Syrian Electronic Army

By Contributors to Wikimedia projects

Published: 2012-08-13 · Archived: 2026-04-05 14:53:21 UTC

From Wikipedia, the free encyclopedia

Syrian Electronic Army

Syrian Electronic Army logo

Formation	15 March 2011[1]
Dissolved	Inactive 2021-2024 2024
Purpose	Promoting Pro-Assad Activism
Location	• Syria

The **Syrian Electronic Army** (**SEA**; Arabic: الجيش السوري الإلكتروني) was a group of computer hackers which first surfaced online in 2011 to support the government of former Syrian President Bashar al-Assad. Using spamming, website defacement, malware, phishing, and denial-of-service attacks, it has targeted terrorist organizations, political opposition groups, western news outlets, human rights groups and websites that are seemingly neutral to the Syrian conflict. It has also hacked government websites in the Middle East and Europe, as well as US defense contractors. As of 2011, the SEA has been "the first Arab country to have a public Internet Army hosted on its national networks to openly launch cyber attacks on its enemies".[2]

The precise nature of SEA's relationship with the Ba'athist Syria government changed over time and was unclear.[3]

Origins and historical context

[edit]

In the 1990s, Syrian President Bashar al-Assad headed the Syrian Computer Society, which is connected to the SEA, according to research by University of Toronto and University of Cambridge, UK.[2] There is evidence that a Syrian Malware Team goes as far back as January 1, 2011.[4] In February 2011, after years of Internet censorship, Syrian censors lifted a ban on Facebook and YouTube.[2] In April 2011, only days after anti-regime protests escalated in Syria, Syrian Electronic Army emerged on Facebook.[2] On May 5, 2011 the Syrian Computer Society registered SEA's website (syrian-es.com).[2] Because Syria's domain registration authority registered the hacker site, some security experts have written that the group was supervised by the Syrian state.[5] SEA claimed on its webpage to be no official entity, but "a group of enthusiastic Syrian youths who could not stay passive towards the massive distortion of facts about the recent uprising in Syria".[6] As soon as May 27, 2011 SEA had removed text that denied it was an official entity.[2] One commentator has noted that "[SEA] volunteers might include Syrian diaspora; some of their hacks have used colloquial English and Reddit memes.[7] In July 2011, it emerged that Bashar al-Assad's page on Facebook page was run by a member of the Syrian Electronic Army close to the regime, Haidara Suleiman, the son of powerful intelligence officer and former Syrian ambassador in Amman, Bahjat Suleiman.[8] He told AFP that "the official media is unfortunately weak... This is why we use electronic media to show people what's going on."[8]

According to a 2014 report by security company Intelcrawler, SEA activity has shown links with "officials in Syria, Iran, Lebanon and Hezbollah."[9] A February 2015 article by *The New York Times* stated that "American intelligence officials" suspect the SEA is "actually Iranian".[10] However, no data has shown a link between Iran's and Syria's cyber attack patterns according to an analysis of "open-source intelligence" by cyber security firm Recorded Future.[11]

SEA has pursued activities in three key areas:

- Website defacement and electronic surveillance against Syrian rebels and other opposition: The SEA has carried out surveillance to discover the identities and location of Syrian rebels, using malware (including the Blackworm tool),[4] phishing, and denial of service attacks. As of 2013 this electronic monitoring has extended to foreign aid workers.[12]
- Defacement attacks against Western websites that it contends spread news hostile to the Syrian government: These have included news websites such as BBC News, the Associated Press, National Public Radio, CBC News,[13] Al Jazeera, *Financial Times*, *The Daily Telegraph*,[14] *The Washington Post*,[15] Syrian satellite broadcaster Orient TV, and Dubai-based al-Arabia TV,[16] as well as rights organizations such as Human Rights Watch.[17] SEA targets include VoIP apps, such as Viber[18] and Tango.[19]
- Spamming popular Facebook pages with pro-regime comments:[20] The Facebook pages of President Barack Obama and former French President Nicolas Sarkozy have been targeted by such spam campaigns.[21]
- Global cyber espionage: "technology and media companies, allied military procurement officers, US defense contractors, and foreign attaches and embassies".[22]

The SEA's tone and style vary from the serious and openly political to ironic statements intended as critical or pointed humor: SEA had "Exclusive: Terror is striking the #USA and #Obama is Shamelessly in Bed with Al-

Qaeda" tweeted from the Twitter account of *60 Minutes*, and in July 2012 posted "Do you think Saudi and Qatar should keep funding armed gangs in Syria in order to topple the government? #Syria," from Al Jazeera's Twitter account before the message was removed. In another attack, members of SEA used the BBC Weather Channel Twitter account to post the headline, "Saudi weather station down due to head on-collision with camel."[23] After *Washington Post* reporter Max Fisher called their jokes unfunny, one hacker associated with the group told a *Vice* interview 'haters gonna hate.'"[7]

On 31 October 2014, the SEA released a Linux distribution named SEANux.[24][25]

Timeline of notable attacks

[edit]

- July 2011: University of California Los Angeles website defaced by SEA hacker "The Pro".[26]
- August 2011: Anonymous-run social networking platform Anonplus is defaced. Citizen Lab attributes the attack to the Syrian Electronic Army.[27]
- September 2011: The Harvard University website was defaced when an image was replaced with one of Bashar al-Assad accompanied by the message "Syrian Electronic Army were here".[28]
- April 2012: The official blog of social media website LinkedIn was redirected to a site supporting Bashar al-Assad.[29]
- August 2012: The Twitter account of the Reuters news agency sent 22 tweets with false information on the conflict in Syria. The Reuters news website was compromised, and posted a false report about the conflict to a journalist's blog.[30]
- 23 April 2013: The Associated Press Twitter account falsely claimed the White House had been bombed and President Barack Obama injured. This led to a US$136.5 billion decline in value of the S&P 500 the same day.[31][32]
- May 2013: The Twitter account of *The Onion* was compromised by phishing Google Apps accounts of *The Onion*'s employees. The platform was also used by the hackers to spread pro-Syrian tweets.[33][34]
- 24 May 2013: The ITV News London Twitter account was hacked.[35]
- On 26 May 2013: the Android applications of British broadcaster Sky News were hacked on Google Play Store.[36]
- 17 July 2013: Truecaller servers were hacked into by the Syrian Electronic Army.[37] 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 released Truecaller's alleged database host ID, username, and password via another tweet.[38] On 18 July 2013, TrueCaller confirmed on its blog that only their website was hacked, but claimed that the attack did not disclose any passwords or credit card information.[39]
- 23 July 2013: Viber servers were hacked, the support website replaced with a message and a supposed screenshot of data that was obtained during the intrusion.[40][41][18]
- 15 August 2013: Advertising service Outbrain suffered a spearphishing attack and SEA placed redirects into the websites of The Washington Post, Time, and CNN.[42]

- 27 August 2013: NYTimes.com had its DNS redirected to a page that displayed the message "Hacked by SEA" and Twitter's domain registrar was changed.[43]
- 28 August 2013: Twitter's DNS registration showed the SEA as its Admin and Tech contacts, and some users reported that the site's Cascading Style Sheets (CSS) had been compromised.[44]
- 29–30 August 2013: *The New York Times*, *The Huffington Post*, and Twitter were knocked down by the SEA. A person claiming to speak for the group stepped forward to tie these attacks to the increasing likelihood of U.S military action in response to al-Assad using chemical weapons. A self-described operative of the SEA told ABC News in an e-mail exchange: "When we hacked media we do not destroy the site but only publish on it if possible, or publish an article [that] contains the truth of what is happening in Syria. ... So if the USA launch attack on Syria we may use methods of causing harm, both for the U.S. economy or other."[45]
- 2–3 September 2013: Pro-Syria hackers 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 SEA".[46]
- 30 September 2013: The Global Post's official Twitter account and website were hacked. SEA posted through their Twitter account, "Think twice before you publish untrusted informations *[sic]* about Syrian Electronic Army" and "This time we hacked your website and your Twitter account, the next time you will start searching for new job"[47]
- 28 October 2013: 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 pro-government video on YouTube.[48]
- 9 November 2013: SEA hacked the website of VICE, a no-affiliate news/documentary/blog website, which has filmed numerous times in Syria with the side of the Rebel forces. Logging into vice.com redirected to what appeared to be the SEA home page.[49]
- 12 November 2013: SEA hacked the Facebook page of Matthew VanDyke, a Libyan Civil War veteran and pro-rebel news reporter.[*citation needed*]
- 1 January 2014: SEA hacked Skype's Facebook, Twitter and blog, posting an SEA related picture and telling users not to use Microsoft's e-mail service Outlook.com —formerly known as Hotmail—claiming that Microsoft sells user information to the government.[50]
- 11 January 2014: SEA hacked the Xbox Support Twitter pages and directed tweets to the group's website.[51]
- 22 January 2014: SEA hacked the official Microsoft Office Blog, posting several images and tweeted about the attack.[52]
- 23 January 2014: CNN's HURACAN CAMPEÓN 2014 official Twitter account showed two messages, including a photo of the Syrian Flag composed of binary code. CNN removed the Tweets within 10 minutes.[53][54]
- 3 February 2014: SEA hacked the websites of eBay and PayPal UK. One source reported the hackers said it was just for show and that they took no data.[55]

- 6 February 2014: SEA hacked the DNS of Facebook. Sources said the registrant contact details were restored and Facebook confirmed that no traffic to the website was hijacked, and that no users of the social network were affected.[56]
- 14 February 2014: SEA hacked the Forbes website and their Twitter accounts.[57]
- 26 April 2014: SEA hacked the information security-related RSA Conference website.[58]
- 18 June 2014: SEA hacked the websites of British newspapers *The Sun (United Kingdom)* and *The Sunday Times*.[59]
- 22 June 2014: The Reuters website was hacked a second time and showed a SEA message condemning Reuters for "publishing false articles about Syria". Hackers compromised the website, corrupting ads served by Taboola.[60]
- 27 November 2014: SEA hacked hundreds of sites through hijacking Gigya's comment system of prominent websites, displaying a message "You've been hacked by the Syrian Electronic Army(SEA)." Affected websites included the *Aberdeen Evening Express*, Logitech, Forbes, *The Independent* UK Magazine, *London Evening Standard*, *The Telegraph*, NBC, the National Hockey League, Finishline.com, PCH.com, Time Out New York and t3.com (a tech website), stv.com, Walmart Canada, PacSun, *Daily Mail* websites, bikeradar.com (cycling website), SparkNotes, millionshort.com, Milenio.com, Mediotiempo.com, Todobebe.com and myrecipes.com, Biz Day SA, BDlive South Africa, muscleandfitness.com, and CBC News.[61]
- 21 January 2015: French newspaper *Le Monde* wrote that SEA hackers "managed to infiltrate our publishing tool before launching a denial of service".[62][63]
- 17 May 2018: Two suspects were indicted by the United States for "conspiracy" for hacking several US websites.[64]
- October 2021: Facebook discovers the presence of several fake accounts run by the SEA and its affiliated organizations. The accounts had reportedly been used to target Syrian opposition figures and human rights activists, as well as members of the YPG and White Helmets.[65][66]
- 10 May 2016: Syrian Electronic Army member Peter Romar was extradited from Germany to the United States to face charges brought by the Department of Justice for engaging in a "a multi-year criminal conspiracy to conduct computer intrusions against perceived detractors of President Bashar al-Assad, including media entities, the White House and foreign governments."[67][68]
- 28 September 2016: Peter Romar pled guilty to charges of helping the Syrian Electronic army extort cash from hacking victims.[69][70]

- Advanced persistent threat
- Hacktivism
- Internet censorship in Syria
- PLA Unit 61398
- Tailored Access Operations

1. ^ *"Syrian Electronic Army"*. *Syrian Electronic Army. Archived from the original on 1 September 2014.*

2. ^ Jump up to: *a b c d e f* Noman, Helmi (May 30, 2011). *"The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army"*. Open Net Initiative. Retrieved 22 July 2013.
3. ^ Perlroth, Nicole (17 May 2013). *"Hunting for Syrian Hackers' Chain of Command"*. New York Times. Retrieved 22 July 2013.
4. ^ Jump up to: *a b* Wilhoit, Kyle; Haq, Thoufique (August 29, 2014). *"Connecting the Dots: Syrian Malware Team Uses BlackWorm for Attacks"*. FireEye Inc, cyber security company. Archived from the original (blog) on October 26, 2014. Retrieved October 15, 2014.
5. ^ Gallagher, Sean (May 8, 2013). *"Network Solutions seizes over 700 domains registered to Syrians"*. Ars Technica. Retrieved October 15, 2014. "The Syrian Computer Society acts as Syria's domain registration authority and regulates the Internet within Syria, and is also believed to be connected to Syria's state security apparatus. The Syrian Computer Society registered .sy domain names for the Syrian Electronic Army's servers, giving the hacker group a national-level domain name (sea.sy) rather than a .com or other non-government address, signifying its status as at least a state-supervised operation."
6. ^ Fowler, Sarah (April 25, 2013). *"Who is the Syrian Electronic Army?"*. BBC News. Retrieved October 15, 2014.
7. ^ Jump up to: *a b* Peterson, Andrea (2013-08-15). *"The Post just got hacked by the Syrian Electronic Army. Here's who they are"*. The Washington Post. Retrieved 2013-08-28.
8. ^ Jump up to: *a b* Nahhas, Lynne (11 July 2011). *"Syria's secret war against the cyber dissidents"*. AFP.
9. ^ Robertson, Jordan. *"Three Things You Should Know About the Syrian Electronic Army"*. No. 24 March 2014. Bloomberg. Retrieved 2 February 2015.
10. ^ Sanger, David E. (1 February 2015). *"Hackers Use Old Lure on Web to Help Syrian Government"*. The New York Times. New York Times. Retrieved 2 February 2015. "... the cybervandalism carried out in recent years by the Syrian Electronic Army, which American intelligence officials suspect is actually Iranian, and has conducted strikes against targets in the United States, including the website of The New York Times."
11. ^ King, Rachael (September 5, 2013). *"Data Shows No Link Between Syrian Electronic Army and Iran"*. Wall Street Journal. Retrieved 2 February 2015.
12. ^ Perlroth, Nicole (17 May 2013). *"Hunting for Syrian hackers' Chain of Command"*. New York Times. Retrieved 22 July 2013.
13. ^ *"Syrian Electronic Army claims hack of news sites, including CBC"*. CBC/Radio-Canada. 2014-11-27.
14. ^ Love, Dylan (22 May 2013). *"10 Reasons to Worry About the Syrian Electronic Army"*. Business Insider. Retrieved 22 July 2013.
15. ^ *"Editor's note"*. The Washington Post. August 15, 2013. Retrieved August 15, 2013.
16. ^ "Syrian Electronic Army: Disruptive Attacks and Hyped Targets", OpenNet Initiative, 25 June 2011
17. ^ *"NPR.org Hacked; 'Syrian Electronic Army' Takes Responsibility"*. NPR. 2013-04-16. Retrieved 2013-04-16.
18. ^ Jump up to: *a b* Crook, Jordan (2013-07-23). *"Viber Attacked By Syrian Electronic Army"*. TechCrunch. Retrieved 2019-03-08.
19. ^ Rubenking, Neil J. (2013-07-23). *"Syrian Electronic Army Hacked Tango Chat App; Is Your Site Next?"*. PC Magazine. Retrieved 2019-03-08.
20. ^ Abbas, Mohammed (June 21, 2012). *"Syria activists using U.S. tech to beat curbs"*. Reuters. Retrieved June 21, 2012.

21. ^ Sarah Fowler "Who is the Syrian Electronic Army?", BBC News, 25 April 2013
22. ^ *"Syrian Electronic Army - Hacktivision to Cyber Espionage?" (PDF). intelcrawler.com. IntelCrawler (PGP). 20 March 2014. p. 94. Retrieved 22 March 2015.*
23. ^ *Schroeder, Audra (2013-05-02). "Is it time to start taking the Syrian Electronic Army seriously?". The Daily Dot. Retrieved 2013-08-28.*
24. ^ *"SEANux - a version of Linux from the Syrian Electronic Army". Graham Cluley. Cluley Associates. 13 October 2014. Retrieved 14 November 2014.*
25. ^ *SyrianElectronicArmy (31 October 2014). "#SEANux is now released and available for download!" (Twitterfeed).*
26. ^ *Sterling, Bruce (6 July 2011). "Syrian Electronic Army Invades University of California Los Angeles". Wired. Retrieved 10 September 2013.*
27. ^ *Keizer, Gregg (2011-08-08). "Syrian hackers retaliate, deface Anonymous' social network". Computerworld. Retrieved 2023-01-03.*
28. ^ *Coughlan, Sean (26 September 2011). "Harvard website hacked by Syria protesters". BBC. Retrieved 10 September 2013.*
29. ^ *Holt, Kris (26 April 2012). "Syrian hackers take down LinkedIn's official blog". The Daily Dot. Retrieved 10 September 2013.*
30. ^ *Howell, Martin (5 August 2012). "Reuters Twitter account hacked, false tweets about Syria sent". Reuters. Retrieved 10 September 2013.*
31. ^ Spillus, Alex "Who is the Syrian Electronic Army?", *The Telegraph*, 24 April 2013
32. ^ Peter Foster "'Bogus' AP tweet about explosion at the White House wipes billions off US markets", *The Telegraph*, 23 April 2013
33. ^ *"The Onion's Suspected Twitter Hack Reveals The Syrian Electronic Army's Morbid Humor". TechCrunch. 6 May 2013. Retrieved 2022-02-01.*
34. ^ "How the Syrian Electronic Army Hacked The Onion", Tech Team, *The Onion*, 8 May 2013
35. ^ *"ITV News Twitter account hacked by Syrian Electronic Army". Reuters. May 24, 2013. Retrieved 22 March 2015. "Just kidding. The Syrian Electronic Army was here. "*
36. ^ *Richard Chirgwin (26 May 2013). "Sky News Google Play page defaced". The Register. Situation Publishing. Retrieved 22 March 2015.*
37. ^ "Truecaller Database hacked by Syrian Electronic Army" Archived 2013-07-20 at the Wayback Machine, Sabari Selvan, E Hacking News, 17 July 2013.
38. ^ "TrueCaller hacked, 1 million Indians' data at risk", *The Times of India*, 18 July 2013.
39. ^ "Truecaller Statement" Archived 2013-07-20 at the Wayback Machine, True Software Scandinavia AB, 18 July 2013.
40. ^ "Phone and texting app 'Viber' hacked by Syrian Electronic Army", Scott Buscemi, 9to5Mac, 23 July 2013. Retrieved 24 July 2013.
41. ^ "Free calling app 'Viber' website defaced; database hacked by SEA", Mohit Kumar, *The hacker News*, 23 July 2013. Retrieved 24 July 2013.
42. ^ "Syrian hackers Use Outbrain to Target The Washington Post, Time, and CNN" Archived 2013-10-19 at the Wayback Machine, Philip Bump, *The Atlantic Wire*, 15 August 2013. Retrieved 15 August 2013.
43. ^ *Choney, Suzanne (August 28, 2013). "New York Times hacked, Syrian Electronic Army suspected". NBC News. Retrieved 2013-08-28.*

44. ^ *"Syrian Electronic Army Claims It's Taken Over Twitter's Domain (Updated)"*. *Gizmodo*. *2013-08-27*. *Retrieved 2013-08-28*.
45. ^ Syria's cyber retaliation signals new era of warfare, *USA Today*
46. ^ *"US Marines website hacked – Indistan News"*. *Archived from the original on 24 September 2015*. *Retrieved 14 November 2014*.
47. ^ *"GlobalPost hacked by the Syrian Electronic Army"*. *GlobalPost*. *Retrieved 14 November 2014*.
48. ^ *Paulson, Amanda (29 October 2013). "Syrian Electronic Army says it hacked Obama accounts". Christian Science Monitor. Retrieved 5 November 2013.*
49. ^ *Jha, Abhishek Kumar (9 November 2013). "Syrian Electronic Army hacks, 'vice.com' website redirected to SEA official Website". TechWorm.*
50. ^ *Shira Ovide (1 January 2014). "Skype Social Media Accounts Hacked by Syrian Electronic Army". Wall Street Journal. Dow Jones. Retrieved 22 March 2015.*
51. ^ *Mandalia, Ravi (11 January 2014). "SEA hijacks official Xbox Support Twitter account". Techienews.co.uk. Retrieved 12 January 2014.*
52. ^ *Lucian Constantin (21 January 2014). "Syrian Electronic Army hacks Microsoft's Office Blogs site mere hours after redesign". PCWorld. Retrieved 14 November 2014.*
53. ^ *Winograd, David (24 January 2014). "CNN Sites Get Hacked". Time. Retrieved 24 January 2014.*
54. ^ *Catherine E. Shoichet (January 23, 2014). "Some CNN social media accounts hacked". CNN. Retrieved January 23, 2014.*
55. ^ *"Syrian Electronic Army hacks Paypal and eBay websites"*. *Archived from the original on February 22, 2014*. *Retrieved 14 November 2014*.
56. ^ *Mohit Kumar (6 February 2014). "Facebook domain hacked by Syrian Electronic Army". The hacker News - Biggest Information Security Channel. Retrieved 14 November 2014.*
57. ^ *Eduard Kovacs (14 February 2014). "Forbes Hacked by Syrian Electronic Army [Updated]". softpedia. Retrieved 14 November 2014.*
58. ^ *Brandon Stosh (29 April 2014). "Syrian Electronic Army Hacked and Defaced RSA Conference Website - Freedom hacker". Freedom hacker. Retrieved 14 November 2014.*
59. ^ *"SyrianElectronicArmy on Twitter"*. *Twitter*. *Retrieved 14 November 2014*.
60. ^ *Payne, Samantha (22 June 2014). "Reuters Hacked by Syrian Electronic Army via Taboola Ad". International Business Times. Retrieved 23 June 2014.*
61. ^ *Brandon Stosh (27 November 2014). "Syrian Electronic Army Hacks Forbes, Ferrari, Daily Telegraph, Independent, Intel Among Hundreds of Others". Freedom hacker - Breaking Hacking and Security News. Retrieved 27 November 2014.*
62. ^ *Samuel, Henry (21 January 2015). "Le Monde hacked: 'Je ne suis pas Charlie' writes Syrian Electronic Army". Retrieved 23 March 2016.*
63. ^ *"The hackers managed to infiltrate our publishing tool before launching a denial of service"*. *Reuters*. *21 January 2015*. *Archived from the original on February 1, 2015*. *Retrieved 21 January 2015*.
64. ^ *"Two Members of Syrian Electronic Army Indicted for Conspiracy"*. *17 May 2018*.
65. ^ *Culliford, Elizabeth (2021-11-16). "Facebook says hackers in Pakistan targeted Afghan users amid government collapse". Reuters. Retrieved 2022-02-01.*
66. ^ *"Hackers in Syria, Pakistan taken down by Meta after sustained cyber attacks"*. *Middle East Monitor*. *2021-11-18*. *Retrieved 2022-02-01*.

67. ^ *"Syrian Electronic Army Member Extradited to the United States". www.justice.gov. 2016-05-10. Retrieved 2022-05-03.*
68. ^ *Nakashima, Ellen (2016-05-09). "Syrian hacker extradited to the United States from Germany". Washington Post. ISSN 0190-8286. Retrieved 2022-05-03.*
69. ^ *"Guilty plea for Syrian Electronic Army accomplice". BBC News. 2016-09-30. Retrieved 2022-10-10.*
70. ^ *Weiner, Rachel (2016-09-28). "Syrian refugee pleads guilty in hacking scheme; FBI says masterminds still at large". Washington Post. ISSN 0190-8286. Retrieved 2022-10-10.*

- Syrian Electronic Army on X old account
- Youtube Channel
- Pinterest profile of the Syrian Electronic Army
- VK profile of the Syrian Electronic Army
-
- syrianelectronicarmy.com, first SEA website which was later[*when?*] redirected to its .sy replacement
- sea.sy, SEA's newer website, which SEA started in late May 2013; it has its access revoked by the Syrian Computer Society (site displays blank loading page on browser, and widget returns "ERROR 403: Forbidden" as of August 2013)
- The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army, Helmi Noman, May 30, 2011, published by Information Warfare Monitor, a public-private partnership between University of Ottawa and Secdev Group, including screenshots of SEA activities.
    - google cache of an SEA website mentioned in Information Warfare Monitor report citing "syrian.es.sy" email ID as a contact address and links to a Facebook page named "Vict0r Battalion - Syrian Electronic Army". The page is no longer available starting from September 2013.
- Understanding the Syrian Electronic Army (SEA), HP-Security Research Blog
- Syrian Cyber Hackers Charged - Two From ‘Syrian Electronic Army’ Added to Cyber’s Most Wanted (FBI)
