Cyber-Terrorism Activities

Report No. 5

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

International Institute for Counter-Terrorism (ICT)

Additional ICT resources are available on ICT's website: www.ict.org.il

Highlights

This report 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:

- A visitor to the Hanein jihadist Web forum suggested that forum users study the "art of defense against [computer] breaches and hackers", and he published a list of study topics for those who were interested, including: security mechanism breaches, various programming languages, the establishment of an internet and monitoring forum, and damage to servers.
- The Palestinian Gaza Hacker Team Web forum published a pocket guide of sorts on how to protect computers, and email and Facebook accounts, and opened a new department for advanced virtual courses on hacking into Web sites using the SQL injection technique, an effective method of attack using Defacement.
- The Global Islamic Media Front posted on various jihadist Web forums, a mobile encryption program for sending text messages and encrypted files using cellular telephones.
- A visitor to the 'Ushaq Al-Hur Al-Islamiya jihadist Web forum suggested that his fellow visitors download an application that transmits current news about operations carried out by Ahrar Al-Sh'am Al-Islamiya, a Salafi-jihadist group operating in Syria.
- The increased use of digital currency, with an emphasis on bitcoins, and the inclusion of many trading sites on the list of businesses that accept virtual currency payments, have aroused the interest of several countries regarding the establishment of policies and the regulation of digital currency.
- Officials continue to enforce the law even on the darknet. In a combined operation, authorities in the United States successfully located and arrested the founder of the illicit trading site, Silk Road, which had served as a popular trading site with over 120,000 business transactions worth approximately 9.5 million bitcoins.

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, June-September 2013[1]

Al-Qaeda's Leadership

- During June-August 2013, Sheikh Ayman al-Zawahiri, leader of Al-Qaeda, dispatched three messages to the Muslim Nation. In the first message he called on Palestinians, and all Muslims around the world, to concentrate their efforts on liberating Palestine from the Zionist regime. In the second message, he reiterated his call to liberate Palestine from the Jews and for its inclusion in the future Islamist caliphate to be established in the region. He also encouraged Muslims to act against the anti-Islamic policies of the United States. In the third message, he criticized the military revolution in Egypt as well as Morsi's ousting. According to him, the revolution was made possible thanks to collaboration among Coptic Christians, the secular camp, supporters of the military regime, and the anti-Islamic camp, under the direction of the United States. The democratic process by which Morsi was elected to Egypt's presidency is proof of this, as it is worthless and doomed to fail.
- In September 2013, al-Zawahiri redefined [Al-Qaeda's] policy of jihad, and the strategy derived from it. In this framework, he commanded the mujahideen to avoid friction with minorities and with the civilian population, and to concentrate

[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/ResearchPublications/JihadiWebsitesMonitoring/JWMGPeriodicalReviews/tabid/344/Default.aspx.

on terrorist attacks against American and Israeli targets. He called on the Muslim Nation to carry out individual terrorist attacks against American targets, especially those on [Muslim] soil, and to cause damage to the United States' economy, which is vulnerable and liable to bring about the country's downfall.

- At the same time, Al-Qaeda published messages by members of its senior leadership. For instance, Sheikh Maulana Aasim Umar, a senior member of Al-Qaeda in Afghanistan, called on Muslims living in India to join global jihad against the United States and its allies. Another senior leader, Sheikh Hussam Abd al-Rauf, called on Muslims in the Arab world to honor the achievements of the Arab revolutions and not to relinquish power to remnants of the previous regimes.
- Sheikh Adam Yahiye Gadahn al-Amriki, a senior leader of Al-Qaeda, also dispatched two messages during this period. He emphasized that the liberation of Syria and the fall of Bashar al-Assad's regime are important cornerstones in the liberation of Palestine from the Jews. He called on the mujahideen not to lay down their weapons following the fall of the Baath regime in Syria but rather to re-direct them at the State of Israel. In the second message, he called on mujahideen and Muslims to attack American diplomats throughout the Middle East, especially at the U.S. Embassy in Yemen.

The Arabian Peninsula

- During the second half of July 2013, Sheikh Ibrahim Rubeish, mufti of Al-Qaeda in the Arabian Peninsula (AQAP), announced the death of Sheikh Abu Sufyan Said al-Shihri, deputy leader of Al-Qaeda in the Arabian Peninsula. The announcement was widely and intensively discussed on jihadist Web forums.
- Another issue that was discussed extensively in the jihadist discourse centered around an announcement made in August 2013 by Sheikh Nasir al-Wahishi, an Al-Qaeda leader in the Arabian Peninsula, in which he expressed his intention to work to free Sunni prisoners from jails.

Syria

- Abu Mohammad al-Julani, leader of the Al-Nusra Front, called on all jihadist groups fighting in Syria to work together to bring down the Syrian regime and establish shari'a [Islamic law]. In addition, he threatened to respond to involvement by Lebanese Hezbollah and the Shi'ite population in the region, and called on them to end their support of the Syrian regime and its actions against

the Sunni population. He even swore to take revenge on the Alawites for the August 2013 chemical attack [against them].

- In addition, various jihadist groups in Syria sent a threatening message to anyone who dares to help the Syrian regime. For instance, the Abdullah 'Azzam Brigades harshly criticized Lebanese Hezbollah's blatant involvement in the Syrian civil war, demanding that it stop its activities right away and calling on the Sunni people of Lebanon to support the Sunni struggle in Syria.
- The August 2013 takeover of the Mannagh Military Airport in Aleppo Province in Syria by the Islamic State of Iraq and Al-Sham, together with other local Islamist jihadist organizations, was also widely discussed on jihadist Web forums.

Iraq

- The Islamic State of Iraq and Al-Sham (ISIS), Al-Qaeda's affiliate in Iraq, claimed responsibility for breaking into the Abu Gharib and Al-Taji prisons near Baghdad on July 21, 2013, during which several hundred prisoners – mostly members of Al-Qaeda – were freed. The discourse on the jihadist Web forums encouraged this trend and called for additional operations to bring about the release of more jihad activists.
- In September, the spokesman for the Islamic State of Iraq and Al-Sham declared the armies of Egypt, Libya, Tunisia, Iraq and Syria heretical as a result of their attempts to prevent the implementation of shari'a and their anti-Islamic activities. In light of this, al-Adnani called on Muslims, especially those in Iraq and Egypt, to wage violent jihad against their nations' armies.

Egypt-Sinai Peninsula

- The discourse among Salafi-jihadist groups in Egypt, the Sinai Peninsula, the Arab world and jihadist Web forums has become markedly more radical as a result of the removal of former President Mohamed Morsi, a Muslim Brotherhood representative, by the Egyptian army, led by General Sisi, in June 2013. Criticism of the Egyptian army for this action has increased, as have calls [on Muslims] to wage jihad and launch an armed struggle against the Egyptian army.
- Against the backdrop of the deaths of four jihad activists from Ansar Beit Almaqdes in the Sinai Peninsula, who were apparently killed in August 2013 by an Israeli unmanned aerial vehicle (UAV), or "drone", Salafi-jihadist

organizations in the Sinai Peninsula and Gaza Strip accused the Egyptian army of collaborating with Israel to defend of its borders. In light of this, jihadist organizations in the Sinai Peninsula called on local Bedouins to assist the mujahideen in their fight against the Egyptian army and to avenge the killings.

The Maghreb [North Africa]

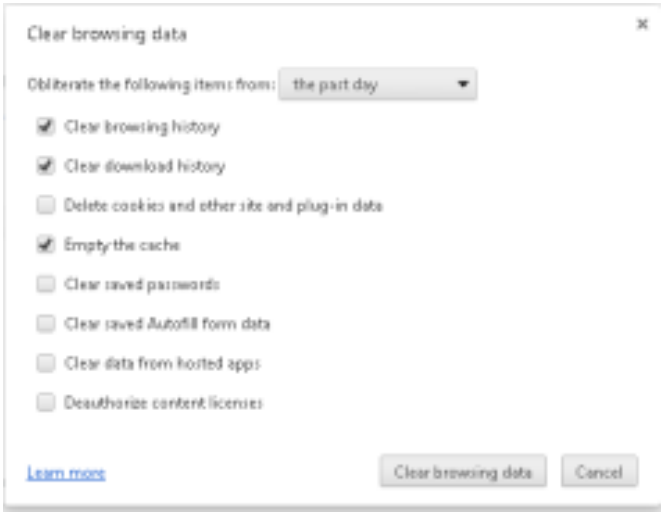
- The Signed-in-Blood Battalion and the United Group of Allah and Jihad, Salafi-jihadist groups operating in the Maghreb, announced their merger under a new name, Al-Murabitun. Their former leaders gave up their positions and transferred leadership of the new organization to a person whose identity had not yet been revealed.
- Al-Qaeda in the Islamic Maghreb (AQIM) is focusing its attention on Morocco and spreading propaganda criticizing the Moroccan Kingdom. It accused the Kingdom of collaborating with the West, refusing to implement shari'a, embracing democracy, persecuting its opponents, and more.

Somalia

- Starting in the second half of July 2013, the discourse on jihadist Web forums pointed towards an internal rift among the leadership of Al-Shabab Al-Mujahideen in Somalia. Sheikh Abu al Zubayr, leader of the movement, was accused of administering self-serving policies designed solely to satisfy his personal interests by killing opponents from within the group's ranks while ignoring the main goal: the implementation of shari'a.
- Jihadist forums affiliated with the Somali Al-Shabab Al-Mujahideen reported the killing of jihad activist and member of the movement, Omar Hamami, also known as Abu Mansur al-Amriki, by other group members as a result of internal conflicts between activists. The administrators of these forums expressed their understanding of the group's motivation in killing al-Amriki and blamed him for his own death for having deviated from the path of jihad in displaying personal whims that threatened unity among the group's ranks.
- Al-Shabab Al-Mujahideen's attack on the Westgate shopping mall in Nairobi on September 21, 2013 stirred up a lively dialogue on jihadist Web forums. Official jihadist groups and visitors to jihadist Web forums praised the terrorist attack and called for similar attacks in other places against enemies of Islam.

Defensive Tactics

- A visitor to the 'Ushaq Al-Hur Al-Islamiya jihadist Web forum recommended that forum members use caution when browsing on Google Chrome and offered guidelines for deleting their browser history. The visitor emphasized that by deleting their browser history, it is possible to prevent the information from being used against them.[2]



Guidelines for deleting browser history on Google Chrome

- A visitor to the Hanein jihadist Web forum suggested that forum users study the "art of defense against [computer] breaches and hackers", and he published a list of study topics for those who were interested, including: hacking security mechanisms, various programming languages, the establishment of an internet and monitoring forum, and damage to servers. Interested parties who wanted to join were asked to send their requests personally to the visitor who published the post and to the forum administrator. In response, another visitor asked that the sessions be taught after the month of Ramadan as it is difficult to focus during that time.[3]
- A visitor to the 'Ushaq Al-Hur Al-Islamiya jihadist Web forum warned his colleagues not to search the term "pressure cooker" on Google's search engine as a result of an article published by Reuters that reported on a married couple who were investigated by six intelligence agents in the United States for their alleged

[2] http://www.i7ur.com/vb.
[3] http://www.hanein.info/vb.

involvement in a terrorist attack, solely due to the fact that the wife had tried to find the best way to cook lentils. The investigation of the couple was apparently related to the fact that the terrorist attack at the Boston Marathon on April 15, 2013 was carried out using explosive devices that were concealed in a pressure cooker.[4]

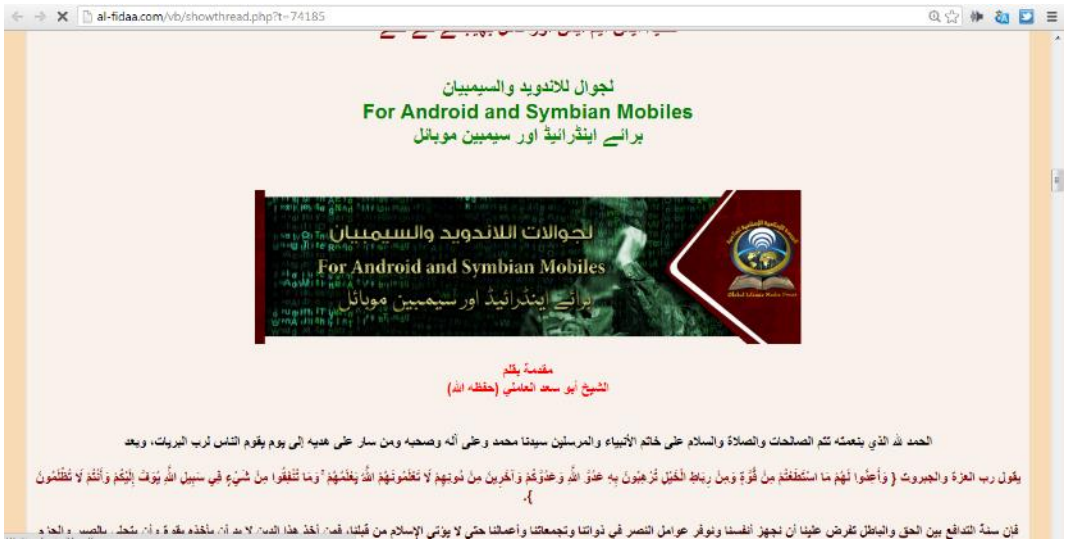
Photo of a pressure cooker

- Information Security – The Valiyat Dagestan Web site published an instructional video on how to circumvent censorship and block[ed content] in cyberspace. The video discussed the use of VPNs, fake identities and various Internet applications in order to bypass blockages by the "heretics". The video further emphasized that the Web site was soon expected to launch an independent VPN service that would be able to help visitors to the site circumvent blockages in cyberspace.[5] Another video was posted to the site that explained how to encode and encrypt information saved on magnetic media, such as a USB flash drive.[6]
- A visitor to the Lovers of the Maidens of [Islamic] Paradise jihadist Web forum warned his colleagues about the use of applications such as Viber, WhatsApp, Mobile Twitter and Line, claiming that the Saudi regime was using them to spy on its own people.[7]
- The Global Islamic Media Front published a mobile encryption program for sending text messages on Android and Symbian mobile phones, on different jihadist Web forums. In his introduction to the launch of the software, Sheikh Abu Sa'ad al-'Amili, a prominent Salafi-jihadist and frequent contributor to Web forums, noted that the media serves as a crucial arena in which jihad is being waged against the enemy and, therefore, media outlets should be considered

[4] http://www.i7ur.com/vb.
[5] http://vdagestan.com/kak-obojti-blokirovku-zapreshhennyx-sajtov-chast-1.djihad.
[6] http://vdagestan.com/kak-zashifrovat-dannye-na-fleshke-i-na-dr-elektronnyx-nositelyax.djihad .
[7] http://www.i7ur.com/vb.

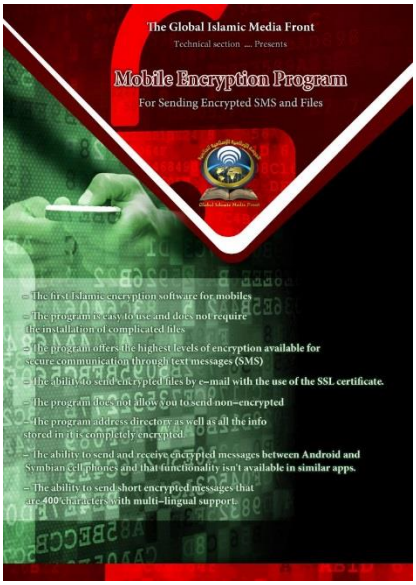
important. He added that the enemy was clearly very concerned due to the large amount of manpower and financial resources allocated to this field. In light of this, he said that it was imperative to establish channels of communication between Muslims and the mujahideen, who defend the borders, in a secure way that cannot be tracked by the enemy. Such conduct would thwart efforts to spy on and monitor confidential information in the hands of the mujahideen. Al-'Amili then emphasized that the current [mobile encryption] program came as a shock to the enemies of Islam. He added that, in light of the increased prevalence of cell phone use among Muslims and the mujahideen, and the important role that it plays in the planning of jihad operations, it would be necessary to establish a secure channel of communication in the field. Following the introduction, it was noted that the technology department of the Global Islamic Media Front was pleased to provide the Muslim Nation, especially the mujahideen and their supporters, with a mobile encryption program:

> "This program features asymmetrical encryption, along with the ability to encrypt SMS and files, sending and receiving emails, and receiving messages effectively and efficiently with the use of advanced techniques to maintain security and privacy, both during sending and receiving, or when saving messages. We announce that this program, like all the sites and programs that we develop, is the property of all Muslims."[8]



[8] https://shamikh1.info/vb (Arabic).

The banner of the announcement posted on jihadist Web forums regarding the launch of a mobile encryption program



The English version of the banner detailing the encryption software's features

- The Palestinian Gaza Hacker Team Web forum published a pocket guide of sorts on how to protect computers, and email and Facebook accounts.[9]

The pocket guide published on the Gaza Hacker Team Web forum

[9] http://gaza-hacker.net/cc/.

- The Africa is Muslim jihadist blog, which is administered by AQIM and also has a Twitter account, launched a series of new publications on September 18, 2013 titled, "The Electronic Jihad Series". The first part of the series was written by Sheikh Abu Musa al-Shinqiti about the advantages of using the Tor system - a free software network that enables anonymous Internet browsing.[10]

The banner page of the first part of "The Electronic Jihad Series"

Offensive Tactics

- A visitor to the Al-Jihad Al-Alami Web site published a Web site hacking guide on the site's computer section. The guide explained how to find loopholes to enable hacking into Web sites and included illustrated instructions on shell, dos and unix. The author explained how to hack into Web sites via the servers on which they are stored.
- On September 5, 2013, administrators of the Palestinian hackers Web forum, the Gaza Hacker Team, announced the opening of a new department for advanced virtual courses on breaching Web sites using the SQL injection technique. According to the announcement, approximately 60% of breaches are carried out using this method. It added that the forum is committed to electronic jihad and aspires to provide hackers with the most professional and up-to-date information. For instance, one course dealt with the "regular injection" technique and the "blind SQL" technique.[11]

[10] https://twitter.com/Africamuslima/status/380421881217548288.
[11] http://www.gaza-hacker.com/cc/showthread-t_48434.html

Forum banner announcing the opening of a new course breaching Web sites using the SQL injection technique

Guidance

- A visitor to the Ushaq Al-Hur Al-Islamiya jihadist Web forum suggested that his colleagues download an application that transmits current news about operations carried out by Ahrar Al-Sh'am Al-Islamiya, a Salafi-jihadist group operating in Syria.[12]

Image from the Ushaq Al-Hur Al-Islamiyya jihadist Web forum

[12] http://www.i7ur.com/vb.

- A visitor to the Ansar Beit Almaqdes jihadist Web forum asked forum users with YouTube accounts to help distribute online videos that promote Salafi-jihadist values, such as the operational activities of prominent groups affiliated with Al-Qaeda. The visitor emphasized that he wanted to recruit forum users to distribute these videos in order to prevent YouTube administrators from removing them from the site.[13]

Cyber-Crime and Cyber-Terrorism, June-September 2013

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 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")[14] Internet between June-September 2013.

Digital Currencies

The increasing use of digital currency, with emphasis on bitcoins, and the increasing number of trading sites that accept virtual currency payments, have prompted several actions:

1. Governments and law enforcement agencies around the world have begun to consider some form of regulation for these currencies. Discussions about how to cope with the phenomenon are being held in various countries around the world:
    a. Israel: The Tax Authority has begun to look into the issue in cooperation with the Ministry of Justice's money laundering department.

[13] http://vb.beit-almaqdes.net/showthread-t_1152.html

[14] 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.

b. Germany: The German Ministry of Finance recognized the bitcoin currency as a financial instrument or "private money", which can be used for commerce and tax purposes.
c. Thailand: The Central Bank of Thailand imposed a total ban on the use of bitcoins.
d. United States: The authorities opened an investigation into the poor supervision of the virtual currency market and summoned 22 companies engaged in commerce for questioning. In addition, the court raised the need to set policy. At the end of August, Tradehill (one of the largest bitcoin trading sites in the United States) suspended its activities due to what it said were banking and regulatory issues.
e. Great Britain: Discussions are being held at the governmental level to formulate policy action.

2. Silk Road, the illegal trading site operating on the darknet, was shut down at the beginning of October 2013 after a joint operation by law enforcement authorities in the Unites States and several other countries. The bitcoin was the common method of payment on the Web site, and the closure of the site, as well as the arrest of the site's administrator, led to a decrease of over 20% in the bitcoin's exchange rate. An in-depth analysis of the Silk Road Web site appears below on page 31.
3. The increased use of the bitcoin, coupled with the widely-discussed need for virtual currency regulations, have led to the emergence of additional virtual currencies such as the LiteCoin, which is based on an algorithm similar to that of the bitcoin but with improvements in production and usage.[15]

Trends in Cyber Activities in the Banking and Financial Services Sector

In recent months, there has been a marked increase in phishing attempts directed at banking customers around the world, with over 37 million attacks. In a survey carried out by Kaspersky Labs[16] in the summer of 2013, it was found that almost 30% of Internet users had received fake emails containing phishing attempts targeting financial sites.

[15] http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1232/currentpage/1/Default.aspx.
[16] http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year.

Financial regulatory bodies around the world have begun to address the need for guidance by financial organizations, including a strategy for coping with cyber-risks. In Great Britain, for example, the Central Bank demanded that the entities under its supervision present a plan for dealing with the effect of these cyber-attacks within six months.[17] In mid-November, financial institutions in Great Britain took part in Operation Waking Shark 2 – a simulated "war game" intended to measure their level of readiness for fending off cyber-attacks.[18]

In August 2013, Kaspersky Labs and SafeSoft were reported to have collaborated on a protection solution for ATM machines in Ecuador.[19] In 2012, these two companies predicted that ATM machines would present a threat to banks and that existing security systems would be vulnerable to cyber-attack. Towards the end of September, SafeSoft reported on a new malware named Ploutus found in ATM machines in Mexico. In this case, cyber-criminals operated in an integrated fashion by taking advantage of CD-Rom drive access in order to infect the ATM machines with malware that served as a Trojan Horse and provided the attackers with full access to money, which they could withdraw from the ATM machines without a credit or debit card.[20]

Trends in Cyber-Crime Enforcement

At the start of October it was reported that Paunch, the creator of the Blackhole Exploit Kit, and his partner in Russia were arrested. The Blackhole Exploit Kit is a software program sold on the black market, on the darknet, and used to hack into computers. The software works by continuously updating itself regarding new security vulnerabilities that enable hacking. The software costs between $50-$500 to rent for one day up to a month, and it costs $1,500 per year to purchase a license for the program.[21] The reported arrest was verified by Troels Oerting, head of the European Cyber-crime Center, which was established last year at Europol in order to combat cyber-crime in the European Union.

[17] http://www.bitdefender.co.uk/security/uk-banks-prepare-for-cyber-attacks.html.
[18] http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10359520/Banks-put-to-the-test-over-cyber-security.html.
[19] http://www.safensoft.com/archiv/n/774/1770.
[20] http://www.safensoft.com/archiv/n/774/1778.
[21] http://resources.infosecinstitute.com/cyber-weapon-of-mass-destruction-the-blackhole-exploit-kit/.

Hacker Activity in the Middle East and the Muslim World

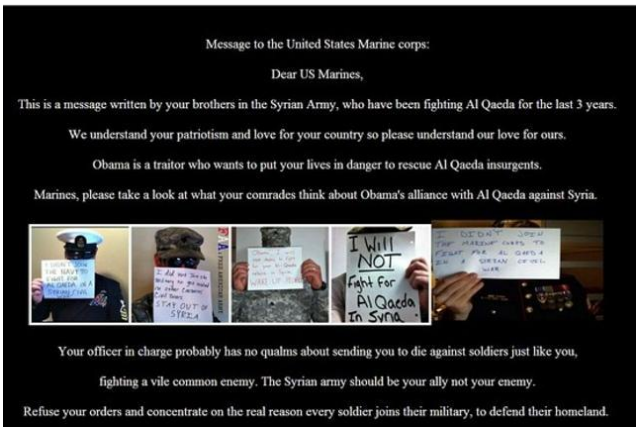
Attacks on U.S. Targets

- During the beginning of September 2013, the Syrian Electronic Army, which serves the Syrian regime led by Bashar al-Assad, hacked into the official homepage of the U.S. Marine Corps at http://www.marines.com/home. The breach was carried out against the backdrop of threats made by the American government to attack Syria in response to the Syrian regime's use of chemical weapons during its civil war. The group posted the following message:

  "Dear US Marines, This is a message written by your brothers in the Syrian Army, who have been fighting Al Qaeda for the last 3 years. We understand your patriotism and love for your country so please understand our love for ours. Obama is a traitor who wants to put your lives in danger to rescue Al Qaeda insurgents. Marines, please take a look at what your comrades think about Obama's alliance with Al Qaeda against Syria.

  Your officer in charge probably has no qualms about sending you to die against soldiers just like you, fighting a vile common enemy. The Syrian army should be your ally not your enemy. Refuse your orders and concentrate on the real reason every soldier joins their military, to defend their homeland. You're more than welcome to fight alongside our army rather than against it.

  Your brothers, the Syrian army soldiers. A message delivered by the SEA."[22]



The announcement posted to the U.S. Marine Corps Web site alongside photos of U.S. soldiers opposing an American attack on Syria

[22] https://twitter.com/Official_SEA16.

- Hackers publicized their intention to attack targets in the United States on September 11, the same date as the OpIsrael Reborn Operation. This attack originated with the Tunisian Hackers group,[23] which created a Facebook event for the operation that about 1,500 Facebook users joined. The page included a call to carry out DDoS attacks on several Web sites in the United States,[24] including the New York Stock Exchange.[25] The hackers also published a video documenting both this attack[26] and the attack on the U.S. Marine Corps Web site.[27]

The Tunisian Hackers Group Facebook page

- Hackers also published alleged proof of having hacked into the Iowa State Bank Web site.[28] They had already announced on August 27 that there would be an attack on the U.S. banking system between September 1 - September 10, during which a different bank would be attacked each day, as described on their list.[29] This was meant to serve as preparation for the peak of the operation, set to take

[23] https://www.facebook.com/TunisianHackers2
[24] https://www.facebook.com/events/611666308878387
[25] https://nyse.nyx.com
[26] http://youtu.be/T575wFFg11c
[27] http://www.marines.com/home
[28] http://64.38.3.250/~bankisb/opusaxhackertn
[29] http://pastebin.fr/28528

place on September 11. Meanwhile, the hackers claimed to have been the ones responsible for leaking most of the following information:

- A list allegedly containing the details of 3,000 credit cards originating in the United States.[30]
- A short list of links and access details of cameras that they claimed were positioned on houses and stores in Israel and the United States.[31]
- An announcement on Facebook[32] directing users to download a file containing 50,000 user names and passwords.[33]
- Published data[34] from the (alleged) official Web site of the city of St. Louis.
- A list allegedly containing the access information of 65 Facebook accounts[35] belonging to U.S. citizens (but in actuality many of the email addresses belonged to people around the world).

All of the above took place alongside operations by the Izz Al-Din Al-Qassam Cyber Warriors, which began the fourth stage of "Operation Ababil"[36] against the U.S. banking system[37] in July due to a video titled, "Muslim Innocence", which it claims can still be viewed online. The attack is estimated to have taken place during July 24-27, when two American banks suffered a DDoS attack.[38]

Pakistan-India

- The cyber conflict[39] continues between hacker groups in Pakistan and India. The tension between the two countries has spread to the cyber-space, with groups of hackers independent of state authorities attacking the Web sites of the "opposing" country. On August 12, as part of this struggle, 4,000 Web sites connected to India were hacked by Pakistani groups. The announcement that was

[30] http://pastebin.com/wDC7RANj
[31] https://www.facebook.com/anonjocker/posts/516553161762235
[32] https://www.facebook.com/Xhack00ertn/posts/147078498835806
[33] http://www.mediafire.com/download/q9z1jhoedehfplh/5000emails.rar
[34] http://pastebin.com/tEkHSkA7
[35] http://pastebin.com/NYSN0y1E
[36] http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1187/currentpage/1/Default.aspx
[37] http://www.middleeast-internet-monitor.com/?p=4091
[38] http://www.bankinfosecurity.com/ddos-back-3-banks-attacked-a-5951
[39] http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1187/currentpage/1/Default.aspx

made publicizing this attack provided details of the sites,[40] as well as the names of the Pakistani hacker groups that took part in the attack:

- Pakistani Cyber Eaglez
- Pak Cyber Pyrates
- P4k!$74n H4x0r$ CR3W (PHC team)
- Pak Cyber Experts
- Team Cyber Switch
- Anon C[O]P member of Anonymous Pakistan.
- CFR Robot Pirates Team

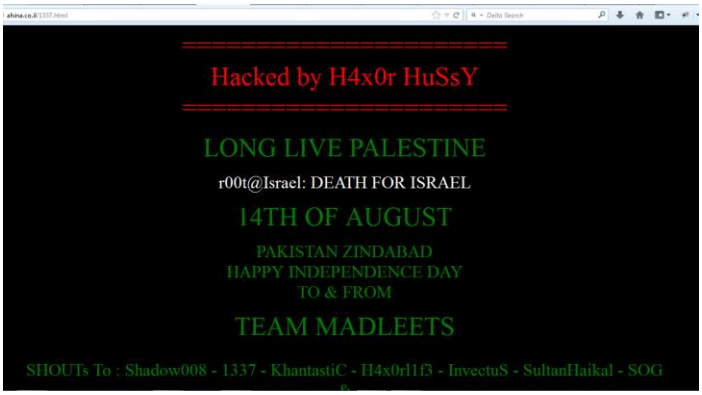
At the moment, it appears that many of the Web sites that were attacked have been fixed, although many links still lead to inactive pages. More specifically, it appears that the attack did not destroy the Web sites themselves, as their home pages still function normally, but rather damaged various pages on their servers. A message to the owners of each Web site was inserted on those pages, claiming that the attack was an act of retaliation for cyber-attacks against Pakistani Web sites carried out by the hacker Bl@ck Dr@gon, whose attacks are documented on his Facebook page.[41] (They even called on the owners of the Web sites to file a complaint with the Indian authorities against the hacker or else they would return and attack a second time.)

Message from the hackers to the owner of a hacked Web site, explaining the motivation behind the attack

[40] http://www.cheers4all.com/2013/08/indian-govt-under-cyber-attack
[41] https://www.facebook.com/indicodebreaker

Attacks on Israeli Targets

- A visitor to the Al-Jihad Al-Alami Web site announced that, according to an article on the "Hacker News" Web site, a Pakistani hacker group called "H4x0r HuSsY" had attacked approximately 650 Israeli servers and Internet sites. The hackers attacked Web sites affiliated with the Israeli government as well as the Web sites of large Israeli companies, and left the following message on each site: "Long Live Palestine – Pakistan – Happy Independence Day From Team Madleets".[42]



The message left by "H4x0r HuSsY" hackers on Israeli Web sites

- The hacker group that calls itself "Anonymous" published a video calling on all Muslim hacker groups to take part in the wave of electronic attacks against American and Israeli Web sites planned for September 11, 2013, to mark the terrorist attacks against the Twin Towers in Manhattan. It called the planned operation "OpIsrael Reborn".[43]

A clip from the video calling on Muslim hacker groups to participate in the cyber-attack operation called for September 11, 2013

[42] http://shabakataljahad.com/vb

[43] https://www.facebook.com/Anonymousunivers;
http://www.youtube.com/watch?v=MNw9YMepjTI

A Muslim hacker group called Anonghost, led by a Mauritanian hacker, expressed its willingness to take part in the campaign. In September, the group claimed responsibility for a series of attacks against Israeli Web sites and email accounts even before the predetermined date. The group also promised to leak 5,000 Israeli credit card account numbers, which they hacked into, to the server on September 11, 2013.[44] The group itself includes Muslims from Morocco, Malaysia, Indonesia, Tunisia, the United States and Ireland.

The banner placed by the hacker group on several Israeli Web sites

- A visitor to the Lovers of Islamic Fairs of Heaven jihadist Web forum shared an announcement, according to which hackers in the Electronic Al-Aqsa Battalion, in cooperation with members of the "Anonymous" international hackers group, brought down 16 Israeli Web sites. The visitor attached a list of the affected Web sites, including that of the Israeli telecommunications company Golan Telecom. Some of the affected sites displayed the following picture when opened. In addition, it was noted that the sites were attacked to mark 13 years of the Al-Aqsa Intifada.[45]

[44] https://www.facebook.com/AnonghostMalaysia
[45] http://www.i7ur.com/vb (Arabic).

The picture that appeared on the hacked Israeli Web sites

- On August 1, the Tunisian Hackers Group published an announcement[46] calling on hackers to attack the Bank Of Israel Web site the following day at 21:00 GMT. The announcement contained the group's Facebook address and reference to a Facebook event[47] that it created on July 25 called "OpTunisia", which contained information about various cyber-attacks, mainly in Tunisia. The page included a reference to the above-mentioned announcement regarding the August 2 attack on the Bank of Israel Web site, but it was clear that attacks on the bank's site had already been coordinated and carried out a day earlier. On the evening of September 25, a video in Arabic was published, seemingly by the group "Anonymous", in which it announced an upcoming attack against Web sites in Israel in response to the "Al Aqsa desecration" without declaring the date of the attack. The announcement was published on the Web site[48] and video channel[49] of the Al-Aqsa Martyrs' Brigades, as well as on the Facebook page of Gaza now.[50] The video referred viewers to the Facebook page of "Anonymous Arab".[51]

[46] http://pastebin.com/hGmxheMP
[47] https://www.facebook.com/events/595397347148059
[48] http://iyrere.wordpress.com/2013/09/25/%D8%AE%D8%A7%D8%B5-%D8%A8%D8%A7%D9%84%D9%81%D9%8A%D8%AF%D9%8A%D9%88-%D8%A3%D9%86%D9%88%D9%86%D9%8A%D9%85%D9%88%D8%B3-%D8%AA%D8%B9%D9%84%D9%86-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D9%82%D8%B1%D9%8A%D8%A8/
[49] http://www.youtube.com/watch?v=L8mOMxAENTg
[50] https://www.facebook.com/photo.php?v=302735096533395&set=vb.114129911998552&type=2&theater
[51] https://www.facebook.com/anonarab.2

Attacks on Targets in the Gulf

- A visitor to the Hanein jihadist Web forum published a list of Twitter accounts belonging to, in his words, "intelligence personnel" operating in the Gulf region. In addition to the published list, the visitor claimed that he had over 4,000 more accounts in his possession.[52]

Attacks on Targets in Syria

- On August 24, a Moroccan hacker published[53] an announcement in which he claimed to have hacked into the mail server of the Syrian Ministry of Presidential Affairs[54] and leaked approximately 80 email addresses and passwords from the server. However, this list was published[55] in its entirety on Facebook at the beginning of December 2012, and even earlier in February 2012.[56] Therefore, the August announcement was another example of cyber-space being used for psychological warfare, which is sometimes more valuable than an actual online attack; it is possible that the list that was published at the time was original and retrieved via a breach of the servers of the Syrian Ministry of Presidential Affairs. However, this did not prevent interested parties from recycling old news reports and distributing them in the hope that they would have a renewed effect, without their credibility and timeliness being called into question.

Attacks on Targets in Jordan

- On September 29, it was reported[57] that parties affiliated with "Anonymous" had hacked into the Web site of the Jordanian Prime Minister. The cyber-attack was intended as a protest against the government's intention to raise taxes and increase prices in the country as part of its austerity plan,[58] in the framework of

[52] http://www.hanein.info/vb
[53] http://pastebin.com/Tc2YHCvT
[54] http://webmail.mopa.gov.sy/
[55] https://www.facebook.com/notes/%D8%AA%D8%B3%D8%B1%D9%8A%D8%A8%D8%A7%D8%AA-%D8%B3%D9%88%D8%B1%D9%8A%D8%A9-syrialeaks/%D8%A7%D9%8A%D9%85%D9%8A%D9%84%D8%A7%D8%AA-%D9%88-%D8%A8%D8%A7%D8%B3%D9%88%D8%B1%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D9%82%D8%B5%D8%B1-%D8%A7%D9%84%D8%AC%D9%85%D9%87%D9%88%D8%B1%D9%8A-%D8%A7%D9%84%D9%85%D8%B3%D8%B1%D8%A8%D8%A9-the-presidential-palace-leaked-emails-/428238947231824
[56] http://pastebin.com/uaYDfCz0
[57] http://arabcrunch.com/2013/09/first-anonymous-attack-against-the-regime-in-jordan-the-group-hacked-briefly-jordans-prime-ministry-website.html
[58] http://jordantimes.com/the-austerity-tragedy

which the price of mobile phone use doubled[59] in July 2013, leading to protests by telecommunications operators as well as an actual decline in revenues and profits.[60] The announcement noted that this was the first operation by these parties against the Jordanian regime, and included reference to a video[61] about increased taxes and prices in Jordan as well as the "Anonymous" group's criticism of the Jordanian government's conduct. However, the video was published on YouTube [a month earlier] on August 13, and uploaded by Anonymous_TN,[62] which is affiliated with "Anonymous" in Tunisia.

Case Studies

Each newsletter issued by the ICT's cyber-desk will discuss in greater detail a recent incident of cyber-attack. This issue highlights groups of hackers from Iran.

Iranian Hacker Groups – Part 2[63]

Emperor Team[64]

The Emperor Team hacker group began to operate in early 2001.[65] The first person to lead the group[66] was Amirhosein Seyrafi (aka "iman" or "iM4n"; see photo below). Seyrafi, a young man in his early 30s,[67] was credited with defacing the Web sites and sub-domains of MSN, Yahoo and Backbox. Seyrafi founded the group together with

[59] http://jordantimes.com/telecom-operators-experts-pan-mobile-phone-tax-raise
[60] http://jordantimes.com/higher-tax-hits-jtg-profit
[61] http://youtu.be/4UqaZTo4Bjg
[62] http://www.youtube.com/channel/UCMsHCvYyRo91nDS5CgJhSaQ?feature=watch
[63] This article was written by Ran Ben Shalom, an ICT Research Intern and BA student at the IDC. For part 1 of the review, see the ICT Cyber Desk's Report No. 4: http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1232/currentpage/1/Default.aspx
[64] Most of the existing information about this group comes from two interviews given by the former head of the group, Amirhosein Seyrafi (see the following), to Internet Web sites. He gave the first interview about 6-7 years ago (http://www.persianhack.com/2013-01-07-12-47-35/86-reports/306-%D9%85%D8%B5%D8%A7%D8%AD%D8%A8%D9%87%20%D8%A8%D8%A7%20%D8%AA%D9%8A%D9%85%20%D8%A7%D9%85%D9%86%D9%8A%D8%AA%D9%8A%20%D8%A7%D9%85%D9%BE%D8%B1%D9%88%D8%B1) as part of a series of interviews conducted by the PersianHack Web site with prominent Iranian hackers. He gave the second interview in November 2012 to the Giga-News Web site (http://www.giganews.ir/?p=87).
[65] More than once, members of the group emphasized that their activities preceded the establishment of Ashiyaneh by about a year.
[66] At the time of the group's establishment, Seyrafi simultaneously served as the head of another group called "Persian Hackers" http://forum.p30parsi.com/t28512/#post207426
[67] http://www.giganews.ir/?p=87

his friend, Behnam Ayari[68] (aka "Arash" or "imm02tal"). Other hackers active in the group are known as "Farhad" (aka sun.solaris), "Roslan" (aka r$p/rsp)[69] and "Hamed" (aka spynet).[70]

Originally, Seyrafi and his friend established the team in order to "gather information" and set up a BBS (Bulletin Board System) network. About a year later, the team's activities in this framework came to an end, but the stage of "security activities", as Seyrafi puts it, began; this stage included the establishment of the "Iman Online" Web site[71] as well as the creation of simple programs such as Mail Bomber, Port Scanner, and a program for Yahoo Messenger. According to Seyrafi, at first the group only wanted to gain publicity but as time went on and its members became more knowledgeable, it began to operate as a means of enjoyment and in order to gain a reputation. Seyrafi explained that, in addition to its activities in Web site defacement,[72] the group had received a request from an Iranian company to attack the database of a governmental organization,[73] which it carried out by penetrating the organization's internal server in an operation that lasted one month and involved around-the-clock work. Seyrafi also claimed that the group had previously hacked into the Web sites of two presidential candidates during elections (he was seemingly referring to the 2005 presidential elections).

Currently, the group occasionally tries to present a "legitimate" front – as do other hacker groups operating in Iran – by claiming, for instance, that its members are only involved in Pen Testing and no longer take part in Web site defacement, etc. And indeed, the group's Web site home page includes the declaration that it "is not involved in activities that are illegal in Iran" (as well as the full text of Iran's Computer Crimes Act). However, posts about recruitment to the group's Web site

---

[68] It seems that Seyrafi and Ayari are no longer active in the group. For information on Seyrafi's activities today see http://ir.linkedin.com/pub/amirhosein-seyrafi/33/833/20a

[69] See the following link for an interview given by this hacker several years ago as part of a series of interviews conducted by the PersianHack Web site with prominent Iranian hackers http://forum.p30parsi.com/t28512/#post207426

[70] It seems that, in the past as well, members of the group earned a living from careers that were not directly related to the computer field and took part in hacking only during their free time.

[71] www.imanonline.com (This website is not active)

[72] Such as the "Satanic Project", which was carried out several years ago; see http://books.google.co.il/books?id=ZNjSnD0kgVgC&pg=PA126&lpg=PA126&dq=iran+hackers+emperor+satanic+project&source=bl&ots=b3drJVoWrU&sig=oB3xRjO4GjizoOljw7-jPNc3XhE&hl=iw&sa=X&ei=1KbSUbHsK4yFtQbUpYGADg&ved=0CCkQ6AEwAA#v=onepage&q=iran%20hackers%20emperor%20satanic%20project&f=false

[73] It is unclear if the organization was in Iran or somewhere else.

defacement team can be found on the site's various forums,[74] as can posts concerning the sale of hacking tools, etc.

Amirhosein Seyrafi, former head of the Emperor Team hacker group[75]

Parastoo

Recently, the media has published a number of reports about an unknown Iranian hacker group called "Parastoo" (which means "swallow" [the type of bird] in Farsi). Since its name first came up in the media on November 25, 2012,[76] it was reported that the group hacked into the computers of the International Atomic Energy Agency (IAEA),[77] the United States Department of Energy,[78] and the IHS Jane's Group.[79] These reports were at least partially reinforced later on when the group published information that it had obtained in the framework of these breaches. The group published announcements regarding the attacks on these targets, in which it demanded an investigation into Israel's weapons of mass destruction, threatened United States Vice President Joe Biden (while mentioning the assassination of Abbas Musawi), and claimed that it possessed information on Mossad activities, Israeli nuclear sites, the military industry, and more. It is interesting to note that in one of the announcements Parastoo mentioned a group called "Remember Imad",[80] which

[74] http://emperor-team.org
[75] http://www.giganews.ir/?p=87
[76] http://pastebin.com/SdYaPUwr
[77] http://thebuzz.co.il/article/7kLxqDFf3yJx2iZW/%D7%A1%D7%91%D7%90%D7%90:_%D7%94%D7%90%D7%A7%D7%A8%D7%99%D7%9D_%D7%9E%D7%90%D7%99%D7%A8%D7%90%D7%9F_%D7%A4%D7%A8%D7%A6%D7%95_%D7%9C%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%A0%D7%95_%D7%95%D7%92%D7%A0%D7%91%D7%95_%D7%9E%D7%99%D7%93%D7%A2_%D7%A8%D7%92%D7%99%D7%A9
[78] http://siliconangle.com/blog/2013/02/28/iran-hackers-threaten-vice-president-domestic-u-s-drone-attack-leak-ihs-janes-cbrn-documents
[79] http://wikileak.ir/en/leaks/13
[80] http://hackmageddon.com/tag/remember-emad; http://tech.walla.co.il/?w=//2557658

also recently carried out a number of operations against Israeli targets,[81] raising the possibility that it also took part in OpIsrael in the beginning of April.[82]

The announcement published by the group in August 2012, claiming to have hacked into an Israeli server[83]

Ajax Team

Ajax Team is another hacker group that has been operating in Iran for a number of years, led by Ali Ali Pur (aka Cair3x). Similar to other hacker groups, Ajax Team carries out at least part of its activity in the framework of a security company. The Web site of Pars Pardazesh Hafez Shiraz Ltd., which was established in 1390 according to the Persian calendar,[84] specifically states that the company was founded "in order to provide services to the private and public sectors…based on over 5 years of experience in the field of IT and in managing the Ajax hacker group".[85] In addition, Ali Ali Pur posted an advertisement on his blog for a Pen Testing training package offered to all interested parties by the Ajax Team and Pars Pardazesh Hafez Shiraz Ltd. It was noted that, similar to the ITSecTeam, the Web site of Pars Pardazesh Hafez Shiraz Ltd. does not include any details about the group's employees, in contrast to similar companies around the world and in Iran.

As with other groups, it seems that the Ajax Team also operates against targets within Iran's opposition. For instance, on June 27, 2012 the group attacked[86] a

[81] http://siliconangle.com/blog/2013/02/28/iran-hackers-threaten-vice-president-domestic-u-s-drone-attack-leak-ihs-janes-cbrn-documents
[82] http://cryptome.org/2013/03/parastoo-jfk-op.htm
[83] http://www.israelhayom.com/site/newsletter_article.php?id=5349
[84] March 21, 2011-March 20, 2012
[85] http://www.pars-security.com/about
[86] It is interesting to note that the group left messages on the Web sites that it attacked emphasizing its young age. See http://www.astalavista.ir/1391/04/10/%D9%87%DA%A9-%D8%B6%D8%AF-%D8%A7%D9%86%D9%82%D9%84%D8%A7%D8%A8/

number of opposition targets[87] to mark the anniversary of the death of Ayatollah Seyyed Mohammad Hosseini Beheshti.[88] A report provided an updated list of the Web sites that were attacked for publicizing "false" and/or "anti-revolutionary" information.[89] As with other groups, the Ajax Team has an anti-Western and anti-Israel stance, and is sensitive to religious, national and patriotic issues;[90] for example, the group leader's blog included a post with instructions on how to hack into the NASA Web site and download a database from one of its servers.[91] In addition, he reported a cyber-attack on Columbia University in the United States to protest the meeting and conference that took place [there] with the participation of the Israeli Prime Minister and the President of the United States.[92] In another post from November 2011, Pur expressed anger that abusive words about the Prophet Mohammed were published in a French weekly.

Other Groups

There are many more hacker groups operating in Iran but this review is not lengthy enough to cover each and every one of them in depth. Nevertheless, it is impossible not to take notice of two additional groups, which are mentioned most often in the field[93] (for instance, the former head of the Emperor Team said in a November 2012 interview with the Giga-News Web site[94] that he had great respect for the activities of these two groups). The first group is called "Shabgard", a long-standing group that still runs an active Web forum today[95] with many members. The second group is called "Simorgh"[96] (which means "phoenix" in Farsi) and is also widely respected. A

[87] http://www.astalavista.ir/1391/04/10/%D9%87%DA%A9-%D8%B6%D8%AF-%D8%A7%D9%86%D9%82%D9%84%D8%A7%D8%A8

[88] Ayatollah Seyyed Mohammad Hosseini Beheshti was killed in June 1981 along with 72 other members of the [Islamic Republic] Party in an explosion that took place at a party conference. The Iranian government attributed the explosion to the People's Mujahideen of Iran.

[89] http://ajaxtm.com

[90] An example of this is a paragraph from the "Ammariyon" Web site (www.ammariyon.ir), which is affiliated with radical circles within the conservative camp, which Ali Ali Pur quoted in one of his posts (http://www.terrorism-info.org.il/data/pdf/PDF_11_092_1.pdf).

[91] See footnote 15 above.

[92] http://ajaxtm.com; According to the author, this act also served to protect Iranian national interests in the nuclear arena, as well as to bless the Iranian people in honor of the Persian New Year ("Nowruz").

[93] http://www.astalavista.ir/1390/11/29/%D9%85%D8%B9%D8%B1%D9%81%DB%8C-%D8%A7%D9%86%D8%AC%D9%85%D9%86-%D9%87%D8%A7%DB%8C-%D9%87%DA%A9-%D9%88-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86/

[94] http://www.giganews.ir/?p=87

[95] www.shabgard.org/forums

[96] http://simorgh-ev.com. The group began operating about ten years ago. Its official activities began with the publication of a small Internet magazine called "Simorgh Security Magazine".

then-retired famous Iranian hacker named Amir Ashiyani (aka ZXO003) was a member of this group. In 2006 he published a comprehensive book on Iranian hacking,[97] which received wide acclaim in professional circles in Iran and is still considered today to be the only book of its kind in Farsi.

The logo of the Simorgh Security Group[98]

"The Syrian Electronic Army"

Does the Internet invent new phenomena or does it develop and enhance existing phenomena? It seems that, in most cases, the Internet does not necessarily invent new phenomena but rather it obviates the physical component, borders and distance that exist in the world as we know it. The Internet provides additional dimensions to the terms, phenomena and activities of the physical world that we have become accustomed to. This applies to online social networks, Internet surveillance, fundraising for various purposes, and even the preparation of terrorist attacks. The Internet enables these and many other phenomena to be carried out in a faster and easier way than in the past.

One example of this is the ability to create an "electronic army" that defends a country from internal and foreign enemies in the cyber arena; one like the "Syrian Electronic Army".

The identity of this group, which began its activities several months after the start of the Syrian revolt, is not sufficiently clear; on its Web site, the group claims[99] to be composed of a few young activists who hack into Web sites on their own initiative,

---

Later on it also branched out into the commercial arena in providing consultation services, Pen Testing, and more. According to the group's Web site, about five years ago the group turned to "underground" activities, which lasted about four years, and returned to commercial activities about one year ago.

[97] http://www.shabgard.org/forums/showthread.php?18168-Anti-Security-Handbook

[98] http://simorgh-ev.com

[99] http://sea.sy/article/id/190/en

with no connection to the Syrian regime. Nevertheless, a study[100] that was carried out a short time after this group began its activities found a link between it and government officials, at least with regard to the group's Web site and a speech given on June 20, 2011, in which Syrian President Assad praised the group's activities and characterized it as a "real army in virtual reality".[101]

The Syrian Electronic Army's Internet presence is remarkable on several levels; it is very current, offers simultaneous reporting in Arabic and English, displays lively activity including graphic aspects, and has its own Web site (which has changed its appearance and URL several times). It also has a prominent presence on various social networks, especially Facebook[102] and Twitter[103] - accounts that are often shut down by company management and then replaced by new ones – as well as Instagram[104] and others.

An analysis of various attacks carried out by the Syrian Electronic Army since the start of its operation demonstrates that its mission is to protect Syrian interests through the use of cyber attacks. It is not involved in protecting Syrian Web sites or computer systems, but rather in executing various attacks against those it considers to be enemies of Syria, both domestic and foreign. The group's various activities attest to its central targets: government officials in countries throughout the region, Western and Arab media outlets, and recently even Internet media applications.

The Syrian Electronic Army's main targets are Western media outlets; it usually hacks into their Twitter accounts and leaves various messages, as it did to *The Financial Times*, 30 Twitter accounts belonging to *The Telegraph*, the BBC, the AFP, *The Washington Post*, *The Onion*, NPR, *The Guardian*, Al Jazeera and many Western and Arab media outlets.

The most memorable attack carried out by the Syrian Electronic Army to date was directed against the Associated Press news agency's Twitter account at the end of April 2013, in which it inserted a false news item about two explosions that had allegedly occurred at the White House and injured President Obama.[105] The significance of the news item, as well as the important standing of its source, had an immediate effect on the financial markets.[106]

---

[100] https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army

[101] http://www.al-bab.com/arab/docs/syria/bashar_assad_speech_110620.htm

[102] https://www.facebook.com/SEA.Official.220

[103] https://twitter.com/Official_SEA16

[104] http://instagram.com/official_sea/

[105] https://twitter.com/APStylebook/statuses/326746884062453760

[106] http://buzz.money.cnn.com/2013/04/23/ap-tweet-fake-white-house/?iid=EL

The Syrian Electronic Army also attacked companies involved in Web-based communication products, including Viber (specifically, its support page[107] and App Store[108]), Tango,[109] Truecaller,[110] and others. At the same time, activists in the group also attacked computer systems (mainly email servers) belonging to government officials in various countries throughout the region, leaking content and email addresses from these servers in an effort to bring shame and damage to Syria's enemies. In this framework, the group hacked into the mail servers of Turkey's Prime Minister,[111] the Turkish Ministry of Interior,[112] government offices in Qatar,[113] the Saudi Arabian Ministry of Defense,[114] the Arab League,[115] and more. These operations were focused on the designated part of these organizations' Web sites.[116]

The increasing news coverage about a possible U.S. strike against Syria, and the tension it generated, led to the following:

Offensive Action – On August 27, the Syrian Electronic Army announced[117] that it had managed to change Twitter's domain registration details and attached a photo[118] verifying it.

The next day, the group published a list[119] of additional Twitter accounts that it had allegedly hacked into, including those belonging to Twitter in the United Arab Emirates[120] (https://twitter.ae) and in Great Britain[121] (http://twitter.co.uk). It also hacked into the DNS[122] server of the *New York Times* and the *Huffington Post*. At the same time, the group announced that the "Name.com" company, which provided it

[107] http://news.cnet.com/8301-1009_3-57595196-83/syrian-electronic-army-hacks-into-viber-database/
[108] http://www.tech-wd.com/wd/2013/07/28/viber-app-store-hacked/
[109] http://news.softpedia.com/news/Syrian-Electronic-Army-Hacks-Mobile-Messaging-Service-Tango-369644.shtml
[110] http://news.softpedia.com/news/Syrian-Electronic-Army-Hacks-Global-Phone-Directory-Truecaller-368708.shtml
[111] http://hackersnewsbulletin.com/2013/06/turkey-prime-ministers-website-hit-by-combo-cyberattack-of-anonymous-and-syrian-electronic-army-gov-emails-leaked.html
[112] http://hackersnewsbulletin.com/2013/06/syrian-electronic-army-hacked-website-of-turkish-ministry-of-interior-and-leaked-login-credentials.html
[113] http://english.al-akhbar.com/content/qatar-leaks-business-foreign-affairs
[114] http://hackread.com/saudi-arabian-defense-ministry-mail-system-breached-secret-emails-leaked-by-syrian-electronic-army/
[115] http://www.middleeast-internet-monitor.com/?p=3108
[116] http://sea.sy/section/id/1/en
[117] https://twitter.com/Official_SEA16/status/372559274771107840/photo/1
[118] https://twitter.com/Official_SEA16/status/372462339456380928/photo/1
[119] https://twitter.com/Official_SEA16/status/372484705238540288/photo/1
[120] https://twitter.com/Official_SEA16/status/372495916055285760
[121] https://twitter.com/Official_SEA16/status/372477933064949760
[122] https://twitter.com/Official_SEA16/status/372474022358810624

with storage services, had suspended its Web site activities[123] (which remained disabled until the morning of September 1).

In addition, on the evening of August 31, the Syrian Electronic Army's Facebook page[124] displayed links to the official Facebook pages of the United States Marine Corps, President Obama, CNN and the Associated Press, along with an explanation in Arabic, perhaps as an indication of the group's future targets.

Nevertheless, the Syrian Electronic Army serves not only as a tool for attacking Syria's enemies, both domestic and foreign, but also for spreading propaganda at the behest of the Syrian regime and its leaders; therefore, as reports about an upcoming American attack increase and tensions grow, the Syrian Electronic Army is increasing its propaganda activities and discussing events via announcements on Twitter. According to these announcements, the group is planning "many surprises"[125] and is prepared to attack.[126]

The Syrian Electronic Army also documented demonstrations against the planned [U.S.] attack,[127] published the Syrian Defense Minister's announcement that his army is ready to deal "with all kinds of military aggression",[128] published various propaganda posters,[129] and called for support for the Syrian Army and President Assad.[130]

Despite the above, as part of the psychological warfare that takes place in the online arena, an unknown entity purporting to be the Syrian Electronic Army recently opened a Twitter account[131] criticizing the Syrian leadership and its use of chemical weapons.

The Syrian Electronic Army is a group that operates in the cyber arena and does not seem to initiate and carry out operations independently, but rather is supported by Syrian government officials to fight Syria's enemies in cyberspace – both domestic and foreign. For the time being, the attacks that the Syrian Electronic Army generates are not of high caliber and cannot inflict any real damage on infrastructure. The group focuses on attacking Internet sites and email servers – attacks that generate more media hype and psychological harm than actual damage.

---

123 https://twitter.com/Official_SEA16/status/372514860866613249/photo/1
124 https://www.facebook.com/SEA.Official.222
125 https://twitter.com/Official_SEA16/status/373530003238973440
126 https://twitter.com/Official_SEA16/status/373596652008796160
127 https://twitter.com/Official_SEA16/status/373291760010543105
128 https://twitter.com/Official_SEA16/status/373263783445008384
129 https://twitter.com/Official_SEA16/status/373077439460548609
130 https://twitter.com/Official_SEA16/status/372498037186129920
131 https://twitter.com/Official_SEA7

Silk Road – Game Over?

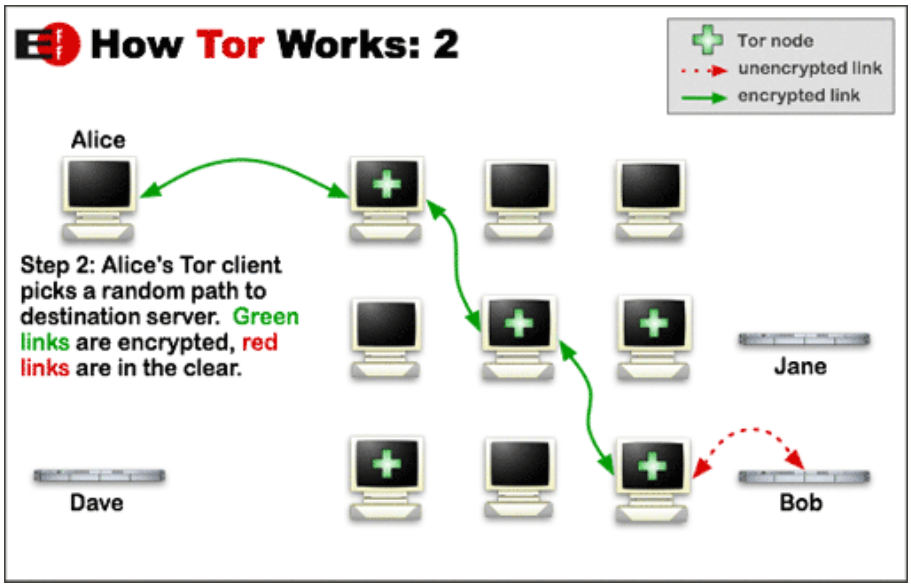
In the previous newsletter published in October,[132] we analyzed the action taken by U.S. authorities to close the Liberty Reserve in an effort to combat the phenomenon of virtual currency use as a platform for transferring black market money between parties. This was a first indication of the growing struggle between law enforcement and criminal activity in the cyber world. In the beginning of October, it was reported that Ross William Ulbricht had been arrested and that the illicit Silk Road Marketplace Web trading site that he managed had been shut down. Unlike with Liberty Reserve, which operated on the visible Internet, Silk Road Marketplace operated on the dubious darknet and made use of The Onion Router (Tor) software, which provides full anonymity and protection to its users and enables illegal activity without fear of being discovered by law enforcement.

In recent years, there has been much debate over how secure and anonymous the darknet really is. The darknet refers to all of the Web sites found at the "edge" of the Internet, far removed from search engines and accessible to a limited number of Web surfers. Tor was launched in September 2002, and over time it gained the support of various entities in the United States, including the U.S. Naval Research Laboratory, DARPA, the U.S. State Department, and other NGOs.

The idea behind the Tor Project began with the U.S. Navy in an effort to create an encrypted and anonymous means of communication for government officials.[133] As opposed to regular computer communication that creates a series connection between two computers, Tor creates a random connection among several computers (computers that have been installed with the designated software), and each connection is encrypted. Tor enables anonymous communication and, in the event that a transmission is intercepted, it is encrypted, making it difficult to decipher the information.

[132] http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1232/currentpage/1/Default.aspx

[133] https://www.torproject.org/about/overview.html.en



An illustration on the Tor Project Web site, demonstrating the transmission of data between two users, Bob and Alice.

In 2007, the Tor Project announced a new service for Tor users called Hidden Service Protocol,[134] which makes it possible to create Web sites and offer services that are hidden from the Internet using the onion domain. Entry to these Web sites is permitted to Tor users only, thereby creating a new world of online content that is not accessible to everyone. While the goal was to create a platform for "positive" uses, the crime world has fully adopted the technology.

[134] https://www.torproject.org/docs/hidden-services.html.en

The investigation of Silk Road began in November 2011 as a joint operation of the FBI, DEA, IRS and Homeland Security Investigation. The indictment against Ross William Ulbricht included charges of narcotics distribution, computer hacking and money laundering. The indictment for money laundering accused him of using bitcoins to disguise and obscure the identity of users of the Web site.

According to the indictment, during the period of February 6, 2011-July 23, 2013, 957,079 users registered with the site and carried out a total of 1,229,465 transactions, approximately 30% of which took place in the United States. Sales on the Web site were estimated at 9.5 million bitcoins, raking in a commission of 600,000 bitcoins from site users (at a rate of 8-15% of the total transactions, depending on the size of the deal). On September 23, 2013, the site put up the following for sale: approximately 13,000 items of drug paraphernalia, 159 hacking service products, 801 digital products (hacking software, credit card data, etc.) and 169 counterfeit products (bills, personal IDs, etc.).

The operation to locate the Web site's founder was lengthy and involved crosschecking a great deal of data and using agents on the ground. Ulbricht posted on various Web forums using fictitious profiles and worked out of coffee shops in order to reduce the chances that a digital signature could connect him to the Web site. During his incarceration, authorities managed to gain access to the site and its collection of data, which included details about its users. About a week after the site was shut down, a number of these users were arrested in Britain and Sweden.[135] In most cases, law enforcement managed to confiscate the users' bitcoins. The bitcoins confiscated from Ulbricht were worth approximately 3.6 million dollars, and investigators estimate that there are additional bitcoin files worth approximately 80 million dollars. Unlike cash that has been confiscated, bitcoins cannot be used or converted into real coins without the owner's password. It is likely that the defendant's cooperation, or lack thereof, with law enforcement will influence the sentence that he receives.[136]

This affair serves as a milestone in the war on darknet crime insofar as it challenges the assumption that Tor software provides its users with full anonymity and protection from law enforcement. Around the time that this affair was publicized, Edward Snowden leaked additional documents belonging to the NSA, which indicated that attempts had been made by intelligence organizations to decode and break the

[135] http://www.huffingtonpost.com/2013/10/08/silk-road-arrest-bitcoin_n_4063300.html
[136] http://business.time.com/2013/10/11/why-the-fbi-cant-get-its-hands-on-silk-road-kingpins-80-million-hoard/

Tor encryption.[137] One published report referred to the need for creative thinking in order to circumvent the encryption and, rather than find a way to decode the message itself, use Trojan horses on computers that use Tor.

In summary, close cooperation between a number of organizations and countries enabled law enforcement to shake up one of the most protected arenas of operation for international criminal and terrorist entities. This action will require criminals and terrorists to invest in methods of concealment and security in order to make it difficult [for the authorities] to monitor their activities on the darknet. The largest illicit trading site in the world was shut down, its users and traders are now known to law enforcement, and it is reasonable to assume that the task of identifying and locating them will require a great deal of work and will focus on the biggest traders. In a study published by Trend Micro,[138] it was found that illicit trading exists not only on the darknet, but also on the Russian Underground, which operates on the visible Internet. These Web forums deal with the field of hacking services, from the supply of forged documents to shelf products.[139] Despite the assumption that the publication of the affair and the exposure of those arrested will be a cause for concern to consumers and traders, and despite the upset that it caused to active members of the darknet, a new Web site called Silk Road 2.0, which is identical to the original site, appeared on the darknet about a month after the first report was published.[140] The question now is how long it will take the authorities to locate and capture the operator, or operators, of the new site.

[137] http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption
[138] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf
[139] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
[140] http://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/

Guest Contributor

Countering Security Solutions – How Cyber-Criminals Easily Evade Detection (Part I) [141]

Invincibility lies in the defense; the possibility of victory in the attack.—Sun Tsu

Over the past 18 months, the security industry has witnessed an interesting trend in financial malware. While malware authors are still improving their product's offensive capabilities, significant time and effort have been invested in the defensive and evasive capabilities of different malware variants. As security solutions improve in detecting, mitigating and removing malware, cyber-criminals realize that they are losing money – not because they fail to infect devices or even steal credentials – but rather because they are quickly discovered after the act due to "on device" software or Web-based (clientless/cloud) solutions. In this article, I will review some of the techniques used by malware authors, the countering techniques implemented by security solutions, and the malware response to these countermeasures. Security and fraud is a timeless game of cat-and-mouse, and I will leave it to the reader to decide who is playing which role.

Evading Device-Centric Security Solutions

In order to fully appreciate the long way that malware defensive solutions have come, I will start by reviewing a rather simple, yet typical, example of malware vs. security vs. malware. One of the most common modules employed by malware for credential stealing is a key logger. By logging all of the keystrokes that a victim makes on Web sites of interest (banking sites, eCommerce sites, Enterprise Outlook Web Access sites, etc.), cyber-criminals can easily re-use the credentials to gain access to those accounts. This was true 15 years ago and it is still true today.

In an effort to prevent key logging, security companies came up with a solution whereby the user is forced to click on a virtual keyboard using the mouse, rather than using a manual keyboard to enter passwords. In this manner, key loggers were effectively bypassed and no credentials were lost. While this solution was not adopted by all banks and eCommerce sites, it still posed a challenge for cyber-criminals.

The countering module was introduced fairly quickly. Malware authors started

[141]This article was written by Etay Maor, an ICT Research Intern who holds an MA in Government with a specialization in Counter-Terrorism and Homeland Security from the IDC.

capturing screenshots every time a victim initiated a mouse click event. In other words, when users clicked on the virtual keyboard, the malware on the device would initiate a screen capture and send it to the malware command and control server, allowing the criminal to see the virtual keystrokes, thereby solving the criminals' problem.

Companies are constantly striving to identify the authenticity of devices that are interacting with their Web sites. As malware was increasing in popularity and use by cyber-criminals, organizations were concluding that it is almost impossible to trust online sessions based solely on username and password combinations. Trust was becoming a complex issue, and an additional layer of security was required. Device ID was introduced as a solution, and remains a major component of most security solutions. In addition to authenticating the user, the device now had to pass certain tests to be deemed trustworthy and to rule out cyber-criminal activity. These tests included hundreds of parameters. Device parameters were constantly being collected by the client (through cookies, flash) and by clientless device ID solutions, including screen resolution, hardware components, operating system parameters, languages installed, and the browser used. This so-called "frictionless authentication" (a term used more commonly today by biometric companies) was, and still is, a very big challenge for cyber-criminals. It effectively means that even if credentials are captured, be it through key logging, form grabbing or screenshots – as soon as a login attempt is made from the cyber-criminal's device it is detected and stopped, and an alert is generated. Once again, cyber-criminals began losing money.

Multiple solutions were created to solve the device ID "problem", some of which will be discussed in the second part of this article. I will focus on three popular and highly effective solutions. The first solution is a crude one, and does not involve a malware-specific component. Software that can fake a device ID can be found in most professional cyber-underground forums. This software, when installed on the cyber-criminal's device, will forge different device ID elements such as OS type and version, hardware parameters, browser ID and more. The malware can gather this type of data, which the cyber-criminal can then fake, thereby solving the device ID issue. This solution, however, is somewhat prone to problems. Device ID systems may check dozens, if not hundreds, of elements. Device-ID-faking software can never fully guarantee that all elements checked will be addressed. A better solution was required and so RDP was introduced.

RDP (Remote Desktop Protocol) and VNC (Virtual Network Connection) enabled

malware operators to take over a device in the same manner that support teams take over a computer in order to assist with technical issues. Most major financial malware today offers a built-in or add-on RDP functionality. Zues, Spyeye, Citadel and many other malware families have introduced this function with other, smaller families following in their path.

The attack is fairly simple. The malware stays dormant on the victim's machine until a successful login to a targeted site is detected (for example, the victim logs into his/her bank account). Once a login is detected, an instant message is sent to the malware operator indicating that the infected device is ready for takeover. The malware then injects an HTML screen to the user, faking a message from the bank Web site, alerting the user to a security or connectivity issue and informing him/her that the session is now paused for 60-120 seconds. While the victim is reading the message and waiting for the session to resume, the malware operator takes over the machine (the victim does not see anything on his/her end) and performs a fraudulent account. In terms of device ID, the session seems perfectly legitimate, as the transaction is coming from a trusted device (the victim's device).

The last example of an easy way to circumvent device ID systems is one that involves mobile devices, specifically iPhones. Apple has an iron grip when it comes to uploading software to iTunes. Earlier this year, Apple publicly announced to developers that software that accesses devices' UDID (iPhone Unique Device Identifier) will not be allowed on iTunes. While this was good news in terms of privacy, it was even better news for cyber-criminals. In addition to the existing lack of entropy in iPhones (all devices have the same language, browser, fonts, etc.), a lack of UDID for security systems opened the door to potential fraud. Cyber-criminals can now log into bank accounts using their iPhone's Safari browser and the credentials that they stole from their victims. Device ID systems cannot identify if an iPhone belongs to a user or a criminal, so it is now up to other security solutions (anomaly detection, behavior profiling) to detect this fraudulent behavior.

In the next part of this article I will discuss and explain how cyber-criminals use their tools to bypass anomaly detection and behavior profiling, and deceive bank call center and branch personnel.

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

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

Shuki Peleg, Information Security and Cyber-Security Consultant

Ran Ben Shalom, Student at the IDC

Michael Barak (PhD candidate), Team Research Manager, ICT

Nir Tordjman, Team Research Manager, ICT