IDC HERZLIYA

ICT International Institute for Counter-Terrorism
With the Support of Keren Daniel

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 11

October – December 2014

Highlights

This report covers the period of October - December 2014 and covers two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The following are among the issues covered in this report:

- On October 16, a fundraising campaign was launched on social networks under the heading, "Help the Mujahideen of Gaza".
- Fursan al-Nashr, a virtual workshop involved in publicity for the Islamic State, launched a series of publications in October 2014 titled, "Security of the Supporter" (*Amn al-Munasir*), explaining how to surf on an Android in a secure and anonymous way using TOR software.
- A visitor to the Shumukh al-Islam jihadist Web forum recommended using Viber and WhatsApp as a platform to publish news items regarding jihadist organizations in Egypt, including distributing publications concerning terrorist attacks and ideology.
- One of the Islamic State's main publicity channels focuses on intensive activity on social networks through the distribution of official messages, informational videos, audio clips and statements, and concentrates efforts on influencing public opinion by disrupting group discourse or online initiatives on social networks that try to criticize the organization.
- The value of the bitcoin virtual currency dropped drastically in 2014, peaking at $1,000 and falling to $300 at the end of the year. Nevertheless, between 40,000-100,000 transactions were made each day in 2014, indicating an increase in bitcoin use.
- A report was published that included an in-depth analysis of the risks of Supervisory Control and Data Acquisition (SCADA) systems in light of the increased number of warnings and publications from security sources in 2014 concerning various malware that damaged infrastructure facilities around the world.

Table of Contents

Electronic Jihad

Global jihad groups are increasingly venturing into cyberspace. Their use of the Internet for "typical" activities – communication, recruitment of operatives, fundraising, propagandizing, incitement to hatred and violence, intelligence gathering, and psychological warfare – is well-established. In recent years, global jihad and other terrorist organizations have begun to use cyberspace as a battleground for what they call "electronic jihad", attacking the enemy by sabotaging its online infrastructure, using the information available to them from the virtual world to cause mayhem in the real world, and developing their own defensive capabilities against cyber-attack. Following is a selection of recent key acts of electronic jihad, and a brief overview of the key themes reflected in jihadist discourse and propaganda.

Key Topics of Jihadist Discourse, October – December 2014[1]

The Indian Subcontinent

- During October-November 2014, Al-Qaeda focused its efforts on advocacy to the Muslim residents of the Indian subcontinent. Ahmad al-Faruq, the head of Al-Qaeda's branch in the Indian subcontinent, accused the Pakistani regime of collaborating with the United States and of systematically killing religious clerics known for their support of the mujahideen. In light of this, he called on Muslims to sanctify war against the Pakistani regime. Another indication of this trend could be seen in the launch of a new English-language magazine, *Resurgence*, by Al-Qaeda. According to the editor, the magazine is designed to serve as a platform for promoting jihad against the regimes in the Indian subcontinent by, among other things, increasing maritime terrorist attacks against commercial vessels.

The Islamic State

- Against the backdrop of the US-led coalition offensive against the Islamic State (IS) in Iraq and Syria, the jihadist discourse denouncing the participating countries became even stronger. Sheikh Abu Bakr al-Baghdadi, the leader of the IS, criticized the coalition offensive and

[1] For a more thorough review of jihadist life on the Web, see the ICT's Jihadi Website Monitoring Group's Periodic reports, at http://www.ict.org.il/ContentWorld.aspx?ID=21

emphasized that it was a war doomed to fail. According to him, the IS continues to expand despite the failing war and is appending additional provinces and territories, like in North Africa. In addition, he declared that he accepts the oath of allegiance by various jihadist groups to the IS and called on Muslims to join the IS provinces closest to where they live. Meanwhile, the organization waged a psychological war against coalition forces by threatening to attack Western targets, such as those of the US and Britain, and by releasing statements saying that the war is doomed to fail.

The coalition's war even triggered angry responses from several Al-Qaeda branches, such as Al-Qaeda in the Islamic Maghreb (AQIM) and the Al-Nusra Front in Syria, which expressed certainty in the war's failure and called on Muslims to resist the coalition forces. Jund al-Khilafa, a Salafi-jihadist organization in Algeria, threatened to execute a French citizen being held captive by the organization if France does not stop its war against members of the IS.

Syria

- The Al-Nusra Front, Al-Qaeda's affiliate in Syria, threatened to kill Lebanese soldiers being held captive by the organization. In order to spare their lives, the organization demanded that the Lebanese army lift its siege from the city of Tripoli and end its aggression against the local Sunni population.

Arabian Peninsula

- Al-Qaeda in the Arabian Peninsula intensified its publicity against the Houthis, a Shi'ite minority in Yemen, against the backdrop of the group's increasing power due to its cooperation with Iran.

The Sinai Peninsula and Egypt

- October-November 2014 saw an increase in operations by the Salafi-jihadist movement in the Sinai Peninsula and Egypt. The jihadist organization, Ansar Bayt al-Maqdis, which operates in Sinai, swore allegiance to the IS and changed its name to the "Islamic State in the Sinai Province". Another organization called "Ajnad Misr", which operates in Egypt, announced the establishment of a media wing called "Al-Kinana", to be responsible for posting publicity

materials, including claims of responsibility for terrorist attacks against Egyptian security forces. In addition, the IS revealed a growing interest in the arena in light of the publication of a collection of tips for the mujahideen in Egypt by one of its members. He recommended bringing the battle against the infidels to Cairo and other large cities, such that Sinai will serve as the base from which they go out to war, attack government headquarters and offices, receive immigrants who came to wage jihad in the country and attack infidel groups like the Christians.

Jihadist Propaganda

- On October 16, a fundraising campaign was launched on social networks under the heading, "Help the Mujahideen of Gaza". The campaign was attributed to the Palestinian organization, "Al-Nasser Salah al-Deen Brigades - al-Tawhid Brigade".[2] On December 12, 2014 a hashtag[3] for the campaign was created in order to further promote the fundraising campaign for the organization, under the name: "Hand in hand in order for us to help the mujahideen in Gaza".[4]

[2]#للتواصل_مع_حملة_مدد_مجاهدي_غزة

[3]A hashtag is a word or an unspaced phrase prefixed with the hash character (or number sign), #, to form a label. It is a type of metadata tag .

[4]#يداً_بيد_لنكن_المدد_لمجاهدي_غزة

Banner providing the contact details for giving a donation

Banner explaining how supplies and weapons will be purchased for the mujahideen in the Gaza Strip using donation money

Defensive Tactics

- Fursan al-Nashr, a virtual workshop involved in publicity for the Islamic State, launched a series of publications in October 2014 titled, "Security of the Supporter" (*Amn al-Munasir*), explaining how to surf on an Android in a secure and anonymous way using TOR software. The series included four lessons, accompanied by videos, explaining how to safely and anonymously browse on an Android device by using TOR software.[5]

The banners of the two videos

- A Twitter account named "Security Tips", which expresses support for the IS, published a series of three lessons on the topic of cyberspace titled, "Mujahid Security". The first two lessons provided an introduction to the world of hacking.[6] The third lesson explained how to use the Windows, Mac and Linox operating systems on laptop and desktop computers.[7]

The logo for the "Mujahid Security" series

- At the end of October 2014, the veteran Hanein jihadist Web forum, which focuses mainly on the Iraqi arena, announced that it was ending its activities. According to the forum's management, the reason for this step had to do with a fear of widening the rift among visitors

[5] https://twitter.com/eyes_of_nation/status/521745450656075776
https://www.youtube.com/channel/UChvkjkZAnGPjHILFaNDopcQ
https://shamikh1.info/vb/showthread.php?t=227608 https://www.youtube.com/watch?v=BwEzuCMvSYg
[6] http://justpaste.it/hafv; http://justpaste.it/2nd_amnyat
[7] http://justpaste.it/3d_amnyat

concerning the question of loyalty to the IS or to Al-Qaeda. In addition, an IS activist warned the forum's public not to enter the Twitter account claiming to represent the Hanein Web forum or to click on the links posted on the account, claiming that there may be security issues.[8]

- A visitor to the Shumukh al-Islam jihadist Web forum noted that, in light of the Crusader coalition offensive against the IS, one must exercise precautions and safe surfing on the Internet. Therefore, it published software called CyberGhost VPN, designed to ensure anonymous browsing on the Internet.[9]

A screenshot of the CyberGhost software

- A visitor to the Shumukh al-Islam jihadist Web forum recommended using Viber and WhatsApp as a platform to publish news items regarding jihadist organizations in Egypt, including distributing publications concerning terrorist attacks and ideology. According to him, he had already been busy distributing news on the topic for several months and gained approximately 500 followers through Viber. He recommended expanding the framework for distributing jihadist materials via these platforms in order to reach tens of thousands of users. According to him, one user can distribute materials to 1,000-2,000 people per day, on average. He added that he had turned to the management of the Shumukh al-Islam jihadist Web forum and raised this issue to them but that he did not see the issue formally addressed. In response, the visitor

[8] https://twitter.com/a ss/status/530725090862710784
[9] https://shamikh1.info/vb/showthread.php?t=230176

recommended contacting him personally regarding expanding advocacy for jihadist organizations in Egypt.[10]

Offensive Tactics

- An anonymous jihad activist on the social network, Twitter, who calls himself Suna al-Malahim ("Creators of the Wars"), declared the establishment of a hacker group called "The Islamic State Hacker Group". According to him, the purpose of the group is to hack into the accounts of Shi'ite activists on social networks, such as Twitter and Facebook, and vandalize them.[11] The announcement (see photo below) was signed by the two founders of the group: Suna al-Malahim and Muhattim Jamajim al-Murtadin ("Smasher of Infidel Muslim Skulls").[12] Members of the group posted a video to YouTube documenting how they hacked into several Facebook accounts belonging to Iraqi Shi'ite soldiers.[13]

[10] https://shamikh1.info/vb/showthread.php?t=230365
[11] https://twitter.com/A_H_M_E_D__1/status/529762459880808448.#فريق_هكر_الدولة_الإسلامية .
[12] https://twitter.com/A_H_M_E_D__1/status/530726479844233216
https://twitter.com/a_____ss/status/530376255401500673
[13] https://www.youtube.com/watch?v=RRiXHhYwO-0&feature=youtu.be

The photos show the Facebook accounts of Iraqi Shi'ite soldiers that were breached by the hacker group, according to a jihad activist

The announcement regarding the establishment of a hacker group serving the Islamic State

Guiding

- Fursan al-Nashr, a virtual workshop involved in publicity for the Islamic State, launched a series of publications titled, "Al-Batar lil-Muntaj Course". The first two instructional videos covered how to install and use the Sony Vegas video-producing software.[14] The group itself published 'crack' to enable free use of the software.[15]

The banners of the two videos

[14] #دورة_البتار_للمونتاج

[15] https://twitter.com/alnosrahalyama2/status/536881186472083456

- A prominent visitor in the technical field on the Al-Minbar Al-Iʿlami Al-Jihadi Web forum published an announcement titled, "Are Internet Service Providers Tracking Users?" In the announcement, the writer discussed whether ISP's are cooperating with various governments around the world and providing them with information for tracking Muslims. First, the writer explained basic terms: Internet Service Provider (ISP) is the body through which all Internet surfing traffic passes. SSL encryption is an Internet traffic encryption program that is not widespread in Arab countries where there are no policies protecting users. In addition, the writer explained the law in the United States; under certain conditions, Internet providers must cooperate with the government but a court order is needed and it is illegal to keep private data for more than six months. The visitor even claimed that most American companies – including Google, Facebook and Yahoo – are nothing but an arm of American Intelligence agencies. The writer referred to laws in other countries as well, but explained that in all cases there is great confusion regarding ISP's cooperation with governments and that the matter is not transparent to the public.

  According to the writer, the answer to the question raised is affirmative: governments are aided by ISP's in order to track users and they legislate laws that enable them to get information about Internet traffic for the purpose of investigation. The writer explained that ISP's have information about each and every action taken by a user: Web history, email use, file uploads to an FTP server, etc., and they keep data regarding visit time to various sites. The writer emphasized that every action performed by a user on the Internet can be used against him as long as he is not careful to encrypt his movements.[16]
- A visitor to the Shumukh al-Islam jihadist Web forum published correspondence in which he explained how to build systems to prevent transmission between mobile handsets.[17]

[16] https://www.alplatformmedia.com/vb/showthread.php?t=62386
[17] https://shamikh1.info/vb/showthread.php?t=230201

- A visitor to the Shumukh al-Islam jihadist Web forum published a series of online classes on how to upload propaganda materials to the 'archive' storage site.[18]

- A jihad activist uploaded to his Twitter account an explanation on using the 'rapidleech' Web site in order to post and share videos.[19]

[18] https://shamikh1.info/vb/showthread.php?t=227297
[19] https://twitter.com/abu_osid/status/510782206902824960

- A Twitter user named Abu Khadija al-Muhajir, who is identified with the IS, published a guidebook on how to securely use the Internet titled, "Guide for the Supporter" (*Dalil al-Munasir*).

  The writer claimed that one can hide information related to DNS, IP, MAC address, Serial Number of a hard drive in one of the following ways:[20]

  - Creating fake email accounts on Google.[21]
  - Camouflage the IP by using the CyberGhost VPN software.
  - Ensure secure use of cell phones by using the Tor network.[22]
  - An explanation on using the Tor network on unsecured Apple computers.[23]

"Guide for the Supporter"

- A prominent visitor to the Al-Minbar Al-Alami Al-Jihadi Web forum published a statement concerning the closure of Twitter accounts and the planting of malicious links. In the statement, the writer suggested taking several precautions that, according to him, would protect against attacks by Saudi hackers: do not open suspicious links, do not enter an email address on unknown Web sites, and when coming across a suspicious situation that looks like a breach – try to warm Muslims.[24]

[20] https://shamikh1.info/vb/showthread.php?t=227328
[21] https://justpaste.it/D3m_isis
[22] https://justpaste.it/Tor_is
[23] http://justpaste.it/hg6u
[24] https://www.alplatformmedia.com/vb/showthread.php?t=69722

- The administrator of the Al-Jihad Al-Alami Web forum published an announcement regarding the transfer of messages via the forum in which he recommended protecting the security of forum members by sending messages via a private messaging interface, or any other interface, only using the Asrar Al-Mujahideen encryption software.[25]
- One of the administrators of the Al-Platform Media Web forum published a document titled, "Important Advice for Self-Defense and Computer Protection". The document described the various threats to computers, including viruses and spyware, as well as possible solutions such as anti-virus software, Firewall and Web surfing on a secure browser.[26]
- Al-Nusra Al-Yamaniyya, a group of jihad activists in Yemen that supports the IS, published on Twitter links to videos and guidebooks explaining how to use various software to produce PR videos and photos as part of a PR campaign for the IS. For example, it provided an explanation on how to use the Pinnacle Studio 15 HD software.[27]

[25] https://www.alplatformmedia.com/vb/showthread.php?t=70116
[26] https://www.alplatformmedia.com/vb/showthread.php?t=73709
[27] #دورة_الأنصار_في_المونتاج

A banner titled, "The Second Course in a Montage for the Intermediate Level"

Social Media

One of the central components of the Islamic State's PR campaign is focused on intensive activity on social networks through the distribution of official messages, PR videos, audio clips, statements, etc., as well as through a concentrated effort to influence public opinion by, among other things, disrupting the discourse of groups or online initiatives on social networks that try to criticize the organization.

The following are several examples of this issue:

- In the beginning of October, IS activists created hashtags under the title: "Hīt under the Banner of the Caliphate", "Hīt by the Islamic State" and "Liberated Hīt". The correspondence was intended to raise the spirit of IS activists and to sow psychological fear among the Iraqi security forces in light of the occupation of Hīt, which is located in Al-Anbar Province in Iraq – 150 km. from Baghdad. For example, one activist explained that the city serves as an important strategic point for future conquests in Iraq.[28]

[28] #هيت_بيد_الدولة_الإسلامية, #هيت_تحت_راية_الخلافة, #هيت_تتحرر

A map posted by a member of the organization noting the location of Hīt

- In another discussion, several members of the organization tried to incite Sunnis in Tripoli, Lebanon, to protest against the Lebanese army for its oppressive policies against the Sunni population in the country, especially in Tripoli. This discourse was focused on the hashtags, "Tripoli in Al-Sham in Angry Protest", "Lebanon's Muslim Revolution" and "Tripoli in Al-Sham Helping the Caliphate", and gained momentum towards the end of October 2014. One activist noted that the Lebanese army was preventing Sunnis from moving from Lebanon to Syria in order to help in the fight against Bashar al-Assad's security forces and, therefore, Sunnis must protest against this move.[29]

The banner posted by an IS activist – at the bottom of the banner it reads: "Tripoli in Al-Sham in Angry Protest"

[29] #طرابلس_الشام_تنتفض, #ثورة_لبنان_المسلم, #طرابلس_الشام_تستنصر_الخلافة

- Members of the organization made an effort to show that it has earned cross-border support by creating of various hashtags on the subject. On October 13, 2014, for example, the hashtag "Oath of Allegiance by Taliban-Pakistan Leaders to the Caliphate" was created. One activist write, "The Iraqis swore allegiance, the Syrians swore allegiance, the Libyans swore allegiance, the Nigerians swore allegiance, and the mujahideen in Yemen slandered [the organization]."[30] Later that month, the hashtag "Saad al Hunaiti Swore Allegiance to the Caliph" – referring to the former kadi of the Al-Nusra Front – was created.[31] In another hashtag, members of the organization called on the factions fighting in Libya to swear allegiance to the Caliph, Abu Bakr al-Baghdadi.[32] Another hashtag called on Muslims to emigrate to the caliphate in Libya and join the war of jihad against the enemies of Islam.[33] On November 7, 2014 the hashtag "Oath of Allegiance by 30 Kurdish Villages to the Caliph of the Muslims" was created.[34] Other hashtags that were created included: "Soldiers of Yemen Swear Allegiance to the Caliph",[35] "Lions of the Arabian Peninsula Swear Allegiance to the Caliph",[36] and "Ansar Bayt al-Maqdis Swears Allegiance to the Caliph".[37]

A banner showing a former senior commander in the Taliban-Pakistan who swore allegiance to the IS

[30] #بيعة_قادة_طالبان_باكستان_للخلافة
[31] #سعد_الحنيطي_يبايع_الخليفة
[32] #دعوة_الفصائل_الليبية_لبيعة_الخليفة
[33] #دعوة_للهجرة_الى_أرض_الخلافة_بليبيا
[34] #بيعة_30قرية_كردية_لخليفة_المسلمين
[35] #جند_اليمن_تبايع_الخليفة
[36] #أسود_الجزائر_تبايع_الخليفة
[37] نصار_بيت_المقدس_تبايع_الخليفة

- On October 17, 2014 the hashtag "First Jihadist Plane in History" was created. Members of the organization referred to a rumor according to which the IS had used a plane, and they praised the act. Several activists noted that if the rumor is true, it would better to use aircraft in order to bomb targets in the fields of Saudi Arabia. Another activist noted that the IS has several talented pilots who can be provided with planes from enemy bases and another activist tweeted that the IS had managed to take control of a MiG aircraft.[38]

The banner that was posted to Twitter with the caption "Islamic State Pilot"

- On October 21, 2014 it was published[39] on the Al-Akhbar Web site, in English, that a religious cleric in Saudi Arabia had recently ruled that the social network Twitter is a "source of lies". Sheikh Abdul Aziz Āl Sheikh declared in a fatwa that a local television broadcast on October 20 had stated that "if used properly, it could be of real benefit but, unfortunately, it is used for trivial matters", and therefore it serves as "a source of all evil and destruction" because "people flock to it thinking that it is a reliable source of information but it is a source of lies and untruths."
- On October 25, 2014 an advocacy group called "The Shameful Actions of the Secular" ("Fadhaih al-Ulmaniyya"), which focuses on advocacy for the IS, launched an online PR campaign calling on Muslims in Tunisia to avenge the deaths of Tunisian martyrs who were

[38] #أول_طيران_جهادي_في_التاريخ, #اول_طلعة_جوية_للدولة_الإسلامية
[39] http://english.al-akhbar.com/content/saudi-mufti-twitter-source-all-evil

killed by Tunisian security forces and to take action to free women from Tunisian prisons. In the framework of the campaign, the names of senior Tunisian government officials were suggested as targets for assassination due to their alleged involvement in the imprisonment and killing of women in the country.[40]

From left to right: a banner calling for the killing of Mohamed Ali Aroui, spokesman for the Tunisian Ministry of the Interior, due to his involvement in the killing and humiliation of Muslim women; a banner calling to avenge the deaths of Tunisian martyrs – produced by the "Al-Minhaj" media institution, which is involved in advocacy for the Islamic State.

- In the beginning of November 2014, activists from Ansar Bayt al-Maqdis, which joined the IS and changed its name to the Islamic State in the Sinai Peninsula, waged a PR war on social networks against Egyptian activists who condemned the organization and its supporters. Members of the organization created the following hashtags: "Sinai is the Lions' Den of the Monotheists", "The Sinai Province is Expanding and Al-Sisi is Raging with Hysteria", "A Campaign to ban Al-Sisi's Pigs" – which included calls to act against the Egyptian army and its President, Abdel Fattah al-Sisi, for their crimes against the Sunnis.[41] On the other side, Egyptian activists supporting the regime created the following hashtags: "A Campaign to ban Daesh (referring to the IS) Activists on Twitter", "Sinai is a Graveyard for Terrorists", and "We are All the Egyptian Army". The Egyptian activists expressed solidarity with, and support for, the Egyptian army, they called for the publication of official documents from the Egyptian Ministry of Defense and the Egyptian Army lauding their triumphs in eradicating terror nests in the Sinai Peninsula, and they called for reporting to the Twitter management the existence of accounts belonging to the organization in order to shut them

[40] #الثأر_لشهيدات_تونس

[41] #حملة_حظر_خنازير_السيسي, #سيناء_عرين_الموحدين, #ولاية_سيناء_تتمدد_والسيسي_يتخبط

down.[42]

A banner posted by a jihad activist in which it states that Gamal Abdel Nasser and Abdel Fattah al-Sisi are Jews who ruled Egypt and fought against Muslims many times

- In the beginning of November 2014, members of the IS created several hashtags concerning the importance of liberating the Arabian Peninsula from the Saudi regime by, among other things, calling on Muslims in the Saudi Kingdom to act against the regime. For example, the following hashtags were created: "Deployment of the Supporters in the Land of the Two Holy Places",[43] "Operations by Supporters of the State in the Land of the Two Holy Places",[44] "The Islamic State is Preparing to Liberate the Land of the Two Holy Places",[45] and "The Islamic State Soon in the Arabian Peninsula".[46]
- Against the backdrop of the published announcement by the Finance Bureau of the Islamic State during the first half of November 2014, regarding the minting of coins to be officially used in areas under the organization's control, several hashtags were created on the topic, such as "Campaign to Get Rid of the US Dollar Currency" and "Casting a Special Currency for the Islamic State". The discourse was mainly characterized by expressions of joy on the move and wishful thinking that it will cause damage to the global economy and to the finances of Muslim rulers. There were also anti-Semitic remarks that this move could weaken the Jews' grip on the global economy.[47]

---

[42] #سيناء_مقبرة_الارهابيين, #كلنا_الجيش_المصري, #حملة_حظر_دواعش_تويتر
[43] #أستعداد_الأنصار_في_بلاد_الحرمين
[44] #عمليات_أنصار_الدولة_ببلاد_الحرمين
[45] #الدولة_الإسلامية_تتأهب_لتحرير_بلاد_الحرمين
[46] #الدولة_الإسلامية_قريباً_في_جزيرة_العرب
[47] #حملة_التخلص_من_عملة_الدولار_الأمريكي

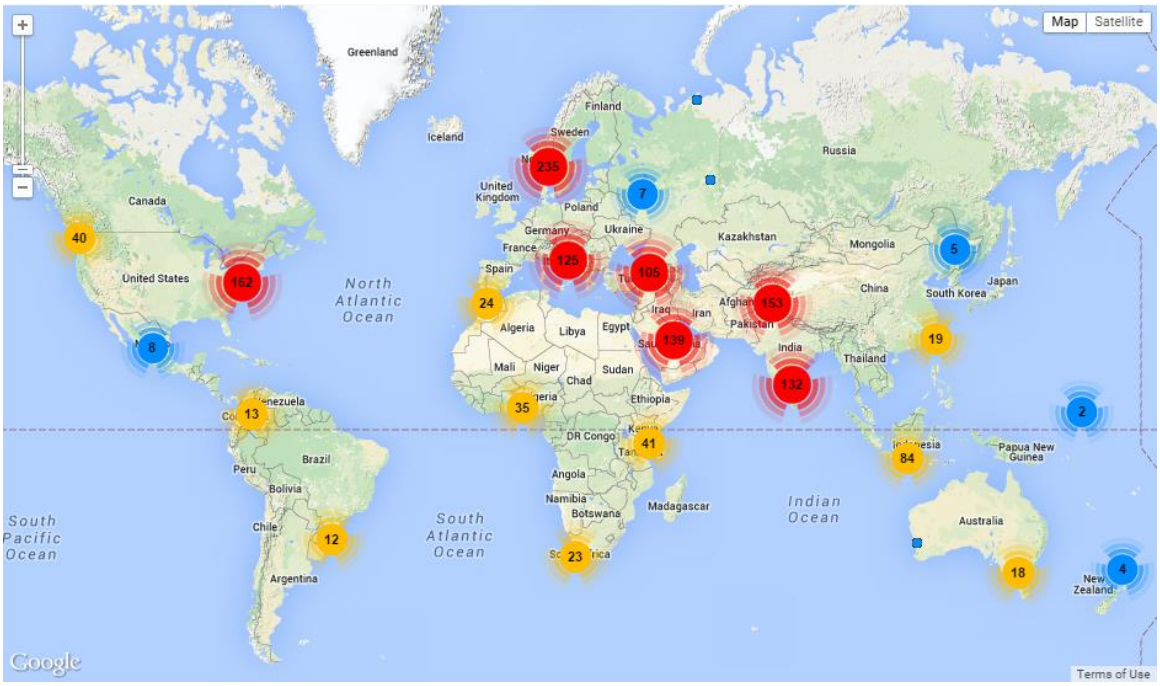
The Islamic State dinar

- The Islamic Emirate in Afghanistan declared the creation of official Twitter and Facebook accounts to serve as its official platforms: https://twitter.com/alemara1arabic and https://www.facebook.com/IEA.ar2.[48]

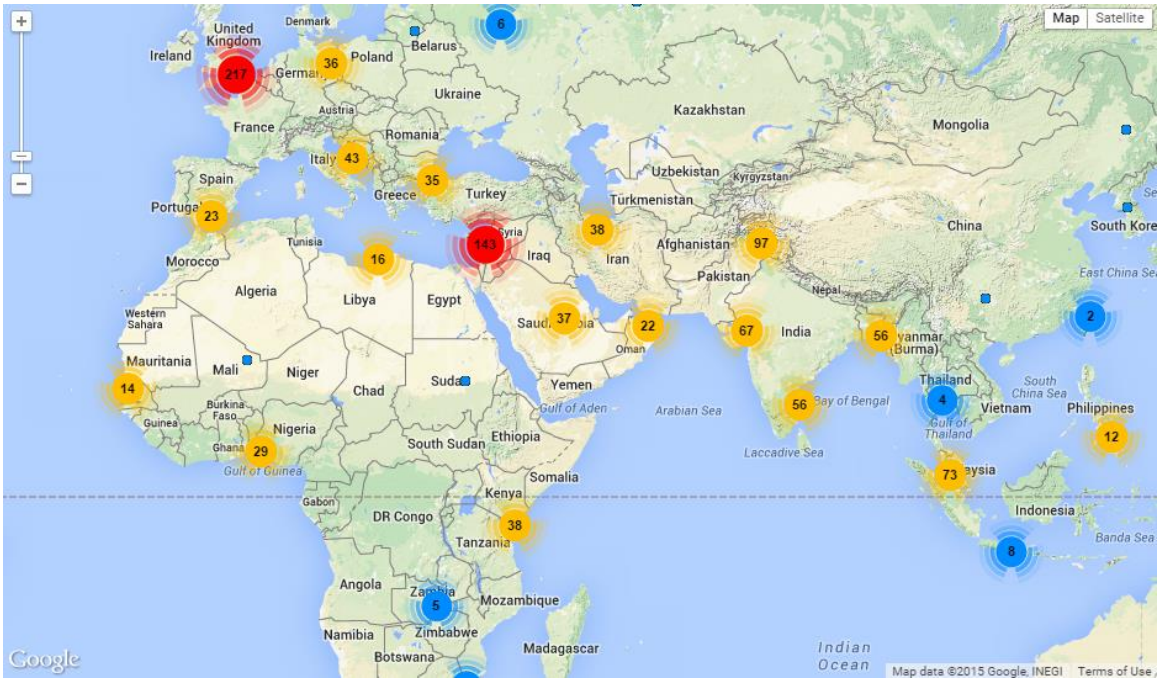
- On October 27, 2014 the Fursan al-Mashr virtual workshop, which is involved in publicity for the Islamic State, announced the reopening of its Twitter account for the fifth time after its previous accounts were closed by the Twitter management.[49]
- A visitor to the Al-Minbar Al-Alami Al-Jihadi Web forum published a guidebook designed to help identify fictitious Facebook pages created by security forces in order to track the mujahideen. The guidebook detailed several recommended precautions, including: beware of friend requests from people with whom you have no common friends, and check if the relevant account is active and shows regular activity or if the only activity apparent on the page is the addition of new friends.[50]

[48] https://al-fidaa.com/vb/showthread.php?t=104225
[49] https://twitter.com/Forsan_N9
[50] http://alplatformmedia.com/vb/showthread.php?t=66517

- In mid-December, Mehdi Masroor Biswas, a 24-year-old from Bangalore, India, who ran the Twitter account, ShamiWitness, was arrested.[51] The account published approximately 130,000 tweets, most of which were in praise of the IS. Mehdi was accused of spreading messages, recruiting and propaganda. An examination of his account activity showed that the account was created in 2009 and had approximately 18,000 followers. Mapping and analysis of some of the users who followed the account showed that the account was popular in the Middle East and in Britain.



[51] http://www.bbc.com/news/world-asia-30461455



Mapping of accounts that followed ShamiWitness[52]

The Syrian Electronic Army

On October 1, the Syrian Electronic Army announced[53] that it had launched a new version of its Web site; the Web address remained the same but the interface was completely changed.[54] The Web site, which was built and designed by the Syrian Electronic Army's 'programming unit', constitutes the fourth version of the organization's site over the years and includes the same categories and links to various social networks as it did previously. On October 12, the Syrian Electronic Army posted a Twitter message regarding the organization's account on the Russian social network, VK. This message referred to a slightly more detailed message on the organization's Web site in which it discussed the move from Facebook to the Russian VK social network due to the repeated closing of the Facebook account by network management and due to the need for a static page for upcoming events.

[52] https://followerwonk.com/IPoY
[53] https://twitter.com/Official_SEA16/status/517060262827134976
[54] http://sea.sy/index/en

A screenshot of the VK Web site

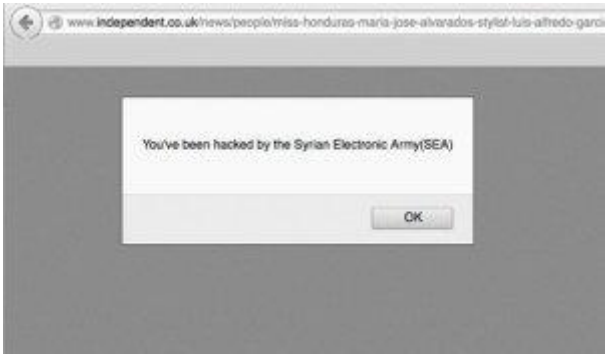
An examination of this account's activity[55] revealed that it is not a new account (according to the account profile, it was created on April 2, 2011) and that it contains messages that start on September 12, 2013 when the profile published hundreds of announcements, photos and links.

On December 9, it was published that the Syrian Electronic Army's programming department had launched the organization's new mobile site.[56]

[55] https://vk.com/syrianelectronicarmy
[56] https://twitter.com/Official_SEA16/status/542410203866476544

Major Attacks

After several months of silence, the Syrian Electronic Army returned to action on November 25 and again attacked several British media outlets, including the Telegraph, the Independent, Forbes, Time Out, PC World, and the Evening Standard. When users entered these Web sites, they received a message that the sites had been hacked by the organization.



The Syrian Electronic Army published an announcement[57] regarding an incident on its Twitter account, according to which it had hacked into the management system of the company, Gigya.

The Telegraph published on its Twitter account an announcement[58] regarding a breach that it

[57] https://twitter.com/Official_SEA16/status/537960538752311301

said originated with a third party.

Later, the Independent also published an announcement about this on its Twitter account[59] and on its Web site.[60]

In the evening hours, the CEO of Gigya published the following statement:[61]

"At approximately 6:45 AM EST we identified sporadic failures with access to our service. An initial inquiry has revealed that there was a breach at our domain registrar that resulted in the WHOIS record of gigya.com being modified to point to a different DNS server. That DNS server had been configured to point Gigya's CDN domain (cdn.gigya.com) to a server controlled by the hackers, where they served a file called "socialize.js" with an alert claiming that the site had been hacked by the Syrian Electronic Army.

---

[58] https://twitter.com/Telegraph/status/537952663321972736
[59] https://twitter.com/Independent/status/537993403708231681
[60] http://www.independent.co.uk/life-style/gadgets-and-tech/news/syrian-electronic-army-hack-hits-sites-using-gigya-but-all-data-safe-9887503.html
[61] http://blog.gigya.com/regarding-todays-service-attack/

To be absolutely clear: neither Gigya's platform itself nor any user, administrator or operational data has been compromised and was never at risk of being compromised. Rather, the attack only served other JavaScript files instead of those served by Gigya.

The WHOIS record was corrected at 7:40 AM EST. However, due to the nature of WHOIS and DNS operation, this fix is expected to take more time to fully propagate. If you still experience issues in the next hour, please contact Gigya Support.

Gigya has the highest levels of security around our service and user data. We have put additional measures in place to protect against this type of attack in the future."

In short, it seems that there was no breach of Gigya's media sites or its systems, but rather there was only a breach of Gigya's domain registrar, which affected its clients among the British media. Indeed, an article that was published on the topic by the Independent[62] noted that "hackers attacked the Gigya DNS entry at GoDaddy".

This was not the first time that the Syrian Electronic Army attacked various media sites, especially British ones, both directly and, as in this case, through a service provider. In this framework, the Web sites of Financial Times, the Telegraph, Forbes, the Sun, the Sunday Times, Wall Street Journal, the ITV television network and CNN's social networks were all hacked.

In addition, in February 2014, a similar incident occurred in which a breach of MarkMonitor's management system enabled these hackers to gain access for half an hour to some of Pay Pal and eBay's domain name addresses.

On December 17, the organization published an announcement according to which it had hacked into the Web site of the International Business Times and posted its own message on the site.

[62] http://www.independent.co.uk/life-style/gadgets-and-tech/news/syrian-electronic-army-hack-hits-sites-using-gigya-but-all-data-safe-9887503.html

In a message showing the presence of members of the organization in managing the news site's content.

While directing to a page containing documentation[63] of the breach and the message that was posted to the site. Within a short while, the news site published an article confirming the breach.[64]

Cyber-Crime and Cyber-Terrorism, October – December 2014

Recent years have seen an increasing number of cyber-attacks on political targets, critical infrastructure, and the Web sites of commercial corporations. These attacks, which are also receiving increasing amounts of international attention, are perpetrated by states (which do not take responsibility for them), groups of hackers (such as Anonymous), criminal organizations and lone hackers. We believe that terrorist organizations are working in close collaboration with

[63] http://www.zone-h.org/mirror/id/23407363
[64] http://www.ibtimes.com/syrian-electronic-army-hacks-international-business-times-website-1762097

criminal organizations, are learning from their attempts [at cyber-crime], and may even be hiring their services. In light of this, it is important to examine and analyze cyber-crimes attributed to criminal organizations, as well as new development trends and patterns. The following information was culled from the visible (OSINT) and invisible ("Dark Web")[65] Internet between October-December 2014.

Virtual Currency – Bitcoin Updates

The below chart shows the Bitcoin price on the BitStamp trading site for October-December 2014. The columns refer to the volume of the currency and the graph indicates the median price in American dollars on the same day.

During this time, the value of Bitcoin was between $300 to $400.

Bitcoin price chart in BitStamp for October - December 2014[66]

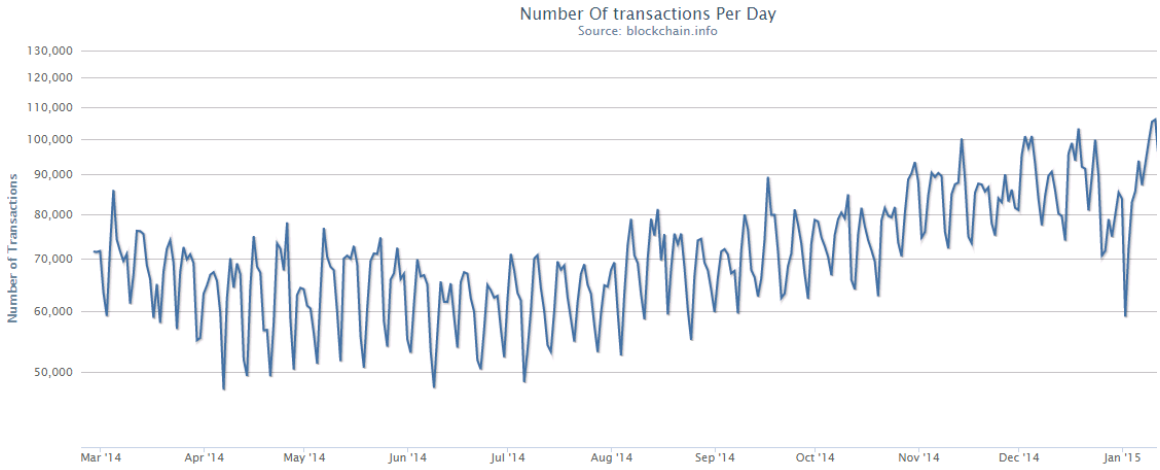
The following diagram shows the average rate throughout 2014, which peaked at 1,000 dollars and saw its lowest rate of approximately 300 dollars at the end of the year.

[65] The "dark Web" or darknet is "A collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks." See P. Biddle, P. England, M. Peinado and B. Willman (no date), "The Darknet and the Future of Content Distribution", *Microsoft Corporation*, http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

[66] http://bitcoincharts.com/charts/bitstampUSD#rg60zczsg2014-10-01zeg2014-12-31ztgMzm1g10zm2g25zvzcv

Bitcoin price chart in BitStamp for 2014[67]

According to data from the Blockchain Web site, between 40,000-100,000 bitcoin transactions were performed each day in 2014,[68] demonstrating an increase in the use of the virtual currency.



Enforcement Activity on the Dark Net

In the beginning of November, it was published[69] that a joint enforcement operation by the EC3, FBI, ICE, HIS and Eurojust had led to the arrest of 17 operators and traders in illicit trading sites on TOR networks. In the framework of this operation, 410 addresses were confiscated and removed

[67] http://bitcoincharts.com/charts/bitstampUSD#rg60zczsg2014-01-01zeg2014-12-31ztgMzm1g10zm2g25zvzcv

[68] https://blockchain.info/charts/n-transactions?showDataPoints=false&show_header=true&daysAverageString=1&timespan=1year&scale=1&address =

[69] https://www.europol.europa.eu/newsletter/global-action-against-dark-markets-tor-network

from the network, some of which redirected to trading sites, and bitcoins at an estimated value of one million dollars were confiscated.

The cooperation of 16 European countries and the United States illustrates an attempt by law enforcement officials to continue operating against illegal trading sites and indicates an operative ability to identify those who are active on the darknet.

United States: A Document of Recommendations for the Cyber Security of Medical Devices

On October 6, it was reported[70] that the American FDA had published[71] guidelines recommending that medical device manufacturers take into account the risks of a breach when designing their products, but it did not require enforcement measures.

The document opens by stating that the increase in use of wireless communication, Internet-based devices and the electronic transfer of medical information has increased the need for effective cyber security in order to ensure the operation and safety of medical devices.

The guidelines were prepared by the FDA in order to support the industry by identifying issues that are detrimental to cyber security, issues that the manufacturers must pay attention to during the design and development of medical devices, and when preparing applications before marketing these devices. However, the document does not constitute enforcement of legal liability but rather it reflects the "current thinking" of the FDA on this topic. The guidelines should be considered as recommendations only unless there is another explicit instruction and not as requirements for these manufacturers.

The document recommends that these manufacturers consider the actions of disclosure, protection, detection, response and recovery. This includes testing the capabilities of medical devices to communicate with other devices, the Internet, another network or various storage tools. Manufacturers should carefully consider the balance between maintaining cyber security and the usability of a device in its intended environment. In this framework, the document recommends the following: restricting access to the device via user identification equipment and even creating

[70] http://arstechnica.com/security/2014/10/fda-medical-device-cybersecurity-necessary-but-optional/

[71] http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

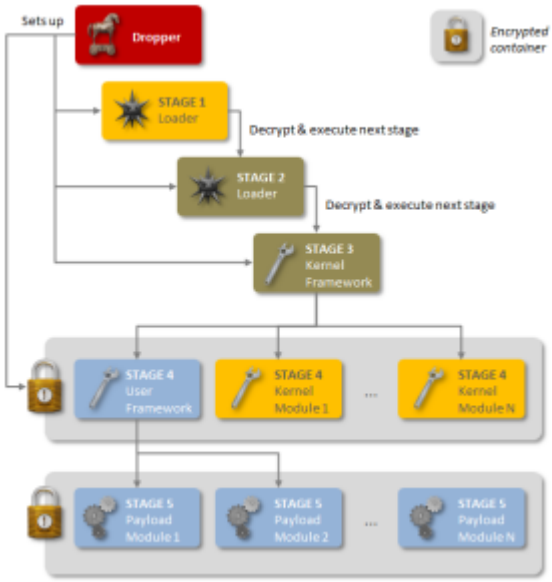
layers of permissions depending on user role; creating physical security for the device and its media tools; requiring permissions before performing software updates; applying features that enable the discovery of security breaches; exercising capabilities that enable the end user to take the appropriate measures with the discovery of a cyber-security incident; using features that would enable the protection of the device's critical operation even if its security is breached; and providing the possibility for equipment configuration recovery through an authorized user.

The document also included a warning about the need to evaluate any risk due to misuse, whether intentional or unintentional, already in the stages of product design. In addition, it stated that medical devices and systems are supposed to monitor and document attacks, and allow technicians to respond to such attacks either by repairing the weakness or through other means and to document cyber security risks that were examined during the design of the device.

Regin – A New Type of Super-Malware

Symantec published a new study regarding the discovery of new sophisticated spyware detection called Reign, which has been used in systematic espionage operations against international targets since 2008. According to the study, this is a complex Trojan horse malware that indicates a very rare technical complexity since, among other things, it gives those who master it a wide range of capabilities depending on the target, with emphasis on creating a powerful framework for surveillance of espionage operations against government agencies, infrastructure entities, businesses, researchers and private entities.

The development of the software, which is built on a structure of five internal steps, apparently took months if not years, and included a complex operation to hide its tracks. This, coupled with Regin's capabilities and resources, indicate that it is one of the cyber espionage tools being used by the state.

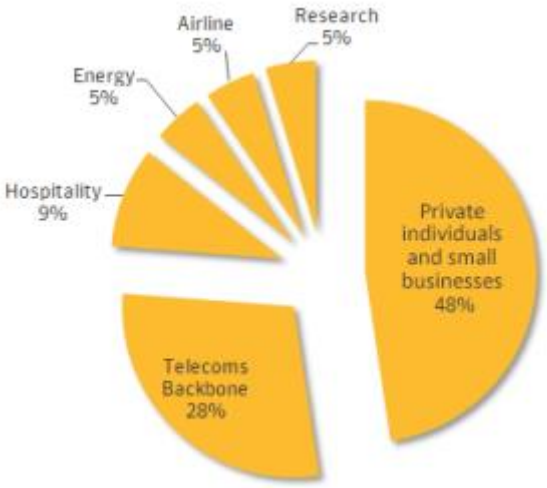


The complexity of the software is such that one cannot learn from one stage about the rest of the stages and their components, as well as its modular structure that enables the updating of its capabilities according to the selected target. This modular method was previously identified in malware such as Flamer[72] and Weevil[73], while its multi-stage architecture is similar to malware that was seen in the past such as Duqu[74] and Stuxnet.[75] Even the infection varies depending on the target.

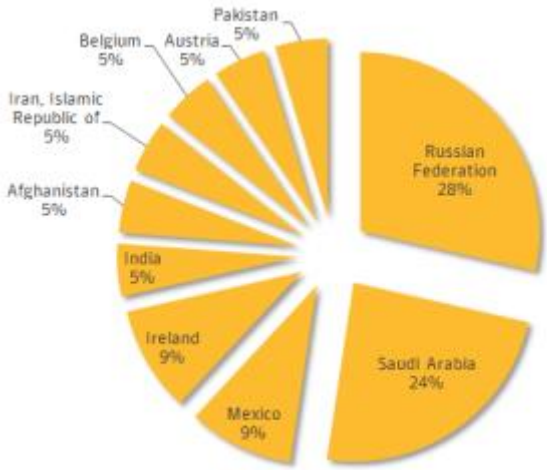
This malware was discovered between 2008 and 2011 among a wide range of organizations and then it was suddenly canceled. A new version of the software was discovered in 2013 onward.

An examination of this spyware's targets shows that they are many and varied, and that half of them are private entities and small business followed by communications providers. According to the study, this is in order to gain access to calls that are routed through this infrastructure.

[72] http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99
[73] http://www.symantec.com/security_response/writeup.jsp?docid=2014-021016-4132-99
[74] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf
[75] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf



In addition, even the geographic distribution of the spyware is varied. Half of the software's targets were in Russia (28%) and Saudi Arabia (24%) while the rest were in eight countries around the world.



The study suggests that some of the targets may have been enticed to enter fake versions of popular sites and that the software was installed through the browser or through the use of an application. In one case, the registry file discovered that the Regin had come from Yahoo's Instant Messenger software.

The basic threat capabilities of this spyware include several features of Remote Administration Tools (RAT), such as a screenshot, control of mouse function, password theft, communications monitoring activity, and deleted file recovery. More complex modules include traffic monitoring of Microsoft IIS Web server and listening (Sniffer) to base station controls of mobile phones.

The spyware developers put a lot of emphasis on camouflage, which means that spying operations could have been used for years. Even if the presence of spyware had been discovered, it would have been very difficult to determine its activities. The spyware also includes a number of camouflage capabilities, including those against forensic operations, several kinds of built-in encryption, and a number of sophisticated capabilities for secret communication with the attacker.

In conclusion, Regin presents a highly complex threat used in espionage or in systematic information collection. Its development and operation required a significant investment of time and resources, suggesting that the state is responsible for this. In addition, the software design makes it appropriate for continuous and long-term surveillance operations against its targets. Symantec also claims that it believes that many of Regin's components, as well as its additional capabilities and versions, have still not been discovered.

Case Study – Critical Infrastructure

Each newsletter issued by the ICT's cyber-desk will discuss in greater detail a recent incident of cyber-attack. This issue highlights the threats of critical Infrastructure.

During the 2014 fiscal year, 79 hacking incidents of energy companies were recorded, incidents that are under investigation by the Department of Homeland Security (DHS) in the United States, as compared to 145 incidents in the previous year. In March 2014, a study was published according to which 150 cyberattacks were carried out in 2013 against the energy sector in the United States. According to the study, the two-day shutdown that occurred in 2003 caused 6 billion dollars' worth of damage although it was not the result of a cyberattack. Another study was published according to which an average of 74 cyberattacks per day were recorded between July 2012 and June 2013, with the energy industry serving as the target for 16.3% of them – a figure that places it in second place after the government and public sector, which served as the target for 25.4% of all the attacks.

It seems that external defenses are not necessarily long-lasting. In the year between April 2013 and April 2014, hackers managed to breach 37% of energy companies, according to research[76] by

[76] http://www.threattracksecurity.com/resources/white-papers/data-breaching-malware-threatens-energy-and-finance-firms.aspx

ThreatTrack Security. The company, FireEye, identified[77] approximately 50 types of malware that attacked energy companies during 2013 alone, and Verizon identified[78] that these companies are destined for attack more than any other industry. The spyware was located on the company's computers for an entire year all because one employee clicked on a wrong link in an email message. It was also discovered that the Russian malware, BlackEnergy, had penetrated the software that controls power turbines in the United States. Even if an investigation had not revealed any attempt to cause damage or to disrupt devices, it would have been able to give the hackers a back door for planting a destructive code in the future.

To date, no malware has caused any part of the power grid to stop working but hackers are still breaching these networks, giving them the ability to turn off the switch. The CEO of TrustedSec, David Kemmedy, unequivocally said: "Our grid is definitely vulnerable he energy industry is pretty far behind most other industries when it comes to security best practices and maintaining systems."[79] One of the reasons for the vulnerability of energy companies is the fact that these industrial systems mostly rely on non-upgraded technology from the 1970's. At a power grid security conference in San Antonio, the Director of the NSA, Adm. Mike Rogers, told the energy companies that the electricity infrastructure was simply not designed to withstand the attacks that exist today, and he added that "power is one of the segments that concerns me the most". As a result of this situation assessment, the FBI and the DHS are maintaining fixed contact that includes meetings and channels of communication with energy providers and service companies with the goal of explaining the risk to them and alerting them as needed.

[77] http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf
[78] http://www.verizonenterprise.com/DBIR/2014/
[79] http://money.cnn.com/2014/11/18/technology/security/energy-grid-hack/

Evolving Cyber Threats Against Critical Infrastructure Control Systems

Classified Threat Briefing Campaign

OVERVIEW and PURPOSE

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have been responding to sophisticated cyber exploitation campaigns against U.S. critical infrastructure industrial control systems (ICSs). These campaigns have involved two different sets of malware; both of which appear to be ICS focused. The characteristics of this activity include the use of ICS zero-day vulnerabilities, malicious ICS payloads, and specific targeting of the operations environment across a variety of sectors including energy, water, critical manufacturing, communications, and more.

To increase awareness of the threat and provide additional context, DHS ICS-CERT and FBI will conduct SECRET level classified briefings in select U.S. cities concerning this cyber activity and provide asset owners/operators with the capabilities to detect intrusions and develop mitigation strategies.

The regional classified (SECRET//REL TO USA, FVEY) briefing sessions will last approximately 2 hours and provide details about recent malicious cyber campaigns, techniques used by the threat actors, and strategies for mitigating risks and improving your cyber defensive posture.

The energy companies, on their part, are taking precautions, employing cybersecurity teams, and separating between internal and external operating networks. It was also argued that energy companies are making use of so many kinds of machines that an army of hackers would be needed in order to black-out an entire city. Nevertheless, it was stated that storms pose greater dangers to the power system than hackers.

In June, the American ICS-CERT published[80] a warning about a Trojan horse malware called Havec that, according to its assessment, operates with the goal of damaging the industry management system (SCADA and ICS). In the beginning of December, an update was published[81] warning of a campaign directed against systems created by specific companies, and referred to a sophisticated malware campaign that has been going on since at least 2011 called BlackEnegy, which was carried out by the Sandworm group.[82] Among the targets of the campaign were suppliers from the following industries: water, energy, asset management and industrial control systems.

[80] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
[81] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B
[82] http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/

In mid-December, the BSI published[83] a report reviewing the main threats and attacks that took place in Germany in 2014, including a reference to the APT attack, which began as a phishing and focused social engineering attack and gave the attacker access to the network of a steel plant. The hacker successfully exploited security flaws to reach the ICS and disrupt the proper functioning of the plant.

In December,[84] South Korea was attacked several times, the target being its nuclear facilitates. As part of the attack, drawings and manuals of nuclear facilities were leaked, as well as information about 10,000 employees. It was estimated that the attacker did not manage to reach the command and control systems. Although the attacker identified himself as an activist opposed to nuclear energy, it is also likely that the attack was carried out by North Korea.

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

Ely Amar, CEO at EA Cyber

Dr. Michael Barak, Team Research Manager, ICT

Adv. Deborah Housen-Couriel, Cyber security and international law expert

Etay Maor, Senior Fraud Prevention Strategist

Dr. Tal Pavel, Expert on the Internet in the Middle East

Shuki Peleg, Information Security and Cyber-Security Consultant

Nir Tordjman, Team Research Manager, ICT

[83] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[84] http://www.reuters.com/article/2014/12/28/us-southkorea-cybersecurity-nuclear-idUSKBN0K603320141228 , http://www.bloomberg.com/news/2014-12-22/s-korea-preps-for-cyber-attack-after-nuclear-reactor-data-leaks.html

ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy. ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

ABOUT ICT CYBER-DESK

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse). and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack). The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations.

Click here for a list of online the ICT Cyber-Desk publications

For tailored research please contact us at Webmaster@ict.org.il.