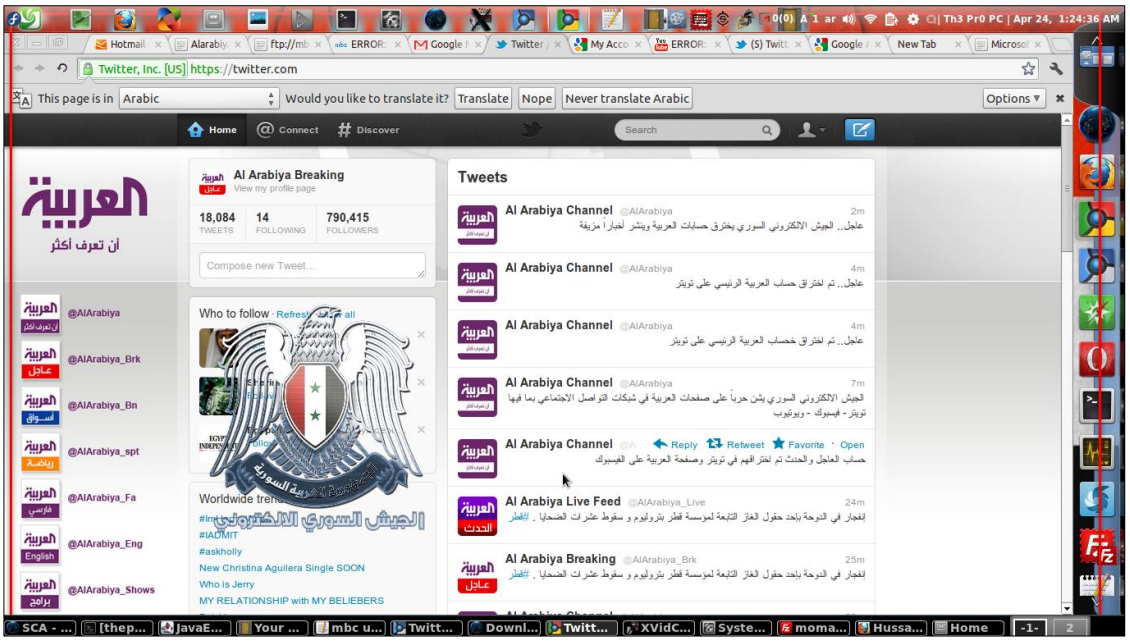
After this defacement, the SEA paused a bit, which may be explained as a preparation stage for further attacks on a new higher level, as the past hacks possibly didn't provide expected results.

March 27, 2012 - Al-Arabiya

This incident is one of the most interesting premeditated compromises. One of the biggest satellite news channels in the Middle East released a series of controversial news posts relating to the State of Qatar.

The first post suggested that Sheikh Hamad bin Jassim, the Gulf Emirate's Prime Minister and Foreign Minister, had been relieved of his duties and replaced by the country's heir-apparent, Sheikh Tamim bin Hamad bin Khalifa Al-Thani. This post was quickly followed by another news item suggesting that there was an explosion at a Qatari natural gas field which killed dozens of people. The news was spreading at a rapid pace as people began predicting a rift within the Qatari Royal Family.

Only after several hours, it became clear that there was neither an oil-field explosion nor a change in government, as clarified and posted by Famous Doha-based blogger, Ammar Mohammad (@Ammr), who works in the New Media division at Al-Arabiya's main rival, Al-Jazeera News Channel.



It was revealed that a number of Al-Arabiya's Twitter's accounts and Facebook have been hacked[18]. Al-Arabiya's main Twitter account announcing that the channel's social media accounts had been hacked.

Most of further Twitter accounts hacks will be done using the following template:

Spear Phishing URL Template
http://twitter{com}.{free hosting.com}/login.do

[18] «Saudi television network hit by Facebook hackers» - http://www.dailydot.com/news/saudi-al-arabiya-facebook-hack-attack/

Used Spear Phishing URL
http://twittercom.hostei.com/login.do

Besides such kind of informational PsyOP's, it was the first time when The Pro named himself as a member of Special Operations Department (SoD) of the so-called SEA on his official WEB-site and to several journalists[19].

April 25, 2012 - LinkedIn's official blog

LinkedIn's official blog was redirecting users to specially prepared page by SEA.

#SEA #Syria #RealSyria @Linkedin Blog blog.linkedin.com Get Hacked By Syrian Electronic Army | @AnonyOps @teedoz @techwd

— Th3 Pro (@Th3Pro_SEA) April 25, 2012

[19] "Syrian Electronic Army Leader: Cyber-War to Continue Against Those "Distorting the Truth About Syria" - http://www.huffingtonpost.co.uk/faisal-abbas/exclusive-syrian-electron_b_1452425.html

A Twitter account labeled as belonging to a member of the Syrian Electronic Army also said LinkedIn had been hacked, linking to a mirror image of what users were reportedly redirected to earlier, writes The Los Angeles Times' Emily Alpert and Rima Marrouch[20].

August 5, 2012 - Reuters Twitter account

Reuters News officially confirmed[21] that one of its Twitter accounts was hacked and false tweets were posted, mainly related to the current armed struggle in Syria. This incident appears to be the second PsyOP by SEA similar to Al-Arabiya case.

About 22 false tweets were published from the Thompson Reuters account, which explained one of the key priorities of the SEA – to provide specially crafted information in big masses, which is a part of a prepared psychological campaign. July 2013 the same attack will be repeated.

[20] «As violence continues unchecked in Syria, so does cyber warfare» - http://latimesblogs.latimes.com/world_now/2012/04/syrian-cyberwar-reportedly-takes-down-linkedin-blog.html

[21] «Reuters Twitter account hacked, false tweets about Syria sent» - http://www.reuters.com/article/2012/08/06/net-us-reuters-syria-hacking-idUSBRE8721B420120806

A bit later a spear phishing attack will be done against several Reuters employees. Using the same style of attack, the malicious fake page will be placed on free hosting with domain similar to original Reuters enterprise corporate e-mail login page.

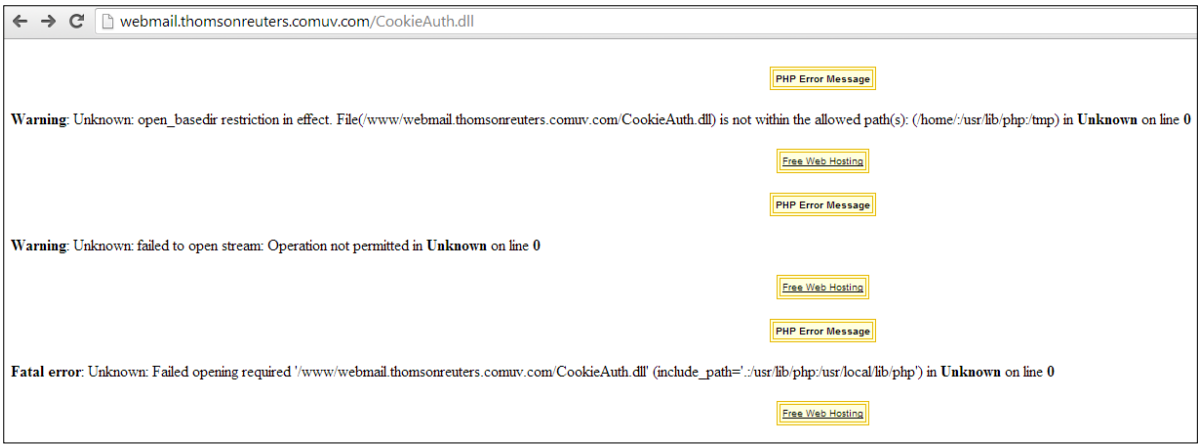
Spear Phishing URL Template 1
http://webmail.thomsonreuters.{free hosting}.com/CookieAuth.dll

Used Spear Phishing URL
http://webmail.thomsonreuters.comuv.com/CookieAuth.dll

Spear Phishing URL Template 2
http://webmail.thomsonreuterscom.{free hosting}.net/CookieAuth.dll

Used Spear Phishing URL
http://webmail.thomsonreuterscom.net63.net/CookieAuth.dll

The malicious page URL still has some traps to fake subdomain.



February 26, 2013 - Agence France Press

Agence France Press @AFPphoto Twitter account has been compromised by SEA.

April 21, 2013 – CBS

The Twitter accounts for two CBS programs 60 Minutes and 48 Hours were compromised by SEA.

For this time, they have chosen a provocative topic relating to the Boston bombing. Tweets coming from the 60 Minutes account suggested the US government was hiding the real culprit of the Boston bombing.

April 23, 2013 – Associated Press

The previous case was like a test attempt to analyze the results from prepared PsyOPS. There didn't seem to be any effect of the economic or political consequences. Eight months were spent by SEA and their hidden ideologists to analyze the received results and to prepare a new wave of planned cyber attack's combined with PsyOPS.

The SEA hijacked the Associated Press Twitter account and falsely claimed the White House had been bombed and President Barack Obama injured. The 143-point fall in the Dow Jones industrial average came after hackers sent these messages.

The fake post was re-tweeted more than 5,000 times within minutes, knocking the Dow Jones down from 14,703 to 14,554. It is the first time when the SEA reached the expected and perhaps not previously forecasted results affecting some critical niches in the real world as the result of a cyber-attack.

The SEA didn't immediately publish information about their responsibility for the hack and was waiting for the reported consequences to society after the hack.

The SEA subsequently published the information about the hack with its logo in the official blog and social media accounts, which was a significant change in their tactics.

After some period of time a new attack was launched on AP employees and many were compromised. Proper notifications were done to IT-Security Managers.

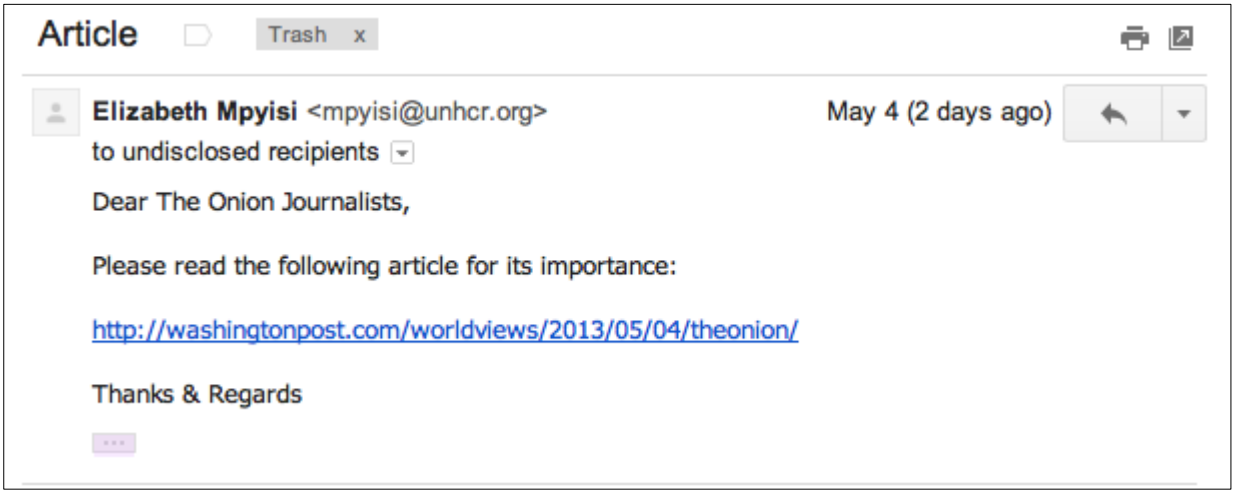
Spear Phishing URL Template
mail.ap{org}.{free hosting}/owa/auth/logon.aspx

Used Spear Phishing URL
http://mail.aporg.netai.net/owa/auth/logon.aspx

May 4, 2013 - The Onion

Starting around the period of time the SEA seems to ramp up their cyber-attacks. Most of them will be targeted on famous news agencies and famous private companies, which will lead to a serious discussion of their activities in the press.

The SEA reverts to their perfected technique – spear phishing, sending a malicious URL under the legend of a trusted resource spoofing the original e-mail source.

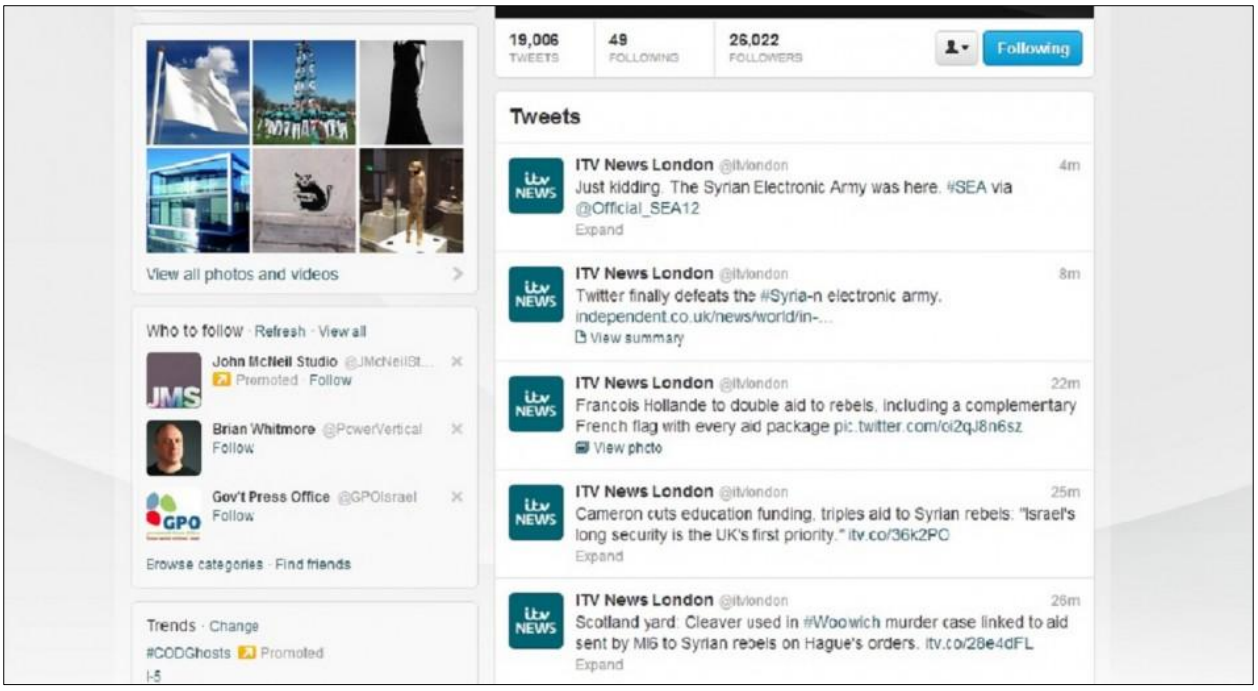


Gaining access to employees e-mail accounts, the SEA starts to target social media managers using HootSuite platform for content management for some famous social networks, such as Twitter.

May 2013 - The ITV news London

The ITV news London Twitter account was hacked on the May 24, 2013 by the SEA. The Android applications of British Broadcaster Sky News were also hacked on May 26, 2013 at the Google Play Store.

Similar to the previous cases, the SEA has tweeted several fake posts – Scotland Yard: Cleaver used in #Woolwich murder case linked to aid sent by MI6 to Syrian rebels on Hague's orders.



In other tweets the group claimed rebels were running from the decisive battle for the city of Qusair, off the Lebanese border and that French president Hollande was sending complementary French flags as part of aid to Syrian rebels.

May 17, 2013 – Financial Times

Hackers replaced headlines on the FT's website with: “Hacked By Syrian Electronic Army” and put messages on the newspaper's Twitter feed.

FT, Reuters, AP and AFB are among the media giants targeted by the SEA which provided them great exposure all over the world. It seemed each new breach helped them to blur their true covert actions.

July 17, 2013 – Truecaller

Truecaller servers were allegedly hacked into by the Syrian Electronic Army. The group claimed on its twitter handle to have recovered 459 GiBs of database, primarily due to an older version of Wordpress installed on the servers.

The hackers also released TrueCaller's alleged database host ID, username, and password via another tweet. On 18 July 2013, Truecaller issued a statement on its blog stating that their servers were indeed hacked, but claiming that the attack did not disclose any passwords or credit card information.

July 23, 2013 – Viber

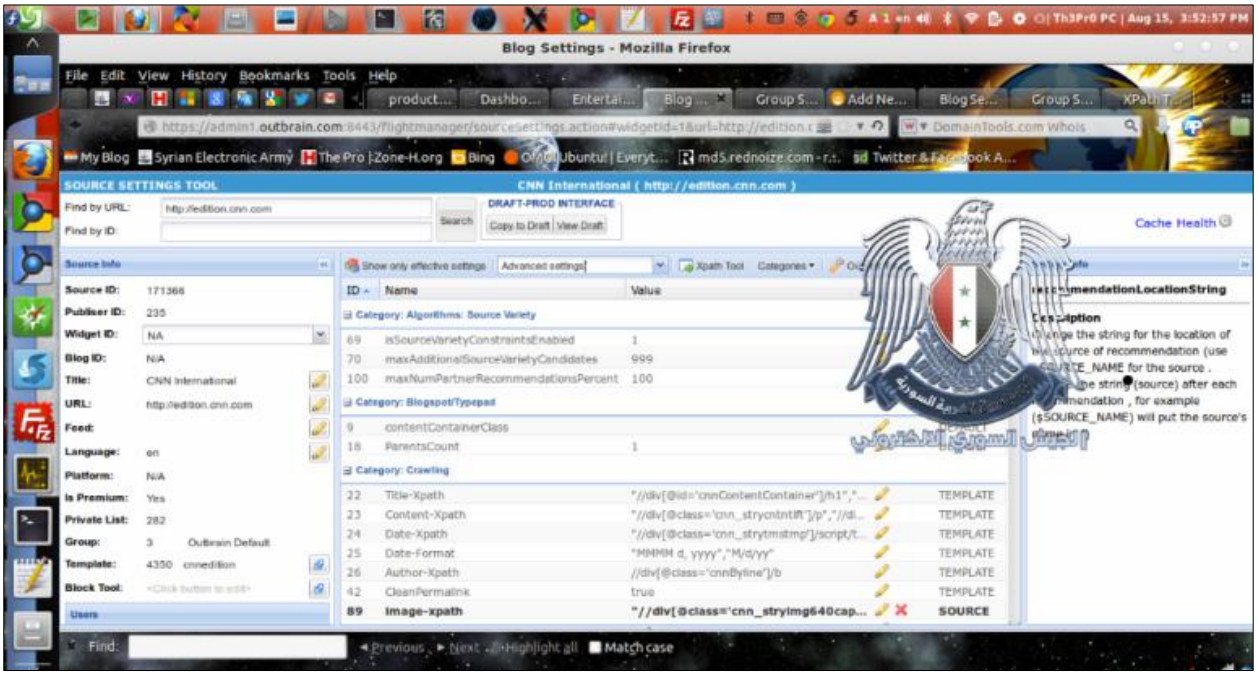
Viber servers were allegedly hacked into by the SEA. The Viber support website was replaced with a message and a supposed screenshot of data that was obtained during the intrusion.

August 15, 2013 – Washington Post, CNN, Time

The Washington Post website was hacked by the SEA in a pretty similar style to previous news agencies. In a tweet sent in the morning, the SEA claimed that it hacked the Web sites of The Post, CNN and Time magazine in one strike.

Such coordinated wave of attacks on American news outlets confirmed that the Syrian Electronic Army was ramping up their psyops warfare niche abilities, successfully taking down three major news outlets, CNN, WAPO and Time.

The bad actors received an access to Outbrain, acting as a widget that promotes your own content to the people already on your website.



All of the resources were hacked through a third party – Outbrain. Such an approach, hacking of third party resources and services, will be very efficient in further cyber-attacks by the SEA and allows them to achieve excellent results quickly.

The attacks against US media companies continued.

August 27, 2013 – NYTimes

NYTimes.com had its DNS redirected to a page that displays the message Hacked by SEA and Twitter's domain registrar was changed.

August 28, 2013 – Twitter

Twitter had its DNS registration hacked to show the SEA as its Admin and Tech contacts, and some users reported that the site's CSS had been compromised.

August 29, 2013 – The New York Times, Huffington Post, and Twitter

The New York Times, Huffington Post, and Twitter were knocked down by the SEA.

September 2, 2013 - US Marine Corps

The SEA broke into the internet recruiting site for the US Marine Corps, posting a message that urged US soldiers to refuse orders if Washington decides to launch a strike against the Syrian government.

The site, www.marines.com, was paralyzed for several hours and redirected to a seven-sentence message delivered by the SEA.

September 30, 2013 – Global Post

The SEA hacked the website of U.S. news company the Global Post, targeting their official twitter account and website (globalpost.com).

October 28, 2013 - Organizing for Action

By gaining access to the Gmail account of an Organizing for Action staffer, the SEA altered shortened URLs on President Obama's Facebook and Twitter accounts to point to a 24-minute propaganda video on YouTube.

November 9, 2013 – VICE

The SEA hacked the website of VICE, which is an affiliate news/documentary/blog website which has filmed numerous times in Syria with the side of the Rebel forces. When logging into vice.com you are redirected to what appears to be the homepage of the SEA.

November 12, 2013 - Matthew Van Dyke

The SEA hacked the Facebook page of Matthew Van Dyke, a Libyan Civil War veteran and pro-rebel news reporter.

January 1, 2014 – Skype

The SEA hacked the official Facebook and Twitter pages for Skype as well as the official website's blog. The same Twitter attack tactics were used.

January 23, 2014 – CNN

The SEA hacked CNN's official Twitter account and posted two messages, including a photo of the Syrian Flag composed of binary code. The Tweets were removed by CNN within 10 minutes.

February 3, 2014 – Markmonitor DNS

This was one of the most ambitious attacks by the SEA. Lots of domains of major corporations were hijacked and their WHOIS details were changed.

February 10, 2014 – NBC Universal

NBC Universal was informed by IntelCrawler that one of the top-level news executives at NBC was compromised. The SEA was preparing a larger targeted attack, but the attack was mitigated.

The bad actors received NBC Universal SSO account and planned to intercept all the communications for further defacement, as it was done before. Around this time, various other news agencies, including The Register, BBC, AP and Reuters were notified by IntelCrawler about new compromised accounts in order to prevent new reputational abuse.

February 14, 2014 – Forbes

The Syrian Electronic Army hacked the Forbes official website and their twitter accounts. A “C” level Forbes executive was also compromised and all notifications were sent to their IT department.

February 19, 2014 – FC Barcelona

The Syrian Electronic Army hacked the FC Barcelona official Twitter accounts. The compromised accounts were @FCBarcelona, @FCBarcelona_es and @FCBarcelona_cat.

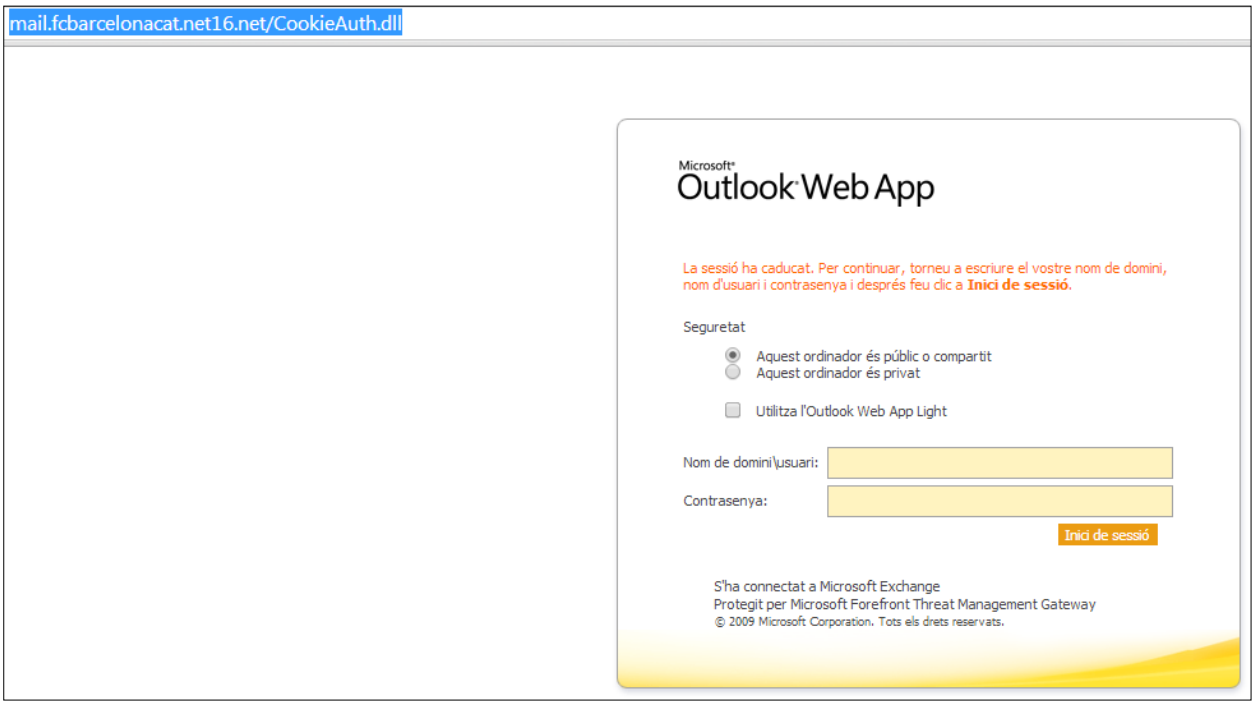
a6035612@srv36.000webhost.com	FCB: fcbarcelona1899	February 18th 2014
a6035612@srv36.000webhost.com	FCB: fcb1613	February 18th 2014
a7294257@srv48.000webhost.com	ICT-QA: homer	October 11th 2013

The Syrian Electronic Army posted a Special Hi to @RealMadrid and then disclosed the real motive of the attack, which was according to their opinion, a negative view on Qatar.

Spear Phishing URL Template
http://mail.fcbarcelonacat.{free hosting}/CookieAuth.dll

Used Spear Phishing URL
http://mail.fcbarcelonacat.net16.net/CookieAuth.dll

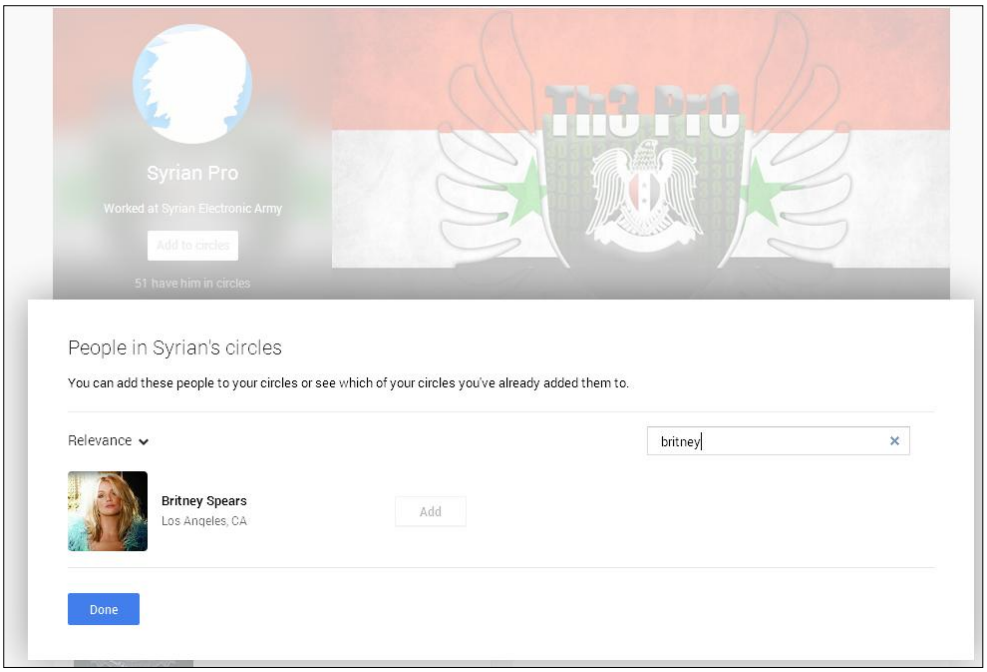
The page is still active and designed in Spanish language as original enterprise Outlook WebApp login page.



Unrevealed and Planned Targets

In March 2014, “The Pro” will add to his Google Plus profile[22], the celebrity Britney Spears.

[22] https://plus.google.com/116471187595315237633/posts



"The Pro" has gained server access to Britneyspears.com and Selenagomez.com, but both incidents were prevented by victim notifications. The motivation of "The Pro" here appears personal.

Hello,

We've received an administrator password reset request for
britneyspears.com.
To initiate the process, please click the following link:

<https://www.google.com/a/cpanel/britneyspears.com/ResetAdminPassword?c=Bm6cM1vJX4G0Dg7xSLtI9Q&hl=en&rs=0>

If clicking the link above does not work, copy and paste the URL in
a new browser window instead. The URL will expire in 24 hours for security
reasons.

Please disregard this message if you did not make a password reset request.
If you continue to experience difficulties accessing your account, visit the
Help Center at http://www.google.com/support/a .

This is an automatically generated message. Replies are not monitored or
answered.

Sincerely,
The Google Apps Team

Hello,

We've received an administrator password reset request for selenagomez.com.
To initiate the process, please click the following link:

<https://www.google.com/a/cpanel/selenagomez.com/ResetAdminPassword?c=n05OG8lcs6uZYt_Fvitqlg&hl=en&rs=0>

If clicking the link above does not work, copy and paste the URL in
a new browser window instead. The URL will expire in 24 hours for security
reasons.

Please disregard this message if you did not make a password reset request.
If you continue to experience difficulties accessing your account, visit the
Help Center at http://www.google.com/support/a .

This is an automatically generated message. Replies are not monitored or
answered.

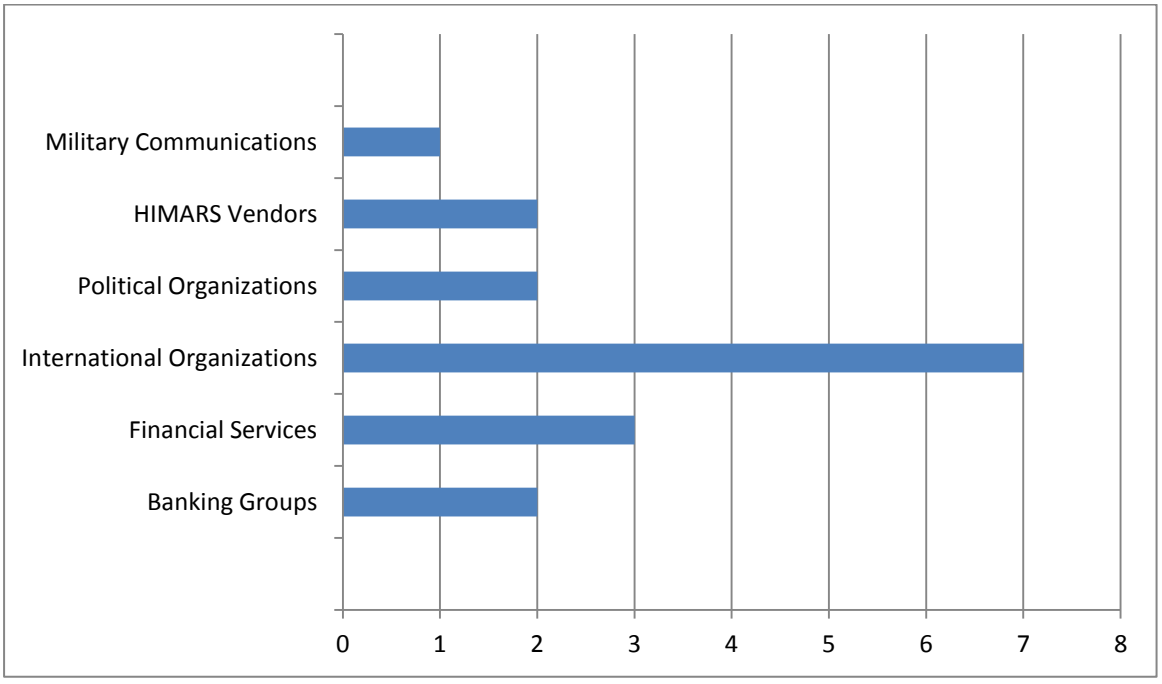
Sincerely,
The Google Apps Team

SEA: Cyber Espionage Behind the Curtain

Besides the known public hacks revealed by the SEA in the press, there is a large cyber espionage campaign targeted against foreign governments and officials from different countries.

Their masked hacktivison is initially unveiled with a serious of attacks against Qatar and the Turkish government in the beginning of 2013.

Besides governments, the SEA will target several organizations from various industries with tactics of modern cyber warfare[23], which may affect geopolitical relations and financial markets.



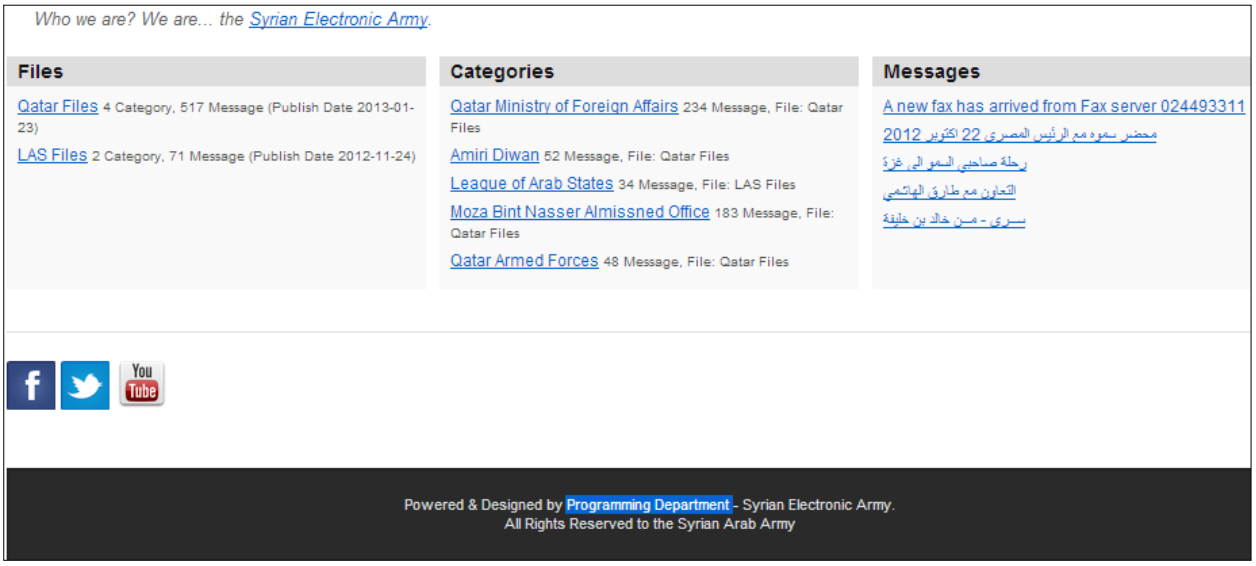
May 3, 2013 – Qatar

Right after the AP was hacked by the SEA and the world was reading the press with great attention, monitoring the Dow Jones index etc., the SEA attacked several ministries and government organizations of Qatar, including Qatar Armed Forces and Ministry of Foreign Affairs.

http://web.archive.org/web/20130503093831/http://leaks.sea.sy/ (snapshot from 3d May, 2013)

[23] High Mobility Artillery Rocket System (HIMARS)

According to IntelCrawler, the created page exposure was the method of legitimizing a la Wikileaks the targeted Cyber Espionage campaign.

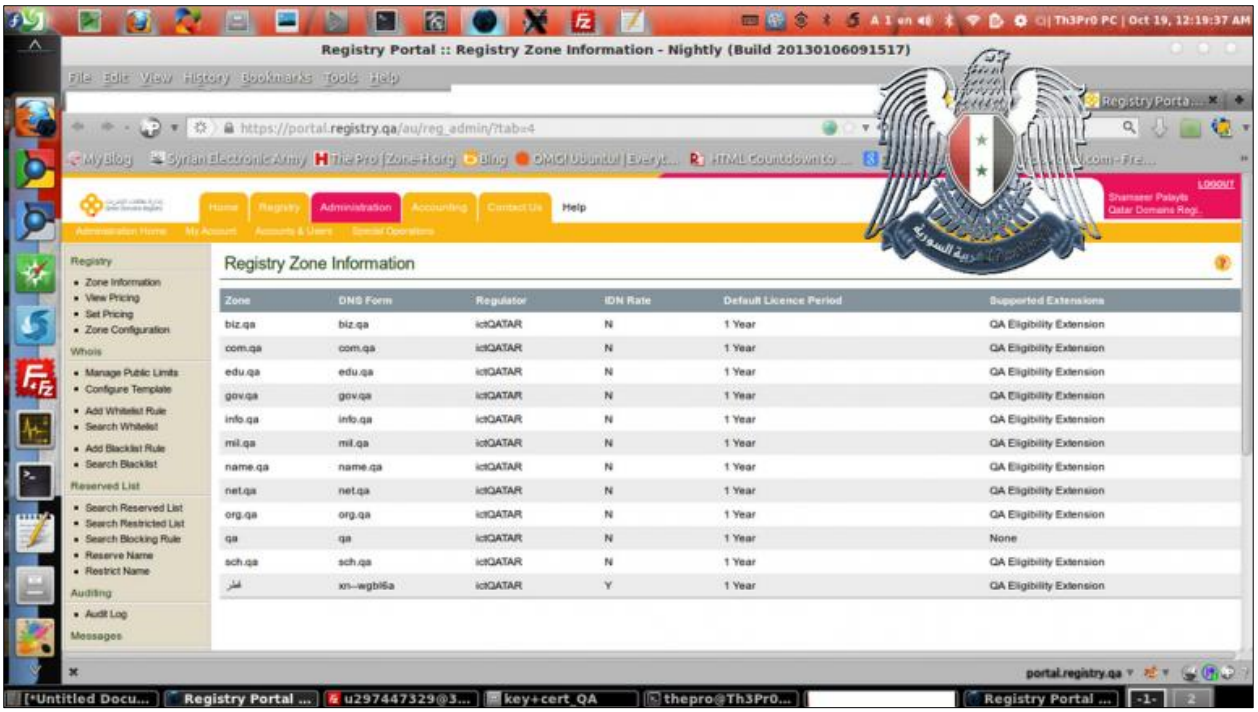


One new department – Programing Department of Syrian Electronic Army was mentioned on the created website, with a brand new “Syrian Arab Army” appearing in the footer.

The leaks in the Qatari file included documents from the Qatari Foreign Ministry, the Defense Ministry, and the email of the Amiri Diwan of Qatar. The document had various contents that included general files, special files, and very sensitive confidential files. The files were of a variety of subjects, with some being correspondence from the Qatari embassy to the ministry of foreign trade.

It also included financial files that belonged to internal and external Qatari companies. The documents also included the internal affairs of Qatar itself and the relationship with Qatar and many other Arabic and western nations. These documents show how Qatar uses money to pressure these countries to implement its special agendas. Finally, these documents will expose minutes of meetings between Qatar and Arabic/western leaders. The Syrian Electronic Army selectively picked certain documents for release.

On October 19t, 2013, after several months, the SEA will mask these actions under a hacktivist's campaign against Qatar by hacking Qatar Domain Registrar (portal.registry.qa) and DNS records modification, doing more PR releases of own actions, but hiding the intercepted documents and communications from government networks.



The same resources will be named there, including moi.gov.qa, facebook.qa, gov.qa, vodafone.qa, aljazeera.net.qa, google.com.qa, ooredoo.com.qa, diwan.gov.qa, qaf.mil.qa, mofa.gov.qa, moving accents to famous brands, such as Google and Vodafone.

The initial attack will be started through spear phishing against Supreme Council of Information & Communication Technology employees[24]. During the previous two months before the hack, more than 30 government e-mail accounts will be compromised. Some indicators of compromise (IOC) – using free hosting for placing spear phishing pages, are below.

a7294257@srv48.000webhost.com	ICT-QA : fansari	October 11th 2013
a7294257@srv48.000webhost.com	ICT-QA: ralmansoori	October 11th 2013

[24] http://ict.gov.qa

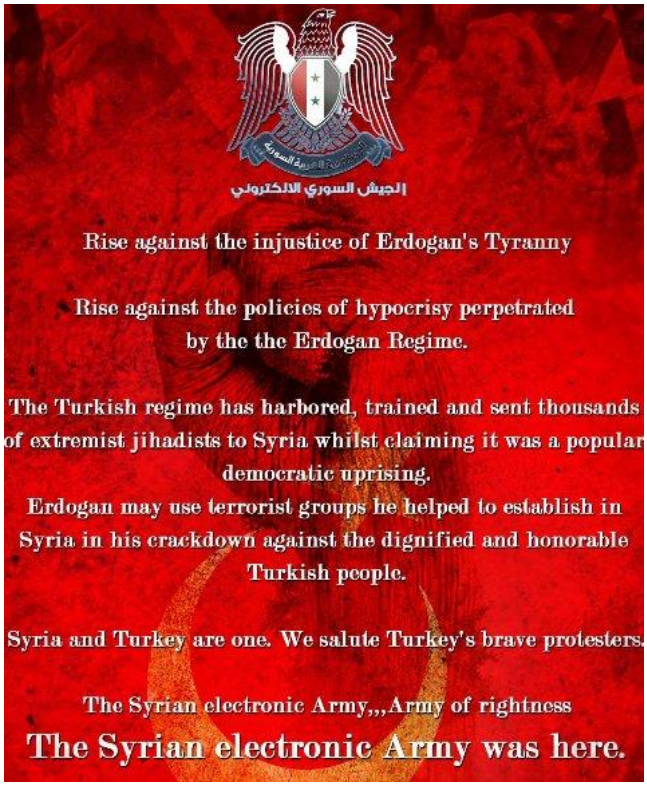
a7294257@srv48.000webhost.com	ICT-QA: homer	October 11th 2013
a7294257@srv48.000webhost.com	ICT-QA: salkuwari	October 11th 2013
a7294257@srv48.000webhost.com	ICT-QA: mfakhroo	October 16th 2013
a7294257@srv48.000webhost.com	ICT-QA: aibrahim	October 24th 2013

An interesting post from the company Sysmox in Morocco seems to be up on the Qatar situation:

June 5, 2013 – Turkish Government

Operative information received by IntelCrawler explains that a large number of people were hired for this compromise and were well paid and not related to the Syrian Electronic Army members, thus acting as hired mercenaries.

They took part in an operation against Turkish Government and had breached Turkish Ministry of Interior together with so called Anonymous Turkey.

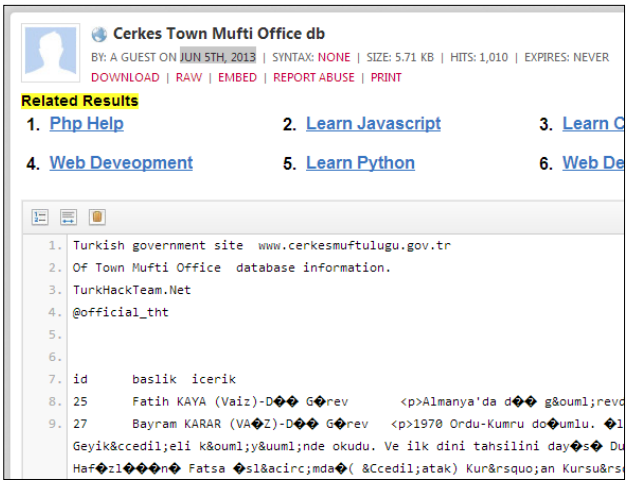


It seems to be that for that time the actions of the SEA were not properly coordinated. One of such signs was the relation of Tunisian hackers[25] to the incident and the same time the SEA pointed the link on intercepted data after the breach to own website – http://leaks.sea.sy. After some time the post and the resource disappeared.

[25] Google Cache http://webcache.googleusercontent.com/search?q=cache:bm_owde1bZEJ:https://www.facebook.com/permalink.php%3Fstory_fbid%3D402533339861914%26id%3D301351556646760+&cd=3&hl=en&ct=clnk&gl=en

Close to the evening of June 6, 2013 some strange Turkish hackers tried to mask the incident under the actions of Anonymous Turkey and unknown hacking groups in ongoing operation #OpTurkey, blurring the initial relation to the incident the same day.

http://pastebin.com/pF93F7Uf#sthash.ZCUcJAEq.dpuf
http://pastebin.com/CcGuBD9H#sthash.ZCUcJAEq.dpuf



September 8, 2013 – France

The SEA has compromised several officials from the French Senate, but this fact was not revealed in public for some reason.

Previously, the SEA had claimed responsibility for attacking the website of the French embassy in Damascus on June 24, 2011 and 10 Israeli websites on June 25, 2011. Users that try to access the news page of the French embassy in Damascus (http://www.ambafrance-sy.org/spip.php?rubrique112), were redirected to http://th3pro.pro/fr/ and displayed a page with text in French and Arabic claiming the defacement attack was to protest the negative stand of the French government on Syria and its participation in the conspiracy against Syria.

The message also states the attack was to protest the inaccurate report of French news channel France 24 concerning the resignation of the Syrian Ambassador to France.

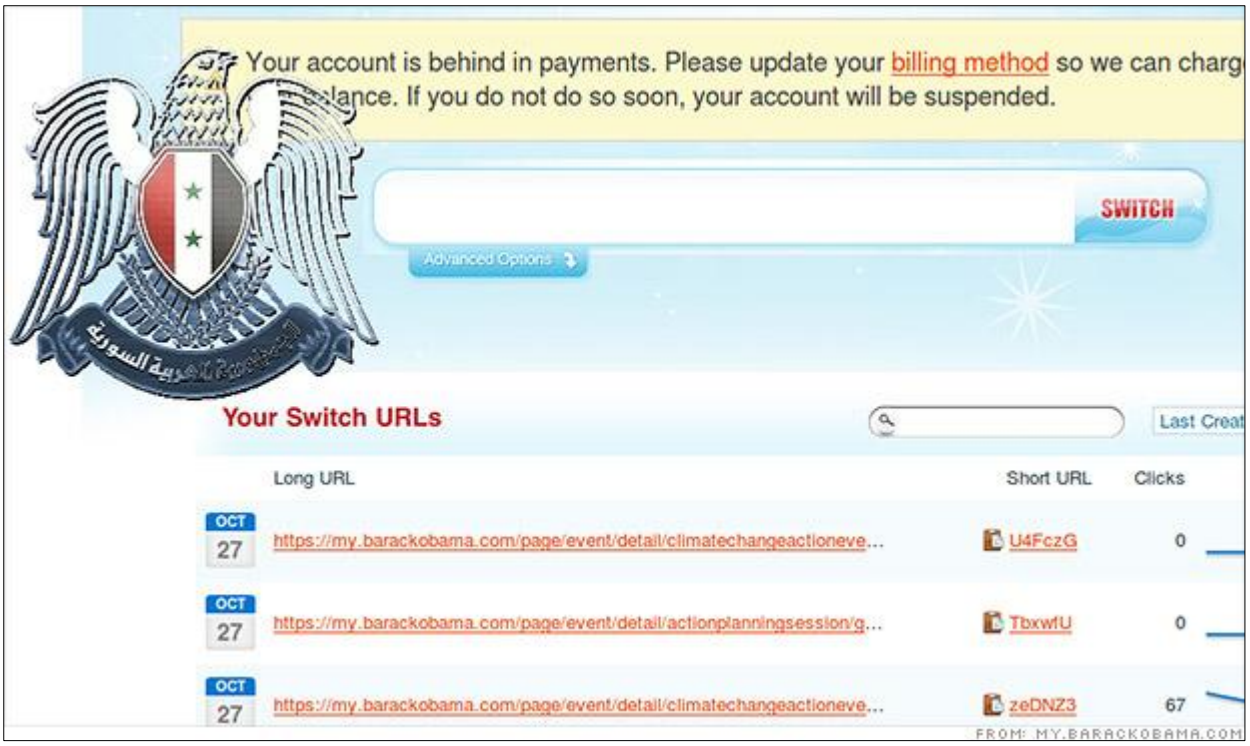
October 28, 2013 – United States of America

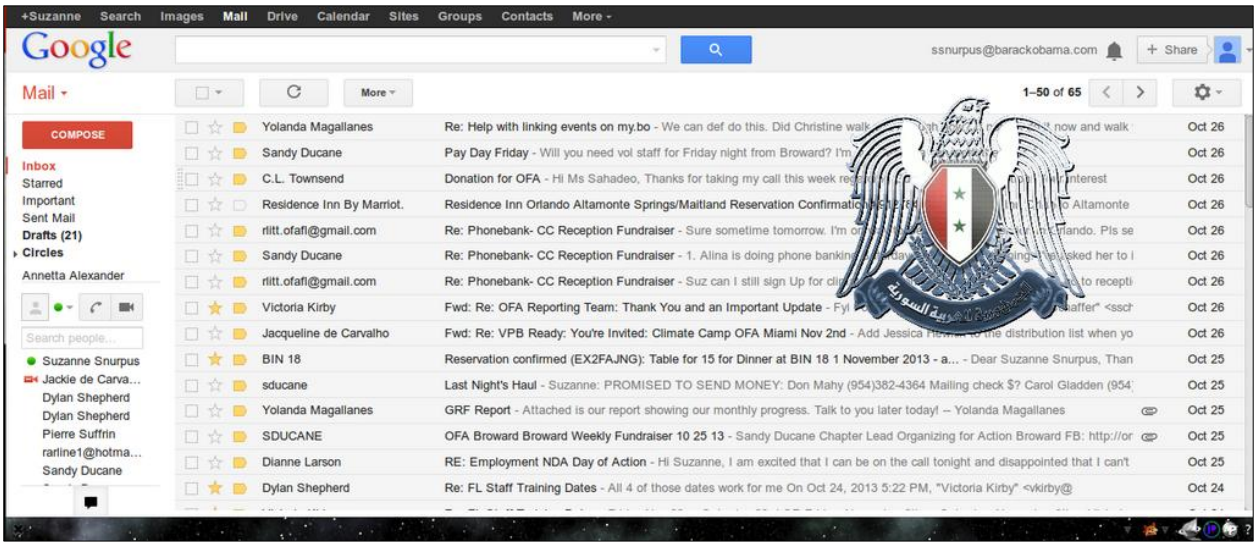
On this date the Syrian Electronic Army had received an access to US President Barack Obama's Twitter and Facebook accounts.

After IntelCrawler's analysis, several e-mails of employees responsible for the website were also hacked, but not published in press, which was used for monitoring of their messages.

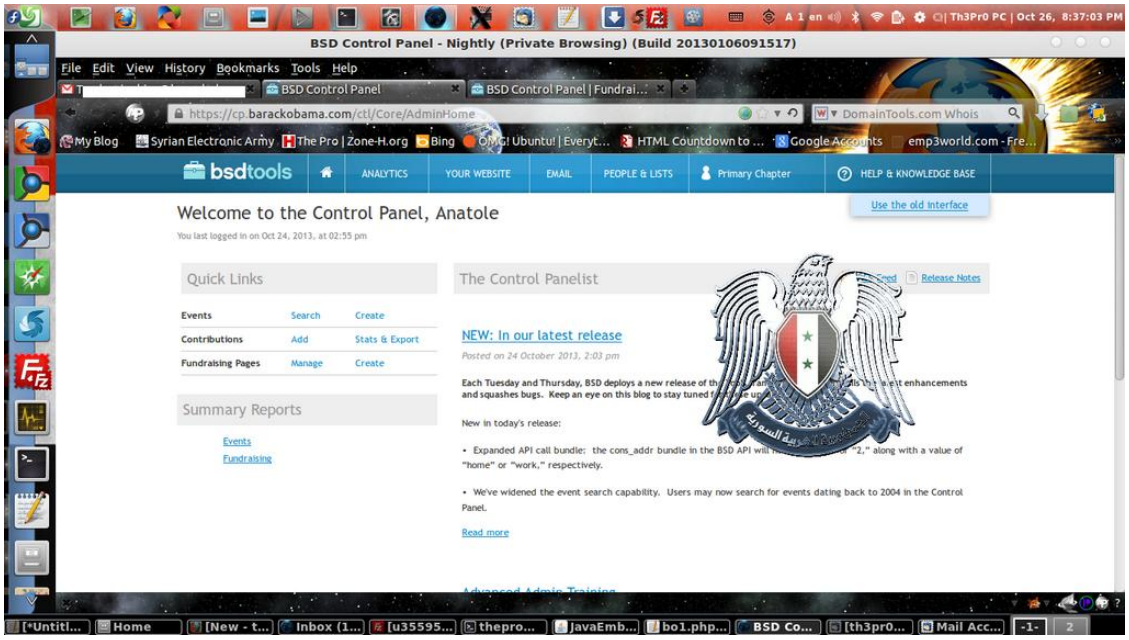
ssnurpus@barackobama.com
ajenkins@barackobama.com
apinedo@barackobama.com

In talking with a Turner.com journalist, The Pro confirmed that the SEA hacked OFA emails (@barackobama.com) and accounts on shortswitch.com (shortlinks service) that host OFA.BO, as well as http://donate.barackobama.com and http://my.barackobama.com websites.





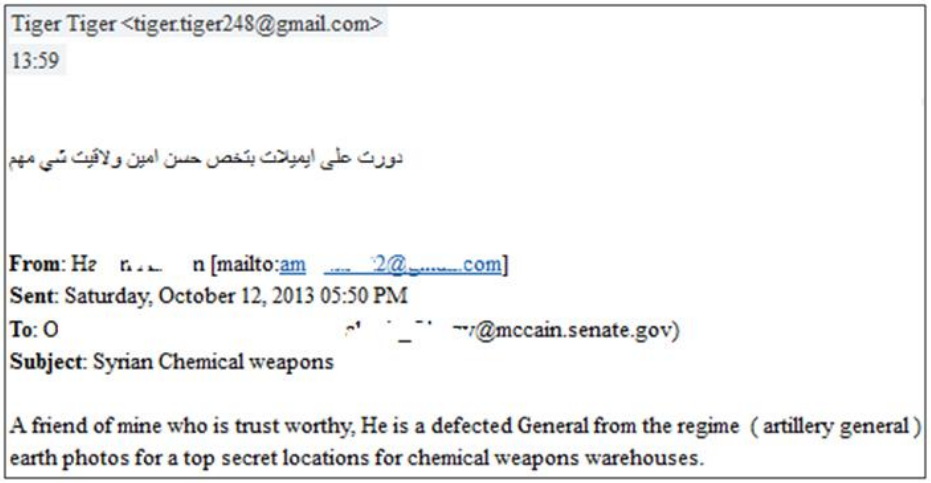
It seems to be that the initial aim of bad actors was targeted interception of White House e-mails, but they received no results, only social media accounts, and monitoring credentials to official website.



The SEA has published some quite ambitious statements, providing no evidence to support them. After this incident, the SEA will continue to monitor US government officials moving to State Department e-mails and various military subcontractors involved in specific kinds of projects.

February 18, 2014 the SEA has published an intriguing post that they have intercepted some of the emails from the United States Senator's office from Arizona – John McCain.

One of the SEA leaders – Tiger had gained an access to a former US DOD employee's email account, who now acts as a pro rebel Syrian advocate. That account may have had contact with a senior Syrian research expert in Senator John McCain's office. The SEA touted this breech in the press but only discussed issues with regards to Ukraine. They selectively omitted any reference to the intelligence they gleaned from McCain's office on Syria, which did seem to include travel plans to Syria.



Tiger Tiger <tiger.tiger248@gmail.com>
13:59

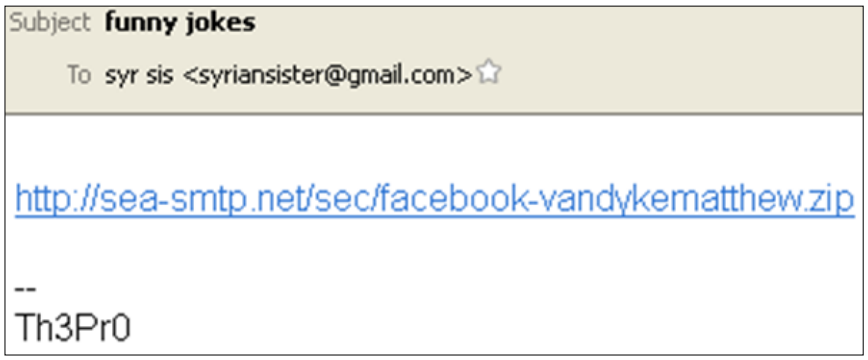
دورت على ايميلات بتخص حسن امين ولاقيت شي مهم

From: Ha n [mailto:am 2@.....com]
Sent: Saturday, October 12, 2013 05:50 PM
To: O r@mccain.senate.gov)
Subject: Syrian Chemical weapons

A friend of mine who is trust worthy, He is a defected General from the regime (artillery general) earth photos for a top secret locations for chemical weapons warehouses.

The SEA has compromised the personal email account of an extremely high former US intelligence director/military official, possibly with the use of a fake Google authenticator page. The breach was reported by coordinated actions.

During long term monitoring there were found several hidden network storages used by SEA members for internal purposes. Some of them were registered on fake names and excluded from search engines indexing.


Subject **funny jokes**

To syr sis <syriansister@gmail.com>

http://sea-smtp.net/sec/facebook-vandykematthew.zip

--
Th3Pr0

SEA-SMTP.NET WHOIS
Domain Name: SEA-SMTP.NET Registry Domain ID: 1843139913_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.dynadot.com Registrar URL: http://www.dynadot.com Updated Date: 2014-02-13T23:54:46.0Z Creation Date: 2014-01-16T19:34:15.0Z Registrar Registration Expiration Date: 2015-01-16T19:34:15.0Z Registrar: DYNADOT LLC Registrar IANA ID: 472 Registrar Abuse Contact Email: abuse@dynadot.com Registrar Abuse Contact Phone: +1.6502620100 Domain Status: clientTransferProhibited Registry Registrant ID: Registrant Name: Edwin johansyah Registrant Street: surabaya Registrant City: surabaya Registrant State/Province: jawa timur Registrant Postal Code: 60213 Registrant Country: ID Registrant Phone: +62.856487278884 Registrant Email: edwinjouhansyah@gmail.com Registry Admin ID: Admin Name: Edwin johansyah Admin Street: surabaya Admin City: surabaya Admin State/Province: jawa timur Admin Postal Code: 60213 Admin Country: ID Admin Phone: +62.856487278884

Admin Email: edwinjouhansyah@gmail.com
Registry Tech ID:
Tech Name: Edwin johansyah
Tech Street: surabaya
Tech City: surabaya
Tech State/Province: jawa timur
Tech Postal Code: 60213
Tech Country: ID
Tech Phone: +62.856487278884
Tech Email: edwinjouhansyah@gmail.com
Name Server: ns1.dynadot.com
Name Server: ns2.dynadot.com
DNSSEC: unsigned

There were also found several suspicious domain names, such as “shopcard.info” and “mslineondeal.info”, which planned to be used in targeted cyber-attack on various military agencies. The domains still have a HTTP-redirect to DISA – Defense Information Systems Agency:

The list of the found domain names:

kostenlosfilmegucken.biz	shopcard.info	coresta.net
respondtofloods.info	spdas.info	poolball.org
adurotheband.com	rockmeusa.org	florence-hotel.org
edps.info	catechnolgiesinc.biz	jshcm.org
cameltoehoneys.com	tedcookson.info	executiveinnandsuites.org
standforwelcome.org	fotoepilazioneoderme.info	commissiondelacapitalenationale.info
lboro.info	mudbytes.org	usi-uk.org
hamiltonpas.org	mslineondeal.info	bccla-pg.org
openqry.org	dhani.info	udesr71.org

June 5, 2013 – Jordan

The Royal Jordanian Air Force, Jordan Armed forces, Ministry of Foreign Affairs of Jordan, including several of its offices in other countries were compromised by the SEA.

Using targeted spear phishing attack the bad actors received information about one of the accounts and then started to distribute it across embassies and others.

Spear Phishing URL Template
http://jaf.<{FAKE PAGE}>mil.jo/d<{FAKE PAGE}>ocs/2014_2_23-251.PDF<FAKE PAGE>

Used Spear Phishing URL
امن هذا حـ بـ يب http://jaf.<http://www.lewaa-iskenderun.com/rjaf.php>mil.jo/d<http://www.lewaa-iskenderun.com/rjaf.php>ocs/2014_2_23-251.PDF<http://www.lewaa-iskenderun.com/rjaf.php>

A major and general in the Jordanian Army in charge of military procurements were hacked. Millions of dollars of ammo, night vision goggles, sniper pads, and WMD defense systems designed by US defense contractors were just some of the intelligence compromised. US military defense contractor details were exposed.

The SEA has stolen credentials of various government resources and Jordan embassies, which were also used for intelligence.

1	server	user name	password	IP server	URL
2	Weekly report	nabil.s	&		http://w eports.nitc.gov.jo/ViewReport.aspx
3	Heat account	****	**	10 0	http://1 4:8180/HeatWebUI/calllogging/CallLogging.html
4	JAF server	srv5233781218\administrator	A	10	mstsc
5	Delegated Administrator	nicadmin	A	**	http://m .nic.net.jo/da/DA/Login
6	Trend Micro	Admin	m	**	https:// .150:8445/loginPage.imss
7	ExAdmin(exchange)	ExAdmin	P	10	mstsc
8	LDAP	admin	M	10	http://1 6/dscc7/dcc7Module/Login
9	MGT (Management Station)	root	T	10	putty
10	nagios.nitc.gov.jo	nagiosadmin	N	10	http://n itc.gov.jo/
11	SAN	root	S	10 789	https:// 55.11:6789/console/jsp/login/BeginLogin.jsp
12	Frontend node 1 (Mail)	root	m	10	putty
13	Frontend node 2 (Mail)	root	m	10	putty
14	Backend node 1 (Mail DB)	root	m	10	putty (M
16	Backend node 2 (Mail DB)	root	m	10	putty (M
17	Frontend node 1(Web)	root	H	10	putty
18	Frontend node 2(Web)	**** , su -	H	10	putty
19	Frontend node 3(Web)	root	H	10	putty
20	Backend node 1 (Web DB)	root	H	10	putty (M
21	Backend node 2 (Web DB)	root	H	10	putty (M
22	Log Server	root	B		putty
23	php my admin	nitcroot	R 5	10	http://1 0:82/phpMyAdmin/index.php
24	php my admin	???	?:	10	http://1 3:82/phpMyAdmin/index.php
25	php my admin	root	N	10 0	http://1 8:8080/phpMyAdmin/index.php
26	First San Switch	admin	IB	10	
27	Second San Switch	admin	IB	10	
28	IBM Console	iscadmin	is	10 3	https:// 63:9043/ibm/console
29	Tape Library IP Address	admin	se	10	http://1 9/
30	ITM server (gojitm01)	administrator	P	10	
31	OmniFind server (gojomn01)	administrator	P	10	
32	NDP SERVER	administrator	rc 123	10	

January 16, 2014 – Saudi Arabia

Hackers of the SEA have breached and defaced a total of 16 Saudi Arabian government websites. Besides compromised e-mails of government, the SEA will concentrate on strictly confidential documents about warfare and modern artillery equipment.

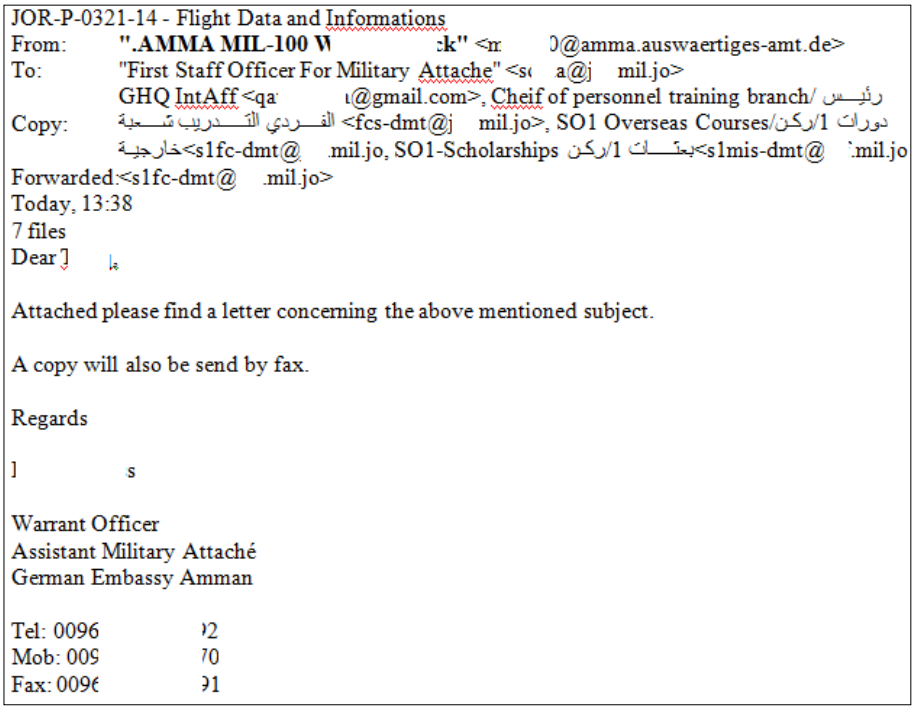
Some of the users will be compromised using the following spear phishing template:

«http://igoogle.travel/ServiceLogin.Auth?&passive=1209600&cpbps=1&continue=https://mail.google.com/mail/« masked under document «https://mofa.gov.sa/uploads/docs/47812_8232.PDF«.

March 8, 2014 – Germany

KFW.DE and Federal Foreign Office employee's communications were compromised by SEA after receiving an access to Jordan military entities and MOFA.

The interests of the SEA were very selective and concentrated also on Military Attaché communications, as well as cooperation between Turkey, Jordan and Qatar with other countries.



JOR-P-0321-14 - Flight Data and Informations
From: ".AMMA MIL-100 W :k" <m)@amma.auswaertiges-amt.de>
To: "First Staff Officer For Military Attache" <s a@j mil.jo>
GHQ IntAff <qa ı@gmail.com>, Cheif of personnel training branch/ رئيس
Copy: الفردي التدريب شعبة <fcs-dmt@j mil.jo>, SO1 Overseas Courses/ركن 1/ دورات
خارجية<s1fc-dmt@ .mil.jo, SO1-Scholarships ركن 1/بعثات<s1mis-dmt@ `.mil.jo
Forwarded:<s1fc-dmt@ .mil.jo>
Today, 13:38
7 files
Dear]

Attached please find a letter concerning the above mentioned subject.

A copy will also be send by fax.

Regards

] s

Warrant Officer
Assistant Military Attaché
German Embassy Amman

Tel: 0096)2
Mob: 009 70
Fax: 009(91

Besides named countries, the SEA has intercepted several of messages from following countries and organizations:

- DFID - UK Department for International Development;
- European Commission;
- German Federal Foreign Office (Auswärtiges Amt);
- Group of Friends of the Syrian People;
- Italian Ministry of Foreign Affairs;
- Ministry of Foreign Affairs of the United Arab Emirates
- Turkish Ministry of Foreign Affairs;
- UK Foreign & Commonwealth Office.

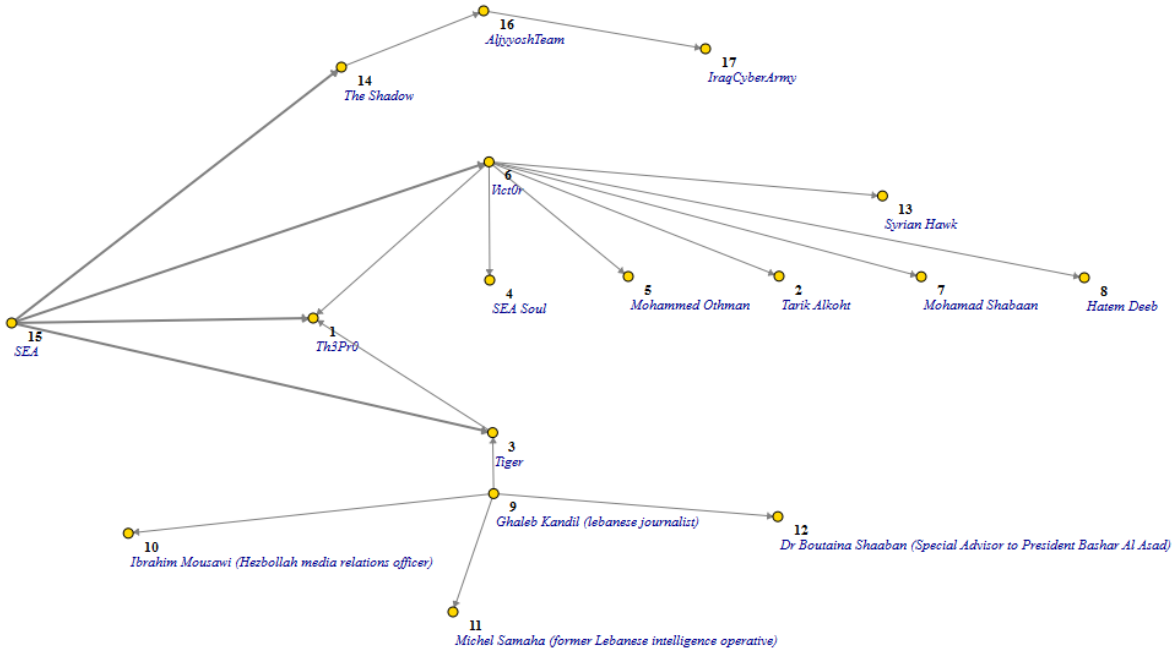
Conclusion

The Syrian Electronic Army may have started out as a hacktivist organization, but as the evidence in this report shows, they are now a full blown cyber espionage entity which is very well organized and coordinated and has some source of consistent funding. They also may have linkage with some of the well know terrorist groups in the middle-east.

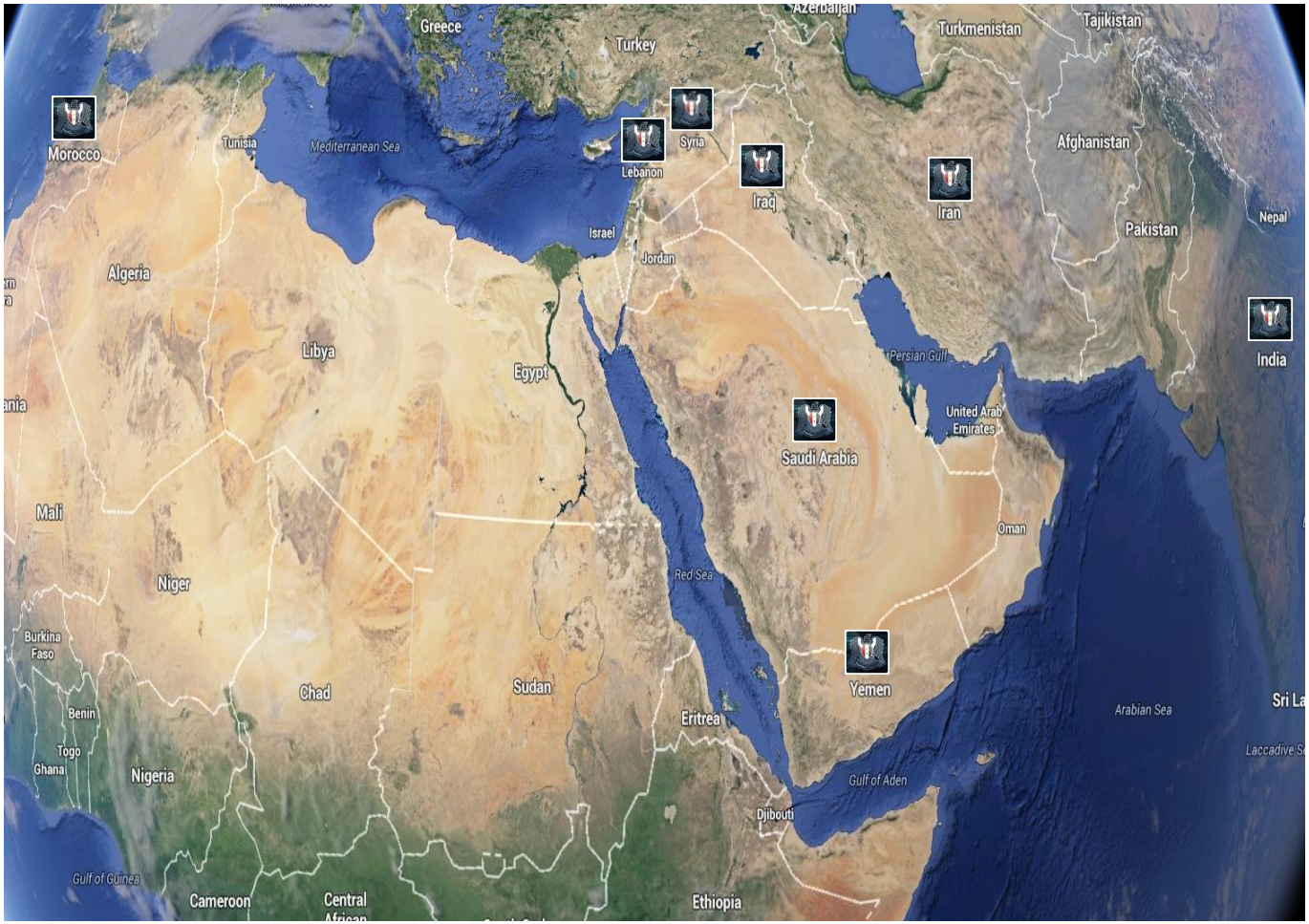
As we peeled back their self-reported hacktivision, the real targets became clear. With successfully compromised strategic people and web sites, their access to very sensitive data and intelligence has given them documents and programs that could dramatically affect the security of the western world.

As IntelCrawler has uncovered 20 new SEA breaches with more than 270 government and corporate compromised e-mail accounts, it’s clear that the SEA is still sliding under the radar of the computer security industry.

Appendix A. Social Links Graph



Appendix B. Geographical Correlation Map of SEA Members Presence

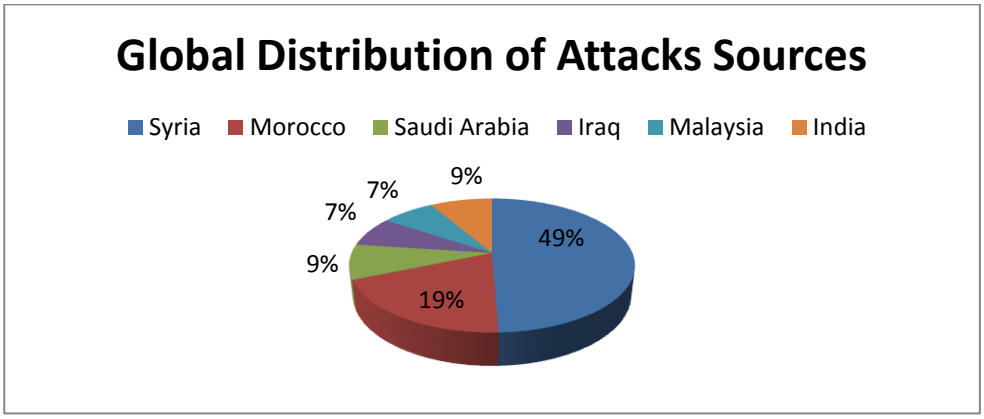


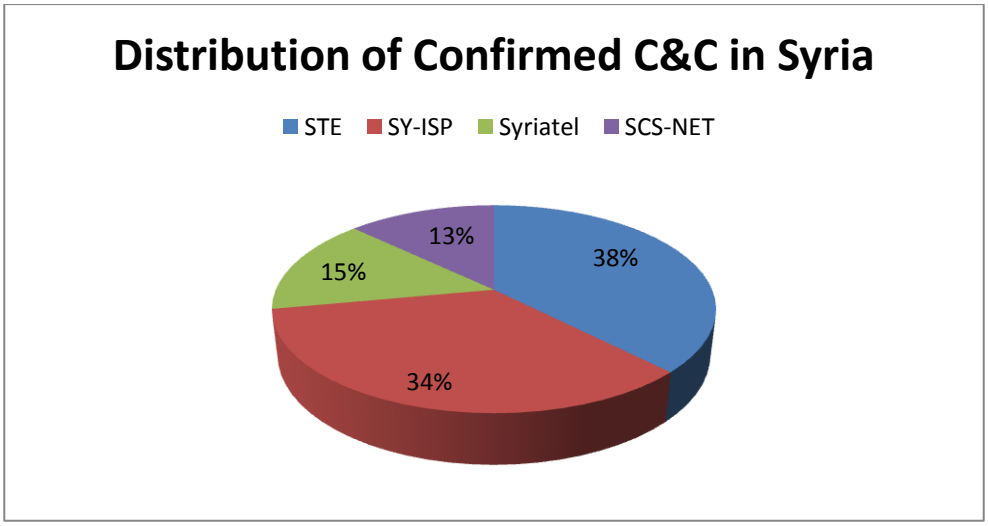
Appendix C. Malware Distribution Campaigns

During 2012-2014 we have detected more than 60 specific malware distribution campaigns with Syrian roots. Most of the cases used RAT malware such as Blackshades RAT, XTreme RAT, njRAT, Dark Comet RAT, ShadowTech RAT with ability to log keystrokes, capture webcam images, collect files and transfer them.

All of them can be characterized as highly targeted campaigns that deliver a nasty piece of malware capable of conducting surveillance on victims and their PCs without their knowledge.

Most of found C&C servers will be linked to AS29256, which is related to STE (Syrian Telecommunications Establishment) – ste.gov.sy.





№	IP address	Net Block	ISP	ASN	Geolocation
1	46.213.210.210	46.213.128.0 - 46.213.255.255	Syriatel Mobile Telecom	AS29256	DIMASHQ, DAMASCUS
2	216.6.0.28	216.6.0.0 - 216.6.1.255	STE (Syrian Telecommunications Establishment)	AS6453	DIMASHQ, DAMASCUS
3	31.9.48.7	31.9.0.0 - 31.9.127.255	SY-ISP-TARASSUL	AS29256	DIMASHQ, DAMASCUS
4	82.137.200.88	82.137.200.0 - 82.137.207.255	STE (Syrian Telecommunications Establishment)	AS29386	HALAB, ALEPPO
5	46.57.215.104	46.57.192.0 - 46.57.255.255	Syriatel Mobile Telecom	AS29386	DIMASHQ, DAMASCUS
6	31.9.48.119	31.9.0.0 - 31.9.127.255	Syriatel Mobile Telecom	AS29386	DIMASHQ, DAMASCUS
7	94.252.198.112	94.252.192.0 - 94.252.255.255	Syriatel Mobile Telecom	AS29386	DIMASHQ, DAMASCUS
8	82.137.200.92	82.137.200.0 - 82.137.207.255	SY-ISP-TARASSUL	AS29386	HALAB, ALEPPO
9	213.178.227.196	213.178.227.0 - 213.178.228.255	Syrian Computer Society	AS29256	DIMASHQ, DAMASCUS
10	213.178.235.108	213.178.232.0 - 213.178.239.255	Syrian Computer Society	AS29256	DIMASHQ, DAMASCUS
11	82.137.203.60	82.137.200.0 - 82.137.207.255	SY-ISP-TARASSUL	AS29386	DIMASHQ, DAMASCUS
12	82.137.203.45	82.137.200.0 - 82.137.207.255	SY-ISP-TARASSUL	AS29386	DIMASHQ, DAMASCUS

Table 1 – The fragment list of detected C&C servers and attackers sources

Appendix D. Indicators of Compromise

The following list of e-mails and IP addresses shows the sources of spear phishing notifications for the SEA using compromised WEB-resources and various free hosting platforms. It can be used for SIEM/IDS/SOC rules as one of the signs of potential SEA attack.

№	E-mail	IP	GEOLOCATION
1	santorin@ns1.thaiwebhostingserver.net	202.142.223.143	THAILAND, KRUNG THEP, BANGKOK
2	a3947804@srv36.000webhost.com	31.170.160.100	UNITED STATES, OHIO, AMSTERDAM
3	a2462942@srv32.000webhost.com	31.170.160.96	UNITED STATES, OHIO, AMSTERDAM
4	a5021178@srv33.000webhost.com	31.170.160.97	UNITED STATES, OHIO, AMSTERDAM
5	foodcpi@ns1.thaiwebhostingserver.net	202.142.223.143	THAILAND, KRUNG THEP, BANGKOK
6	a2615433@srv20.000webhost.com	31.170.163.246	UNITED STATES, OHIO, AMSTERDAM
7	a4989000@srv23.000webhost.com	31.170.163.253	UNITED STATES, OHIO, AMSTERDAM
8	a9647274@srv29.000webhost.com	31.170.163.249	UNITED STATES, OHIO, AMSTERDAM
9	a2059260@srv12.000webhost.com	31.170.163.251	UNITED STATES, OHIO, AMSTERDAM
10	a6692336@srv29.000webhost.com	31.170.163.253	UNITED STATES, OHIO, AMSTERDAM
11	a2059260@srv12.000webhost.com	31.170.163.247	UNITED STATES, OHIO, AMSTERDAM
12	chocksam@www1.thaihostingserver.net	203.150.8.139	THAILAND, KRUNG THEP, BANGKOK
13	a9932417@srv17.000webhost.com	31.170.163.247	UNITED STATES, OHIO, AMSTERDAM
14	a4613614@srv45.000webhost.com	31.170.163.248	UNITED STATES, OHIO, AMSTERDAM
15	a5548438@srv20.000webhost.com	31.170.163.246	UNITED STATES, OHIO, AMSTERDAM
16	a6035612@srv36.000webhost.com	31.170.163.246	UNITED STATES, OHIO, AMSTERDAM
17	momentok@www1.thaihostingserver.com	203.150.8.141	THAILAND, KRUNG THEP, BANGKOK
18	a3399268@srv9.000webhost.com	31.170.160.73	UNITED STATES, OHIO, AMSTERDAM
19	a4864639@srv38.000webhost.com	31.170.163.247	UNITED STATES, OHIO, AMSTERDAM
20	a2936161@srv48.000webhost.com	31.170.163.248	UNITED STATES, OHIO, AMSTERDAM

№	E-mail	IP	GEOLOCATION
21	a9346965@srv16.000webhost.com	31.170.163.252	UNITED STATES, OHIO, AMSTERDAM
22	jfet@www1.thaihostingserver.com	203.150.8.141	THAILAND, KRUNG THEP, BANGKOK
23	a2631791@srv27.000webhost.com	31.170.163.253	UNITED STATES, OHIO, AMSTERDAM
24	a9264811@srv34.000webhost.com	31.170.163.252	UNITED STATES, OHIO, AMSTERDAM
25	a9463644@srv32.000webhost.com	31.170.163.244	UNITED STATES, OHIO, AMSTERDAM
26	a2091554@srv26.000webhost.com	31.170.163.250	UNITED STATES, OHIO, AMSTERDAM
27	a7779409@srv34.000webhost.com	31.170.163.248	UNITED STATES, OHIO, AMSTERDAM
28	u867721029@srv24.main-hosting.com	31.170.166.251	UNITED STATES, OHIO, AMSTERDAM
29	a2095094@srv44.000webhost.com	31.170.163.246	UNITED STATES, OHIO, AMSTERDAM

Table 2 – The list of source IP addresses for spear phishing notifications for SEA