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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 9

April – June 2014

Highlights

This report covers the period of April - June 2014, the 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:

- In addition to the intense activity on social media and networks, Al-Nusra al-Maqdisiyya lil-Dawla, a Palestinian organization identified as a supporter of the Islamic State launched an application named Fajr al-Bashair, "the first jihadist application, an application that provides news and updates regarding the Islamic State in the Android store – Google Play".
- The Technical Committee of the Markaz al-Fajr jihadist media institution published a computer software titled, "The Mujahid's Protection" for the Android device. According to the committee, this software is intended to provide secure browsing and an encrypted connection between jihad fighters.
- Various hacker groups in the Arab world continue to distribute guidebooks, translated into Arabic, on issues of defense (encryption and security software, creating aliases on social networks, etc.) and attack (instructions for carrying out defacement attacks using XSS, LFI, SQL Injection, etc.).
- An overview of groups in the cyber arena, including Anonymous4Palestine, Syrian Revolution Soldiers, SEA, and the European Cyber Army, as well as the activities of the group, Anonymous, against various targets.
- An analysis of several incidents in which Trojan Horse malware was sent via email as part of an attack focused on Israeli users. The emails that were sent impersonated topical and recent news items in order to deceive the end user.
- A case study regarding OpIsrael 2014, which was launched in the beginning of April 2014, during which various hacker groups attacked civilian and government targets in Israel for various purposes, including disabling sites and services, leaking information or damaging information systems. The review includes a presentation of the attacks that were successful as well as false reports of attacks.

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, April – June 2014[1]

The rift between the Islamic State and Al-Qaeda

During April-June, the jihadist discourse dealt with the rift between the Islamic State (IS) and Al-Qaeda. Sheikh Ayman al-Zawahiri, leader of Al-Qaeda, revealed a series of letters between his organization and the IS that, in his opinion, proved that the IS had previously sworn allegiance to the Al-Qaeda leadership and, therefore, should be considered an extension of Al-Qaeda in Iraq. However, under the leadership of Abu Bakr al-Baghdadi, the IS took an unfortunate turn when it decided to adopt a separatist policy and defy the dictates of the Al-Qaeda leadership. Nevertheless, al-Zawahiri emphasized the importance of maintaining unity among the ranks of the mujahideen and focusing on fighting against the Bashar al-Assad regime, while resolving disagreements through special shari'a courts.

Against the backdrop of al-Zawahiri's remarks and the growing rift between the two organizations, supporters of Al-Qaeda accused the IS of distorting the principle of jihad and spilling the blood of innocent Muslims. For instance, Sheikh Muhammad al-Maqdisi, a senior leader in the Salafi-jihadist movement in Jordan, ruled that the IS was a deviant organization operating against the mujahideen and, therefore, no one should join its ranks and the organization should be boycotted.

[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

In response, the IS accused the Al-Qaeda leadership of betraying its principles and deviating from the path of its previous leaders, such as Sheikh Osama bin Laden, by showing meekness in the face of secular powers, cooperating with them and attempting to sabotage the establishment of an Islamic State and caliphate. The success of the IS (which changed its name in June from the Islamic State of Iraq and Al-Sham) in seizing control of a significant part of Western Iraq as well as Mosul in Nineveh Province, the breakdown of the Iraq-Syria border, and the organization's declaration of the establishment of an Islamic caliphate in June increased its popularity with many jihadists around the world. Some of them, such as the Abu Sayyaf group in the Philippines, swore allegiance to the Islamic Caliphate and its leader, Abu Bakr al-Baghdadi.

The Indian Subcontinent

During this period, the jihadist discourse also focused on the India arena. Mawla Asim Umar, a senior member of Al-Qaeda in Pakistan, called on Muslims in Kashmir to wage jihad against the Indian authorities. According to him, Muslims in India and Kashmir must aid the effort to establish an Islamic caliphate. Ansar al-Tawhid fil-Hind, a Salafi-jihadist organization in India with links to Al-Qaeda, also called on jihadist leaders around the world, especially in the Middle East and South Asia, to attack Indian targets both on Indian soil and around the globe.

The Pakistani government was also presented as an enemy of Muslims. In the beginning of June, the Islamic Movement of Uzbekistan called on Muslims in Pakistan to wage jihad against the Pakistani government and army due to their operations against Muslims in the country and their collaboration with the United States. In addition, the organization claimed responsibility for an attack that its members carried out at the Karachi Airport in Pakistan on June 9, 2014. Regarding Afghanistan, the Shura Council of the Islamic Emirates in Afghanistan announced its intention to carry out a wave of attacks against various government targets in Afghanistan, such as military facilities and diplomatic sites.

China

China's position in the jihadist discourse has also been steadily rising. In the beginning of April, Sheikh Abu Dhar Azzan, who serves as a mufti in the Turkestan Islamic Party, emphasized that jihad against China is necessary because of its collaboration with Pakistan and its persecution of Muslims.

Western hostages as a bargaining chip for jihadist organizations

The jihadist discourse was also focused on the prisoner exchange deal that was reached between the United States and the Taliban in Afghanistan, in the framework of which captive American soldier, Bowe Bergdahl, was returned in exchange for five senior members of the Taliban in Afghanistan who were released from Guantanamo Bay Prison. Sheikh Ayman al-Zawahiri's call to kidnap Westerners in order to hold them captive as bargaining chips to free Muslim prisoners was also a focus of the jihadist discourse. Sheikh Adam Gadahn, a senior member of Al-Qaeda, also called for efforts to be made to put an end to US involvement in the internal affairs of Arab countries, such as Egypt.

The Levant (Al-Sham)

The civil war in Syria and its spillover into Lebanese territory also occupied a significant part of the jihadist discourse during this time period. Siraj al-Din Zurayqat, a member of the Abdullah Azzam Brigades, threatened to attack the Lebanese Hezbollah if the latter did not stop serving as a tool to fulfill Iranian interests in Lebanon. According to him, Sunni soldiers in the Lebanese army must defect and defend Sunnis in the country.

The release of Sheikh Abu Muhammad al-Maqdisi, a senior member of the Salafi-jihadist movement in Jordan, from a Jordanian prison in June was applauded by many jihadist fighters.

The Maghreb

Al-Qaeda in the Islamic Maghreb (AQIM) called on Muslim citizens of Libya to defend their honor and Islam from the aggression of Libyan leader, General Haftar, in light of Operation Karama, which was launched to destroy terrorist nests in the country. According to the organization, the campaign was a Zionist-Crusader conspiracy supported by Egypt and funded by the Gulf States that must be immediately thwarted.

Somalia

Al-Shabab Al-Mujahideen militants in Somalia threatened to carry out additional terrorist attacks like the one that its members carried out at the Westgate Mall in Kenya. In addition, the

organization called on Muslims to travel to Somalia in order to help wage jihad against enemies of Islam.

Nigeria

Abubakar Shekau, leader of Boko Haram in Nigeria, claimed responsibility for the abduction of Nigerian Christian schoolgirls from their school, and vowed to spill the blood of Christians and to fight against democracy. According to him, most of the abducted students had declared their conversion to Islam. In addition, he expressed a willingness to release the Christian students who did not convert in exchange for the release of all Muslim prisoners in Nigeria.

Jihadist Propaganda

- The Al-Battar jihadist media institution, which is affiliated with the Islamic State, published an article titled, "The Electronic Islamic State Army: Lone Wolves". The article praised the organization's online information system and ascribed to it significant importance in light of attempts made by enemies of the organization to tarnish its image through false propaganda and distortion.[2]

The article banner

[2] http://justpaste.it/fd3p

- Al-Nusra al-MaqdIsiyya lil-Dawla al-Islamiyya , a Palestinian organization identified as a supporter of the IS, launched Fajr al-Bashair, "the first jihadist application", on Google Play. According to the attached description, the application provides news and updates regarding the IS and its activities directly to the user's account in order to promote the organization's message and spread it to Muslims, wherever they are.[3] The application[4] (Android), called فجر البشائر, was available from April 15, 2014. It was described as "a news application that published the latest news and events in Syria, Iraq and the Islamic world".

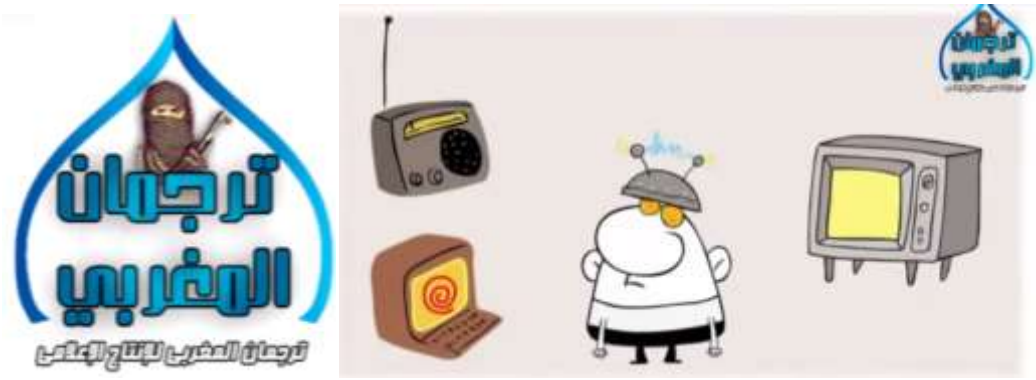
A posting on Twitter regarding the new publication

[3] http://www.hanein.info/vb/showthread.php?t=362588
[4] https://play.google.com/store/apps/details?id=com.pashaeer.myapp

Fajr al-Bashair, "the first jihadist application"

- An anonymous media group named Turjaman al-Maghribi al-Ilami, which is affiliated with the IS, produced a propaganda video in praise of the organization. The animated video presented the common citizen as a victim of continuous brainwashing by the global media and influenced by biased reporting aimed at painting members of the IS in a negative and demonic light.[5]

[5] https://www.youtube.com/watch?v=fOopGGUbsV8



From left to right: the logo of the media group, a clip from the animated propaganda video

- A video was published by the Electronic Brigades of the Islamic State in which a masked speaker identified as a member of the IS's technical team addressed Arab and Western media outlets and accused them of slander towards IS mujahideen. At the end of the video, the speaker warned that the IS would demonstrate its power in cyberspace by carrying out a surprise attack.[6]
- Ansar al-Sharia in Libya posted an announcement on its Twitter account regarding the launch of a prize-winning contest. In the framework of the contest, which was held on Facebook and Twitter, photos were published to which visitors had to respond. According to the announcement, the best response would win the first place prize of a G3 sniper's rifle. The second place prize was a Kalashnikov rifle, the third place prize were hand grenades, and the fourth place prize were two Kalashnikov magazines.[7]

[6] http://www.hanein.info/vb/showthread.php?t=367774
https://www.youtube.com/watch?v=Cx85CFxbZ7Y
[7] https://twitter.com/AnsarShariaa_ly/status/454613597398650880

Prize-winning jihadist contest

- The Fursan al-Nashr media group published a public appeal for graphic artists and writers to participate in a media campaign to free Mai al-Talq and Aminah al-Rashid,[8] two female prisoners accused by the Saudi authorities of trying to cross the border in Yemen and join Al-Qaeda there.[9] Meanwhile, a video was posted on YouTube that showed a group of veiled women protesting against the arrests and calling for the release of al-Talq and al-Rashid.[10]

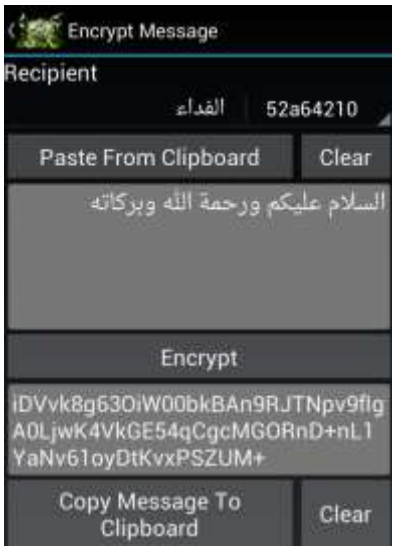
Defensive Tactics

- The technical committee of the jihadist media institution, Markaz al-Fajr, published computer software titled "Security of the Mujahid" for Android. According to the committee, the software was designed to provide secure Web surfing and encrypted connection capability among jihad fighters. In addition, it announced the launch of a special

[8] http://www.hanein.info/vb/showthread.php?t=363169
[9] http://www.arabnews.com/news/560061
[10] http://www.youtube.com/watch?v=wUmlmuelR_A

site for this software at: http://alfajrtaqni.net/index.html.[11]

The homepage of the technical committee of the Markaz al-Fajr jihadist media institution



From left to right: the banner of the software, part of the software display

- A prominent visitor to the Al-Platform Media jihadist Web forum published an announcement regarding "methods and software to protect your computer and cell phone from tracking". In the announcement, the writer explained the significance of a MAC address, a unique address for each communication device, and how to encrypt it. In

[11] http://al3aren.com/vb/showthread.php?p=4661

addition, the writer advised software users to encrypt IP and DNS addresses, and to use a TOR browser, among other recommendations.[12]

- A department administrator of the Al-Platform Media jihadist Web forum published an announcement regarding "12 Steps to Protect a PC from Hackers". The announcement provided recommendations such as avoid using file-sharing software (P2P), use Virtual PC software such as VMWare, and select complicated passwords.[13]
- Visitors to the Hanein jihadist Web forum discussed the Iraqi authorities' monitoring of Facebook and Twitter sites as a result of the security situation in the country. The visitors exchanged advice on the matter, mentioned the need to conceal the IP address while surfing in order to avoid tracking, and noted several software programs that can be used to override blocked access to sites such as Hotspot Shield or VPN Gate.[14]

Offensive Tactics

- The forum administrator of the Tunisian hacker group, "Fallega", which is affiliated with global jihad, published an instructional video on how to hack into Yahoo email accounts. One suggestion was to obtain an account password by answering questions to verify the identity of the email account holder, after which a new password would be sent to the email address.[15] Another member of the forum posted an instructional video on how to install VMWare Tools using Kali Linux, a type of toolbox used for hacking.
- A Tunisian hacker called Tunisian Cracker, a member of the Tunisian Kalashnikov hacker group, published a series of guidebooks titled, "A Web Site Hacking Course", using videos on the Fallega forum. The guidebooks suggested various tools for hacking into Web sites, databases,

[12] http://alplatformmedia.com/vb/showthread.php?t=46243
[13] http://alplatformmedia.com/vb/showthread.php?t=48255
[14] http://www.hanein.info/vb/showthread.php?t=371466;
http://www.hanein.info/vb/showthread.php?t=371524&p=2583593
[15] http://www.fallega.tn/vb/showthread.php?t=1995

servers and PC's, including various methods of executing defacement attacks - SQL Injection,[16] Upload Shell, LFI, XSS.[17]

- Another guidebook that was published on the above-mentioned forum dealt with learning how to hack into Web sites by penetrating the database.[18] A senior visitor to the forum published a guidebook on how to hack into Web sites by using ftp.[19][20] Another senior visitor published a guidebook for advanced hackers on using SQL Injection to hack into Web sites.[21]
- One of the administrators of the Al-Platform Media jihadist Web forum published a guidebook explaining how to use a fake identity on Facebook. For instance, it explained how one can skip the "Confirm Your Identity" step.[22]
- A prominent visitor to the Al-Platform Media jihadist Web forum published a guidebook explaining how to open a Gmail email account and a YouTube account without having to provide a telephone number. This way, the account does not infringe on the user's privacy and it makes it more difficult for intelligence organizations to track the user.[23]

Guiding

- The Al-Battar jihadist media institution, which is affiliated with the Islamic State, published several instructional videos on its Twitter account explaining how to use After Effects, software for editing video files.[24]
- The Al-Platform Media jihadist Web forum published the seventh part of the "Jihadist

---

[16] *SQL injection* is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.
Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications which enables attackers to inject client-side script into Web pages.
Shell is a user interface for access to an operating system's services.
Local File Inclusion (LFI) vulnerability is when a file from the target system is injected into the attacked server page.

[17] http://www.fallega.tn/vb/showthread.php?t=2506, http://www.fallega.tn/vb/showthread.php?t=2507, http://www.fallega.tn/vb/showthread.php?t=2510

[18] http://www.fallega.tn/vb/showthread.php?t=2450

[19] File Transfer Protocol (FTP) is a network protocol used to transfer files between computers and servers.

[20] http://www.fallega.tn/vb/showthread.php?t=2345

[21] http://www.fallega.tn/vb/showthread.php?t=2514

[22] http://alplatformmedia.com/vb/showthread.php?t=51754

[23] http://alplatformmedia.com/vb/showthread.php?t=49501

[24] http://justpaste.it/fjw1

Encyclopedia". The edition included a security section, a military section and a technological section, the last of which included a basic electronics course as well as a course on computer hacking.[25]

Social Media – New Web Sites

- On April 4, the Global Islamic Media Front (GIMF) jihadist media institution published an announcement in Arabic, English, Urdu and Indonesian announcing the creation of an official Twitter account: https://twitter.com/J_Eielamiya.[26]

The announcement of the creation of an official Twitter account

- The Al-Isaba, jihadist media institution of Ansar al-Tawhid fi Bilad al-Hind, a Salafi-jihadist organization in the Indian subcontinent, opened an account on the video-sharing site, YouTube, in April 2014.[27]

[25] http://alplatformmedia.com/vb/showthread.php?t=47506
[26] https://alfidaa.info/vb/showthread.php?t=96731
[27] http://www.youtube.com/channel/UC72MKCg6zAqSI8H35unonzA

- The Al-Bayariq jihadist media institution, which represents Ansar al-Shari'a in Tunisia, announced the creation of new official pages on Twitter (https://twitter.com/AnsarShariaa_tn) and Facebook (https://www.facebook.com/ansarii.tn).[28]
- A new jihadist media site called Jihad News was established at the following address: http://jehadnews.com.[29] It also opened a Facebook page (https://www.facebook.com/jehadnewsCom) and Twitter account (https://twitter.com/jehadnewscom).
- A visitor to the Hanein jihadist Web forum published a new, unofficial link to the Twitter account of Jaish al-Mujahideen in Iraq Twitter: https://twitter.com/mojahden2
- The Twitter account of the Islamic State's jihadist media institution, Al-I'tisam, @wa3tasimu, was removed by Twitter.[30] In addition, starting in mid-June, access to the Islamic State's Twitter accounts in the following provinces was disabled: Northern Baghdad, Kirkuk, Saladin, Diyala, Nineveh, Baghdad, and more. The removal of these accounts may have had something to do with the organization's occupation of Mosul in the beginning of June 2014.[31]
- A prominent visitor to the Al-Platform media jihadist Web forum published an announcement regarding the establishment of a new Twitter account – "The Media Front in Support of the Islamic State". The purpose of the account was to support the Islamic State and publish announcements about its operations. It was not explicitly stated which parties were behind the initiative but the announcement implied that it was the product of several media groups that decided to join forces for this purpose.[32] The link to the Twitter page:

[28] http://alplatformmedia.com/vb/showthread.php?t=44627
[29] http://alplatformmedia.com/vb/showthread.php?t=45816
[30] https://twitter.com/wa3tasimu
[31] http://www.hanein.info/vb/showthread.php?t=371560
[32] http://alplatformmedia.com/vb/showthread.php?t=48996

https://twitter.com/sh_ansaar.

- The Al-Battar jihadist media institution, which is affiliated with the Islamic State, announced on May 7, 2014 that it had launched a Twitter account in English as part of the organization's PR campaign.[33]

The banner announcing the establishment of a Twitter account in English

- During the second half of June 2014, a new Twitter account in Indonesian was created - "Supporters of the Islamic State Caliphate in Indonesia".[34]

[33] https://twitter.com/AL_Bttaar/status/464119800885547009/photo/1
[34] https://twitter.com/ansarmuqowamah1

The logo of the Twitter account of the "Supporters of the Islamic State Caliphate in Indonesia"

Social Networks

- The increasing use of drones by the United States and its allies to attack global jihad activists in Yemen, among other places, has been widely criticized not only by jihadists but also by the civilian population that has been hurt in these aerial attacks. Against the backdrop of this growing criticism, jihadists have taken advantage of the public mood to wage a PR campaign on the social network, Twitter, in order to deride the United States as well as the Saudi regime for its consent in allowing America to use its bases on Saudi soil in order to wage aerial attacks in Yemen. For example, various hashtags were launched, including "US and Saudi Arabia are Killing Yemenites",[35] and "Yemen Massacres in Silence".[36]

Banners that were published on Twitter criticizing the US and Saudi Arabia for the use of drones

[35] _وال_سعود_يقتلون_اليمنيي
[36] #اليمن_يذبح_بصمت

- A similar PR campaign was launched protesting the use of drone strikes against Muslims in Waziristan, along the Pakistan-Afghanistan border. This campaign was concentrated mainly under the hashtag "Waziristan is Massacring Muslims".[37]

Where are the Muslims? Help Muslims in Waziristan

- In June, a widespread PR campaign on was launched by jihadists on social networks and on several jihadist forums, especially the leading jihadist forum Shumukh al-Islam, to free prisoners from the Roumieh Prison in Lebanon. In the framework of the campaign, banners were published condemning the Lebanese government for its policies of persecution against the Sunni population, and criticizing the Shi'ites for collaborating with the Lebanese government against the Sunnis. In addition, they threatened that the Lebanese government would face severe consequences if it did not immediately release Sunni prisoners. For example, one of the banners showed Sheikh Abu Hummam al-Suri, a senior fighter in the Al-Nusra Front (Al-Qaeda's affiliate in Syria), threatening to harm Shi'ites and Hezbollah in Lebanon: "I call on all righteous mujahideen to prepare to move the struggle to Shi'ite cities in Lebanon […].[38]

[37] #وزيرستان_تذبح
[38] https://shamikh1.info/vb/showthread.php?t=224063

From left to right: a banner with a message from Sheikh Abu Maria al-Qahtani, a member of the Shura Council of the Al-Nusra Front, criticizing the Lebanese government; a banner with a message from Sheikh Abu Hummam al-Suri condemning Shi'ites and Hezbollah in Lebanon

- The liberation of Mosul from the Islamic State in the beginning of June 2014 led to lively discourse on social networks among IS members and supporters from around the world, as well as its opponents. The discourse was mainly filled with praise for the organization's success in defeating the Iraqi army and seizing control of Nineveh Province and other areas. According to many IS supporters, the seizure of Mosul was a sign of things to come and heralded the occupation of all of Iraq and beyond. For instance, hashtags were created with the words "Mosul is Liberated",[39] as well as "Iraq is Rising Up Against al-Maliki".[40] On the other hand, there was also discourse on social networks on the part of Arab activists regarding the anticipated threat from the IS to the security of the Gulf States. For instance, Kuwaiti activists expressed great concern over the IS's attempted invasion of Kuwait, as demonstrated by the hashtag "Islamic State on the Border of Kuwait".[41]

The banner posted to the social network, Twitter, under the hashtag: "Mosul is Liberated"

[39] #الموصل_تتحرر
[40] #العراق_ينتفض_ضد_المالكي
[41] #داعش_على_حدود_الكويت

Against the backdrop of Mosul's liberation and the establishment of an Islamic caliphate, visitors to social network sites such as Twitter, as well as visitors to several jihadist Web forums, posted banners calling for attacks on US interests in its battle against the IS or in its use of drones against the Muslim population in Iraq. For example, the hashtags "A Warning to the American Nation" and #CalamityWillBefallUS were launched. In contrast, messages criticizing the organization were also created under the same hashtags by American civilians.[42]

[42] https://shamikh1.info/vb/showthread.php?t=225642; جمعة_تحذير_الشعب_الأمريكي, #CalamityWillBefallUS

Banners threatening to strike the United States if it attacks members of the Islamic State

A message posted by a supporter of the Islamic State: cm hydrogen cyanide found in grocery stores and could kill thousands of Americans

Cyber Attacks

- Fursan al-Islam, the electronic wing of the Army of Islam, a Salafi-jihadist organization in Syria, published several videos documenting the breach and vandalism of the Facebook accounts

belonging to several loyalists to the Assad regime as well as members of Lebanese Hezbollah.[43]

The logo of Fursan al-Islam

- On March 31, a hacker called YMH hacked[44] into the official Web site of the Training Authority of the Egyptian Army[45] and documented the breach,[46] in which it expressed confusion over the political situation in Egypt. It stated that "we do not know who to fight, al-Sisi or the Muslim Brotherhood, put aside the politics and enjoy a small cup of tea." On March 23, the same hacker hacked into two addition government sites in Egypt; the Web site of the Tourism Development Agency[47] (documentation of the breach[48]) and the Web site of the Military Technical College[49] (documentation of the breach[50]). The same message was posted on all three sites.
- On May 2, it was reported[51] that one of the servers of the University of North Carolina Wilmington had been breached, which had enabled the hackers to gain access to personal information belonging to employees and students. The server contained a database including the names, addresses and social security numbers of university employees and temporary workers. It also included personal details of university graduates, advisors and those who were tested in foreign languages at the university between 2002 and 2006. According to an

[43] http://www.youtube.com/watch?v=kG7hsVBYPe0; http://www.youtube.com/watch?v=J-2fNJ5dqxg, http://www.youtube.com/watch?v=7LDbzNwYFKs
[44] http://hackread.com/epypt-armed-forces-website-hacked/
[45] http://www.mcf.mil.eg/
[46] http://www.zone-h.org/mirror/id/22140785
[47] http://www.tda.gov.eg/
[48] http://www.zone-h.org/mirror/id/22066292
[49] http://www.mtc.edu.eg
[50] http://www.zone-h.org/mirror/id/22066468
[51] http://news.softpedia.com/news/University-of-North-Carolina-Wilmington-Suffers-Data-Breach-440448.shtml

announcement[52] that was published regarding this matter on the university's Web site on April 29, there was no evidence that the information was used or exploited by cybercriminals or. It also stated that the server hosted a page designed for phishing activities but that the hackers had somehow managed to obtain the password for the server's administrative account. The university removed the file and the sensitive data it contained from the server, and updated all of the operating systems and applications on all of the servers. It also placed restrictions on access to the server and increased the frequency of security checks. Existing applications were removed to separate and more secure servers, and special software was activated for locating identifying personal information stored on the university's computers. In addition, the university sent an announcement via email and snail mail to those who may been affected by the incident, and the Enforcement and Regulation authorities were updated with the details of the incident.

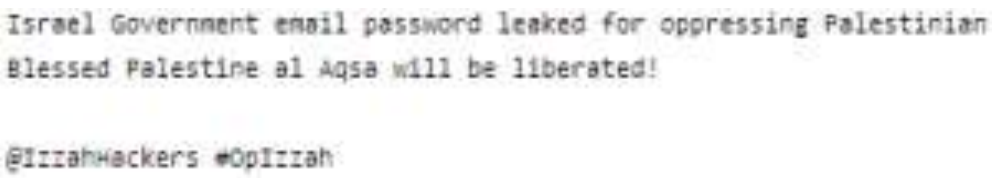
- On May 7, news agencies in France reported[53] that the information systems of the Orange telecommunication company in France had been hacked and that information on 1.3 million of its clients had been stolen in the second significant attack on the company in recent months. In the previous incident, which was discovered only recently on April 18, the hackers managed to obtain the names, email addresses, mobile and landline phone numbers, and birthdates of existing and potential clients – information that could be used to commit fraud, including phishing activities. The breach was apparently carried out by hacking into the system that was used to distribute promotional information to interested parties via SMS or email. Nevertheless, the company claimed that the payment details of its clients were not stolen. The company had previously announced in February 2014 that the online details of 800,000 had been stolen.
- On May 15, the Tunisian Hackers Team published an announcement[54] containing information about its breach of the Bangladesh Police Web site database.[55] The upper part of the announcement included messages lauding the supremacy of Islam – "We Will Raise the ISLAMIC FLAG Everywhere On White House And Over The Pentagon And In Every Country In The World

[52] http://uncw.edu/datasecurity/index.html
[53] http://www.securityweek.com/frances-orange-hit-hackers-data-raid
[54] http://pastebin.com/9aT3PGak
[55] http://www.police.gov.bd/

From East To West" – and went on to list the tables and contents of the database that was stolen from the site. However, the announcement mainly focused on the tables' structure and included very little information gleaned from them.

- On May 18, Anonymous Tunisia published an announcement[56] in which it claimed to have hacked into 570 Israeli Web sites. The announcement began with congratulations extended to several hackers – "Lola – Nabster Junior – Vinux – 5orda – AnonRev – ANONXOXTN". On some of the sites that were hacked, a page ending in "lola/anontn.html" was planted, which made it possible to identify the hacker responsible for some of the breaches. A sample testing revealed that the breach was carried out by hacking into the company, InterClick,[57] which built these sites – most of which belonged to small business owners – thereby enabling the sites to be accessed and vandalized. It should be noted that this list had already been published on May 11.[58]
- On May 25, LulzSecJR published a claim of responsibility[59] for hacking into 75 Indonesia government Web sites as part of an operation called OpMerdeka.[60]
- On June 12, a Twitter announcement was posted[61] in which IzzahHackers claimed responsibility[62] for leaking 18 email addresses belonging to the Ministry of Health.

[56] http://pastebin.com/KBH1xkfg
[57] http://www.interclick.co.il
[58] http://pastebin.com/drwe9i24
[59] http://pastebin.com/8gSrHp28
[60] https://twitter.com/hashtag/OpMerdeka?src=hash
[61] https://twitter.com/IzzahHackers/status/477054150203965440
[62] http://pastebin.com/b6HVP03t



A sample testing revealed that these email addresses can be found on various Web forums.

On June 15, SENTINELCELLOFFICIAL published an announcement[63] containing 25 email addresses ending with the "gov.il" suffix, as well as passwords. The announcement directed the Web user to a Facebook page[64] that was created on June 11, which has only 19 'likes'.

A brief examination revealed that this list had already been distributed, in full,[65] by AnonGhost as part of OpIsrael 2014. Therefore, the current forum contained nothing new and only recycled a list that had been previously published.

Syrian Electronic Army

- On April 24, a lecture[66] was given by Ira Winkler, President of Secure Mentem, in the framework of the RSA Conference 2014, which dealt with the Syrian Electronic Army's methods of attack and ways to cope with them. After the lecture, the company published an announcement according to which the Syrian Electronic Army had tried to hack into the conference site and that the company was investigating the attack.[67]

  In response, an announcement was posted on April 27[68] on the organization's Twitter account, which directly addressed the lecturer;

[63] http://pastebin.com/DZbYR7c7
[64] https://www.facebook.com/SentinalCell1337
[65] http://pastebin.com/raw.php?i=61vpGj8W
[66] http://www.rsaconference.com/videos/188/syrian-electronic-army-their-methods-and-your
[67] http://www.securementem.com/syrian-electronic-army-hacked-rsa-conference-site
[68] https://twitter.com/Official_SEA16/status/460193773549813760

The message also referenced a page[69] apparently documenting the breach;

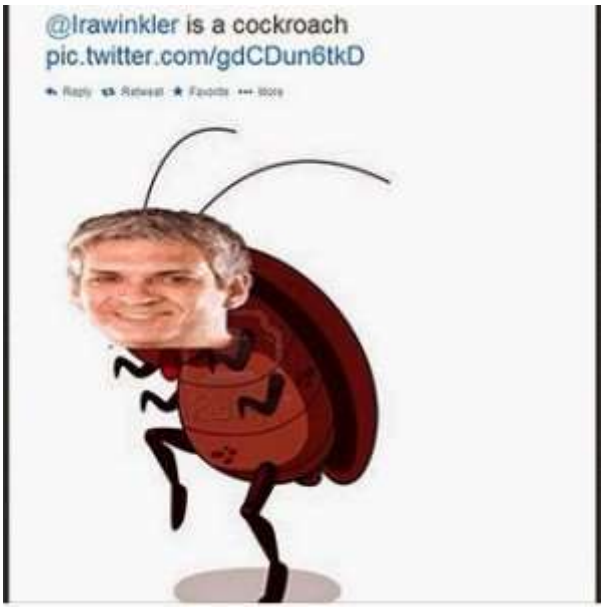
Another announcement[70] along the same lines;

Another announcement[71] was published two days later containing an analysis of the attack on the

[69] http://archive.today/KnsPn
[70] https://twitter.com/Official_SEA16/status/460371698257510401
[71] https://twitter.com/Official_SEA16/status/461128915399245824

conference site;

All of these led to an escalation in which four Twitter accounts belonging to the Wall Street Journal - @WSJD, @WSJPEurope, @WSJAfrica, and @WSJVintage – were hacked. This breach was reported[72] on May 6 and a message was posted[73] on the accounts that were hacked showing a photo of Ira Winkler on a drawing of a cockroach;



In addition, the organization hacked into the Reuters Web site on June 22, 2014 and planted a statement calling on the news agency to stop publishing false news reports against the Syrian

[72] http://www.wptv.com/news/science-tech/wall-street-journal-twitter-account-hacked-by-syrian-electronic-army

[73] http://2.bp.blogspot.com/-2te2Wze9Tho/U2pAiVahjJI/AAAAAAAALqg/y-fwqrW_7OI/s1600/wsj-twitter-accounts-hacked.jpg

regime. The breach was carried out by hacking into the Taboola Ad services, which was installed on the Reuters site as a result of phishing attacks.[74]

On June 18, an announcement[75] was posted on the Syrian Electronic Army's Twitter account regarding the breach that it carried out of the British media sites, The Sun and The Sunday Times.

[74] http://sea.sy/index/en
[75] https://twitter.com/Official_SEA16/status/479229118236487681

On the Twitter account[76] of The Sun, an announcement[77] was posted confirming that its Web site had been hacked;

Eleven minutes later another announcement[78] was posted, according to which the site was operating once again;

No such announcement appeared on the Twitter account of The Sunday Times.

On June 28, an announcement[79] was posted on Twitter, in Arabic, by the Syrian Electronic Army regarding the breach that it carried out of the Israel Defense Forces blog at idfblog.com. The

[76] https://twitter.com/TheSunNewspaper
[77] https://twitter.com/TheSunNewspaper/status/479217983941001216
[78] https://twitter.com/TheSunNewspaper/status/479220917361721344
[79] https://twitter.com/Official_SEA16/status/482962049668894721

announcement included a link to the page that was vandalized.[80]

An examination of this Web address, which serves as the official blog of the IDF in English, revealed that at the time the attempt was made to access the site, visitors to the site were directed to a page that had been prepared in advance in case of such a situation – Sea.sy.

[80] http://www.zone-h.org/mirror/id/22586423

Groups and Organizations

Anonymous4Palestine

In recent months, we have witnessed the online presence of a new entity in the cyber-arena – Anonymous4Palestine – which has also taken part in some of the online attacks against the enemies of Hamas, both within and outside the Gaza Strip. This initiative first appeared several months ago when the group managed to protect Hamas from a threat, which seemed significant at the time, to its power in the Gaza Strip. During the period between July 2013 and November 2013, an underground movement dubbed 'Tamrad' gained tens of thousands of followers from the Gaza Strip on social networks, in an effort to overthrow Hamas. On the other hand, it has taken severe and far-reaching steps in order to suppress the budding revolution.

In an effort to show solidarity with Hamas, and in order to defend its rule in the Gaza Strip, Anonymous4Palestine began to wage attacks on Web sites affiliated with the 'Tamrad' movement[81] and its supporters.

In addition to these operations, the group also took part in previous attacks on sites belonging to Fatah.

Another link between the group and Hamas can be found in the form of posters on the group's Facebook[82] page;

[81] https://www.facebook.com/tamradgaza1

[82] https://www.facebook.com/pages/Anonymous4Palestine/203189089853136

And others expressing the group's support for Hamas.

The group has been active on Facebook since the beginning of October 2013 and on Twitter[83] since February 2014, and it has posted several videos on YouTube.[84]

A review of the group's activity on social networks revealed that, in addition to its operations against the enemies of Hamas in the internal Palestinian arena, the group also carried out attacks against Israel in the framework of the 'OpIsrael' online attack, which was carried out this year for the second time on April 7, 2014 (this year, also under the name OpIsraelBirthday).

[83] https://twitter.com/Anonymous4Pales
[84] http://www.youtube.com/channel/UC5Spu6uFS5oqudS2t28aVCg

In addition, the group published several announcements on its Facebook account during March 2014 regarding the operation and its expected online attack against Israel as part of "the electronic struggle against the occupation".

Syrian Revolution Soldiers

On May 21, the Syrian Revolution Soldiers published an announcement[85] regarding a breach of six Jordanian government Web sites that the group carried out;

- Agricultural Credit Corporation
- Jordan Deposit Insurance Corporation
- Natural Resources Authority
- Ministry of Planning and International Cooperation
- Land Transport Regulatory Commission
- King Hussein 1 – a Web site in honor of the late King Hussein

The announcement also stated that the breach was carried out in order to "penetrate several locations Jordanian government because of lack of attention to the Syrian refugees".

An examination revealed that, in addition to the breaches noted in the announcement, the group also hacked into two other sites on the same date;

- United Arab Jordan Company for Investment and Financial Brokerage[86]
- Regency Palace - Amman[87]

In addition, there were announcements on the group's Twitter account regarding the breach of two

[85] http://pastebin.com/xWvErGR
[86] https://zone-h.org/mirror/id/22405218
[87] https://zone-h.org/mirror/id/22405219

Jordanian companies – the Securities Depository Center;[88]

And the Samra Electric Power Company;[89]

However, both of these sites are not currently in operation.

It seems that the group's activities began in the beginning of April 2014,[90] and included the breach of hundreds of Web sites around the world, on which they posted messages criticizing the world's disregard for the crisis in Syria and placing emphasis on the plight of Syrian refugees.

These attacks included the May 4 breach of 41 Pakistani government Web sites,[91] the May 6 announcement regarding the breach of 22 Syrian government sites,[92] and the May 7 announcement

[88] https://www.sdc.com.jo/arabic
[89] http://www.sepco.com.jo
[90] https://zone-h.org/archive/notifier=SRS/page=30
[91] https://www.facebook.com/photo.php?fbid=1386246214948318&set=a.1386156918290581.1073741828.1386066371632969&type=1
[92] http://pastebin.com/TpXXQcsZ

regarding the breach of 15 Syrian sites,[93] including ten government sites.

However, the group's activity on social networks is a recent occurrence; the operators of its Facebook page[94] noted that the group began to operate on March 15, 2011 but that activity on its Facebook page only began on May 1, 2014.

European Cyber Army

On April 28, 2014 a message was posted[95] on the Twitter account of the European Cyber Army, according to which its activity had seemingly come to an end;

Since the announcement was posted, no activity has been detected on its Twitter account and it seems to have been the last message posted on the account,[96] which had been very active for a

[93] https://www.facebook.com/photo.php?fbid=1386374464935493&set=a.1386156918290581.1073741828.1386066371632969&type=1
[94] https://www.facebook.com/SRS.Official2
[95] https://twitter.com/ECA_Legion/status/460622050269597697
[96] https://twitter.com/ECA_Legion

short while; 2,590 followers after 936 tweets that began on January 12, 2014.

The group's activities included online attacks against Syrian targets,[97] especially the Syrian Electronic Army, and other targets around the world.

Anonymous

In recent days, groups affiliated with Anonymous have called for online attacks against the Islamic State and its supporters.

On June 21, 2014 a four-and-a-half minute long video[98] was posted on YouTube by TheAnonMessage titled, "Anonymous: Operation #NO2ISIS", which has received approximately 2,800 views to date. The video described the targets of the attack as "government-owned websites belonging to Turkey, Qatar, and Saudi Arabia".

On June 25, 2014 the first tweets regarding the hashtag, OpNo2ISIS,[99] began to appear. The first message that was posted included a reference to the following video;

[97] http://middleeasternet.com/?p=9539
[98] http://youtu.be/_kJtvFUMELM
[99] https://twitter.com/search?q=%23OPNO2ISIS

A similar hashtag[100] was also created on Facebook.

Despite the fact that the video transcript did not give a start date for the operation, a message posted about it stated that an attack against the three above-mentioned countries would begin in the coming days ("In the next few days we will begin defacing the government websites of these countries so that they understand this message clearly").

Cyber-Crime and Cyber-Terrorism, April – June 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 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

[100] https://www.facebook.com/hashtag/opno2isis

was culled from the visible (OSINT) and invisible ("Dark Web")[101] Internet between April - June 2014.

Virtual Currency – Bitcoin Updates

The below chart shows the Bitcoin price on the BitStamp trading site for April-June 2014. The columns refer to the volume of the currency and the graph indicates the median price in American dollars on the same day. Beginning in mid-May, the currency rate of the bitcoin jumped to $650.

Bitcoin price chart in BitStamp for April - June 2014[102]

The Spread of Malware via Email

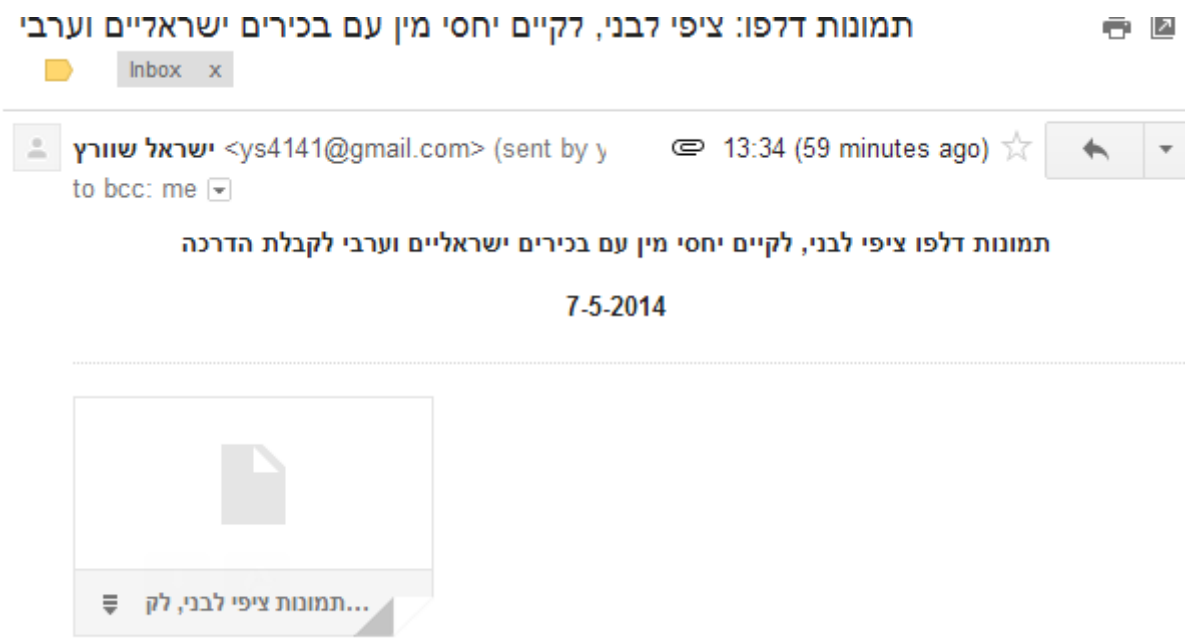
Some of the cyber-attacks, which are based mainly on human engineering, involve the spread of malware via email, a phenomenon that takes place on a daily basis. In contrast to the dangers posed by phishing, in which the user is required to enter the Web site and supply details or passwords, these emails mostly contain "juicy" titles with a virus-infected file attached, whether via backdoor or other malware that infects the computer to enable it to be controlled by the attacker's botnet.

At 13:34 on May 7, 2014, an email was received from the email address, ys4141@gmail.com,

[101] 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.

[102] http://bitcoincharts.com/charts/bitstampUSD#rg60zczsg2014-04-01zeg2014-06-30ztgMzm1g10zm2g25zvzcv

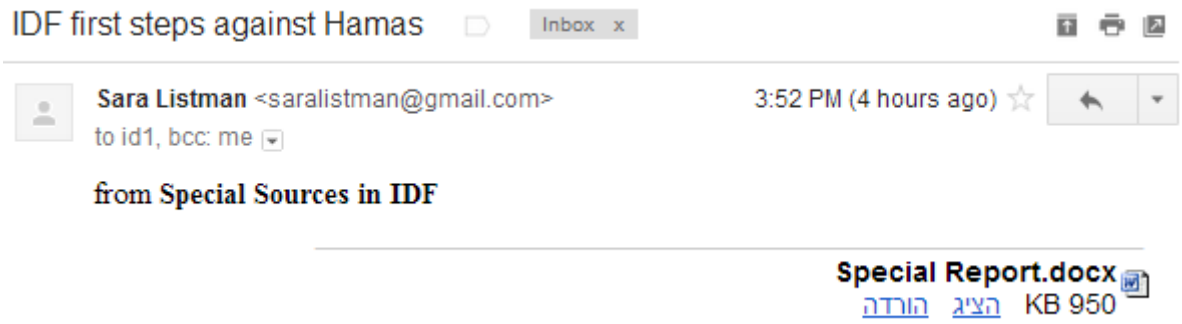
bearing the name “Israel Schwartz” and the subject, “Leaked images: Tzipi Livni having sex with Israeli and Arab officials”.



The email included the text “Leaked photos of Tzipi Livni having sex with Israeli and Arab officials for instructional purposes – May 7, 2014” and included a RAR file attachment titled, “Photos of Tzipi Livni having sex with VIP”. This file contained another file with the “.SCR” suffix.

At 11:15 on May 28, 2014, an email was sent with the subject, “Hamas has drones in Gaza” from Itzhak Hadari, from the email address hadariyitzhak@gmail.com. This followed the email with a similar format that was sent on May 7.

On June 2, 2014 another malware-containing email was sent out in Israel regarding the IDF, seemingly sent by Sara Listman, with the subject "IDF first steps against Hamas". The recipient's email address was listed as id1@israeldefense.co.il.



A detailed research report[103] prepared by the company, MORI.R.T. regarding this malware revealed that these two emails were also similar in that they contained identical malware. The report also included an in-depth technical analysis of this malware.

On June 10, 2014 an email was sent from "Ohad Levin", who serves as "Researcher and Director of Internet Media" at "Ashkubit Hashomron" with the subject, "Chief of General Staff Gantz: The Air Force was prepared to attack 50,000 Al-Qaeda fighters".

[103] http://morirt.com/malware/HamasUAV-Report.pdf

The email itself included a link to the Web site, ashkubit.com, and was signed by the same "Ohad Levin". Indeed, there is a writer on this site named "Ohad Levin".

As in the past, a file weighing 1.7 MB was attached to this email and the file was named "Chief of General Staff Gantz.rar".

Such attempted attacks may have been isolated with the goal of infecting the target with malware that would open the back door to attacks, or may have been part of a broader operation such as the creation of a botnet network for the purpose of DDOS attacks or the collection of data such as passwords, financial details, etc.

njRAT – Malware for Cybercrime in the Middle East

On March 31, 2014 the security company, Symantec, reported[104] that it had noticed an increase in the number of local hacker groups in the Middle East that base their activities on a known malware called njRAT, which serves as a tool enabling remote access (RAT). However, the uniqueness of this tool lies in the fact that it was developed and supported by Arabic speakers (version 0.64 of the software was uploaded to one site[105] on September 24, 2013 and to a second site on October 17,

[104] http://www.symantec.com/connect/blogs/simple-njrat-fuels-nascent-middle-east-cybercrime-scene
[105] https://hostr.co/0RYRK2uXjpuU

2013[106]). There are many videos in Arabic on YouTube that explain how to use this malware.[107]

In most cases, the software was used in order to manage computer networks for criminal activity, but according to Symantec there is evidence that several groups used the malware to attack governments in the region.

The company examined 721 examples of this malware and high level of contagions was discovered, including 542 command and control (C&C) servers as well as 24,000 computers infected worldwide. Approximately 80% of the C&C servers were located in the Middle East and North Africa, including: Saudi Arabia, Iraq, Tunisia, Egypt, Algeria, Morocco, the Palestinian Authority and Libya.

It was discovered that most of the IP addresses of those servers led to ADSL lines, indicating that most of the attackers probably used the malware from their homes in the Middle East. The report claimed that the malware has been available since 2012 and there were three versions of it, all of which can be spread through USB devices. Nevertheless, a study that was carried out on this software in the beginning of December 2013[108] determined that there were at least four versions – 0.36, 0.41, 0.64 and 0.5.0E. This publication is the continuation of in-depth research regarding the malware that was published by General Dynamics Fidelis Cybersecurity Solutions[109] on June 28, 2013.

This study provides further elaboration on the software;

- It is a Trojan Horse malware developed on VB.net.
- The name of the file is "Authorization.exe" and it is sent within a scr file.
- The software enables Keylogger camera access feature, the theft of access information stored in the browser, the upload and download of files, a desktop view, and the implementation of various changes to the victim's computer.
- The IP address used in the malware (217.66.231.245) is located within the range of Palestinian Internet Services, based in the Gaza Strip.

---

[106] http://up.dev-point.com/downloadf-07168af203491-rar.html

[107] http://www.youtube.com/watch?v=yJxp9GBxgwc
http://www.youtube.com/watch?v=Fp_MmzCQJLc
http://www.youtube.com/watch?v=yJxp9GBxgwc
http://www.youtube.com/watch?v=0N7KqvlP4tQ
http://www.youtube.com/watch?v=Lh4oDbISexI

[108] http://www.fidelissecurity.com/files/files/FTA%201010%20-%20njRAT%20The%20Saga%20Continues.pdf

[109] http://threatgeek.typepad.com/files/fta-1009---njrat-uncovered-1.pdf

- The attackers disguise the malware using various icons for malware, such as MS Word and PDF icons in certain cases.
- The malware attacks government, media and energy entities throughout the Middle East.
- The malware is distributed though phishing operations as well as through infected USB devices.
- The malware can be minimized and hidden using several tools in order avoid detection by security software.
- From the moment that the target computer is infected, the malware has the ability to scan other computers on the same network and find breaches by using, among other things, the access details that it obtained from the victim's computer.

Symantec also discovered that the software became very popular in the Middle East via a large community that provides support through guidelines and manuals for software development. In addition, it identified 487 groups that carried out attacks using this tool.

According to the company, the software was written by a resident of Kuwait who owns Twitter account "njq8",[110] which seems to have been created in the beginning of May 2013. The account contains information regarding the various versions of the software as well as an announcement from December 11, 2013 regarding the release of version[111] 0.7.d. He signed one of his announcements[112] "Nasser al-Matiri". In addition, his name was mentioned on various Arabic-language forums in the context of this software.

Gameover and Cryptolocker in the Gulf States

An article from June 5, 2014 stated[113] that, according to Symantec, the United Arab Emirates is ranked third in the world for damage caused by a virus that struck one million computers and led to the theft of tens of millions of dollars – Gameover Zeus. The virus infected between 40,000-80,000 computers in the UAE. Calculations based on data provided by Symantec revealed that 8% of all computers infected with this virus were located in the Gulf States. Experts said that this was a

[110] https://twitter.com/njq8
[111] https://twitter.com/njq8/status/411010761608007680
[112] https://twitter.com/njq8/status/365240895831941121
[113] http://www.arabianbusiness.com/up-80-000-computers-in-uae-may-have-been-hit-by-cyber-virus-targeting-bank-accounts-report-552894.html

sophisticated malware that evades detection by anti-virus software and infects the user's computer from the moment that the user opens the PDF file or clicks on the link provided in the email. From the moment it is installed on the computer, the malware has the ability to intercept financial transactions and re-write them so that the payments are routed to other accounts. Furthermore, experts claimed that the malware is also capable of masking unapproved payments so that the account page appears normal.

The malware distribution rate was highest in the United States and Italy - experiencing 13% and 12% of the cases, respectively - while 7% of the cases were found in Britain.

They also claimed that the malware is so sophisticated that it has managed to strike three times, including once this week, since it appeared in 2011. However, it continues to reinvent itself. The FBI reported that computer users have two weeks from the last strike to clean their hard drives and install new antivirus software before the malware attacks again.

It is difficult to stop the malware because it uses the P2P software, so that even if the main server is down the infected computers can still continue to communicate with one another and take action. Computers that are infected with this malware often host another malware called "Cryptolocker", which is activated when the user's financial data is not accessible to the original malware.

Cryptolocker, which requires a ransom using bitcoin from each user. According to Symantec, approximately 3% of computers infected with this malware paid the ransom rather than lose files, and that the ransom payment was the only way for them to gain access to the attacked files.

The United State Justice Department accused a Russian man named Evgeniy Mikhailovich Bogachev of leading the group responsible for this malware. It also claimed that the group had collected 100 million dollars from such ransom demands.

Computer users were instructed to update their antivirus software, change their passwords and monitor their accounts.

Phishing attempt on Israeli bank

In an message[114] posted on June 24 on a blog by Lookout, the company stated that it had discovered a bank application on Google Play designed to steal users' access details but,

[114] https://blog.lookout.com/blog/2014/06/24/bankmirage

surprisingly, not their passwords.

This application, called BankMirage, was intended for clients of Bank Mizrahi. It was claimed that the attackers packaged the original application and redistributed it disguised as the official application of the bank.

This application created a "phishing" attack; from the moment that it was installed and opened, the malware produced an entry form that was used to enter the login information of the user. However, this scam intentionally only stole usernames and not passwords. When the username was entered, a message appeared stating that entry to the system had failed and that the bank's software needed to be re-installed from Google Play. The company stated that the application was removed after Google was made aware of it.

Case Study – OpIsrael 2014

Each newsletter issued by the ICT's cyber-desk will discuss in greater detail a recent incident of cyber-attack. This issue highlights OpIsrael 2014.

In the beginning of 2013, many online sources – both individuals and groups – announced their intention to launch cyber-attacks against Israel and to "wipe it off the face of the Internet", and named the operation OpIsrael. The attacks were set to take place on April 7, 2013, a date that was selected ahead of time since it was Holocaust Remembrance Day. In the framework of preparations for the attacks, preview announcements,[115] videos,[116] and various posters[117] were published.

In mid-January 2014, online activity began to take shape for the purpose of creating a similar event to the one that took place on April 7. Just like before, the OpIsrael 2014 operation was divided into several types and directed at two main sectors, which can be summarized in the following chart;

Type of attack	Target of Attack	Scope of attack
Attacks to disable Web sites	Mostly against government Web sites	A limited number of claims. It is reasonable to assume that the

[115] http://www.middleeast-internet-monitor.com/?p=3311
[116] http://www.middleeast-internet-monitor.com/?p=3370
[117] http://www.middleeast-internet-monitor.com/?p=3125

		number of sites whose operations were actually disabled was low, if there were any at all.
Information leaks from Web sites and information systems	The government and civilian sectors	Hundreds of email addresses and passwords containing the gov.il suffix, and tens of thousands of individual email addresses from the civilian sector.
Attacks on information systems	The civilian sector	An isolated number of unproven claims, mostly regarding breaches of several computer systems.

1. It is important to note that at least some of the reports seem to have been exaggerated, not to mention other reports that were completely false, in an effort to wage psychological warfare as part of the overall campaign.
2. According to media sources, the scope of OpIsrael 2014 seemed significantly smaller, both quantitatively and qualitatively, than the previous year's operation, as was the media coverage of the operation before and during the attack.
3. There were no media reports of cyber-attacks against the infrastructure systems in Israel or against core systems that could paralyze or critically damage the functioning of the state.

Details of the events

Media preparation

In the evening hours of January 14, a Twitter message was posted[118] declaring the intention to carry out a cyber-attack against Israel, named OpIsrael, on April 7, 2014;

[118] https://twitter.com/An0nGhost/status/423195619977478144

As before, videos began to be published regarding the highly anticipated event. One of them, which was titled, "AnonGhost Launch Op Israel Birthday 07/APRIL/2014",[119] was already published at the end of December 2013 on the YouTube account of Anonxox TN[120] and was signed by;

Mauritania Attacker – Virusa Worm – Deto Beiber – Dr.SaM!M_008 – M3GAFAB – Extazy007 – PhObia_PhOneyz – Mr Domoz – Tak Dikenal – AnonxoxTN – Raka 3r00t – PirateX – Bl4ck Jorozz – Younes Lmaghribi – Indonesian r00t – BlackBase Hacker – CoderSec – h4shcr4ck – Mrlele – Donnazmi – TheGame Attacker – Man Rezpector – SaccaFrazi – Spec Tre – HusseiN98D – HolaKo - Mr.Ajword – Root Max – Egy Eagle – THE GREATEST – BiosTeRminat0r.

The video, which had over 1,700 views, claimed that a victory celebration would be held every year on April 7 and contained potential allusions to an attack against critical infrastructure, including financial systems. In addition, another video[121] was published on the same day, and while its title referred to a future event its content referred to events from 2013 despite the fact that the video transcript was different from the one that referred to 2014. At first, three events were created on Facebook for April 7, 2014; the first[122] was created by sources in Algeria and showed the most significant activity. The second[123] displayed a much smaller scope of activity. The third[124] was created by "Norwegian Ghost Cyber Attackers"[125] and, like before, included a list of Israeli government Web sites as targets for attack on this date. In addition, a hashtag for the event was

[119] http://www.youtube.com/watch?v=XvdSBX3xBHg
[120] http://www.youtube.com/user/AnonxoxTN?feature=watch
[121] http://www.youtube.com/watch?v=ylhrOviXWMc
[122] https://www.facebook.com/events/466522783453951/?fref=ts
[123] https://www.facebook.com/events/466522783453951/?fref=ts
[124] https://www.facebook.com/events/466522783453951/?fref=ts
[125] https://www.facebook.com/NorwegianGhostCyberAttackers

created on Twitter (#OpIsrael Birthday).

Despite the fact that the information was posted on Twitter, it seems that the planned activities did not receive a lot of online feedback.

On March 10, a video[126] was published on YouTube by hackers who identified themselves as "Anonymous-Arab" in which they threatened to carry out another attack against Israeli sites on April 7, 2014. The attack would be directed against "as many Israeli sites as possible", including government sites, in order "to erase Israel from the Internet".

The video included an appeal to all Muslim hackers around the world to participate in this online attack, which will be "the strongest electronic earthquake, in terms of its global scope [and its strength] of 9.5 on the Richter Scale, to strike Israel". The video combined clips that were filmed by residents of the Gaza Strip following Air Force attack in the area, as well as articles about the cyber-attacks that were previously carried out against Israel and its citizens.

The video was posted to one of the YouTube channels associated with "Anonymous".[127] The channel to which the video was uploaded began to operate in November 2013 and approximately 24 different videos have been uploaded to it so far, most of which are anti-Semitic, some from jihadist groups and organizations.

Information Leaks

Government

- In preparation for the upcoming event, and in order to maintain media interest and awareness on the matter, a list was published[128] on February 16 by "AnonGhost Team" that contained 25

[126] http://www.youtube.com/watch?v=9Z2tKFLLHkA
[127] http://www.youtube.com/user/999232F
[128] http://pastebin.com/61vpGj8W

email addresses belonging to various government entities in Israel and ending with the "gov.il" suffix. It also included what seems to be the passwords to access those email accounts.

On April 4, a list[129] was published by a Saudi hacker who called himself "SeCuRiTy_511".[130] This list contained 14 email addresses and passwords of Israel Export Institute users. Two days later, another list[131] was published by a group that called itself "Bekasi X Code",[132] which contained 27 email addresses of the institute's users. These announcements also revealed that "security_511" identifies himself as a Saudi hacker. Nevertheless, the title of his Twitter account indicated "Abu dhabi".

- On April 5, a message[133] was posted on Twitter by the same "security_511" in which he claimed to have leaked information from the Web sites of the Ministry of Education and the State Comptroller. The announcement included links to two files; one file[134] contained a list of 14 email addresses and passwords belonging to departments and entities at the Ministry of Education, and the second file[135] contained 13 email addresses and passwords belonging to entities in the State Comptroller's office (one listing included telephone numbers and the other included full names). However, an examination of the announcement revealed that they were published mush earlier; the one referring to the Ministry of Education was already published on March 22 and the one regarding the State Comptroller's office was published a week earlier.

[129] http://pastebin.com/0eH9vuMj
[130] https://twitter.com/security_511
[131] http://pastebin.com/MVZDMiVP
[132] https://www.facebook.com/groups/BekasiXCode
[133] https://twitter.com/security_511/status/452215371916128256
[134] http://pastebin.com/b0NcvGfR
[135] http://pastebin.com/EH65BhK2

- "Anonymous Ibero"[136] posted a message on Twitter[137] regarding the leak of encrypted email addresses and passwords belonging to the Israeli government. The list[138] itself included approximately 80 email addresses belonging to entities from various offices, all ending with the "gov.il" suffix. Attached to the list were the encrypted passwords.

- A message was posted claiming to have leaked telephone numbers[139] belonging to the Israeli government and referring to a file[140] containing the information. The list, which was published by AnonGhost and AnonSec, included approximately 80 mobile and landline phone numbers

[136] https://twitter.com/Ibero_Anon
[137] https://twitter.com/Ibero_Anon/status/453175265645309952
[138] http://pastebin.com/MBFgjsLS
[139] https://twitter.com/An0nGhost/status/453015872169582592
[140] http://pastebin.com/VSzHw3Mw

from Israel that they claimed were “Israeli government phone numbers”.

- A message was posted on Twitter[141] regarding the leak of 350 email addresses belonging to elements within the Israeli government, including a link to a file[142] containing information that seemed to have been taken from a database table with the following fields; user_email, user_password, user_name, user_sname, pass_recovery, validation, registration_date, registration_ip, lastvisit_date, lastvisit_ip, user_urlink, visible, active.
- A message was posted on Twitter[143] regarding the leak of 375 email addresses belonging to elements within the Israeli government. An examination of the list[144] revealed that it was the same file containing 350 email addresses (see previous announcement) to which 25 email addresses and passwords ending with the “gov.il” suffix were added.
- A message was posted on Twitter[145] regarding the leak of access details belonging to Ministry of Agriculture users. The file[146] included the user names, access passwords and email addresses of six employees at the Volcani Institute.
- A message was posted on Twitter[147] regarding the leak of 2,064 email addresses and telephone numbers belonging to elements in the Israeli government. The message included reference to a TXT file,[148] which was not available.
- A three-part publication of leaked email addresses belonging to the Ministry of Science, Technology and Space; Twitter messages regarding the first,[149] second[150] and third[151] part. Each one referred to a file containing several email addresses with the “most.gov.il” suffix as well as passwords. In some cases, the files contained names and telephone numbers as well. There was also an announcement[152] in Arabic that compiled the links to all three files.

---

[141] https://twitter.com/An0nGhost/status/453190906318184448
[142] http://pastebin.com/nqM1mD9b
[143] https://twitter.com/An0nGhost/status/453361282864144384
[144] http://pastebin.com/cf2g06ij
[145] https://twitter.com/An0nGhost/status/453561701653573632
[146] http://pastebin.com/ghavH2nH
[147] https://twitter.com/HagashTeam/status/452985075702177792
[148] http://contactocomm.net/il.txt
[149] https://twitter.com/security_511/status/452945342473199616
[150] https://twitter.com/security_511/status/452952810381127680
[151] https://twitter.com/security_511/status/452960892674916352
[152] https://twitter.com/security_511/status/453096604070068224

- A message was posted[153] on Twitter regarding the leak of email addresses belonging to the Ministry of Public Security. The message included reference to a file[154] containing eight email addresses as well as passwords. Seven of them had the "mops.gov.il" suffix and one of them had the "mop.gov.il" suffix, perhaps due a typo by the author of the message.
- A message was posted on Twitter[155] regarding the leak of email addresses belonging to the Ministry of Health. The message included reference to a file[156] containing eight email addresses ending with the "ziv.health.gov.il" suffix as well as passwords. Another message[157] included reference to a file[158] containing six additional email addresses, this time ending with the "moh.health.gov.il" suffix.
- On April 16, "security_511" posted a series of messages on Twitter in which he exposed details of Bank of Israel employees, including name, contact information, email address and access passwords; Shula Mishli,[159] Nadine Baudot-Trajtenberg,[160] Yoav Soffer,[161] Etkes Haggay,[162] and Binyamin Alon[163] (published on April 13). The names of the employees whose details were leaked were listed in the message,[164] which was published by "security_511" on April 15 and referred[165] to a list of 21 bank employees. It should be noted that a message[166] was already posted on April 9 indicating the Bank of Israel as the next target.

Civil sector

- On April 6, a message was posted[167] in which "AnonGhost Team" claimed responsibility for the

[153] https://twitter.com/security_511/status/453079983851048961
[154] http://pastebin.com/BZkAegrL
[155] https://twitter.com/security_511/status/453237247291441152
[156] http://pastebin.com/NNZG7qhF
[157] https://twitter.com/security_511/status/452981705805414400
[158] http://pastebin.com/en4PUtq1
[159] https://twitter.com/security_511/status/456520657409306624
[160] https://twitter.com/security_511/status/456387368249876480
[161] https://twitter.com/security_511/status/456387188939173888
[162] https://twitter.com/security_511/status/456386717306474496
[163] https://twitter.com/security_511/status/455293922877923328
[164] https://twitter.com/security_511/status/456297366358728704
[165] http://pastebin.com/9H3fVFVc
[166] https://twitter.com/An0nGhost/status/453658216409616384
[167] http://pastebin.com/MYARx01X

breach of the Web site belonging to the Interreligious Coordinating Council in Israel[168] in the framework of the #OpisraelBirthday campaign. The message described the leak of the site's database including the following fields: address, cell_phone, city, country, email, first_name, funds, home_phone, id, ilcontact, last_name, password, postal, state title, userhash, userlevel. This list included approximately 850 records of entities, most of which were from the United States and some from Israel, Britain and Canada.

- Another list[169] from the same date was published by "AnonSec" and apparently included "1381 EMAILS AND PASSWORD LEAKED". In actuality, the list contained 1,380 records, including some duplicates, of email addresses. Some of the email addresses had a ".il" ending, some were based on the username because the users seemed to be Israeli, and others did not seem to have a clear link to Israel based on the email address. Listed next to the email addresses were passwords, dozens of which were ".aabbccdd". As before, it seems that these access passwords were fake and were created automatically by the hackers, or that they were access passwords to the site that was hacked. Based on past experience, it is very likely that these were not the passwords to the email addresses themselves.
- Another message[170] from "AnonGhost"[171] claimed to have published a list containing 1,350 email addresses belonging to Israelis. This list had the same characteristics as the one described above.
- A message[172] was posted on Twitter on April 7, claiming to have leaked 25,000 email addresses belonging to Israelis. It referred to a file[173] that included an unavailable TXT file[174] and claimed that the email addresses were taken from the Web sites, http://www.toyota.co.il and http://www.jeep.co.il.
- A message[175] was posted on Twitter regarding the leak of 1,143 email addresses belonging to

[168] http://icci.org.il
[169] http://pastebin.com/nrMS691B
[170] https://twitter.com/An0nGhost/status/453015326444486656
[171] https://twitter.com/An0nGhost
[172] https://twitter.com/An0nGhost/status/452982606406385664
[173] http://pastebin.com/B5eGXva3
[174] http://opisraelbirthday.com/leaks/25,000%20EMAILS%20AND%20PASSES%20LEAKED.txt
[175] https://twitter.com/An0nGhost/status/453556018904305664

Israelis. The source of the file[176] itself seemed to be a table copied from the hacked database.

- A message[177] was posted on Twitter, claiming to have hacked into one million Facebook accounts belonging to Israelis, but it did not provide a link.
- A message[178] was posted on Twitter, with reference to a TXT file[179] containing a long list of Israeli Web sites that were allegedly hacked, some via a breach of the host server.
- A message[180] was posted on Twitter regarding the leak of 6,766 email addresses belonging to Israelis. The link directed users to a page[181] titled "HusseiN98D" and contained a summary of "AnonGhost's activity between February 16, 2014 and April 21, 2014, which included four parts of a file regarding the 6,766 email addresses.
- A message[182] was posted on Twitter regarding the leak of email addresses and passwords from the "Haaretz" newspaper. The file[183] itself included eight email addresses ending with the "haaretz.co.il" suffix, as well as passwords.
- A message[184] was posted on Twitter regarding the leak of email addresses belonging to the electric company. The message included reference to a file[185] containing nine email addresses ending with the "iec.co.il" suffix as well as passwords.
- A message[186] was posted on Twitter with reference to two files; the first file[187] claimed to contain a list of 8,227 email addresses belonging to Israelis. In actuality, the file contained approximately 6,400 email addresses, most of which belonged to Israelis, including eight with a "gov.il" suffix. The attached passwords were encrypted. The second file[188] apparently included 8,227 records (at the most recent count) but many were missing or omitted. It is possible that there was duplication between the two lists.

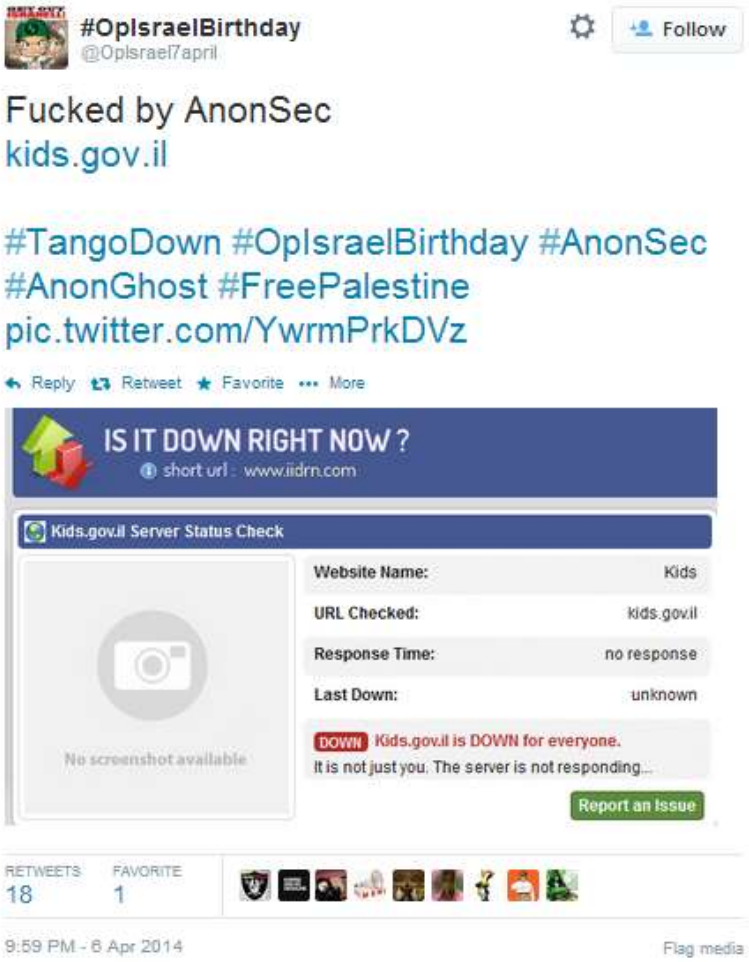
---

[176] http://pastebin.com/dfjCY4BB
[177] https://twitter.com/An0nGhost/status/453353393005010946
[178] https://twitter.com/An0nGhost/status/453202384584716289
[179] http://anonsechackers.us/OpIsraelBirthday/defaces.txt
[180] https://twitter.com/An0nGhost/status/453224549396795392
[181] http://pastebin.com/u/HusseiN98D
[182] https://twitter.com/security_511/status/452993922172989441
[183] http://pastebin.com/uAkMafu7
[184] https://twitter.com/security_511/status/452969901800849408
[185] http://pastebin.com/MhsvFtvc
[186] https://twitter.com/security_511/status/453093053780467712
[187] https://www.quickleak.org/3c1Zxbxp
[188] http://forextalks.ru/f/x.txt

Web site attacks

Government

- A message[189] was posted on Twitter, claiming to have brought down the Web site "On Top: Mimshal Zamin[190] for Kids";[191]



- On April 7, a message[192] was posted on Twitter containing instructions for attacking Israeli government Web sites. The message directed the user to select a Web site address of a

[189] https://twitter.com/OpIsrael7april/status/452883403835068416/photo/1
[190] Mimshal Zamin is the name of the Israeli eGovernment project.
[191] http://kids.gov.il
[192] https://twitter.com/MissOpTurkey/status/453089432682655744

government office from a page listing these addresses[193] (the list was dated February 23, 2013) and to paste another link to the page in order to carry out a DDoS attack.[194]

- A short while later, a message[195] was posted on Twitter claiming to have brought down the Web site of the Presidential Residence. In actuality, the Web address that was given

[193] http://justpaste.it/IsraelGovSites
[194] http://pastehtml.com/view/ct6qaqwp6.html
[195] https://twitter.com/AnonyInfo/status/453091597899399170

(http://president.gov.il) still does not lead to this site[196] so it seems that it is an inactive address and there is likely no truth to the claim that the site was brought down.

- Another message claimed[197] to have hacked into the government Web site of the "Volcanic Institute"[198] in the framework of AnonGhost's attacks on government Web sites.
- Messages were posted claiming to have brought down the Web sites of the Broadcasting Authority,[199] the Ministry of Economy,[200] the Ministry of Defense,[201] the Ministry of Education,[202] the Ministry of Foreign Affairs and the Prime Minister's Office,[203] the Mossad[204] and the Judicial Authority.[205]

The Civil Sector

- A message was posted claiming[206] to have brought down a list of 30 Israeli Web sites using a DDoS attack, posting the hashtag, #OpIsraelBirthday, at the top of the message.

[196] http://www.president.gov.il/Pages/Default.aspx
[197] https://twitter.com/An0nGhost/status/452995747055951872
[198] http://www.agri.gov.il
[199] https://twitter.com/security_511/status/453277398705127424
[200] https://twitter.com/security_511/status/453253688484978688
[201] https://twitter.com/security_511/status/453083155546013697
[202] https://twitter.com/security_511/status/453091853496115200
[203] https://twitter.com/PalestinianMiss/status/453182898984976384
[204] https://twitter.com/PalAnonymous/status/452951920454688768
[205] https://twitter.com/MissOpTurkey/status/452952969651449856
[206] http://pastebin.com/AKKUQaxi

- A message[207] was posted regarding the breach of 478 Israeli Web sites, with reference to a list[208] of the sites that were allegedly hacked in this campaign. An examination of samples from the list revealed that they were small businesses whose Web sites were created by "interclick",[209] based on the WordPress platform.
- A message[210] was posted on Twitter regarding the vandalism of over 2,000 Israeli Web sites. An examination of the list[211] revealed that it was only composed of several hundred Israeli Web sites belonging to small businesses.

Computer Systems

- On March 24, two messages were posted on the Twitter account of the Tunisian hackers, "XhàckerTN",[212] both of which lacked links or any proof to validate the claim. The first message[213] claimed that 4,890 Israeli computers had been infected with a Trojan Horse by the group;

[207] https://twitter.com/An0nGhost/status/452989434724876288
[208] http://pastebin.com/YC4SwFKH
[209] http://www.interclick.co.il
[210] https://twitter.com/An0nGhost/status/453367609405476864
[211] http://pastebin.com/iixvsGHX
[212] https://twitter.com/XhckerTN
[213] https://twitter.com/XhckerTN/status/448084775929397248

And the second message[214] claimed that 101 databases ending with the "il" suffix had been leaked.

The message also included a reference[215] to the Facebook[216] page of this group, dedicated to the cyber-attack against Israel on April 7.

- A message[217] was posted on Twitter with reference[218] to another message claiming to have leaked the access details of 43,000 routers and modems in the framework of this campaign. The latest one included a link[219] to a TXT file.

[214] https://twitter.com/XhckerTN/status/448216693383639041
[215] https://twitter.com/XhckerTN/status/448436975406972928
[216] https://www.facebook.com/xhackertnofficiel/posts/1415118955414393
[217] https://twitter.com/An0nGhost/status/452985041254354944
[218] http://pastebin.com/Najw77sn
[219] http://opisraelbirthday.com/leaks/43.000%20THOUSAND%20ISRAELI%20IP'S,ROUTERS,MODEMS%20SNIFFED%20BY%20THE%20GREATEST.txt

- On April 9, a message[220] was posted on Twitter claiming to have hacked into the routers of the Linux system;

[220] https://twitter.com/An0nGhost/status/453982564273750017/photo/1

Israeli Response

In response to the actions taken in the framework of this campaign, Israeli hackers carried out several attacks against targets throughout the Middle East and the Muslim world. For instance, on April 6 the Israeli Elite Force[221] published an announcement[222] on its Facebook page regarding the

[221] https://www.facebook.com/IsraeliElite/posts/455378641261917

vandalism of 111 Web sites from Indonesia as well as several other events.

Continued Operation?

On April 16, a message[223] was posted on Twitter by "AnonGhost" indicating that they were planning another attack against Israel for June 7. Despite the fact that the message was dated April 16, 2014 the date of the planned operation was noted as June 7, 2013. This may have been due to a clerical error. The message[224] was re-tweeted throughout Twitter.

The message referenced the Web site, http://opisraelbirthday.com, which does not exist at the present time.

Guest Contributor – The Quiet War[225]

We are at war.

Of course, there are no maneuvering divisions or fighter plane squadrons battling in the air to

---

[222] https://www.facebook.com/IsraeliElite/posts/455378641261917
[223] https://twitter.com/An0nGhost/status/456319635785129984
[224] https://twitter.com/AN0N_AL_AQSA/status/459074041358585856
[225] This article was written by Elad Shapira, a mobile security researcher at AVG, who holds a BSc in computer science from Herzliya Interdisciplinary Center.

testify to this, but we are at war.

A quiet war. A cyber-war.

The IDF, like other advanced armies, added the cyber arena to the four traditional arenas of warfare: sea, air, land and space.

The following are several important points regarding warfare in the cyber-arena.

Technological advancement on the one hand and vulnerability on the other hand

The more computerized and advanced a country becomes, the more vulnerable it is to cyber-attacks directed against its infrastructure, and the more dependent a country is on computerized systems and technological infrastructure, the greater the potential for damage.

After all, a country that is already "third world" cannot be shifted to be "third world", as the country is not developed enough to have advanced technology system and infrastructures.

A country that is not developed has far less to lose in this type of digital conflict.

Israel, specifically, faces an even greater problem since its civilian infrastructure also serves its military infrastructure, making it more vulnerable. The following are examples of the consequences of an attack on various critical infrastructures:

- Water infrastructure – Damage to the water quality would also harm the quality of drinking water consumed by the army. Scenarios can also be imaged in which floods could paralyze populated areas or the movement of army forces.
- Electrical infrastructure – Generators and other solutions would not manage to keep all of the army's electrical infrastructure operating over a long period of time. Military and technological systems, such as military command networks and military command and control systems, require electricity and connectivity between many entities in order to operate, and the systems would cease to operate in their absence – causing the IDF to lose its qualitative advantage on the battlefield.
- Gas infrastructure – An attack on the gas infrastructure would lead to the incineration of every area that houses a gas facility, and would cause damage on a scale that neither bombs nor ballistic missiles could achieve. Incidentally, this is one of the reasons that Israel stations its gas facilities in the sea and not on the shore, since an attack on one facility would only cause damage to the facility itself, and not strike a double blow to both the facility and civilians.

- Traffic control infrastructure – Damage to traffic control infrastructure could cause huge traffic jams (that not even Waze could help with) and delay the arrival of reserve forces on their way to the front, and the IDF bases its military doctrine on, among other things, the arrival of reserve forces during a conflict.

  In this instance, damage would also be caused to railway traffic, which could prevent the movement of civilians and soldiers by train.
- Telephone and cell phone company infrastructure – The IDF uses "Mountain Rose" (a mobile communications network encrypted for use by the IDF) but we know that soldiers often use cell phones to contact their families (and how could one possibly go several hours without checking Facebook statuses?) and to trade information with one another. Therefore, damage to the telephone and cell phone companies that provide personal communications services, inter alia, for military purposes has the potential to cause great harm.
- Communications infrastructure – Should the ability of the state and its government to communicate with its citizens using various forms of media, such as television, radio and Internet sites, be breached and compromised, the public would be cut off from updated information, would not know how to act, and would be subject to manipulation, disinformation and propaganda on the part of the enemy.
- Financial infrastructure, funds and banks – The paralysis and disabling of the economic system caused by a breach of the banks (which would no doubt please some bank customers) or the Israeli Stock Exchange could lead to a shutdown of the Israeli economy due to its dependence on financial stability.

Attacks on the state's critical infrastructure could disrupt and paralyze the day-to-day life of each and every citizen, anywhere and at any time. Therefore, the protection of this infrstaructure through the development of offensive capabilities is a national necessity.

Identifying a state of war during a digital conflict

As the title indicates, it is a "quiet war".

The borders are blurred and many questions arise:

- How do we define when a digital conflict begins?
- When does escalation occur?

- When is it an all-out war, and when is there a cause for war, a counter-attack or a preventative attack?
- An attack on which targets would lead to an escalation and confrontation?
- Was an offensive action carried out in order to wage an attack or to collect intelligence?
- Is the technological infrastructure being attacked as a target in and of itself or as a means of attacking another target?

In the event that only one government site is breached and an individual electric company facility is attacked, leading to a electrical blackout only in Ohio (we have no problem with Ohio) – does it constitute a declaration of war by the enemy? Does it constitute a preliminary step before actual war? Were they only trying to "test the waters" before the imminent attacks? Is there a more interesting target than Ohio (again, we have no problem with Ohio), which was only attacked in order to see if a later strike on a different target would be successful?

Use of the cyber-dimension provides an advantage during the period between standard wars, especially in order to obtain intelligence information ahead of the next conflict or in order to sabotage the capabilities of the other side during the next conflict.

It should be noted that the defensive side does not want to react to each and every digital attack so as not to reveal its offensive capabilities in the digital arena and possibly impede a future advantage.

The identity of the players and their professional capabilities

In the digital chess game, it is difficult to determine who the players are and what capabilities they have in this arena.

- Is it a single, highly skilled hacker?
- Is it a group of hackers?
- Are they based in one country or many countries?
- What is the hacker's level of professional knowledge?
- What is he trying to achieve?
- Does he have the motivation and ability to carry out the attack?

Cyber warfare is one of the clearest cases of asymmetric warfare, in which a lone individual or small group of people can cause damage at a national level, making it an interest of terrorist

organizations, such as Hezbollah and others, to develop offensive capabilities in the cyber-arena.

The use of the Internet infrastructure to carry out attacks can impede efforts to discover who is responsible for an attack. Skilled hackers can disguise their activity anonymously or hide and incriminate others.

As a result, a hacker can cause damage and not be punished for it since he cannot be incriminated with certainty.

An easy life for the offense – a lot of grief for the defense

In cyberspace, as in football, the offense receives much more credit or, in this case, enjoys an easier life.

What will be remembered is not the striker's misses but rather his accidental block that allows his team to score a goal.

A sentence that I personally like and that best describes the idea behind cyber-attacks is: "99.99% protected is 100% hacked" – the attacker needs to only find one weakness or problem to allow him to carry out a successful attack, whereas the defense must work hard to remain protected all of the time.

The attacker has a built-in advantage because of the open way in which information flows freely on the Internet and new technologies are always being developed.

Agenda

The hacker may have many agendas behind his desire to carry out a cyber-attack, including:

- States - In order to declare an enemy in the cyber dimension, in addition to the sea, air, land and space dimensions.
- Financial profit – For example, criminal organizations that want to make money from unsuspecting users or companies in various ways (including extortion, credit information theft, forgery, sending advertisements, and sending text messages from cell phones to premium numbers).
- Political – To promote public awareness in favour of a political idea.
- Social – For example, the announcement of a breach that enables the community to play a computer game for free or an attack against a food company that raised the price of cottage

cheese.

No geographic restriction

There are no traditional geographic restrictions in cyberspace that could influence fighting technique like topographical terrain conditions or weather.

An attack can be carried out quickly against other entities even at a great physical distance.

In the specific case of Israel, the lack of this restriction provides others with the ability to wage this type of warfare not only from neighboring countries, as is the case in standard warfare.

There is also no need for attackers to endanger their lives and they are able to repeat their attempts without fear of possible injury.

It is also difficult to obtain intelligence warnings about a future attack (unless the attackers boast and try to make arrangements on various social networks in order to bolster their power, or if they do so openly) since there are no satellite photos that can be used in order to identify the movement of forces, like in a regular war, and due to the fact that offensive capabilities are usually developed by small teams or groups.

Legality

This section is intended for those of you debating whether or not it is possible to learn about cyberspace and perhaps even engage in this area during your military service, and whether or not "hacking is legal".

I always define knowledge in the field of cyberspace as "stabbing" since a hacker, as I understand it, is someone who knows how to use a knife.

A knife has many uses – one can use it to cut a salad or to stab another person.

Like a firearm, like a gun, it can be used to protect or to attack.

A person's values, education, ethics and goal are what determine how he uses the power in his possession.

It is important to note that someone can study and train in the field of cyberspace legally without causing malicious damage by using dedicated sites or software that simulates targets.

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

Dr. Michael Barak, Team Research Manager, ICT

Nir Tordjman, Team Research Manager, ICT

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.