Syrian Electronic Army

en.wikipedia.org/wiki/Syrian_Electronic_Army

Contributors to Wikimedia projects

Jump to navigation Jump to search

This article needs to be **updated**. Please help update this article to reflect recent events or newly available information. *(October 2020)*

Syrian Electronic Army

Syrian Electronic Army logo

Formation	15 March 2011[1]
Website	sea.sy

Syrian civil war

Timeline

  - January–April 2011
  - May–August 2011
  - September–December 2011
  - January–April 2012
  - May–August 2012
  - September–December 2012
  - January–April 2013
  - May–December 2013
  - January–July 2014
  - August–December 2014
  - January–July 2015
  - August–December 2015
  - January–April 2016
  - May–August 2016
  - September–December 2016
  - January–April 2017
  - May–August 2017
  - September–December 2017
  - January–April 2018
  - May–August 2018
  - September–December 2018
  - January–April 2019
  - May–August 2019
  - September–December 2019
  - 2020
  - 2021
  - 2022

- *Casualties*
- *Cities*
  map
- *Terrorism*
- *Massacres*

Civil uprising in Syria (March–August 2011)

- Daraa
- Baniyas
- Homs (May–August 2011)
- Talkalakh
- Rastan and Talbiseh
- 1st Jisr ash-Shugur
- 1st Jabal al-Zawiya
- Hama
- Latakia

Start of insurgency (Sept. 2011 – April 2012)

- Homs (2011–14)
  - Homs offensive
- 1st Idlib Gov.
  - Syrian–Turkish border
  - Jabal al-Zawiya
  - 1st Idlib City
  - Saraqeb
- 1st Rastan
- Hama Gov.
- Shayrat & Tiyas ambush
- Daraa Gov.
- 1st Rif Dimashq
  - 1st Zabadani
  - Douma
- Deir ez-Zor (2011–2014)
  - Hatla
- Aleppo Gov.
  - Azaz
- 2nd Rastan
- 1st al-Qusayr
- 2nd Idlib Gov.
  - Taftanaz

UN ceasefire; Rebel advances (May 2012 – Dec. 2013)

- 3rd Rastan
- Houla
- Northern Homs
- Al-Haffah
- Al-Qubeir
- Al-Tremseh
- 3rd Idlib Gov.
- 1st Damascus
  - Bombing
- Aleppo
  - Anadan
  - Menagh Air Base
  - Base 46
  - Khan al-Assal
  - 1st Aleppo offensive
  - 2nd Aleppo offensive
- *Syrian Kurdistan*
  - Hasaka campaign
    - Ras al-Ayn
    - al-Yaarubiyah
  - Tell Abyad
  - *Kurdish–Islamist conflict*
- Nubl & Al-Zahraa
- 2nd Rif Dimashq (1st Darayya)
- Abu al-Duhur Airbase

- Quneitra Gov.
- 3rd Rif Dimashq
  - 1st Yarmouk camp
  - 2nd Darayya
- Darayya & Muadamiyat
- Aqrab
- 1st Hama offensive
  - Halfaya
- 1st Safira
- Shadadeh
- 2nd Damascus
- 1st Raqqa campaign (1st Raqqa)
- 1st Daraa offensive
- 4th Rif Dimashq
  - Jdaidet al-Fadl
  - Tadamon
  - Ghouta
- Al-Qusayr offensive
  - 2nd al-Qusayr
- Eastern Ghouta
- 2nd Hama offensive
- Bayda and Baniyas
- 1st Latakia offensive
- Ma'loula
- Sadad
- 5th Rif Dimashq
- 1st Qalamoun
- Adra

Rise of the Islamic State (Jan. – Sept. 2014)

- *Inter-rebel conflict*
    - Northern Aleppo
    - Markada
    - 1st Deir ez-Zor offensive
- al-Otaiba ambush
- Maan
- Hosn
- Morek
- 2nd Daraa offensive
- 2nd Latakia offensive
- 4th Idlib Gov.
- Al-Malihah
- 2nd Wadi Deif
- 2nd Qalamoun
    - Arsal
- Deir ez-Zor (2014–2017)
- 1st Shaer gas field
- 1st Eastern Syria
    - Tabqa Airbase
- 3rd Hama offensive
- 6th Rif Dimashq
- 1st Quneitra
- Kobanî

U.S.-led intervention, Rebel & ISIL advances (Sept. 2014 – Sept. 2015)

- *U.S.-led intervention*
- Homs school bombing
- 3rd Daraa offensive
- 2nd Safira
- 2014 Idlib city raid
- Nusra–FSA conflict
- 2nd Shaer gas field
- 1st Al-Shaykh Maskin
- 2nd Deir ez-Zor offensive
- 3rd Aleppo offensive
- An-26 crash
- 4th Daraa offensive
- Southern Syria
- Eastern al-Hasakah offensive
- 1st Sarrin
- Hama/Homs offensive
- Bosra
- 5th Idlib Gov
  2nd Idlib city
- Al-Fu'ah-Kafriya
- Nasib
- 2nd Yarmouk camp
- 1st Northwestern Syria
- 3rd Qalamoun
- 1st Palmyra
- Western al-Hasakah offensive
- 1st Al-Hasakah city
- Tell Abyad
- Daraa/As-Suwayda
- 2nd Quneitra
- 2nd Sarrin
- 5th Daraa
- 2nd Al-Hasakah city
- 2nd Kobanî
- 4th Aleppo offensive
- 2nd Zabadani
- 2nd Palmyra
- Al-Ghab
- 1st al-Qaryatayn
- Douma market
- 7th Rif Dimashq
- Kuweires offensive

Russian intervention (Sept. 2015 – March 2016)

- *Russian intervention*
- 3rd Quneitra
- 2nd Northwestern Syria
- 3rd Latakia offensive
  - Su-24 shootdown
- 5th Aleppo offensive
- al-Hawl
- Homs offensive
- 6th Aleppo offensive
- 4th Hama offensive
- Tell Tamer
- Tishrin Dam
- 2nd Al-Shaykh Maskin
- al-Qamishli bombings
- Orontes River
- 3rd Deir ez-Zor offensive
- 1st Sayyidah Zaynab
- 7th Aleppo offensive
- 1st Ithriyah-Raqqa
- Al-Shaddadi
- Homs bombings
- 2nd Sayyidah Zaynab
- Khanasir
- 2nd Tel Abyad
- Al-Tanf
- 2nd Al-Qaryatayn
- 3rd Palmyra
- 2nd Maarat al-Nu'man

Aleppo escalation and *Euphrates Shield* (March 2016 – February 2017)

- 8th Aleppo offensive
- 6th Daraa
- 9th–11th Aleppo offensives
- Al-Dumayr
- 1st East Ghouta inter-rebel conflict
- 1st Qamishli
- Aleppo bombings
- 8th Rif Dimashq
- 3rd Shaer gas field
- Northern Raqqa
- Jableh & Tartus
- Manbij
  - Tokhar
- 2nd Ithriyah-Raqqa
- 9th Rif Dimashq
- 12th–14th Aleppo offensives
  - 12th
  - 13th
  - 14th

- 4th Latakia offensive
- 1st Abu Kamal
- 3rd Qamishli
- Atmeh
- al-Rai
- 3rd Al-Hasakah City
- Operation Euphrates Shield
  - Northern al-Bab
  - Dabiq
  - al-Bab
- 5th Hama offensive
- 1st Western al-Bab
- 1st Eastern Qalamoun
- September bombings
- 4th Quneitra
- Deir ez-Zor airstrike
- Aleppo aid convoy attack
- 15th Aleppo offensive
- Khan al-Shih
- 1st Idlib inter-rebel conflict
- 2nd Western al-Bab
- 16th Aleppo offensive
- 2nd Raqqa campaign
- 17th Aleppo offensive
- 4th Palmyra
- Wadi Barada
- 1st Syrian Desert
- Azaz bombings
- 5th Palmyra
- 4th Deir ez-Zor offensive
- 18th Aleppo offensive
- 2nd Idlib inter-rebel conflict
- 7th Daraa
- Qaboun
- 8th Daraa

Collapse of Islamic State in Syria (Feb. – Nov. 2017)

- Eastern Homs offensive
- al-Jina mosque
- 6th Hama offensive
- Tabqa
- Khan Shaykhun
- US Shayrat strike
- Aleppo bus bombing
- April 2017 Turkish airstrikes
- 2nd East Ghouta inter-rebel conflict
- 2nd Syrian Desert
- Maskanah
- East Hama
- 2nd Raqqa
- 9th Daraa
- Southern Raqqa
- Iranian Deir ez-Zor strike
- Ja'din
- Jobar
- 5th Quneitra
- Central Syria
- 3rd Idlib inter-rebel conflict
- 4th Qalamoun
- Deir ez-Zor (2017–2019)
- 2nd Eastern Syria
    - Deir ez-Zor city
    - Euphrates Crossing
    - Mayadin
    - 2nd Abu Kamal
- 7th Hama offensive

Rebels in retreat and *Operation Olive Branch* (Nov. 2017 – Sep. 2018)

- 3rd Northwestern Syria
- Atarib
- Harasta
- Beit Jinn
- *3rd Syrian Desert*
    5th Deir ez-Zor offensive
- 1st Southern Damascus
- Olive Branch
    - Afrin
    - *SDF insurgency*
- Khasham
- Feb. 2018 Israel–Syria incident
- 10th Rif Dimashq (Douma)
- 4th Idlib inter-rebel conflict
- 2nd Southern Damascus
- U.S.-led missile strikes
- Northern Homs
- 2nd Eastern Qalamoun
- 3rd Southern Damascus
- Deir ez-Zor SAA-SDF clashes
- House of Cards
- 1st As-Suwayda
- 2nd Southern Syria
- 2nd As-Suwayda
- 3rd As-Suwayda
- 2nd Qamishli

Idlib demilitarization
(Sep. 2018 – April 2019)

- Idlib demilitarization
    5th Idlib inter-rebel conflict
- Sep. 2018 missile strikes
- Iranian Eastern Euphrates strike
- Northern border clashes
- *Daraa insurgency*
- Manbij bombing
- Baghuz Fawqani
    U.S. airstrike

First Idlib offensive, *Operation Peace Spring*, & Second Idlib offensive (April 2019 – March 2020)

- 4th Northwestern Syria
- Tell Rifaat
- Raqqa & Azaz bombings
- Hass bombing
- Operation Peace Spring (2nd Ras al-Ayn)
- Operation Kayla Mueller
- Northern Syria bombings
- Qah
- 5th Northwestern Syria
  - Balyun
  - Operation Spring Shield
- 2nd U.S.-led missile strikes
- 1st Daraa clashes

Idlib ceasefire (March 2020 – present)

- 6th Idlib inter-rebel conflict
- Ayn Issa
- Qamishli & Al-Hasakah siege
- 3rd Qamishli
- 2nd Daraa clashes
- 7th Idlib inter-rebel conflict
- 3rd Al-Hasakah city
- Abu Khashab massacre

Syrian War spillover and international incidents

Lebanon spillover

- Lebanese–Syrian border
- Sidon
- Iranian embassy bombing
- North Lebanon clashes

- Syrian–Turkish border incidents
  - Turkish F4 shootdown
  - Reyhanlı bombings
  - Turkish occupation of northern Syria
- Kurdish riots

Jordanian–Syrian border incidents

Israeli–Syrian ceasefire line

- February 2018 incident
- May 2018 incident

Iraqi–Syrian border incidents

- Akashat
- al-Shabah
- Western Nineveh
- Western Iraq

Spillover in Iran

- 2017 Tehran attacks
- 2017 Deir ez-Zor missile strike

Spillover in Turkey

- Russian Su-24 shootdown
- Andrei Karlov
- Balyun airstrikes
- Kafr Takharim airstrikes

Iran–Saudi Arabia proxy conflict

Spillover in Europe

Foreign involvement in the Syrian civil war

Foreign intervention in behalf of Syrian Arab Republic

- Russian involvement
  - 2015 military intervention
- Iranian involvement
  - 2017 missile strike
  - Iran–Israel conflict
- 2012 Hezbollah involvement

Foreign intervention in behalf of Syrian Rebels

- Foreign rebel fighters
- Turkish involvement
  - Turkey–ISIL conflict
  - Tomb of Suleyman Shah relocation
  - Euphrates Shield
  - 2017 airstrikes
  - Idlib Governorate operation
  - Afrin operation
  - 2019 Turkish offensive into north-eastern Syria
- Israel's role

U.S.-led intervention against ISIL

- U.S.-led Intervention
  - Timeline
  - List of attacks
  - 2014 rescue operation
  - May 2015 raid
  - 2017 missile strikes
- Qatari involvement
- Jordanian intervention
  - Operation Martyr Muath
- Lebanon's role
- Saudi involvement
  - 2018 bombing
- Dutch involvement
- German intervention
- French intervention
- Australian intervention
- UK intervention

The **Syrian Electronic Army** (**SEA**; Arabic: الجيش السوري الإلكتروني) is a group of computer hackers which first surfaced online in 2011 to support the government of 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 Syrian government has changed over time and is unclear.[3]

Origins and historical context

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]

Online activities

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]

Operating system

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

Timeline of notable attacks

2011

- July 2011: University of California Los Angeles website defaced by SEA hacker "The Pro".[26]
- September 2011: Harvard University website defaced in what was called the work of a "sophisticated group or individual". The Harvard homepage was replaced with an image of Syrian president Bashar al-Assad with the message "Syrian Electronic Army Were Here".[27]

2012

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.[29]

2013

- 20 April 2013: The Team Gamerfood homepage was defaced.[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 homepage.
- 12 November 2013: SEA hacked the Facebook page of Matthew VanDyke, a Libyan Civil War veteran and pro-rebel news reporter.

2014

- 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.[49]
- 11 January 2014: SEA hacked the Xbox Support Twitter pages and directed tweets to the group's website.[50]
- 22 January 2014: SEA hacked the official Microsoft Office Blog, posting several images and tweeted about the attack.[51]
- 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.[52][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]

2015

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]

2018

17 May 2018: Two suspects were indicted by the United States for "conspiracy" for hacking several US websites.[64]

2021

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]

Legal actions

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]

See also

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

References

1. ^ "Syrian Electronic Army". Syrian Electronic Army. Archived from the original on 1 September 2014.
2. ^ 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. ^ a b Wilhoit, Kyle; Haq, Thoufique (August 29, 2014). "Connecting the Dots: Syrian Malware Team Uses BlackWorm for Attacks" (blog). FireEye Inc, cyber security company. 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. ^ 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. ^ 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". 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. ^ Love, Dylan (22 May 2013). "10 Reasons to Worry About the Syrian Electronic Army". Business Insider. Retrieved 22 July 2013.
14. ^ "Editor's note". The Washington Post. August 15, 2013. Retrieved August 15, 2013.
15. ^ a b Crook, Jordan (2013-07-23). "Viber Attacked By Syrian Electronic Army". TechCrunch. Retrieved 2019-03-08.
16. ^ Rubenking, Neil J. (2013-07-23). "Syrian Electronic Army Hacked Tango Chat App; Is Your Site Next?". PC Magazine. Retrieved 2019-03-08.

17. ^ *Abbas, Mohammed (June 21, 2012). "Syria activists using U.S. tech to beat curbs". Reuters. Retrieved June 21, 2012.*
18. ^ Sarah Fowler "Who is the Syrian Electronic Army?", BBC News, 25 April 2013
19. ^ *"Syrian Electronic Army - Hacktivision to Cyber Espionage?" (PDF). intelcrawler.com. IntelCrawler (PGP). 20 March 2014. p. 94. Retrieved 22 March 2015.*
20. ^ *Schroeder, Audra (2013-05-02). "Is it time to start taking the Syrian Electronic Army seriously?". The Daily Dot. Retrieved 2013-08-28.*
21. ^ *SyrianElectronicArmy (31 October 2014). "#SEANux is now released and available for download!" (Twitterfeed).*
22. ^ *Sterling, Bruce (6 July 2011). "Syrian Electronic Army Invades University of California Los Angeles". Wired. Retrieved 10 September 2013.*
23. ^ *Coughlan, Sean (26 September 2011). "Harvard website hacked by Syria protesters". BBC. Retrieved 10 September 2013.*
24. ^ *Holt, Kris (26 April 2012). "Syrian hackers take down LinkedIn's official blog". The Daily Dot. Retrieved 10 September 2013.*
25. ^ *Howell, Martin (5 August 2012). "Reuters Twitter account hacked, false tweets about Syria sent". Reuters. Retrieved 10 September 2013.*
26. ^ Spillus, Alex "Who is the Syrian Electronic Army?", *The Telegraph*, 24 April 2013
27. ^ Peter Foster "'Bogus' AP tweet about explosion at the White House wipes billions off US markets", *The Telegraph*, 23 April 2013
28. ^ *"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.*
29. ^ *Richard Chirgwin (26 May 2013). "Sky News Google Play page defaced". The Register. Situation Publishing. Retrieved 22 March 2015.*
30. ^ "Truecaller Database hacked by Syrian Electronic Army" Archived 2013-07-20 at the Wayback Machine, Sabari Selvan, E Hacking News, 17 July 2013.
31. ^ "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.
32. ^ *Choney, Suzanne (August 28, 2013). "New York Times hacked, Syrian Electronic Army suspected". NBC News. Retrieved 2013-08-28.*
33. ^ *"US Marines website hacked – Indistan News". Archived from the original on 24 September 2015. Retrieved 14 November 2014.*
34. ^ *Paulson, Amanda (29 October 2013). "Syrian Electronic Army says it hacked Obama accounts". Christian Science Monitor. Retrieved 5 November 2013.*
35. ^ *Shira Ovide (1 January 2014). "Skype Social Media Accounts Hacked by Syrian Electronic Army". Wall Street Journal. Dow Jones. Retrieved 22 March 2015.*
36. ^ *Mandalia, Ravi (11 January 2014). "SEA hijacks official Xbox Support Twitter account". Techienews.co.uk. Retrieved 12 January 2014.*
37. ^ *Lucian Constantin (21 January 2014). "Syrian Electronic Army hacks Microsoft's Office Blogs site mere hours after redesign". PCWorld. Retrieved 14 November 2014.*
38. ^ https://twitter.com/CNN/status/426486628946022401

39. ^ Winograd, David (24 January 2014). "CNN Sites Get Hacked". Time. Retrieved 24 January 2014.
40. ^ Catherine E. Shoichet (January 23, 2014). "Some CNN social media accounts hacked". CNN. Retrieved January 23, 2014.
41. ^ "Syrian Electronic Army hacks Paypal and eBay websites". Archived from the original on February 22, 2014. Retrieved 14 November 2014. `{{cite web}}` : CS1 maint: unfit URL (link)
42. ^ Mohit Kumar (6 February 2014). "Facebook domain hacked by Syrian Electronic Army". The hacker News - Biggest Information Security Channel. Retrieved 14 November 2014.
43. ^ Eduard Kovacs (14 February 2014). "Forbes Hacked by Syrian Electronic Army [Updated]". softpedia. Retrieved 14 November 2014.
44. ^ Brandon Stosh (29 April 2014). "Syrian Electronic Army Hacked and Defaced RSA Conference Website - Freedom hacker". Freedom hacker. Retrieved 14 November 2014.
45. ^ "SyrianElectronicArmy on Twitter". Twitter. Retrieved 14 November 2014.
46. ^ Payne, Samantha (22 June 2014). "Reuters Hacked by Syrian Electronic Army via Taboola Ad". International Business Times. Retrieved 23 June 2014.
47. ^ 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.
48. ^ Samuel, Henry (21 January 2015). "Le Monde hacked: 'Je ne suis pas Charlie' writes Syrian Electronic Army". Retrieved 23 March 2016.
49. ^ "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.
50. ^ Culliford, Elizabeth (2021-11-16). "Facebook says hackers in Pakistan targeted Afghan users amid government collapse". Reuters. Retrieved 2022-02-01.
51. ^ Nakashima, Ellen (2016-05-09). "Syrian hacker extradited to the United States from Germany". Washington Post. ISSN 0190-8286. Retrieved 2022-05-03.

External links

- Syrian Electronic Army on Twitter 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 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@gmail.com as a contact address and links to a Facebook page called SEA.Vic0r.2 at Vict0r Battalion - Syrian Electronic Army The page is no longer available as of September 2013.
- Understanding the Syrian Electronic Army (SEA), HP-Security Research Blog

Hacking in the 2010s

Timeline

Major incidents

2010	Operation Aurora Australian cyberattacks Operation ShadowNet Operation Payback
2011	DigiNotar DNSChanger HBGary Federal Operation AntiSec Operation Tunisia PlayStation RSA SecurID compromise
2012	LinkedIn hack Stratfor email leak Operation High Roller
2013	South Korea cyberattack Snapchat hack Cyberterrorism Attack of June 25 2013 Yahoo! data breach Singapore cyberattacks

2014	• Anthem medical data breach • Operation Tovar • 2014 celebrity nude photo leak • 2014 JPMorgan Chase data breach • Sony Pictures hack • Russian hacker password theft • 2014 Yahoo! data breach
2015	• Office of Personnel Management data breach • Hacking Team • Ashley Madison data breach • VTech data breach • Ukrainian Power Grid Cyberattack • SWIFT banking hack
2016	• Bangladesh Bank robbery • Hollywood Presbyterian Medical Center ransomware incident • Commission on Elections data breach • Democratic National Committee cyber attacks • Vietnam Airport Hacks • DCCC cyber attacks • Indian Bank data breaches • Surkov leaks • Dyn cyberattack • Russian interference in the 2016 U.S. elections • 2016 Bitfinex hack
2017	• 2017 Macron e-mail leaks • WannaCry ransomware attack • Westminster data breach • Petya cyberattack 2017 cyberattacks on Ukraine • Equifax data breach • Deloitte breach • Disqus breach
2018	• Trustico • Atlanta cyberattack • SingHealth data breach
2019	• Sri Lanka cyberattack • Baltimore ransomware attack • Bulgarian revenue agency hack • Jeff Bezos phone hacking

Hacktivism	Anonymous associated events CyberBerkut GNAA Goatse Security Lizard Squad LulzRaft LulzSec New World Hackers NullCrew OurMine PayPal 14 RedHack TeaMp0isoN TDO UGNazi Ukrainian Cyber Alliance
Advanced persistent threats	Bureau 121 Charming Kitten Cozy Bear Dark Basin Elfin Team Equation Group Fancy Bear Guccifer 2.0 Hacking Team Helix Kitten Iranian Cyber Army Lazarus Group (BlueNorOff) (AndAriel) NSO Group PLA Unit 61398 PLA Unit 61486 PLATINUM Pranknet Red Apollo Rocket Kitten Syrian Electronic Army Tailored Access Operations The Shadow Brokers Yemen Cyber Army

Individuals	• George Hotz • Guccifer • Jeremy Hammond • Junaid Hussain • Kristoffer von Hassel • Mustafa Al-Bassam • MLT • Ryan Ackroyd • Sabu • Topiary • Track2 • The Jester
Major vulnerabilities publicly disclosed	• Evercookie (2010) • iSeeYou (2013) • Heartbleed (2014) • Shellshock (2014) • POODLE (2014) • Rootpipe (2014) • Row hammer (2014) • JASBUG (2015) • Stagefright (2015) • DROWN (2016) • Badlock (2016) • Dirty COW (2016) • Cloudbleed (2017) • Broadcom Wi-Fi (2017) • EternalBlue (2017) • DoublePulsar (2017) • Silent Bob is Silent (2017) • KRACK (2017) • ROCA vulnerability (2017) • BlueBorne (2017) • Meltdown (2018) • Spectre (2018) • EFAIL (2018) • Exactis (2018) • Speculative Store Bypass (2018) • Lazy FP State Restore (2018) • TLBleed (2018) • SigSpoof (2018) • Foreshadow (2018) • Microarchitectural Data Sampling (2019) • BlueKeep (2019) • Kr00k (2019)
Malware	

2010	• Bad Rabbit • SpyEye • Stuxnet
2011	• Alureon • Duqu • Kelihos • Metulji botnet • Stars
2012	• Carna • Dexter • FBI • Flame • Mahdi • Red October • Shamoon
2013	• CryptoLocker • DarkSeoul
2014	• Brambul • Carbanak • Careto • DarkHotel • Duqu 2.0 • FinFisher • Gameover ZeuS • Regin
2015	• Dridex • Hidden Tear • Rombertik • TeslaCrypt
2016	• Hitler • Jigsaw • KeRanger • MEMZ • Mirai • Pegasus • Petya (NotPetya) • X-Agent

2017	BrickerBot Kirk LogicLocker *Rensenware* ransomware Triton WannaCry XafeCopy
2019	Grum Joanap NetTraveler R2D2 Tinba Titanium Vault 7 ZeroAccess botnet

Retrieved from "https://en.wikipedia.org/w/index.php?title=Syrian_Electronic_Army&oldid=1088747838"