IDC HERZLIYA

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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 10

July – September 2014

Highlights

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

The following are among the issues covered in this report:

- Documentation of training videos and written tutorials on the topics on cyber-security and protection. The discourse concerned intelligence efforts to identify cyber-criminals online and included explanations on how to surf the Web anonymously using various software programs and techniques.
- A group of hackers called the "Islamic State Electronic Battalions" claimed responsibility for the breach of Twitter accounts belonging to "White Shroud", an organization that operates against the Islamic State in Syria-Iraq.
- During Operation 'Protective Edge' there was an increase in attempted cyber-attacks against Israeli targets in the framework of the OpIsrael and OpSaveGaza operations, including a breach of the IDF spokesperson's Twitter account and a fictitious announcement regarding a feared nuclear leak in the Dimona area.
- There was an increase of cases in which the details of millions of credit cards used at retail chains throughout the United States were leaked, from the start of 2013 and throughout 2014, which caused lasting economic damage.
- There was an increase on the usage of darknet-based malware in an effort to increase the anonymity of the user in carrying out an attack. The malware, which uses TOR and I2P, encrypts data traffic between the attacked computer and the control and command server.

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, July – September 2014[1]

Al-Qaeda Leadership

To mark the anniversary of the September 11 terrorist attacks, the spokesman for Al-Qaeda, Hussam Abdul Rauf, attacked the fraudulent propaganda campaign being waged against Al-Qaeda and its leader, Sheikh Ayman al-Zawahiri. According to him, contrary to the claims of critics, the organization continues to hold power, maintains effective control over its branches and is even expanding into new arenas of jihad. According to him, the local governments continue to oppress their citizens and any expression of civil disobedience. In light of this, Abdul Rauf called on Muslims to oppose the local governments.

Adam Gadahn, a senior Al-Qaeda operative, also criticized the regimes in Muslim states, especially the Pakistani government, and accused them of collaborating with the West. Gadahn encouraged Muslims in Pakistan to attack American targets and diplomatic targets in Pakistani territory until the Americans are expelled from Pakistan, and in order to facilitate the fall of the Pakistani government.

In addition, Al-Qaeda addressed the family of American captive, Warren Weinstein, to put pressure on the American government to meet the organization's demands in exchange for his release.

[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

According to the organization, the American government is not interested in a deal and even seeks Weinstein's death and, therefore, it is not holding any negotiations for his release.

The Establishment of a New Branch of Al-Qaeda in the Indian Subcontinent

In the beginning of September, the Al-Qaeda leadership announced the establishment of a new branch called "Al-Qaeda in the Indian Subcontinent" (AQISC). The announcement received supportive reactions in the jihadist discourse, and was a sign of the effort being made to expand Al-Qaeda's activities in this arena as well. It was also announced around the same time, at the end of September, that a Pakistani warship had been attacked in Karachi. Although details about the incident were not published, the Al-Qaeda leadership rushed to claim responsibility for the attack, and released details about its targets and the manner in which it was carried out.

The Islamic State

The Establishment of the Islamic State

In the beginning of July 2014, Sheikh Abu Bakr al-Baghdadi, leader of the Islamic State, announced the establishment of an Islamic State, led by him. The announcement sparked a heated discourse among jihadists and mixed feelings during the months of July-September. On the one hand, many jihadists, including local commanders in various locations, such as Jama'at al-Tawhid wal-Jihad in West Africa, expressed support and swore allegiance to the caliphate. On the other hand, jihadists and proponents of the Salafi-jihadist movement, such as Sheikh Abu Muhammad al-Maqdisi (a senior operative in the Salafi-jihadist movement in Jordan), sharply criticized the establishment of the caliphate, claiming that it was not legal since it does not represent the entire Muslim Nation and did not receive a wide consensus. Against the backdrop of this development, several jihadist organizations, including Al-Qaeda in the Islamic Maghreb (AQIM), renewed their oath to Sheikh Ayman al-Zawahiri, the leader of Al-Qaeda.

Responses in the Jihadist Discourse to the Coalition against the Islamic State

The coalition led by the United States against the Islamic State intensified the discourse among jihadists against Western countries. This trend was especially notable in videos in which Western captives, including the American Jewish journalist, Steven Sotloff, appealed to the United States

and Britain to rescind their intention to attack the Islamic State in Iraq and Syria or else Western citizens being held captive by the organization will pay the price. All of those Western captives were later beheaded.

In addition, many jihadist supporters and opponents of the Islamic State expressed solidarity with the organization in light of the coalition's intent to attack the organization. For example, AQAP and AQIM called on Muslims around the world to help their brothers, the mujahideen, fight against coalition forces. The Al-Nusra Front in Syria also criticized Western attacks against Al-Nusra Front sites, which led to the deaths of several of its members as well as innocent civilians, and it accused Arab regimes of collaborating with the West.

Al-Shabab Al-Mujahideen

During the afore-mentioned period, jihadists – mainly those from Al-Shabab Al-Mujahideen, Al-Qaeda's affiliate in Somalia - focused on the death of Sheikh Mokhtar Abu-Zubayr, the leader of Al-Shabab who was killed in the beginning of September 2014. In response to his death, the organization called on Muslims in Somalia to fulfill their obligation and resist the campaign of aggression being waged by Christians against Muslim countries. The organization emphasized that jihad in Somalia would continue even after Abu-Zubayr's death.

Operation 'Protective Edge' in the jihadist discourse

Operation 'Protective Edge' and the battle in the Gaza Strip occupied a significant part of the jihadist discourse during this period. Many jihadists expressed solidarity with the Palestinians' struggle against Israel and called for more terrorist attacks against Israel. Sheikh Abu Dujana al-Basha, a senior Al-Qaeda operative, emphasized that the mujahideen have not stopped striving for the liberation of Palestine. AQAP also expressed its support for the Palestinians, dedicated a special publication to the Palestinians in English titled, "Palestine", and emphasized that the fight against the United States, its allies and infidel Muslim countries, such as Saudi Arabia and Egypt, is a prerequisite to the liberation of Palestine.

Al-Qaeda in the Arabian Peninsula (AQAP)

The months of July-September 2014 saw a significant increase in the scope of propaganda and

operational activities by AQAP against the Yemeni government in light of the war being waged against the organization by the Yemeni army. For example, the organization claimed responsibility for an attack on a military base for drones in the city of Seiyun and for a series of attacks on Yemeni security forces, especially in Hadhramaut Province.

Jihadist Propaganda

- The Islamic State published a computer game titled, "The Sound of Swords", which simulates combat between members of the organization and coalition forces that are attacking IS strongholds. The game is designed to boost the morale of the mujahideen and to sow terror in the hearts of those who oppose the organization. In a video that was distributed to promote the game, words of warning are issued to the West and scenes from the game are shown, including weapons training. The game is somewhat reminiscent of the game, Grand Theft Auto 5; it begins with a battle against the Iraqi army and later against American forces.[2]

Scenes from the game "The Sound of Swords"

- On September 12, it was reported[3] on the Web site of the Anti-Defamation League (ADL) that Hezbollah's television application, Al-Manar, had been posted for the third time but it was removed the day after the report was posted light of the ADL's petition to Google. The previous week, Al-Manar had launched an Android application in the Google Play store through which one could gain access to the contents of the station's broadcasts. The application was posted on the station's Web site and users were asked to install it in order to receive content and news, as well as warnings. The announcement stated that this was the third time that Hezbollah had

[2] https://www.youtube.com/watch?v=QhbX0Kt9s_I
[3] http://blog.adl.org/international/hezbollah-android-app-al-manar

posted this application. The application was first posted in July 2012 and removed[4] a short while later by Google and Apple in light of the ADL's petition.[5] In August 2012, the ADL reported[6] another attempt to post the application for Apple users using "alternative methods", while accusing the ADL of creating a campaign to have the application removed. At the end of March 2014, Hezbollah posted an application enabling access to the station's news for users of both companies. It also stated that in January 2015, Hezbollah began sending messages containing news for subscribers via the WhatsApp application.[7]

Defensive Tactics

- A prominent visitor to the Al-Minbar jihadist Web forum published on the forum's technical department a guidebook to maintaining security while using the social network, Twitter. The guidebook included 12 tips, including the use of an encrypted connection beginning with 'https' and the use of the TOR browser.[8]
- A prominent visitor to the Al-Minbar jihadist Web forum published a guidebook titled, "How to protect yourself from surveillance and detection on the Internet". Among other things, the guidebook explained how to prevent the Gmail email service from recording a user's IP address and even explained how to use the TOR browser.[9]
- A visitor to the Al-Minbar jihadist Web forum with technical experience published an announcement regarding a breach of Facebook, Twitter and Instagram accounts. In the announcement, the author warned against false reports about software for hacking into these sites and emphasized that there was no such software that allows one to hack into these social networks; any such report is an attempt to get the user to download malicious software.[10]
- A prominent visitor to the Al-Minbar jihadist Web forum published an announcement titled, "Practical steps in response to the closure of Twitter accounts belonging to Islamic State

[4] http://www.cnet.com/news/apple-google-remove-hezbollah-tv-app/
[5] http://blog.adl.org/extremism/hezbollah-on-your-iphone-theres-an-app-for-that
[6] http://blog.adl.org/extremism/hezbollah-itunes-googleapps-blame-adl-for
[7] http://blog.adl.org/extremism/whatsapp-hezbollah
[8] http://alplatformmedia.com/vb/showthread.php?t=58688
[9] http://alplatformmedia.com/vb/showthread.php?t=56332
[10] http://alplatformmedia.com/vb/showthread.php?t=55968

supporters". The announcement included several recommendations for courses of action after Twitter management shut down accounts tied to the Islamic State: turn to other social networks, use an alternative site instead of YouTube, create a private server for the distribution of IS publications, hack into television stations, and find alternatives to the file storage site JustPaste.it.[11]

- A prominent visitor to the Al-Minbar jihadist Web forum published on its technical department a YouTube video explaining how to restore suspended Twitter accounts. The publication came against the backdrop of growing discourse among jihadists regarding the fact that Twitter accounts affiliated with jihadist organizations, especially the Islamic State, had been quickly suspended by Twitter management; visitors to the forum complained about this phenomenon and sought alternatives and potential solutions.[12]
- The administrator of the Al-Minbar jihadist Web forum published an announcement regarding securing information while publishing on the Internet. The announcement stated that the Crusader alliance against the IS was trying to gather as much information as possible about the organization, especially about its field commanders; therefore, the forum administrator warned visitors to the forum against hastily publishing information that could harm the Islamic State and information concerning topics that should not be published.[13]

Offensive Tactics

- A group of hackers called the "Islamic State Electronic Battalions" claimed responsibility for the breach of Twitter accounts belonging to "White Shroud", an organization that operates against the Islamic State in Syria and Iraq. The breach took place at the end of July 2014.[14]

[11] http://alplatformmedia.com/vb/showthread.php?t=60713
[12] http://alplatformmedia.com/vb/showthread.php?t=62949; http://www.youtube.com/watch?v=QjnpOruJj5M
[13] http://alplatformmedia.com/vb/showthread.php?t=63820
[14] https://twitter.com/SawaTblanc/status/492341492602896384; https://www.youtube.com/watch?v=dMQWqR82zTw

From left to right: A video documenting the breach of several Twitter accounts belonging to the "White Shroud" organization; the banner that appeared on the organization's Twitter account

- During Operation 'Protective Edge', there was a significant increase in the number of attempts to hack into Israeli Web sites. These attempts were coordinated under various hashtags, including #OpSaveGaza, in which various hacker groups, including "Anonymous", took part.

- The Tunisian hacker group, "Fallaga Team", claimed responsibility for the breach of several Israeli Web sites, including the Facebook accounts of Israeli civilians, the Web site of the Israeli stock market and the Bereishit Institute for Jewish Studies.[15] The Fallaga Team even published a video in which it expressed solidarity with the residents of the Gaza Strip and threatened the State of Israel that it would attack its sites in cyberspace.[16] To this end, the group created a Facebook page offering lessons on how to hack into Israeli Web sites, at the following address: https://www.facebook.com/groups/op.israel.by.fallaga.

[15] https://www.facebook.com/Fallaga.Tn
[16] https://www.youtube.com/watch?v=QEHyrz4yE5Y

- Another hacker group called, "Anon Ghost Team", led by a Muslim of Mauritanian descent, also announced a wide-scale cyber-attack against Israel on July 3, 2014. This announcement was also published with the hashtag #OpSaveGaza on social networks and on a YouTube video.[17]

Guiding

- A supervisor of the Al-Fida jihadist Web forum, known as Abu Jihad al-Muhandis, published a guidebook, translated into Arabic, regarding the Linux Command Line (564 pp.). The guidebook was originally written by William E. Shotts, Jr. and was first published in 2013. According to the supervisor, the book deals with technical issues concerning the operation of the Linux operating system, including Shell, Terminal Emulator, Expansion, Redirect, Permissions, Shell Scripting, and more.[18]

[17] https://www.youtube.com/watch?v=p1IDi9sG81s
[18] http://alfidaa.info/vb/showthread.php?t=101568

The banner of the translated book

- The Al-Hussam jihadist media institution, which is affiliated with the Islamic State, published a guidebook for jihadists on how to avoid surveillance of their cell phones and Internet activity by intelligence officials when uploading and saving jihadist multimedia files. The guidebook stated that the increasing amount of jihadist propaganda materials being published by official and unofficial jihadist media institutions requires increased awareness of significant security breaches, which allow the enemy to more easily identify and locate jihadists. According to the guidebook, such a breach occurs by decoding the metadata (i.e. information about the item). In other words, there have been a number of instances in which data stored in various locations could be traced. According to the media institution, this security breach applied to photos, videos Word files and PDF files, "but photos and videos are the most at risk". In light of this, the media institution recommended a solution on how to remove the metadata. In addition, the guidebook noted that it is better for jihadists to refrain from mentioning their name or location in order to make the work of the intelligence agencies more difficult. [19]

[19] http://justpaste.it/h0t5

The banners of the above-mentioned guidebook

- The Islamic State published a collection of guidebooks on hacking into Web sites, and safe and secure surfing on the Internet. These guidebooks were collected under the name, "The Archives of a Technology Expert", and included:[20]

The banner of "The Archives of a Technology Expert"

  - A guidebook on how to avoid having one's movements tracked on the Internet. The

[20] http://justpaste.it/s3cur1ty11

guidebook recommended using the Privacy Badger software in order to achieve this goal; a plug-in for Chrome and Firefox browsers that hides the users Web activities.[21]

Privacy Badger

- An explanation on how to install and use software for secure browsing on iPhone and iPad devices: SurfEasy VPN.[22]

- An explanation regarding use of the sharing site, vk.com.[23]

[21] http://justpaste.it/gzwe
[22] https://justpaste.it/gvfr
[23] http://justpaste.it/gtal

- An explanation regarding how to use the VPN application on Android in order to change the IP and surf the Web securely.[24]
- A guidebook that suggests seven ways to securely browse the Internet and protect identifying information. For example, the guidebook emphasized that one should not click on unfamiliar links sent to one's email or cell phone. Another tip was to use anti-spyware software such as Anti-Spywar.[25]
- A guidebook on how to post to social networks such as Twitter, and how to open email accounts on sites such as Yahoo, Hotmail and Gmail. [26]

An excerpt from the explanation on how to open a Yahoo email account

[24] http://justpaste.it/gr1h
[25] http://justpaste.it/gyo0
[26] http://justpaste.it/gobt

- An explanation on how to solve the technical problem posed by the message, "the application is not available in your country". The guidebook recommended using the Psiphon 3 software.[27]
- An explanation on how to obtain a fake US telephone number in order to overcome a technical barrier when registering to the social network, Facebook. According Facebook requirements, a telephone number is required in order to complete registration to the social network in order to verify that it is not a fictitious registration. According to the guidebook, this obstacle can be overcome by using the application, textPlus Free Text + Calls.[28]

- An explanation on how to hide files on a Nokia cell phone.[29]
- An explanation on how to download a video file from Facebook to an Android device.[30]
- An explanation on how to protect an Android device from viruses and hacks. The guidebook recommended installing anti-virus software from a reliable source only, such as Google Play. Among the recommended software: Mobile Security, NQ Mobile 360 Security, avast! Mobile Security, AVG AntiVirus, ESET, Malwarebytes Anti-Malware, Norton Security antivirus, and Kaspersky Internet Security.[31]

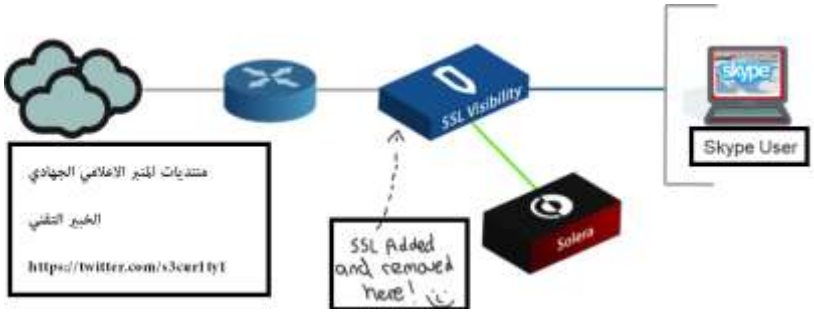
[27] https://justpaste.it/gvf1
[28] http://justpaste.it/gsfm
[29] http://justpaste.it/gino
[30] http://justpaste.it/gmmg
[31] http://justpaste.it/gl92

- An explanation on how to restore a Twitter account that was hacked.[32]
- An explanation on how to install the bitdefender Traffic Light software on a Twitter or Facebook account in order to detect fraudulent links or pages could lead to pages with viruses. [33]
- An explanation on how to send anonymous messages from a fictitious email account. According to the writer, the following sites serve this purpose: http://deadfake.com/Send.aspx ,http://www.5ymail.com ,http://www.anonymailer.net ,https://www.silentsender.com.[34]
- An explanation on how to use the Wondershare SafeEraser application, which is designed to permanently delete files on iPhone or Android devices (Galaxy).[35]

- A detailed explanation on why the use of the chat software, Skype (messages, audio and video), is not recommended as it is able to identify users and spy on them. According to the writer, there is other char software, such as ZRTP and OTR, which are must more secure.[36]
- A recommendation regarding sites that can provide a temporary number to enter when

[32] http://justpaste.it/gkb4
[33] http://justpaste.it/ghd6
[34] http://justpaste.it/gh10
[35] http://justpaste.it/geha
[36] http://justpaste.it/gdt3

registering on social networks, such as: http://sms-verification.com, http://www.receivesmsonline.net, http://receive-sms.com.[37]



- A visitor to the Al-Fida jihadist Web forum published a detailed and illustrated explanation on how to upload jihadist materials to the site, Archive.[38]
- On July 12, at least two messages were posted on Twitter[39] explaining to users how to carry out DDoS attacks, as well as an explanation about entering the required values in the Web pages dedicated to creating these attacks.
- A visitor to the Al-Minbar Al-Alami Al-Jihadi Web forum published a guidebook describing ways to hide from the Crusader alliance while surfing the Internet. Among the topics explained in the guidebook: use of the CyberGhost software to connect via VPN; changing the DNS using various services; and network card configuration to make it more secure.[40]
- A visitor identified with the Islamic State posted a detailed guidebook to Twitter titled, "The Mujahid's Electronic Suitcase", which was composed of three parts: secure browsing, intrusion detection, spyware software and a guide on hacking into Web sites.[41]

[37] http://justpaste.it/gc1m
[38] http://alfidaa.info/vb/showthread.php?t=102128
[39] https://twitter.com/_FC3O/status/487725065258037248; https://twitter.com/ddos_attacker/status/488006512871489536
[40] http://alplatformmedia.com/vb/showthread.php?t=64991
[41] https://justpaste.it/h6ne

The banner of the 'Muhajid's Electronic Suitcase' Guidebook

Social Media

- The Rabitat al-Ansar jihadist media institution, an unofficial media institution that distributes publications for the Islamic State, asked supporters of the organization to take part in a PR campaign on social networks, to be conveyed through the translation of the organization's official materials, the deployment of IS operatives to carry out suicide attacks, the publication of photos of kidnapped American journalist, Steven Sotloff, and more under the hashtag: #StevensHeadinObamasHands.[42]

Banners that were posted on social networks regarding kidnapped American journalist, Steven Sotloff

- The Shumukh al-Islam jihadist media workshop launched a propaganda campaign on social networks via a series a photos titled, "Crimes against the Sunnis in Arsal, Lebanon". The campaign criticized the Lebanese army and Hezbollah for their actions against the Sunni

[42] https://twitter.com/ansaaar3/status/502956713524211712

population in Lebanon, including children.[43]

One of the photos posted on social networks showing a girl killed in Arsal, Lebanon

- A visitor to the Shumukh al-Islam jihadist Web forum noted that the Islamic State's campaign on social networks, especially Twitter, had proved itself by evoking fear in the United States. For example, it called attention to photos that IS supporters had taken next to the White House with the IS flag, which were posted on Twitter. [44]

A photo that was posted to Twitter containing a message threating the United States

[43] https://shamikh1.info/vb/showthread.php?t=226626
[44] https://shamikh1.info/vb/showthread.php?t=226605

- During Operation 'Protective Edge', Internet activity by the Izz ad-Din al-Qassam Brigades was intermittently blocked, and its accounts on social networks were blocked while new accounts were opened.
- On July 14, [45] it was reported that the Facebook page of the Izz ad-Din al-Qassam Brigades, which had been in operation for only a few days, had ceased to operate. In the evening of July 17, it was discovered that the group's English language operations had been disabled. This was also the case for its Twitter [46] account and Web site.[47] Nevertheless, the group's Hebrew and Arabic Web sites were still active (since they have a different Web address than the English site), as were its Twitter accounts in Hebrew and Arabic. Hamas created a new Facebook page[48] on July 14, as well as a Twitter account in Hebrew and a Web site.[49]

A post on the Izz ad-Din al-Qassam Brigades's Twitter account in Hebrew

- The closure of the Izz ad-Din al-Qassam Brigade's Twitter activities in Arabic and English led to the creation of new accounts.

[45] https://www.facebook.com/permalink.php?story_fbid=783473915008626&id=145834972105860
[46] https://twitter.com/qassamfeed
[47] http://qassam.ps/
[48] https://www.facebook.com/moqawama.gaza
[49] https://twitter.com/hamasinfo

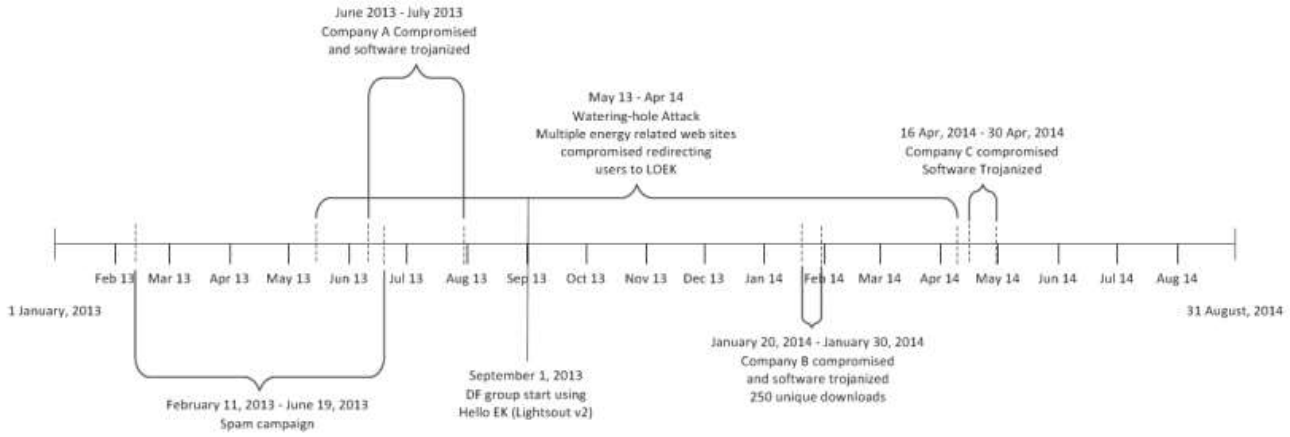
- A representative from the Al-Riah jihadist media institution, which serves as a platform for messages from the Mujahideen al-Masada organization ("The Lion's Den of the Mujahideen") – a Salafi-jihadist organization in the Gaza Strip – informed visitors to the Shumukh al-Islam jihadist Web forum that they can access current information regarding the organization's activities via its new Facebook page at: https://www.facebook.com/pages//مؤسسة-رياح-الإعلامية-الذراع-الإعلامي-لمأسدة-المجاهدين/284841501715654

The banner page of the Al-Riah jihadist media institution

Cyber Attacks

Breaches of Companies in the Energy Sector

In the beginning of July, it was reported that the group known as Dragonfly and Energetic Bear had carried out a series of attacks, beginning in 2013 with Spear Phishing attacks against companies mainly in the energy sector. Some of the attacks implanted Trojan Horses with the potential to damage processing systems. The group is believed to be a Russian hacker group.[50]



The timeline of the group's activities[51]

In the middle of July, it was published [52] that Russian hackers had planted malware on the computer systems of NASDAQ. FBI officials identified the attack in October 2010 and, through a joint investigation with the NSA, arrived at the conclusion that Russian hackers had exploited security breaches to plant malware with the potential to cause damage to its systems.

Breaches of the Twitter Accounts of Various Armies

Close to midnight on July 3, the Syrian Electronic Army (SEA) published an announcement according to which it had successfully hacked into the IDF's official Twitter account.[53] In addition, the

[50] http://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html
[51] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
[52] http://www.businessweek.com/printer/articles/213544-how-russian-hackers-stole-the-nasdaq
[53] https://twitter.com/Official_SEA16/status/484799837796192256

organization published a message that was allegedly posted to this account (@IDFSpokesperson), according to which the nuclear leak that happened near the nuclear reactor in Dimona was likely caused by two rockets hitting the structure.

Several minutes later, an apology was posted on this IDF account;

However, approximately 20 minutes after the first message was posted, the organization posted another message in which it claimed to have taken control of the system administrator of the IDF's Internet activity;

It also attached a screenshot attesting to the breach of the system administrator;

On July 20, the official Twitter account of the Kenyan army was hacked by a pro-Palestinian hacker,[54] seemingly from Venezuela, operating under the name, "Anonymous". The hacker breached and took control of the personal account of Maj. Emmanuel Chirchir, spokesperson for the Kenyan army. [55]

[54] https://twitter.com/Anon_0x03
[55] https://twitter.com/MajorEChirchir

The official Twitter account of the Kenyan army

Cyber-Crime and Cyber-Terrorism, July – September 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

was culled from the visible (OSINT) and invisible ("Dark Web")[56] Internet between July - September 2014.

Virtual Currency – Bitcoin Updates

The below chart shows the Bitcoin price on the BitStamp trading site for July-September 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 July, the currency rate of the bitcoin jumped to $650 while dropping down during August, closing September at the value of $380.

Bitcoin price chart in BitStamp for July - September 2014[57]

In the beginning of July, [58] a document was published that called for bitcoin donations in order to continue the struggle of the Islamic State. The document included religious references and technological aspects that make the bitcoin an ideal means of fundraising, such as the use of Dark Wallet, a virtual wallet that was developed especially to increase security and anonymity of bitcoin use. The document is believed to have been published by a supporter of the Islamic State called,

[56] 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.

[57] http://bitcoincharts.com/charts/bitstampUSD#rg60zczsg2014-07-01zeg2014-09-30ztgMzm1g10zm2g25zvzcv

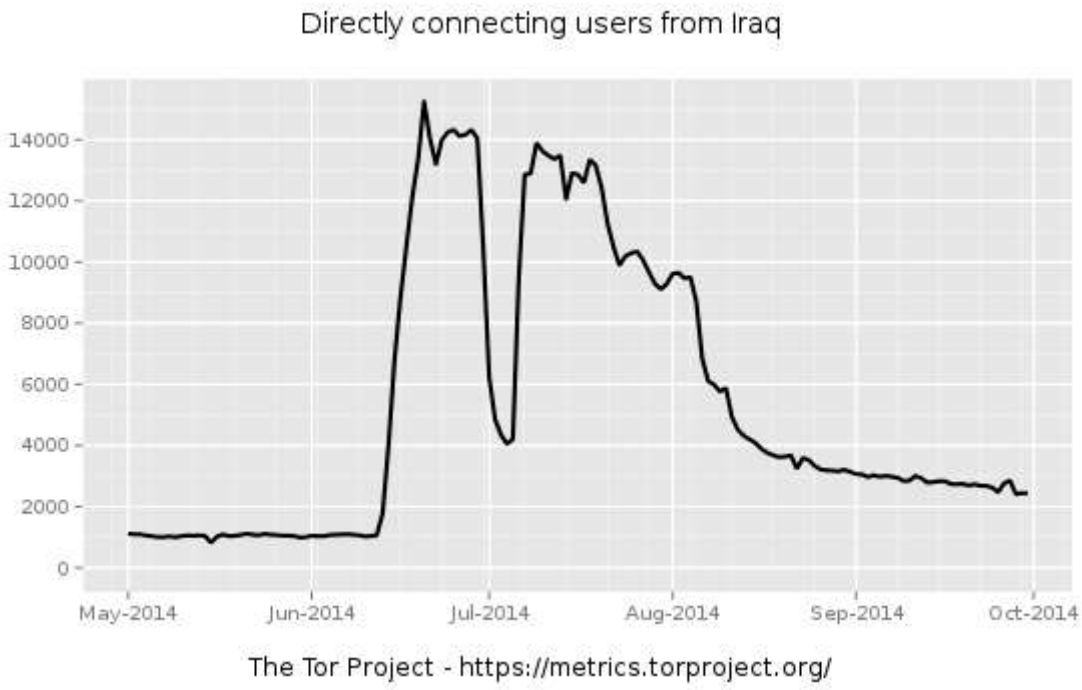
[58] https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf

"Amreeki Witness",[59] who also discussed the possibility of creating a virtual currency specifically for the Islamic State. [60]

Increase in TOR Usage in Iraq

Since mid-July, an increased use of TOR software, which enables anonymous and secure Internet access, was noted in Iraq. This was in addition to reports that were published in mid-June regarding the government's instruction to Internet providers in the country to prevent [61] access to several social networks and other popular sites in order to prevent them from being used by the IS, which is continuing to seize more and more territory from Iraq.

Data on TOR usage in the country indicates[62] that use of this tool increased from an average of approximately 1,000 connecting users per day to approximately 14,000 connecting users since mid-June.



[59] http://www.vocativ.com/tech/bitcoin/bitcoin-fund-jihadists
[60] http://www.deepdotweb.com/2014/09/22/bitcoin-is-not-being-used-by-the-islamic-state
[61] http://www.ibtimes.co.uk/iraq-crisis-twitter-google-youtube-facebook-blocked-by-government-stop-isis-plotting-1452567
[62] https://metrics.torproject.org/userstats-relay-country.html?graph=userstats-relay-country&start=2014-05-01&end=2014-09-30&country=iq&events=off

This data again emphasizes the limited ability of governments today to completely block their citizens' access to online content despite attempts by the Iraqi government to block and prevent new users from downloading and installing the program.[63] In response, an alternative site was offered along with an installation guide in Hebrew.[64] In mid-August, an announcement was published on behalf of the TOR project regarding attempted censorship in Iraq.[65] There is no indication that these attempts were successful but usage dropped in early July and faded in early August.

Wave of Cyber Crime in the United States: Theft of Credit Cards from Card Readers

In addition to recent reports about computer hacks of large companies in the United States, as a result of which tens of millions of records and credit cards were stolen and leaked, including the Home Depot, JPMorgan and many others,[66] many more cases of credit card theft from various companies and businesses were revealed. In the framework of this, on September 17, it was reported[67] that dozens of stores in the Goodwill Industries International chain throughout the United States had been the victims of a breach that continues for over one-and-a-half years. The breach was carried out on the computer systems of C&K Systems, which provides payment processing services. The hackers hacked into the company's systems and remained there from February 10, 2013 until August 12, 2014, according to a company representative. Two weeks earlier, it was reported that over 10% of the company's Point of Sale (PoS) was negatively affected by the data leak as a result of the theft of clients' credit cards that were used in company stores from June 25, 2013, four months after the first breach at C&K. According to the company, it was informed of the breach by a private security investigator on July 30. After hiring an investigative team, it was discovered that the company's systems were infected with the infostealer.rawpos malware.

---

[63] https://uk.news.yahoo.com/iraq-crisis-government-blocks-access-tor-project-following-141424780.html#C7cVGWp
[64] http://arabic-tor.kopimi.co/
[65] https://uk.news.yahoo.com/iraq-crisis-government-blocks-access-tor-project-following-141424780.html#C7cVGWp
[66] http://www.forbes.com/sites/katevinton/2014/09/10/data-breach-bulletin-home-depot-healthcare-gov-jp-morgan/
[67] http://www.tomsguide.com/us/goodwill-data-breach-update,news-19558.html

It was also discovered that this malware, which attacks Windows-based PoS, was in use at the time that millions of credit cards information were stolen from the Home Depot and Target last year. The malware copies the card details when the card is used to make a payment and sends the data to a server controlled by the hackers. The report revealed that C&K's security software did not detect the malware until September 5, 2014. It is not clear if the malware directly affected the cash registers at the Goodwill stores but C&K manages the payment process from the date that the card is swiped until the PoS. Indeed, the company stated that it had only come across 25 instances of stolen credit card fraud as a result of the theft of this data but Goodwill stated that it was no longer using C&K's software in its stores.

One week later, it was reported[68] that another company, Jimmy John's sandwich restaurant chain, had suffered a breach of its systems and of a great deal of data had been leaked. The restaurant chain verified on September 24 that hackers had stolen the credit card details of customers from 216 of its stores (out of 1,900). In an announcement that was published[69] on its Web site, the company stated that it was informed on July 30 of a possible security breach involving credit cards at some of its branches. The investigation, which was said to be ongoing, revealed a breach at 216 stores. By stealing the access details to a service provided by a third party, the criminals were able to get control of the PoS and install malware on it, seemingly on July 1, 2014 despite its claim that a few of its stores were already hacked on June 16. According to the announcement, the malware was removed from most of the stores between August 3-5 and new computers were installed, even though it was reported that several stores did not have the malware removed before August 5. Nevertheless, in an article[70] about the incident, it was claimed that the criminals had stolen information from credit card readers at PoS between June 16 and September 5, 2014 (a month after the date noted by the company in its announcement).

The number of stolen cards was not noted but it was reported that the affected cards were only those that were swiped in those stores and not those that entered manually or online but that, nevertheless, new machines were installed to encrypt the data. In contrast, the name of the PoS service provider in the Goodwill incident, via which the card details were stolen, was not

[68] http://www.huffingtonpost.com/2014/09/24/jimmy-johns-breach_n_5877134.html
[69] https://www.jimmyjohns.com/datasecurityincident/
[70] http://www.huffingtonpost.com/2014/09/24/jimmy-johns-breach_n_5877134.html

mentioned. However, the security investigator who reported[71] the incident back on July 31 stated that the theft of the cards in the store chains was the result of a cyber-attack on a company called Signature Systems, which supplies credit card readers to restaurants. It was also reported that banks had noticed a pattern of fraud on cards that were used in the chain's stores.

These incidents of hacking into companies that supply credit card reading services and implanting malware that saves the details of cards that are swiped through the reader, are part of an ongoing phenomenon that will likely expand to the theft of even more data; the number and identity of the affected companies, the information that was stolen, and possibly even the identity of those responsible for this wave of cyberattacks.

Europol Intensifies its War against Cybercrime

A Europol press report[72] from September 1 announced the establishment of a task force to operate in the field of cybercrime – J-CAT – in order to strengthen the war against cybercrime in the European Union and beyond. The new entity will comprise part of the European Cybercrime Center (EC3), which operates in the framework of Europol, and will coordinate international investigations through collaboration against cybercrime threats and targets such as hidden Web forums, malware and Trojan Horses against banking systems. The task force will be led by Andy Archibald, the Deputy Director of the Cybercrime Unit at the National Crime Agency (NCA) in Britain. This entity, which currently counts Austria, Canada, Germany, France, Italy, Holland, Spain, Britain and the United States as members, was established by the EC3 (the cybercrime task force of the European Union, the FBI and the NCA) and will include liaison officers in this field from among the countries that committed to it, as well as other parties. This, despite the fact that the intelligence will come solely from the European Union and shared among enforcement officials. It was also reported that both Australia and Colombia were committed to this initiative.

The task force will operate from secure offices at the Europol headquarters and will be aided by investigators and experts from cybercrime centers in Europe. The goal is both strategic and operational - to prevent cybercrime, disrupt its operations, capture criminals and confiscate illegal

[71] http://krebsonsecurity.com/2014/07/sandwich-chain-jimmy-johns-investigating-breach-claims/
[72] https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime

profits.

The EC3 is involved in a cross-border investigation of cybercrime and the goal of J-CAT is to add significant value to the international cooperation of law enforcement, and to maximize the effectiveness of coordinated operations due to the nature of cybercrime, which affects every person in every country without regard for geographic boundaries.

The task force will collect information on specific criminal topics from relevant government and private national shared databases, and it will convert this raw data into practical intelligence, and potential targets and networks to investigate. It will cover a wide range of fields, including the creation of malware, testing, distribution, botnets, online scams, breaches, etc.

In addition, this entity will hold targeted consultation meetings with key parties in the private sector and with CERT teams among institutions, organization and agencies in the European Union in order to get information from them regarding cybercrime threats that affect them and society in general.

On September 23,[73] it was reported that Europol and European banks were joining forces in the fight against cybercrime. The European Banking Federation (EBF) and Europol's European Cybercrime Centre (EC3) signed a memorandum of understanding that paves the way for collaboration between law enforcement authorities and the financial sector in the EU. The document enables the exchange of information, statistics and strategic data between the two entities regarding cybercrime threats in order to enable financial institutions to protect themselves, as well as the transfer of information to law enforcement authorities regarding new malware and scamming methods in order to aid them in the investigation and capture of suspects. This collaboration has already led to successful operations and preventative action in the fields of fraud and counterfeit credit cards.

The head of the EC3 said: "Today marks an important day for both EU law enforcement and the banking industry. We have agreed to intensify mutual cooperation, respecting relevant national legislation, to jointly enhance our ability to prevent, prosecute and disrupt cybercrime against the financial sector. This is more than a ceremonial gesture - this is the establishment of a trusted relationship aimed at achieving tangible results that will make life more difficult for criminals and

[73] https://www.europol.europa.eu/content/european-banks-and-europol-join-forces-fight-cybercrime

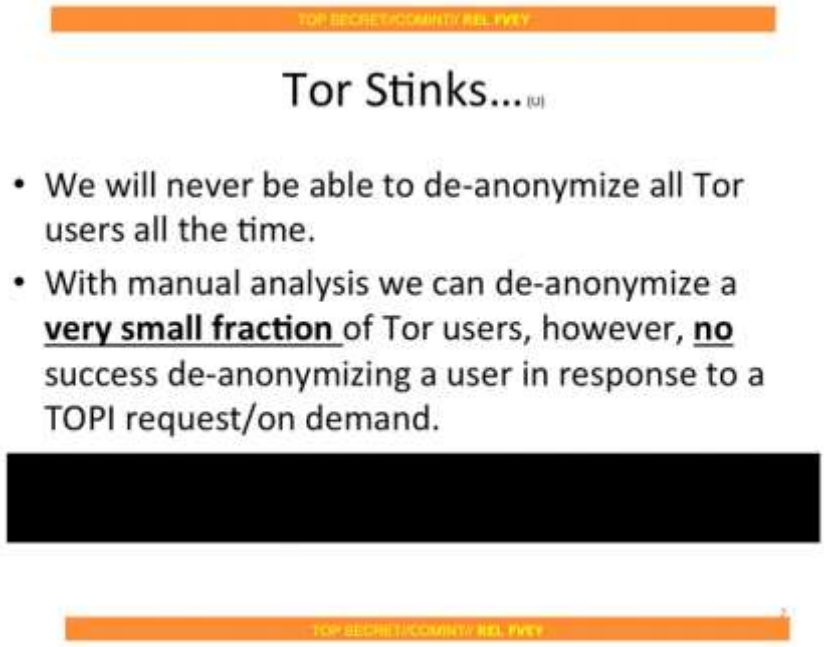
life easier for the banking sector and all of us who use these important services."

The Chief Executive of the European Banking Federation said: "Our members already cooperate intensely with their own, national police authorities in order to fight with financial cybercrime. Our partnership with Europol now adds a European dimension to this important work. International cooperation between banks and law enforcement bodies is essential because it is clear that criminals know no borders."

Darknet Technology in Malwares

The use and utilization of anonymity networks by cybercriminals is nothing new. For years the TOR network has been used for everything from drug trafficking, purchasing of illegal and stolen goods and pedophilia to networking on topics such as explosives, jihad and fraud. Naturally, this type of environment is one that would draw a lot of law enforcement attention. Some operations against illegal hidden services have been very successful,[74] such as the takedown of the FreeHosting pedophilia network using a vulnerability in the TOR browser in combination with malware to de-anonymize members. However, as some of the Snowden files show, even law enforcement agencies (LEAs) had a hard time[75] dealing with TOR's provided anonymity. While the battle against hidden services continues,[76] alongside attempts to identify[77] TOR users, malware authors have been utilizing TOR's infrastructure for malware communication and annoimzation as well as TOR-based fraud services.

[74] http://news.softpedia.com/news/FBI-Controlled-Freedom-Hosting-Tor-Servers-Agency-Admits-383002.shtml
[75] http://s3.documentcloud.org/documents/801434/doc2.pdf
[76] http://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/
[77] http://www.wired.com/2014/12/fbi-metasploit-tor/



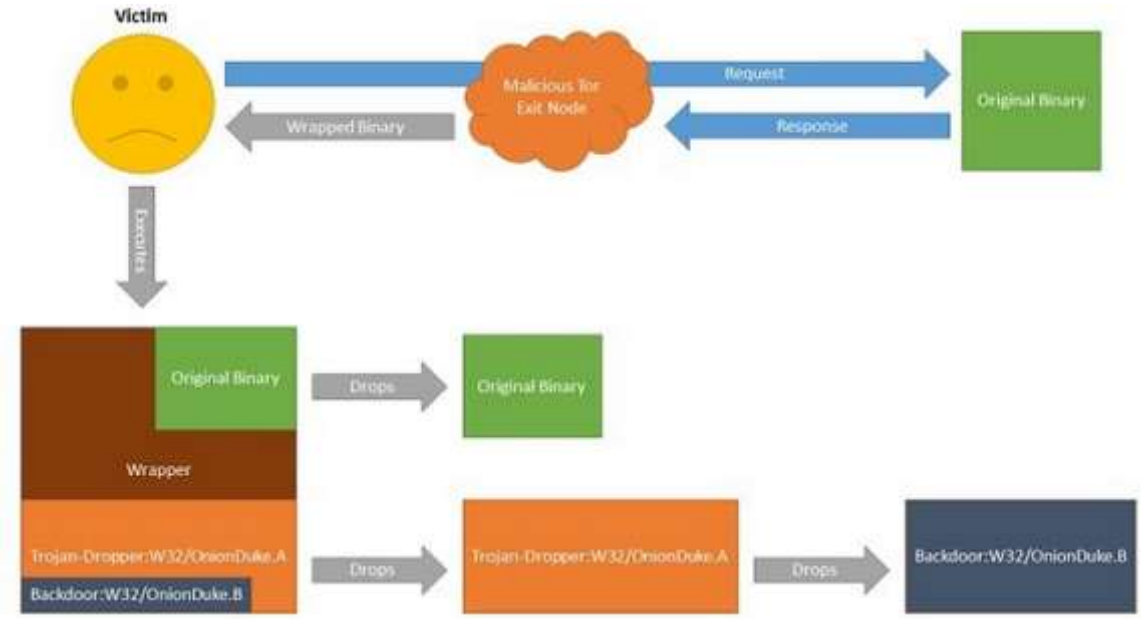
A slide from the NSA presentation on TOR[78]

As early as 2009,[79] malware authors started using TOR to hide their command and control (C&C) server as well as to secure the malware communication. The reasoning for this is simple – if LEAs can intercept or reverse the communication between an infected device and the C&C, they can shut down the malware botnet's operation. Furthermore, TOR-based communication, being anonymous in nature, is harder to identify and blacklist. Malware authors have implemented the use of TOR in various malware families. A 64bit variant[80] of the Zeus malware demonstrated an interesting behavior – upon infection it initializes (on the infected device) a TOR hidden service, a unique TOR domain and a unique private key. This allows the attacker to communicate and take over the device (using VNC) over TOR. Another interesting malware using TOR is Chewbacca[81] – a PoS (Point of Sale) malware used to infect devices and steal credit card data. Chewbacca is not the only PoS malware

[78] http://s3.documentcloud.org/documents/801434/doc2.pdf
[79] http://www.dailydot.com/technology/tor-botnet-microsoft-malware-remove/
[80] http://www.darkreading.com/attacks-breaches/new-zeus-banking-trojan-targets-64-bit-systems-leverages-tor/d/d-id/1141049?
[81] https://blogs.rsa.com/rsa-uncovers-new-pos-malware-operation-stealing-payment-card-personal-information/

using TOR; most recently (December 2014), a malware dubbed LucyPOS[82] was identified in the wild implementing Chewbacca and Dexter (another PoS malware) techniques.

Not surprising, TOR is not only used by financial malware. Recent research identified the OnionDuke malware, an APT component that infects victims via a TOR exit node. The Russian-based exit node wraps legitimate (and illegal) files with the OnionDuke[83] malware, which researchers found is linked to the MiniDuke and CosmicDuke APT family. This malware targets government organizations as well as abuses social media sites. While the malware does not use TOR, it does abuse the TOR project as the (volunteer operated) exit node is used as an infection point in the malware lifecycle.



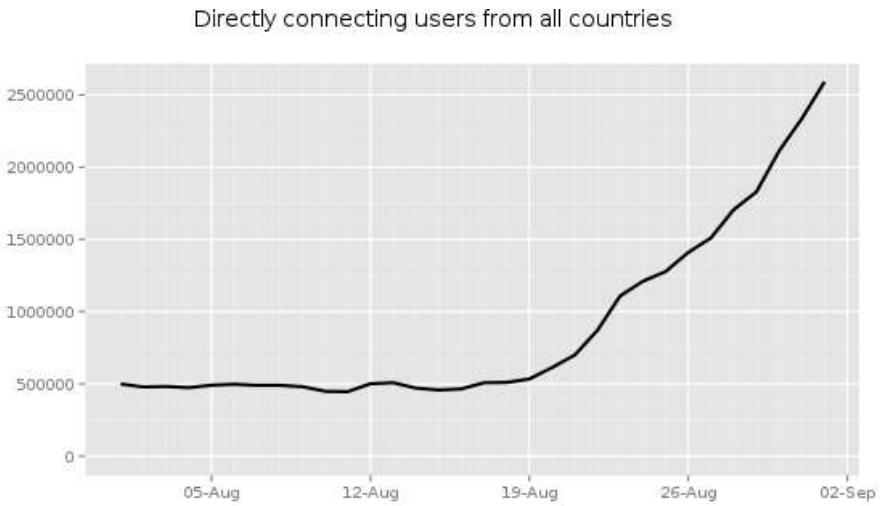
OnionDuke infection pattern[84]

It is worth pointing out that TOR is not the only anonymity network available. I2P (the Invisible Internet Project) is another example of an anonymity network that implements its security features in a different manner than TOR. As with TOR there are a lot of criminal hidden services on this

[82] http://arcticwolf.com/news/siem-services-skills/just-in-time-for-the-holidays-a-new-pos-malware-variant-found/
[83] http://www.securityweek.com/onionduke-apt-malware-distributed-malicious-tor-exit-node
[84] http://arstechnica.com/security/2014/11/for-a-year-one-rogue-tor-node-added-malware-to-windows-executables/

network. The I2Ninja[85] is a malware that utilizes the I2P infrastructure to receive credentials from infected victims, communicate with the C&C and even to support its ticketing system for the malware users (communication of support requests are relayed via the I2P P2P network).

One possible downside of using anonymity networks to launch malware or to serve as an infrastructure is that these networks are rather small in size and any abuse of the network is (relatively) easy to identify. While we tend to think of TOR as an "evil internet", it is in fact used by many privacy driven individuals who also care for its usage and stability. When criminals launched the Mevade[86] botnet, which caused the number of TOR users to significantly increase, security firms and TOR users quickly identified the surge in TOR usage bandwidth and identified the problem. In order to avoid analysis and further toughen investigation by security firms, one malware variant chose to move its infrastructure to its own P2P network – the Gameover Zeus variant. This malware was so successful (in criminal terms) that Microsoft and the FBI conducted a special operation[87] against its infrastructure (the malware returned[88] to operation not long after).



The surge in TOR users following the Mevade botnet actions[89]

[85] http://securityintelligence.com/shadows-i2ninja-malware-exposed/
[86] http://news.techworld.com/security/3468988/mevade-botnet-miscalculated-effect-on-tor-network-says-damballa/
[87] http://www.techradar.com/news/internet/web/microsoft-and-fbi-team-up-to-take-down-gameover-zeus-botnet-1251609
[88] http://www.theregister.co.uk/2014/08/15/gameover_zeus_back_from_the_dead_as_/
[89] http://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/

With the ever-increasing concern cybercriminals have for their privacy and operations, we can only expect to see more usage of anonymity networks, whether to serve as an infrastructure for malware communications, as an infection point, as a way to access stolen credentials (as demonstrated by a criminal offering access to stolen SMS from Android infected devices, over TOR) and, of course, for selling and trading in data, tools and goods. On the one hand there are new tools[90] in the market that aim to make accessing TOR and browsing anonymously easier than ever (some[91] by crowd funding). On the other hand, as with any intelligence versus privacy concerns, law enforcement agencies such as the FBI and the NSA are very much aware of this and are constantly looking for ways to work around and de-anonymize suspicious users. What does this mean for the persistent cybercriminal? Challenges and opportunities, or as Truman said, "A pessimist is one who makes difficulties of his opportunities and an optimist is one who makes opportunities of his difficulties."

Case Study - Legal Developments in Israel

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

Israel's Draft Law on the Struggle against Terrorism, 5771-2011

The Israeli Knesset's Constitution, Law and Justice Committee convened two sessions during this period to discuss the Draft Law on the Struggle against Terrorism, 5771-2011 ("HaMa'avak B'Terror"). The Draft Law had passed a first of three required readings under the previous Knesset's jurisdiction, and was subject to continuity under the current Knesset, which began its deliberations on the Draft Law in February 2014. Although the Draft Law specifically avoids referring to cyberterrorism as a separate category of terrorism, the Committee discussions around the definition of a "terrorist act" found in its Article 2 are relevant to certain activities carried out in cyberspace.

[90] http://www.pcworld.com/article/2465683/how-a-portable-travel-router-can-put-tor-web-surfing-security-in-your-pocket.html
[91] https://www.indiegogo.com/projects/anonabox-the-tor-hardware-router

Specifically, the proposed broad definition includes "…serious harm to vital infrastructures, systems or services; or serious disruption of them; serious damage to the country's economy or environment, or damage to the environment that has caused or is liable to cause serious economic harm." . These types of acts are liable to be carried out, at least in part, through the use of terrorists' cyber capabilities. The Committee did not specifically discuss such capabilities but, during the July 1 session, a representative from the Ministry of Justice emphasized that the intention was to address damage caused by terrorists that is more appropriate to the contemporary world than the damages caused by "traditional" terrorist acts; and noted that the systems protected by the definition include computerized systems (Committee Protocol, July 1, p.4). Committee Chair Elazar Stern also referred in this session to "internet terrorism" (ibid, p. 13).

In the July 14 session, the need to address future forms of terrorism in the law was emphasized (Committee Protocol, July 14, p. 24). Towards the end of the session, mention was made of terrorist acts that violate either the Protection of Privacy Law, 5742-1981 (which protects databases in its Part B, for instance) or the Charge Cards Law, 5747-1986 – or come under the definition of cybercrime (ibid, p. 31). No determination was made about whether such acts should be considered acts of terror.

(Editors' note: The Draft Law cannot enjoy the rule of continuity twice, and will need to be re-submitted to the 20th Knesset in 2015. Similar issues concerning the definition of a "terrorist act" that is committed at least partially in cyberspace are likely to characterize future Knesset debates, as well.[92]

The Council of Europe Convention on Cybercrime, 2001 ("the Budapest Convention")

The Government of Israel continued discussions around accession to the Budapest Convention.[93] The Convention prohibits offences against the confidentiality, integrity and availability of computer data and systems, including illegal access and interception; data and system interference; and computer-related forgery and fraud. One of the Convention's aims is to harmonize member states' criminal law provisions that include or encompass cybercrime offenses. Cyberterrorism is not

[92] The text of the Draft Law is available here: http://www.justice.gov.il/NR/rdonlyres/77CD3245-3A1D-4F8E-AA54-5D8C25344888/29272/611.pdf (in Hebrew only).

[93] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185

specifically mentioned anywhere in the Convention, although the Council of Europe has stated that, in its view, the Convention does in fact address cyberterrorism and the use of the Internet for terrorist purposes.

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

Dr. Michael Barak, Team Research Manager, ICT

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

Etay Maor, Senior Fraud Prevention Strategist

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

Shuki Peleg, Information Security and Cyber-Security Consultant

Nir Tordjman, Team Research Manager, ICT

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.