IDC HERZLIYA

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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 14

July – September 2015

Highlights

This report covers the period of July - September 2015 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:

- Islamic State supporters continued to publish and distribute guidebooks and informational materials on the topic of information security and maintaining anonymity online: "personal computer security", "smart phone security", how to post informational material on Twitter using several accounts simultaneously, how to inspect files and links infected with viruses, how to open a Twitter account without a cell phone number, how to use encrypted email, and more.
- During this period, we continued to see cooperation between players affiliated with the Islamic State, such as Cyber Caliphate, IS Hacking Division and ISIS Cyber Army, and hacker groups that began to identify with the organization. For instance, it was reported that a hacker named Ardit Ferizi stole personal details about US army and government personnel that he sent to members of the organization, who then leaked the information under the name "Cyber Caliphate".
- Members and supporters of the Islamic State continued to hack Web sites and social networks, and leak the information obtained. During this period, we witnessed a "spam campaign" – a virtual campaign that called on Islamic State supporters to report Twitter accounts belonging to opponents of the organization as spam in order to have them closed.
- Web sites on the darknet were used by the Islamic State to transmit and publish guidelines for action, perhaps against the backdrop of the organization's increased technical capabilities or as part of an effort to preserve the anonymity and security of the organization's members in order to protect them from being discovered by the authorities and various security services.
- During this period, and as part of a campaign by the coalition against the Islamic State, the Sawab Center was established for the purpose of disseminating messages against the organization. The center publishes its messages through, among others sources, a Twitter account with approximately 30,000 followers. Meanwhile, Europol launched the European Union Internet Referral Unit (EU IRU) to monitor terrorist propaganda, in order to identify and report such sites to service providers.

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 2015[1]

The Islamic Emirate of Afghanistan

The announcement made by the Islamic Emirate of Afghanistan regarding the death of its leader, Mullah Omar, was at the top of the jihadist discourse during this period. Sheikh Ayman al-Zawahiri's silence on the matter until his re-appearance in the media fuelled the propaganda of the Islamic State, which claimed that this silence proved that al-Zawahiri had fallen off the grid. The Islamic Emirate of Afghanistan finally admitted that it had concealed its leader's death for two years, claiming that 2013 was a decisive year in the organization's struggle against foreign forces. The Emirate went on to announce the appointment of its deputy, Mullah Akhtar Mohammad Mansoor, as the new leader of the Emirate. The announcement regarding the concealment of Mullah Omar's death further fuelled claims by the Islamic State's propaganda machine claim that the Islamic Emirate of Afghanistan is not trustworthy or legitimate, and therefore jihad fighters in the region should join the Islamic State.

[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

Al-Qaeda

Following a one-year absence, Sheikh Ayman al-Zawahiri re-emerged in the media in order to give a eulogy in memory of Mullah Omar, the leader of the Islamic Emirate of Afghanistan, and to swear allegiance to its new leader, Mullah Akhtar Mohammad Mansoor. In return, the latter announced his acceptance of al-Zawahiri's pledge. In addition, al-Zawahiri vowed to work to apply shari'a and continue to wage jihad until the release of all Muslim occupied lands, and he emphasized that the Islamic Emirate of Afghanistan is the only legitimate emirate.

To mark the anniversary of the September 11 attacks, al-Zawahiri released a new series of publications titled, "The Islamic Spring". In the first three parts, which were published during the month of September, he raised several issues including: Al-Qaeda's guiding strategy, an emphasis on the importance of maintaining unity among jihad fighters and cooperation between them against the Syrian regime, and the non-recognition of the caliphate established by Abu Bakr al-Baghdadi. In his opinion, efforts should be concentrated on moving the battle against Western countries to their own territory, especially the United States, and he called on young Muslims living in the West to carry out suicide attacks to this end.

Al-Qaeda in the Arabian Peninsula (AQAP)

During this period, senior AQAP leaders focused on discourse concerning the need to continue fighting against the Houthis in Yemen and against the West, especially the United States. Qasim al-Raymi, the new leader of AQAP who swore allegiance again to Sheikh Ayman al-Zawahiri, called on the mujahideen to continue the struggle against the United States and emphasized the organization's cooperation with the Shi'ites in the war against the Sunnis. Khaled Batarfi, a senior leader in the organization, called on Muslims in the West – especially those in the United States and France – to carry out individual terrorist attacks such as the attack at Charlie Hebdo in Paris, and emphasized that such attacks are a "strategic weapon" that successfully breaks enemy strongholds time and again. Against the backdrop of the wave of terrorist stabbing attacks in Israel, Batarfi expressed solidarity with the Palestinians and encouraged them to continue the wave of attacks in order to defend their honor and the sanctity of Al-Aqsa Mosque.

Al-Nusra Front

During this period, Al-Nusra Front, Al-Qaeda's affiliate in Syria, also conducted an extensive public campaign against the Islamic State. In a new magazine that was launched in English titled, "Al-Risala", it accused the organization of establishing an Islamic caliphate illegally and sinfully, and of causing a rift among the mujahideen. Abdullah al-Shami, a member of Al-Nusra Front's Shura Council, accused the Islamic State of cooperating with the Alawite regime, and clarified that his organization is not interested in cooperating with Turkey in light of its support for the Islamic State.

Al-Shabab Al-Mujahideen

Sheikh Abu 'Ubatdha Ahmad 'Umar, the leader of Al-Shabab Al-Mujahideen, Al-Qaeda's affiliate in Somalia, released his first message since his appointment to the role. He discussed his organization's determination to fight against the Crusader conspiracy to weaken Islam and steal the natural resources of Muslim lands. He called on tribes in Somalia to help the jihad being waged against enemies of Islam and he called on Muslims in Kenya to join jihad as well. According to him, Al-Shabab is ready and willing to absorb into its ranks Muslims from East Africa, especially Ethiopia, Djibouti, Uganda and Central Africa, due to their persecution at the hands of the local regimes. In addition, he announced the establishment of a new military unit called the Sheikh Mukhtar Abu Zubayr Battalion to help in the fight against enemies of Islam.

Al-Qaeda in the Indian Subcontinent

Al-Qaeda in the Indian Subcontinent called on Muslims in Pakistan to go out and fight against the Pakistani regime and its security measures in response to the trend of repression that it carries out against Muslims in the country and its exclusion of Islam.

Egypt

Ajnad Misr announced the renewal of its jihad activities in the Egyptian arena, and threatened to increase terrorist attacks against Egyptian security forces.

Islamic State

The Islamic State (IS) continued to release propaganda against Arab regimes and the coalition partners taking part in the battle against the organization. For example, IS fighters threatened to attack the rulers of Saudi Arabia and the Shi'ite minority in the country. In addition, the organization threatened to attack the secular Algerian regime and its security forces. In addition to these threats, the organization published a series of videos designed to sow psychological terror in the minds of its enemies. For instance, it documented the execution of 25 Syrian army soldiers in an amphitheater in the city of Palmyra. Meanwhile, the organization continued its efforts to recruit Muslims in the West and in the East. For example, the organization called on Muslim residents of Turkistan, Germany and Austria to immigrate to the territories of the Caliphate or to take action in their homelands against the ruling regime. The IS even launched an extensive propaganda campaign aimed at dissuading residents from leaving the territories under its control and immigrating to Europe.

Another prominent theme of the Islamic State's discourse concerned the importance of integrating the gold dinar, which was created by the organization, into the commodity exchange and into the economic life of the caliphate's territories. Most of the messages emphasized the superiority of the gold dinar over the US dollar, which is made of paper, and expressed hope that the new Islamic currency will weaken the global economy.

Jihadist Propaganda

- An IS supporter launched a blog containing content about the organization's informational materials as well as guidebooks for the Internet that were originally written by a cyber expert referred to as "the Islamic State's Tech Person". Among the cyber materials published were guidebooks on the following topics: "personal computer security", "smart phone security", how to post informational material on Twitter using several accounts simultaneously, how to inspect files and links infected with viruses, how to open a Twitter account without a cell phone number, how to use encrypted email, and more.[2] One of the articles, which was previously published on social networks and now appeared on the current blog, emphasized the importance of electronic warfare against the West, and the importance of being vigilant about

[2] http://khelafa1.blogspot.co.il/p/blog-page_6.html

information security and the use of the Internet because of intelligence officials.[3] The guidebooks themselves were also published on Twitter under the heading, "information security", alongside communication with the publisher via the encrypted Telegram chat software.[4]

The blog banner

An online collection of guidebooks about information security that was published by an IS supporter

- Another collection of guidebooks that was also published on social networks by a cyber expert referred to as "the Islamic State's Tech Person", which dealt with the topic of "hacking into the Linux Mint system".[5]

[3] http://khelafa1.blogspot.co.il/p/gps-60-60.html; http://khelafa1.blogspot.co.il/p/blog-page_73.html
[4] http://justpaste.it/techarchive
[5] http://justpaste.it/Linux-archive

The banner title: "Linux hacking course"

- An IS supporter published on Twitter a comprehensive guide to using TOR software for Android devices.[6]

Banner of a guidebook for using TOR software on Android devices

- The AnonGhost hacker group, which includes Islamists who express support for the Islamic State, published several guidebooks for hacking Web sites and computers, such as: a guidebook on how to uncover the passwords of routers,[7] and how to hack into computers using SQL.[8]
- A Twitter account affiliated with the IS in Khurasan (Afghanistan) called "Khurasan News" published details on how to make contact with it using the encrypted Telegram chat program in Pashto.[9]

Defensive Tactics

- Al-Fajr Center, which is affiliated with Al-Qaeda, announced the publication of an update for the transmission of encrypted messages called "Amn al-Mujahid" ("Mujahid Security") for Android devices. Jihadists announced the software on social networks, such as "the Technology Committee Reporter" who recommended that Web users install it at the following addresses:

  http://alfajrtaqni.net/amm.html

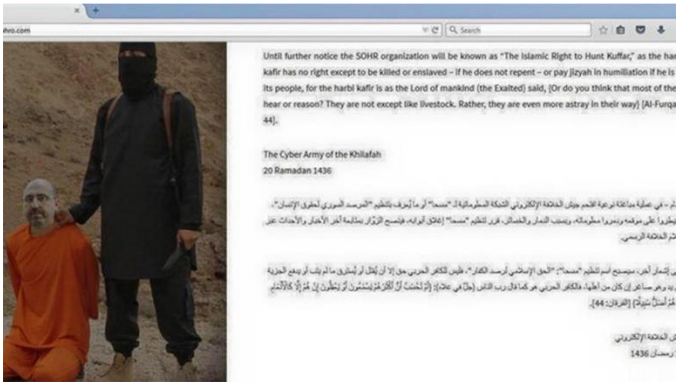
[6] https://twitter.com/nabava1/status/620909279730630656; https://dump.to/orbottor
[7] http://www.anonghost.ml/2015/10/blog-post.html
[8] https://www.youtube.com/watch?v=UX2z2QdlvCA&feature=youtu.be&a
[9] https://twitter.com/KhNewsss/status/648691322770075652;
https://twitter.com/KhNewsss/status/648691322770075652

http://alfajrtaqni.net/english.html.[10]

- A visitor called the "Technology Committee Reporter", a jihadist involved in computer issues on social networks, warned users not to use the "truecrypt" chat software for encrypting conversations, claiming that the software was developed by the Russians for spying purposes.[11] In another tweet, the same visitor explained how to disguise jihadist applications installed on their cell phones.[12]

Offensive Tactics

- A hacker group called "the Electronic Caliphate Army" claimed responsibility for the breach of the Syrian Web site, Al-Marsad, which serves as a platform for civil rights. As a result of the breach, the site ceased to operate and its database was destroyed. A photo was planted on the home page showing a masked IS fighter holding a knife and standing next to a body, as well as a photoshopped image above it showing the head of Al-Marsad Web site manager, Rami 'Abd al-Rahman, as a message threatening his life.[13]



- A hacker group called "Fadhaih al-'Almaniyya" claimed responsibility for a breach of a series of French Internet sites in the beginning of August 2015. According to the group, the breach

[10] https://archive.org/details/DmLE5Q;https://twitter.com/alfajrtaqni/status/618821796918247424 ; https://twitter.com/alfajrtaqni/status/618825829657657344
[11] https://twitter.com/alfajrtaqni/status/631295237990682624
[12] https://twitter.com/alfajrtaqni/status/641176667042398208
[13] http://www.syriahr.com/2015/07/جيش-الخلافة-الإلكتروني-يهكر-المرصد-ال/

was carried out in revenge for the situation in Tunisia and the heresy that prevails there.[14]

- At the start of July 2015, the Tunisian hacker group, Al-Fallaga, which has ties to global jihad, announced the launch of an electronic attack campaign against Israeli sites under the heading, "Op Electronic Badr". It added that the intention of the campaign was to leak Israeli credit card numbers, bank account numbers and more.[15] The group even opened a Facebook page to coordinate the attack and share the breach of Israeli sites with users.[16]

[14] http://justpaste.it/Fr102
[15] https://twitter.com/amalouh1/status/617321971647389696; #بدر_الالكترونية
[16] https://www.facebook.com/events/1638104659741156/


Hacked by Fallaga Team |
xml.telesport.co.il/index.html
جيش الفلقة الإلكتروني
HACKED BY Asser & AdmiNet & Dant3é
Tunisian Fallaga Team [Facebook.com/Elfellaga]
عمليـــة بـــدر الالكترونـــــية الفلاقـــة التونسيـــة
DON'T COLSE UR EYES IT IS NOT A DREAM IT'S A FUCKING REALITY UR WEBSITE HAS BEEN HACKED BY As
Hey Son OF "Kafira" This is a message from Tunisian Fallaga Team To the thing named "Israel" ...
We Are They Same Persons who Fucked you on the 7 april 2013 and We Are Back To Fuck You again...
We will strike any and all websites that we deem to be in Israeli Cyberspace in retaliation. The number o
attacked Israeli websites is approximately 10,000.
Op #Electorinic_Bader , Fallaga Special Operations Against Zionist , monkey brothers.
Cyber war has been declared on Zionist cyber space and you will see exactly what we are capable of.
Our Target is your Governement's Websites ... We Will Take You OFF From The Internet !
Your Credit Cards , Your Bank's Accounts , Your Servers , Your Facebook , Twitters ... Are In Danger !
We Never Forget what You Do against the Humanity ... In GaZa Millions OF People Were Dead ... Palastini
Muslims,Innocent Childrens, Womens Are Killed In The Force's Attacks...
Zionist Forces Destroyed Palestinian's Families , Homes ,schools, hospitals,mosks ... But No One Cares ! its
time to stop killing innocent peoples , and stop killing palastinians childs coz all da world know that zionist
the real terrorist.
Governement and Peopel of the thing named "Israel" will be a goal of Palestinian resistance rockets. To s
your self your Family... You MUST Forced your government to release every
prisoners on hunger strike... and to get out From Palestine Coz:
IN OUR MAPE IT WILL STAY PALASTINE FOR EVER , TILL WE DIE ..


جيش الفلقة الإلكتروني
HACKED BY darkshadow-tn
Tunisian Fallaga Team
#מוות לציונים | #Death To Zionist | #الموت لصهاينة
الرعد ما تـرون لا ما تسمعـون يا بني صهيون
اليوم حربٌ شاملة و غدا رسالـــة يا قتلة الاطفال يا قتلة الانبياء
اليوم موعدك و غدا اقسم لاسحبنك انت مكانو لصرف الصحي يا ابن اليهودية يا ابن الكافرة
ارحلو من ارضنا
فلسطين 27 الف كم مربع أن نفرط في حبة رمل
عمليـــة بـــدر الالكترونـــــية الفلاقـــة التونسيـــة
DON'T COLSE UR EYES IT IS NOT A DREAM IT'S A FUCKING REALITY UR WEBSITE HAS BEEN HACKED BY FALLAG GASSRINI & Dr LAMOUCHI
Hey Son OF "KaFira" This is a message from Tunisian Fallaga Team To the thing named "Israel" ... We Are They Same Persons who Fucked you on the 7 april 2013 , 2014 we Are AlFallaga Team Tunisian Cyber
Resistance and We Are Back To Fuck You again, We will strike any and all websites that we deem to be in Israeli Cyberspace in retaliation. The number of attacked Israeli websites is approximately 10,000.
Op #Electorinic_Bader , Fallaga Special Operations Against Zionist , monkey brothers.
Cyber war has been declared on Zionist cyber space and you will see exactly what we are capable of.
Our Target is you

In the framework of this attack, several Palestinian hackers posted reports on Facebook regarding breaches of the Web sites belonging to Bank Hapoalim, the Mossad and other Israeli government Web sites.[17]

- In the beginning of July 2015, the AnonGhost hacker group, which includes Islamists who express support for the IS, hacked into the Web site of the Malaysia Police Department and planted a photo with captions praising the Islamic State.[18]

[17] https://www.facebook.com/events/854253637998054/
[18] https://twitter.com/AnonGhost_MY

Review of Organizational Activities

During this period, members and supporters of the Islamic State continued to attack Web sites and social networks, and to leak the information obtained. In this framework, a virtual "spam campaign" was launched, which called on Islamic State supporters to report Twitter accounts belonging to opponents of the organization as spam in order to have them closed.

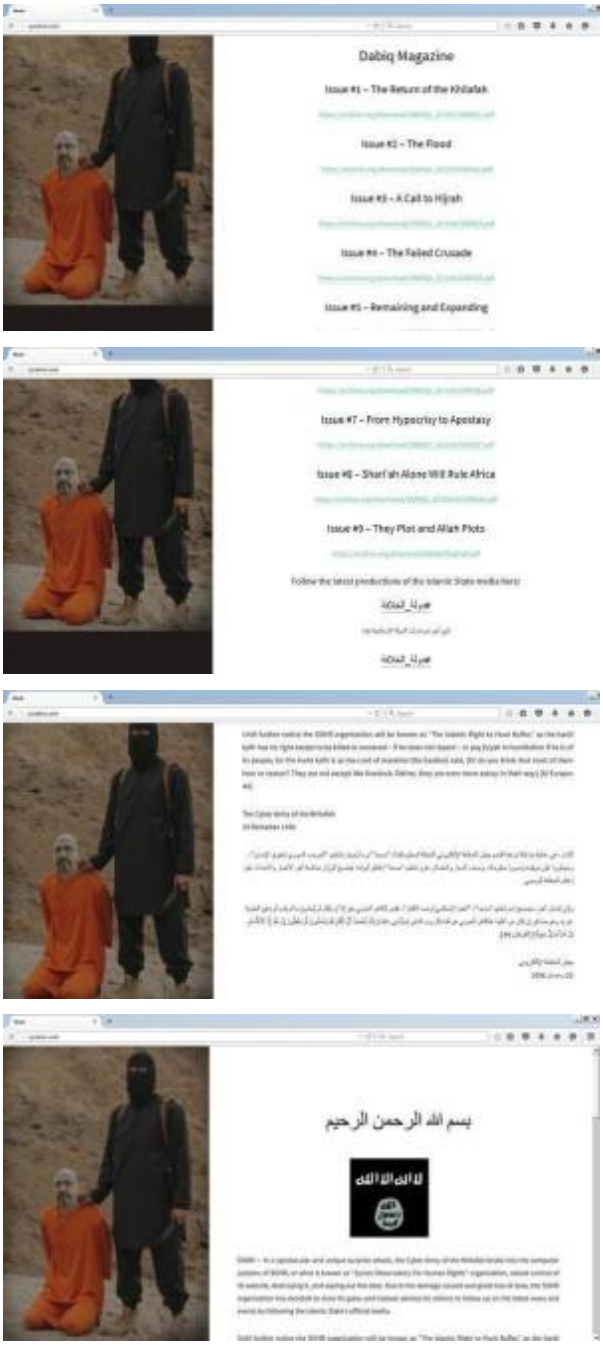
Another interesting development involved the darknet. Web sites serving the Islamic State were discovered, which indicates an increase in the technical capabilities of IS members as well as an effort to increase their anonymity in order to protect their identities from various authorities and security forces.

Islamic State affiliates

On the evening of June 8, 2015 a tweet[19] was posted, claiming that the Cyber Army of the Khilafa had hacked into the Web site of the Syrian Observatory for Human Rights, headed by Rami Abdulrahman, which is based in Britain. This may refer to a different hacker group or a different transliteration of the word "caliphate".

The message included four screenshots from the hacked Web site before its operation was terminated:

[19] https://twitter.com/activistm8/status/618827970984083457



On the same day, it was reported[20] that the Web site of the "Office of the State Minister of Georgia on European and Euro-Atlantic Integration" was hacked by the "Cyber Islamic State" and directed to a page documenting the breach. The breach was even documented on Google:[21]

[20] https://www.hackread.com/isis-hackers-euro-atlantic-integration-nato-site/
[21] http://zone-h.com/mirror/id/24559786?zh=1

The next day, it was reported[22] that the Web site of the Argonne National Laboratory – which is owned and funded by the Ministry of Energy and Science in the United States - was breached and a different address was planted (Argonne's Laboratory Computing Resource Center (LCRC)). This incident was also documented.[23]

In the beginning of July 2015, it was discovered that several different Twitter accounts attributed to Cyber Khilafah had posted a link to a Web site on the darknet that can be accessed using TOR. This site operates using TOR's hidden service protocol, which provides anonymity to the site owner and the user surfing the site. One can see that there are various accounts, in some of which the user names are significant and in others are just a sequence of letters. The content published on the accounts is identical and in Arabic. It could not be determined if there is a connection between Cyber Kahilafah and Cyber Caliphat. It is possible that the difference in transliteration is due to the difference between English and Arabic.

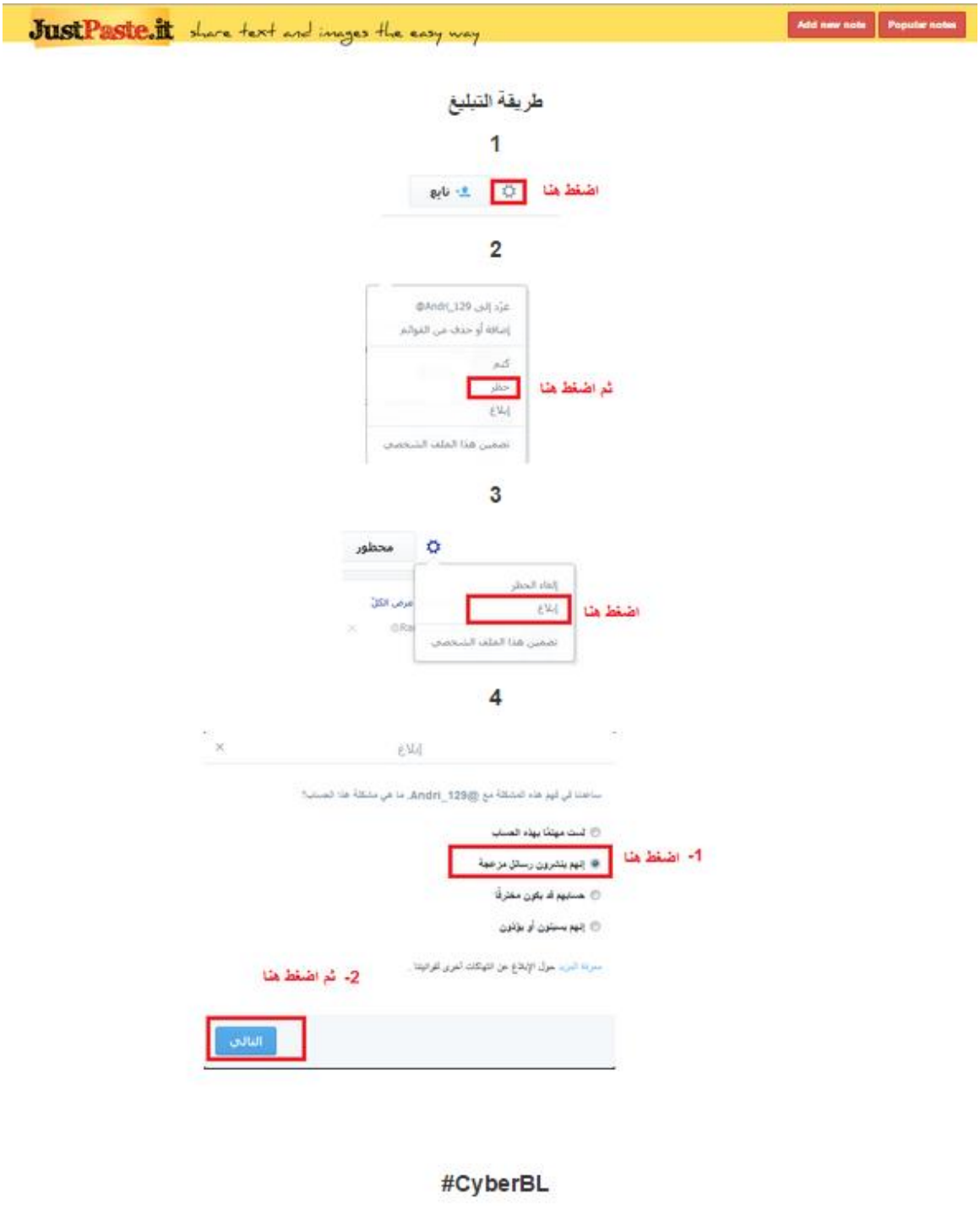
[22] https://www.hackread.com/pro-isis-hackers-us-dept-of-energy/
[23] http://zone-h.com/mirror/id/24569854

- Cyber Khilafah (@CyberyKahilafah)
- Cyber Khilafah (@Cyber43ahilafah)
- Cyber Khilafah (@Cyber49ahilafah)
- Cyber Khilafah 2 (@bLij81tvJFiP9Da)
- Cyber Khilafah (@CyberPKahilafah)
- Cyber Khilafah 2 (@bLij31IvJFiP9Da)
- Cyber Khilafah (@Cyber18ahilafah)
- Cyber Khilafah 2 (@bLi031IvJFiP9Da)
- Cyber Khilafah (@Cyber40ahilafah)
- Cyber Khilafah (@CyberoKahilafah)

Screenshot from Twitter

Information was also found about the "spam" operation against Twitter accounts that threaten the Islamic State, which received the hashtag "CyberBL". Since the start of 2015, IS fighters have taken a hit on Twitter, as members of Anonymous began to work systematically to locate, report and block accounts belonging to IS supporters. Members of the organization declared retaliation in a similar manner by reporting members of Anonymous as "spammers".[24] Some of the targets were members of Anonymous who participated in the OpISIS operation and some were targets were accounts of Saudi Web surfers. As part of these activities, Cyber Kahilafah posted a guidebook explaining, stage-by-stage, how to block a Twitter account by reporting it as spam.

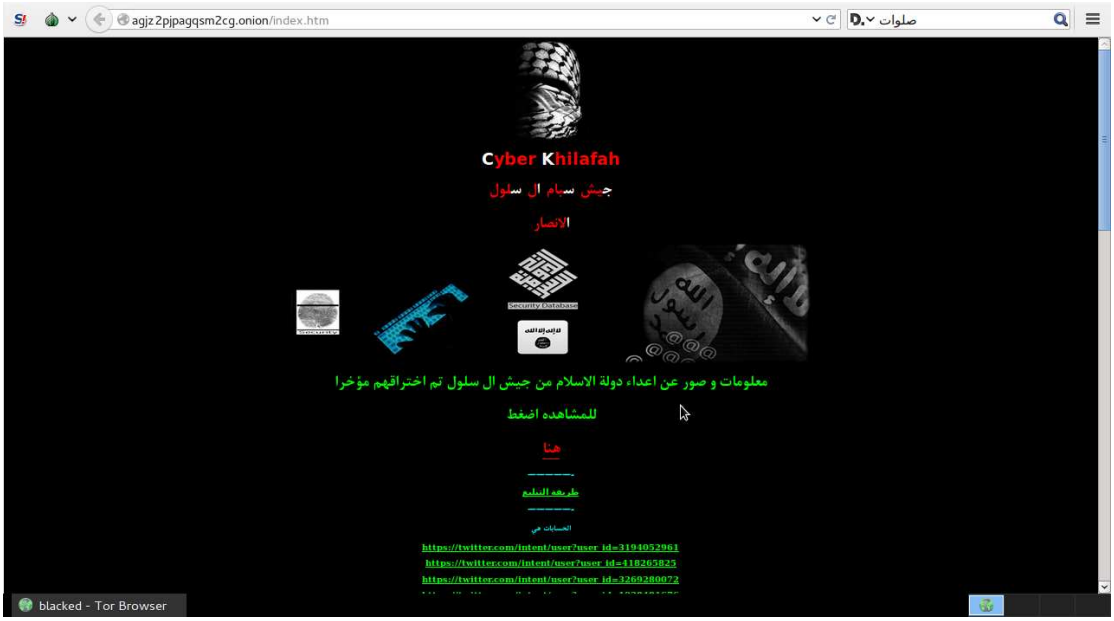
[24] http://varacyber.com/component/com_content/Itemid,101/catid,8/id,1503/view,article/



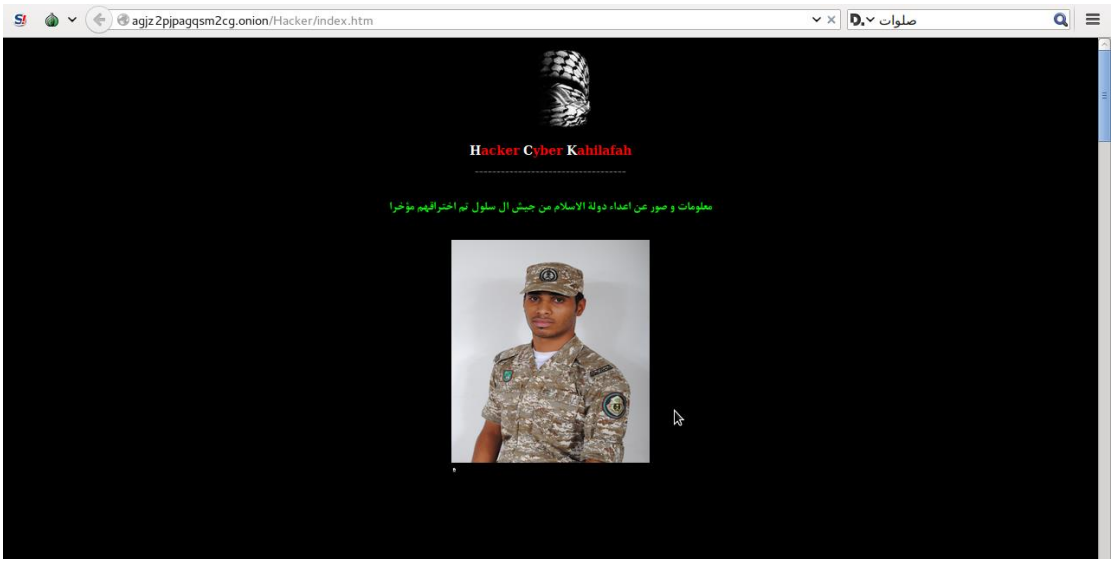
A guidebook explaining how to report a Twitter account as sender of spam

The Islamic State also left its print on a Web page on the darknet that included links to Twitter accounts marked as targets for blocking, as well as a link to another page containing photos of soldiers and officers in the Saudi Arabian army under the title, “Information and pictures that have

been recently hacked about the enemies of the Islamic State from the Āl Salūl [Saudi] army". It is very likely that these photos were taken from the Internet and do not reflect a leak of breached data.



The homepage on the darknet



A page containing photos of Saudi soldiers

In the early morning hours of August 13, a tweet[25] was posted on an account affiliated with the Islamic State according to which it would disclose the details of US army and government officials taking part in operations against the organization:

Later, another tweet posted on an account identified with the "Islamic State Hacking Division" provided three links to a Web page on the darknet containing the above-mentioned file:

The file itself opened with the following message:

[25] https://twitter.com/cyberkhaliphate/status/631625082264268801

The file contained 1,481 listings with the following fields: first and last name, unit, email address, password, location, zip code and telephone number. An examination of the listings revealed that many of them belonged to US army and government units, including military and diplomatic representatives around the world.

On August 28, an announcement[26] was posted by individuals identifying themselves with the "Islamic State Electronic Army" in which they claimed to have carried out another leak containing the details of US army personnel:

The list contained the details of 36 US army personnel from Afghanistan, Kuwait and Iraq, including: full name, unit, city, zip code, cell phone number. However, this list also contained several duplicate names.

In the beginning of September, it was reported that members of the IS had managed to hack into the email accounts of British Cabinet ministers. It is believed that the breach was carried out in order to collect intelligence information that would enable an attack against the royal party. Among the suspected attackers was Junaid Hussain, a hacker who grew up in Britain, who was accused of

[26] http://justpaste.it/usarmyarab

hacking into the email accounts of Tony Blair and fled to Syria.[27] According to the United States, Hussain was responsible for recruiting supporters of the organization to carry out attacks against Americans, as well as for leaking data about army and government officials. On August 24, Hussain was killed in a US air strike in the area of Raqqah, Syria.[28] In mid-October, it was reported that a hacker named Ardit Ferizi, who was from Kosovo but lived in Malaysia, was involved in the leak of details about US army soldiers after a successful breach of the servers of a civilian company that contained records about the soldiers. After an extortion attempt and ransom demand in order to avoid the release of the materials, the hacker made contact with two known IS members and sent them the information. The information was leaked under the accounts: Islamic State Hacking Division and Cyber Chaliphat.[29] The report reinforces the assessment according to which hackers with ability and experience can join forces with terrorist organizations and significantly improve their ability to carry out attacks.

Islamic State Supporters

During this period, we continued to see operations carried out by individual hackers and hacker groups that support the Islamic State, as well as announcements on social networks claiming responsibility for the breaches of Web sites and accounts belonging to companies and official institutions of countries throughout the world. These messages were designed to scare the public and to threaten more cyber-attacks, but most served only as psychological warfare and did not pose a real danger.

Phénoméne Dz is a pro-IS hacker located in Algeria (DZ is the domain name for Web sites in Algeria) who targets Western countries allied with NATO. He has hacked Web sites in Egypt, Syria, Iran, Ukraine, Brazil, Serbia, United States, and Barbados. His main activity is Web site defacements.[30]

- On August 9, *Phenomene Dz* defaced the Web site of the Accademia della Crusca, an Italian language research institution. The hacker left IS-related symbols on the Web site, as well as

[27] http://www.dailymail.co.uk/news/article-3231740/Government-ministers-emails-hacked-ISIS-Jihadis-plot-assassinate-politicians-royals-uncovered-GCHQ.html
[28] http://www.defense.gov/News-Article-View/Article/615305/iraq-progresses-in-isil-fight-key-extremist-confirmed-dead
[29] http://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges
[30] http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/phenomene-dz-a-pro-isis-pro-palestinian-hacker-from-algeria/

images of injured children, a video, and language praising the IS. He also left the following message in English: "When America and Iran Zionists kill Muslims in Iraq, Palestine, Afghanistan, Vietnam ... no one hears your average barking. But when the Islamic state is to defend ourselves ... you respond with alliances! And we will respond with suicide bombings! I defend my religion, my brothers and sisters because your government is the real terrorist! With his support and his silence! This war has just begun ... and Insha Allah it will be for us." The Web site was defaced for about 24 hours.[31]

AnonGhost is a hacktivist collective of around 15 pro-Palestinian hackers based throughout Africa, the Middle East, and Europe.[32] They have brought the fight against Israel to the cyber arena, and hack government, military, and civilian Web sites in both the United States and Israel in support of freeing Palestine. *AnonGhost's* main activities are defacements and the utilization of malware to steal and dump sensitive information.

- On July 13, *AnonGhost* hacked the Twitter and Facebook accounts of the Malaysian Police and flooded the feed with pro-IS messages. The profile picture and cover photo of the Facebook page were changed to an image of a gunman waving an Islamic flag with "Khilafah has returned" printed on it. Also posted on the Facebook page was an image of militants alongside the words "Viva Islamic State!" *AnonGhost* initially began as a pro-Palestinian group, but has shifted to support IS ideology as well.[33]

Lov3rDns is a Yemen-based hacker that has been active since 2012. He has targeted the United States and Saudi Arabia in the past and is known for hacking several official Web sites of major businesses such as Coca Cola, Firefox, McAfee, and Avast Security.[34] Lov3rDns's activity includes Web site defacements.

- On July 11, *Lov3rDns* defaced the official social network domain of President Barack Obama. The defaced message left on the web site insulted Obama with the N-word and told him to

[31] http://www.lastampa.it/2015/08/09/italia/cronache/hacker-dellisis-allattacco-dellaccademia-delle-crusca-questa-guerra-appena-iniziata-sNlipLpz3qtzyh0YfCR7zK/pagina.html
[32] http://www.ibtimes.co.uk/anonghost-hackers-deface-un-website-following-al-asqa-mosque-tensions-1474258
[33] https://www.hackread.com/isis-hackers-malaysia-police-facebook-twitter-hack/
[34] http://www.meethackers.com/2015/07/barack-obama-hacked.html#.VjpGlYSu9nk

leave Yemen alone, and included a Yemeni flag. The hacked subdomain was used during Obama's presidential campaign and has been hacked more than once.[35]

Moroccanwolf is a hacker from Morocco with over 10,000 known defacements. It is not clear if it is a person or a group. It is considered pro-IS as it has used IS content as part of its defacement attacks. Most of the attacks were mass defacements.[36]

- On August 26, *Moroccanwolf* defaced a UK National Health Service site in protest of the lack of humanitarian involvement by Western governments in the Syrian conflict. The message left on the Web site read: "Hacked by Moroccanwolf. Message to the Government: this site has been hacked because of the world's silence about the three years of massacres that occur in Syria and this still happening. This security breach is not to make damage, it is only to…" and the rest of the message is unfinished. A YouTube video was also posted that covered similar material.[37]

IS-affiliated hackers take on several different forms, but several individuals and collectives do not self-identify with a moniker or group name. Therefore, not much is known about them.

- On September 2, hackers claiming to be part of IS defaced the Wayne County Board of Education Web site. The hack involved redirecting users who tried to access the Web site to another Web site promoting terrorism.[38]
- On September 11, hackers affiliated with the IS hacked into UK ministerial email accounts. The hack was a sophisticated espionage operation that was uncovered by a security company. The hackers targeted information held by David Cameron's senior ministers, such as details about events that government members and members of the Royal family were expected to attend. Names, email addresses and passwords of Foreign Office staff were stolen and leaked by the hackers.[39]

Additional Groups

[35] https://www.hackread.com/obama-election-social-network-hacked-yemen-hacker/
[36] http://kevin.borgolte.me/notes/team-system-dz-isis-isil-defacement-campaign/
[37] http://www.theregister.co.uk/2015/08/26/nhs_site_defaced_with_screed_protesting_syrian_conflict/
[38] http://www.statejournal.com/story/29943796/hacker-claiming-to-be-part-of-islamic-state-hacks-wayne-county-wv-board-of-education-website-redirects-visitors-to-site-promoting-terrorism
[39] http://www.telegraph.co.uk/news/politics/11859005/Cabinet-ministers-email-hacked-by-Isil-spies.html

The following is a summary of operations carried out by individual hackers and hacker groups against various targets. Most of the attacks involved Web site defacement and the dissemination of political messages against governments around the world. These operations continued to include content related to the Israeli-Palestinian conflict and the situation in Syria. Most of the attacks involved Web site defacement and did not present significant risk or harm.

AlfabetoVirtual appears to have emerged in June of this year. The hacker is a pro-Palestinian individual who hacks Web sites all over the Western world to perpetuate a pro-Palestine, pro-Gaza message. Some of his targets include: the United States, Canada, Spain, Germany, England, Brazil, South Africa, Italy, and France.[40] His only activity is Web site defacements.

- On July 10, *AlfabetoVirtual* defaced the official web site of New York City Comptroller, Scott M. Stringer. While the hacker bypassed all security restrictions, it could not deface the entire Web site. A short message of support for Palestine was left on the site's header and the site's description was changed to "Hacked by AlfabetoVirtual." Based on the wording of the defacement, it appeared the hacker was a Spanish speaker, perhaps based in Argentina.[41]

Dr.MwNs is likely a Syrian hacker whose main target is Turkey. Besides the understanding that his main activity is Web site defacements, more information about *Dr.MwNs* is not available.

- On August 5, *Dr.MwNs* hacked the official Web site of the Sri Lankan Prime Minister. *Dr.MwNs* defaced the Web site in the name of #ForSyria, and left a "Hacked by Dr.MwNs" note on the homepage. The hacker also had an Arabic song playing in the background.[42]

JM511 is a Saudi Arabian hacker that has targeted Web sites in the United States, Germany, Ukraine, Denmark, Vietnam, the United Kingdom, Canada, South Korea, and Russia.[43] JM511 has been hacking since at least 2004 and his main activities include Web site defacements and SQL injections to steal sensitive data.[44]

[40] http://www.zone-h.org/archive/notifier=AlfabetoVirtual
[41] https://www.hackread.com/palestinian-hacker-new-york-comptroller-office/
[42] https://www.hackread.com/sri-lankan-prime-ministers-office-website-hacked/
[43] http://www.zone-h.org/archive/notifier=JM511/page=21
[44] https://krypt3ia.wordpress.com/2014/03/14/assessment-team-jm511/

- On August 8, *JM511* hacked the Employment Agents Movement (TEAM), the largest network of independent recruiters. He dumped 2613 records in a massive data breach. JM511 bypassed security, and accessed and leaked the login credentials of thousands of registered recruitment agencies. He used SQl injection vulnerability to access the server.[45]
- On August 23, *JM511* hacked AutoZone's web site and dumped 49,967 customers' details with an SQLi attack. AutoZone is a leader American retailer of auto parts. The details included billing addresses, email addresses and passwords, telephone numbers, customers' cities, and dates of birth of thousands of customers. No financial data was dumped.[46]
- On that same day, *JM511* dumped data from the University of California at Los Angeles after warning the university twice. The hacker also warned other universities of potential hacks. In the data dump, JM511 included user ID's, usernames, passwords, and email addresses. The attack was conducted via SQLi, and the initial warning message read: "You've bEEn #warned #2times @UCLA."[47]

Mr.H4rD3n is a hacker whose loyalties are unclear. His hacks mostly concern the Syrian conflict and he may be based somewhere in Morocco.[48] His main activity is Web site defacements.

- On August 13, *Mr.H4rD3n* defaced the official Web site of the Embassy of Azerbaijan to Russia. The defaced message was a statement opposing the conflict in Syria: "Hacked? Mr.H4rD3n is coming for you…free Syria and leave the war for Syrian motherfuckers." It was unclear which side of the Syrian conflict the hacker was in support of.[49]

RootDevilz, Jonturk75, and *Bozkurt97* are a group of Turkish hackers allegedly opposed to many Western and democratic nations for their certain actions or inactions in worldwide conflict. Some of their targets include Israel, India, China, the UN, the EU, and several major companies in the United States. Their only activity is Web site defacements.

- On August 16, *RootDevilz, Jonturk75,* and *Bozkurt97* defaced the official Web site of Unicef India with a message against China, the United States, the UN, the EU, and Israel. The

[45] https://www.hackread.com/uk-recruitment-portal-data-breach/
[46] http://www.databreaches.net/50000-autozone-customers-data-hacked-exposed/
[47] http://www.databreaches.net/more-american-universities-hacked-by-jm511/
[48] https://www.youtube.com/watch?v=Sy71wMHFJV4
[49] https://www.hackread.com/azerbaijan-embassy-russia-hacked-syria/

defaced message was left in both English and Turkish and read: "Unicef India owned. Hearts a petrified monster Israeli Zionists. You will find us in the face of all the games you've played." The hackers were asked why they would hack the Web site of a humanitarian institution. They said their only reason for targeting the Web site was to deliver a message to China, which is behind the massacre of Uyghur Muslims in the Xinjiang region of China; the United States for killing people around the world; the EU against immigrants; Israel for killing Palestinians; India for killing Kashmiris; and the UN for not taking action against any of them.[50]

Mr.Xpr! is an individual from the Iran Hack Security Team who is allied with Yemen and opposed to Saudi Arabia. Aside from hacking Web sites in Saudi Arabia, *Mr.Xpr!* has targeted the United States and Iran in the past. This specific hacker of the Iran Hack Security Team is not that active, and his main activity is Web site defacements.[51]

- On August 21, *Mr.Xpr!* defaced the official Web site of the Royal Saudi Air Force. The defaced message simply said: "Hacked by Mr.Xpr! Iran Hack Security Team." The hacker stated the reason for targeting the Saudi Air Force Web site was to protest against the Saudi-led war in Yemen, saying: "We want Saudi Arabia to stop killing people in Yemen. We will keep on targeting Saudi defense related sites."[52]

Anonymous

This collective targets governments throughout the United States, Israel, Europe, and even as far east as India. Anonymous' main activities are denial of service attacks, defacements, and the theft and dumping of sensitive information. The collective has several affiliate groups that operate against governments, regimes and terrorist organizations, such as the Islamic State. Those operations include Web sites defacements, network disruption, and information leaks.

- On July 2, Anonymous, in the name of *@OpBill-C51*, hacked the Quebec Parental Insurance Plan Center, the Ministry of Labor, Employment, and Social Solidarity, and the National Review Commission Web sites. C-51 is a controversial anti-terror bill. Anonymous leaked the

[50] https://www.hackread.com/unicef-india-website-turkish-hackers/
[51] http://www.zone-h.org/archive/notifier=Mr.XpR
[52] https://www.hackread.com/saudi-airforce-hacked-iranian-hackers/

data it collected online, which contained databases of the targeted Web sites, last names, thousands of email addresses, along with their matching passwords. Since the passage of the controversial bill, Anonymous has hacked and breached several Canadian Web sites in protest.[53]

- On July 3, *AnonOpsIndia* hacked India's Bharat Sanchar Nigam Limited (BSNL). *AnonOpsIndia* is affiliated with Anonymous. The hack was a protest against the Indian Government's stance on net neutrality and the way it is handling Digital India, and it involved injecting several documents to BSNL's server and replicating the entire BSNL database, which has sensitive data of over 30 million users. When asked about the hack, the group said it was not happy with the way the Indian Government has been trying to integrate government departments with the people of India: "The government, instead of spending taxpayers' money on surveillance projects to snoop on taxpayers, should spend that money on hiring security experts who would keep data secure." Part of the hack mocked the administrators of the BSNL Web site, admonishing them for their shoddy online security.[54]
- On July 12, Anonymous released a series of emails that showed a conservation officer defending his decision to refuse to kill two black bear cubs on Vancouver Island. Early in July, conservation officer Bryce Casavant was suspended for refusing to kill two black bear cubs after their mother was killed. He believed the cubs could be rehabilitated and took them to a nearby veterinarian hospital, rather than killing them. The chief information officer from the Ministry of Environment said there was no proof the government's email system had been hacked.[55]
- On July 12, Anonymous hacked an Indiana radio station and broadcast a message. The signal was intercepted at 7:30pm on a Sunday night, and Anonymous broadcast a message for 30 minutes before the music playlist was returned. Part of the message said: "We are Anonymous. We would like to take a few minutes of your time to inform you about the United States Governments' plan to murder over 100-million citizens. The United States of

[53] https://www.hackread.com/anonymous-breaches-canadian-government-servers/
[54] http://betanews.com/2015/07/04/bsnl-india-hacked-anonymous/
[55] http://www.cbc.ca/news/canada/british-columbia/anonymous-hackers-release-emails-ordering-bear-cubs-be-killed-1.3147003

Secrecy has kept you all blind." The radio station was unable to identify where the transmission had originated.[56]

- On July 18, Anonymous crashed the Royal Canadian Mounted Police Web site in a denial of service attack. It stated the hack was in response to the shooting death of a member of Anonymous in a police shooting in Dawson Creek, British Columbia, Canada. The group also threatened to release the identity of the police officer that was involved in the shooting of the Anonymous member.[57]
- On July 22, Anonymous hacked into the network of the tribunal that adjudicates disputes between public servants and the Canadian federal government. It was unclear whether or not any personal information had been stolen or leaked in the hack, or if anything was taken at all. It was also unclear as to how long the hackers were in the system.[58]
- On July 23, Anonymous hacked the United States Census Bureau and leaked the details of 4,200 employees. The leaked information included names, passwords, email and physical addresses, phone numbers, and positions within the government. Anonymous stated that the reason for the attack was in response to the Trans-Pacific Partnership (TPP) and Transatlantic Trade and Investment Partnership (TTIP), which are priorities for the Obama Administration. They promise reform of the global political-economic system by converging Atlantic and Pacific nations. Anonymous specifically opposed the secret manner in which the agreements were drawn up. The US Census Bureau responded and said none of the stolen information was confidential.[59]
- On July 25, Anonymous claimed to have breached secure Canadian computers and accessed classified national security documents. The hacktivist collective said the hack was in retaliation for a fatal shooting of an Anonymous protestor in British Columbia. Additionally, the group threatened to disseminate the sensitive documents if the officer who shot the protestor was not promptly arrested. This hack suggested a "deeper penetration of a higher

[56] http://wthitv.com/2015/07/13/we-are-anonymous-we-do-not-forgive-we-do-not-forget-radio-station-investigates-hack/
[57] https://www.hackread.com/anonymous-targets-canadian-police-rcmps-website/
[58] http://www.orangeville.com/news-story/5753454-federal-tribunal-targeted-in-cyberattack/
[59] http://www.ibtimes.co.uk/anonymous-hacks-us-census-bureau-over-ttip-agreement-leaking-employee-details-online-1512244

echelon of government computers containing far more sensitive information."[60]

- On August 2, Anonymous hacked and shut down several Taiwanese Government Web sites in the name of OpTaiwan. They said the hacks were just the beginning of a series of larger attacks to come. Some of the hacked Web sites included the Office of the President, National Academy of Education Research, Ministry of Education, and Ministry of National Defense. The attacks were denial of service attacks, which effectively shut down the Web sites for several hours. Anonymous members from China, Hong Kong, Taiwan, Canada, and the United States coordinated this particular attack.[61]
- On August 8, an Anonymous affiliate by the name of *MexicanHTeam* defaced the Web site of the Mexican Ministry of Communications and Transportation. The hack was in retaliation for the murder of a Mexican photojournalist. The Web site was defaced with the message: "Justice for Ruben," and the group tweeted and mocked the Mexican government's lack of ability to protect their own Web sites.[62]
- On August 12, Anonymous hacked the South African government contractor State Information Technology Agency and leaked its entire database. Anonymous carried out the attack in the name of *#OperationSA* and *#OpMonsanto*, which is a campaign against the sudden change in Internet censorship and Monsanto's (an agricultural company) dominance in the country. Through an SQLi attack, the leaked data was divided into four parts and contained records of full names, usernames, emails and passwords, addresses, phone and fax numbers of officials, and full names and phone numbers of South African government officials. According to Anonymous: "We will fight Monsanto and its poisonous food products. We want to make sure the South African people are not alone in this war against human rights abuses and Internet censorship laws."[63]
- On August 18, a hacker affiliated with Anonymous hacked the Clayton Valley Charter High School in California. The hacker sent an email to county education officials to alert them to "corruption and manipulation." The hacker attached emails between school staff members,

[60] http://news.nationalpost.com/news/canada/anonymous-says-it-hacked-canadas-security-secrets-in-retaliation-for-police-shooting-of-b-c-activist
[61] https://www.hackread.com/anonymous-brings-down-taiwan-govt-websites/
[62] https://www.hackread.com/anonymous-mexico-ruben-espinosa/
[63] https://www.hackread.com/opmonsanto-anonymous-hacks-south-african-govt/

police, and county officials, but the content of the emails was not revealed.[64]

- On September 18, Anonymous shut down all of the Web sites operated by Embarcadero Media Group, which runs several newspapers in the Bay Area in San Francisco. The Palo Alto Weekly, The Almanac, Mountain View Voice and Pleasanton Weekly were all targeted in the hack. A picture was posted of a figure in a Guy Fawkes mask and the following message: "Embarcadero Media Group (Almanac) has failed to remove content that has been harmful to the wellbeing and safety of others. Failure to honor all requests to remove content will lead to the permanent shutdown of all Embarcadero Media Group Websites. We do not forgive, we do not forget, we are legion." The sites were down for over a day.[65]
- On September 19, *AntiSec* and *HagashTeam*, both Anonymous affiliates, defaced eight Vietnamese government Web sites against online censorship and human rights violations in Vietnam. The defaced message spoke to the fact that on the 70th anniversary of independence, the Vietnamese government released over 18,200 prisoners but none of them were political prisoners. The hackers claimed to stand with the repressed citizens of Vietnam.[66]
- On September 22, Anonymous hacked the Web site of the Philippines' National Telecom Commission. The collective defaced the site as a form of protest against the slow local Internet connection speed. The Internet connection in the Philippines ranks only above Afghanistan and is atrocious when compared to other Asian countries. Part of the message left on the Web site read: 'We are calling forth the attention of the National Telecommunications Commission for this matter in hand…we are asking for fairness in charging and serving our data services."[67]
- On September 25, Anonymous leaked a high-level confidential federal document as part of their recent vendetta against the Canadian government. They released the document to ten media organizations. The document contained information about the redevelopment of

[64] http://www.databreaches.net/ca-anonymous-responsible-for-clayton-valley-charter-high-computer-hack/
[65] http://www.nbcbayarea.com/news/local/Anonymous-Cripples-Silicon-Valley-East-Bay-Community-Newspaper-Websites-328255691.html
[66] https://www.hackread.com/anonymous-hacks-vietnam-government-against/
[67] http://news.softpedia.com/news/anonymous-defaces-philippines-telecom-commission-website-protesting-slow-internet-speeds-492336.shtml

Canada's key diplomatic centers in Britain. This was the second Canadian document leaked by Anonymous, and called into question the level of security surrounding Canadian infrastructure.[68]

- On September 27, *Ghost Italy* hacked Banca Intesa and Unipol Banca, two major Italian banks, and dumped several databases related to external contractors. *Ghost Italy* is a local cell of Anonymous and hacked the banks in the name of *#OpBankDump* in an SQLi attack. Over 6000 emails, phone numbers, user names and passwords of users, employees, and corporate clients of the banks were dumped. The hacktivist collective stated, "The attack was made to show much they do not take our data and our privacy, they pay without money million Euros to protect us and at the end they do it in vain."[69]

Cyber-Crime and Cyber-Terrorism, July-September 2015

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")[70] Internet between July - September 2015.

[68] http://news.nationalpost.com/news/canada/anonymous-leaks-another-high-level-federal-document-as-part-of-vendetta-against-government

[69] http://www.repubblica.it/tecnologia/2015/09/28/news/anonymous_opbankdump_unipol_intesa-123815381/?ref=HRER2-1&refresh_ce

[70] 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.

The US and UAE Establish a Digital Communications Center to Counter the Islamic State

On June 8, 2015 the US Media Department announced the launch of the Sawab Center (in Arabic: "correct path") in collaboration with the UAE.[71] This center is supposed to serve as a response to Islamic State online propaganda by publishing content and disseminating moderate messages against the organization. The center will promote additional relationships with countries participating in the coalition against the IS, which was established in September 2014, as well as with private and business entities around the world. The center will also be involved in spreading the messages of those who are willing to speak out against terrorist propaganda, methods of recruiting manpower and money, and to expose the true nature of the organization.

In the framework of these activities, a Twitter account[72] was launched in the beginning of July with messages in English and Arabic. The second message, in English, defined the goal of the center:[73]

The use of both languages indicates that the site is directed at Arabic-speaking Muslims and to young people in the West who could be influenced by IS propaganda or serve as potential recruits. It should be noted that the account does not make an effort to hide who stands behind it – on the contrary, it is identified with official US authorities (the account includes a number of tweets from President Obama) and the UAE (the account mentions donations and humanitarian activities carried out by Gulf countries for refugees and the like).

An analysis of the account's content revealed that it is focused on the following messages:

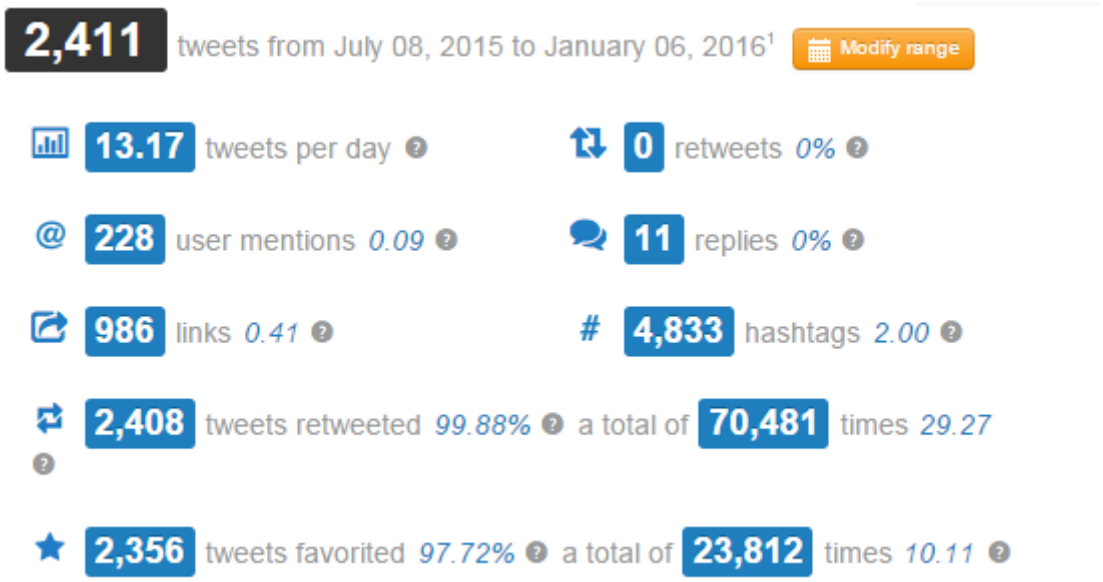
- Practical guidelines on how to report IS Twitter accounts in order to get them shut down.[74]

[71] http://www.state.gov/r/pa/prs/ps/2015/07/244709.htm
[72] https://twitter.com/sawabcenter
[73] https://twitter.com/sawabcenter/status/618722930579484672
[74] https://twitter.com/sawabcenter/status/695862607274602497

- Updates on the progress of the military struggle against the IS in the field and on counter-terrorism operations around the world (arrests, dismantled terror cells, etc.).
- Descriptions of IS operations and propaganda as brainwashing.
- Claims according to which the IS is in bad shape (both militarily and financially).
- Display of the suffering of the civilian population under IS control (for instance, Yazidi women, the Kurds, children, etc.).

The following English and Arabic hashtags can be found on the account: "Stop IS Propaganda" (#أوقف_دعاية_داعش), #ForceOfHumanity, #UnitedAgainstDaesh, and more.

An analysis of the posts on the Twitter account through the end of 2015 revealed that the account gained approximately 29,000 followers, had approximately 13 tweets per day, and each tweet was shared approximately 30 times, on average, which increased its exposure.



Data about the Twitter account activity[75]

[75] http://www.twitonomy.com/profile.php?sn=sawabcenter

Favorite tweets on the Twitter account[76]

EU Internet Referral Unit at Europol

In the beginning of July, Europol launched the European Union Internet Referral Unit (EU IRU) as part of the decision made by the EU to respond to the propaganda spread on the Internet,

[76] http://www.twitonomy.com/profile.php?sn=sawabcenter

especially on social networks. On March 12, 2015 the Council of Ministers decided to establish the unit based on the "Check-the-web project". This project, which began to operate in 2007, includes the documented portal, and maps Web sites and Islamic propaganda content. The portal is available to law enforcement authorities in 28 countries belonging to the EU.[77]

The job of the new unit is to provide a response to the extensive activity on social networks by identifying propaganda content and reporting it to the service providers in order to have it shut down.[78] The new unit began its operation with approximately 15 experts from national authorities throughout the world and plans to enlarge its numbers through July 2016. This unit joins a series of actions taken by the EU as part of its war on terror, and its operations against IS members and supporters among EU nations and on the Internet.

Developments and Trends in the Banking Sector

During this period, several attacks against the financial and banking sector were reported, demonstrating an increase in the level of planning as well as in the complexity of attacks and fraud around the world. Among other things, there were complex APT attacks by criminal groups, which included tracing employees of the organization, that combined with DDoS attacks to create a smoke screen; a new malware that, in addition to stealing financial data and credit card details, protects the system from other new malwares; and a new attack by the Carbanak group that had previously claimed to have stolen over one billion dollars from 100 financial institutions around the world.

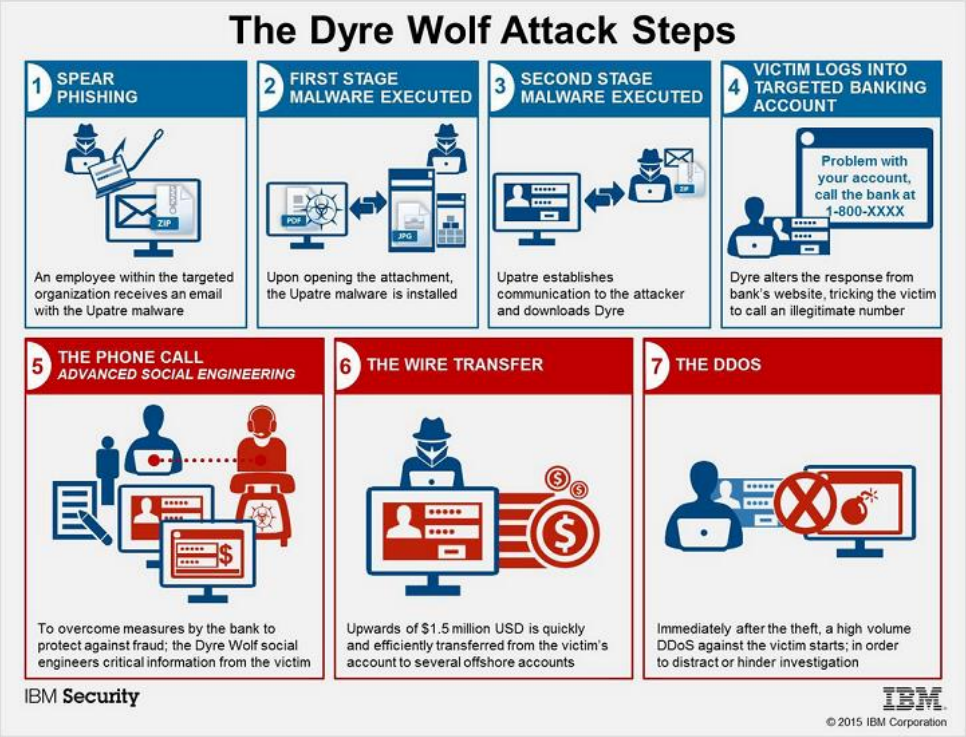
- On July 14, a study by IBM was published about a Trojan Horse malware called "Dyre",[79] which attacked 17 banks in Spain to date. The new update expands the capabilities of this malware, which in its previous version attacked only 3-5 banks based in Spain, in an apparent trial run prior to the real attack, which also included banks in Spanish-speaking countries such as Chile, Colombia and Venezuela. This malware attacked throughout Europe, first in Britain, France and then Spain, causing companies in Spain 14 billion Euro worth of damages as a result of cybercrime in 2014.

[77] http://data.consilium.europa.eu/doc/document/ST-7266-2015-INIT/en/pdf
[78] https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda
[79] https://securityintelligence.com/dyre-malware-takes-summer-holiday-in-spain/

The malware's name is derived from the sentence *"I am Dyreza"*, which is found in the lines of code and represents RAT activity that began in mid-2014. At that time, the goal was only to bug encrypted access details. Since then, it has quickly developed in an aggressive manner, both technically and criminally, turning it into one of the most advanced malware that exist today due to its extensive capabilities and constant updates designed to avoid various detection mechanisms, including anti-virus software.

These attacks constitute a combination of APT and fraud, during which the hackers obtain intelligence about the target organization while investing resources in breaching its systems and laying the groundwork for fraud activities before implementing the extensive money transfer. The group included a team that focused on identifying a pattern of work by bank employees for future phishing purposes in order to bypass the system that identifies anomalies. The attack was executed in several stages: A spear phishing attack in which the malware was spread in a targeted fashion to employees of the organization via an email containing the infected file. When the employee opened the file, the malware installed on the computer and created a connection between the computer and the hacker, which enabled the hacker to update and install additional malware remotely in order to locate the necessary details and data to execute the money transfers. After collecting the information, transfers to overseas bank accounts were executed. After the transfers were completed, a DDoS attack was carried out on the organization in order to distract the persons charged with maintaining the organization's system.

- The attack involved "workers" who implemented the fraud itself in shifts between Monday and Friday, from morning to evening, according to the time zones in the United States, as well as a team dedicated to carrying out the major scams, bank accounts and especially large money transfers between 500,000 to 1.5 million dollars. Since the big scams were carried out simultaneously as the small operations, the assumption is that there was a separation between the various teams.



- It was also assumed that the team was located in the Ukraine or Russia based on the work hours and the fact that 80% of the servers' malware's servers have IP addresses from those countries.

  The study also revealed that the strength of malware can modify the behavior of the browser in an immediate and specific manner according to the target bank of the attack, while sending the victim to a fake Web site prepared by the hackers ahead of time for this purpose and maintaining the SSL connection with the active bank only in order to create the false impression of a real and secure bank Web site. In this way, the manipulation of the bank's page was carried out in a dynamic manner.

  The company's experts recommend that banks warn their online banking customers, and ask them to report any suspicious email and to work with their fraud prevention service provider in order to reduce the malware risks as much as possible.

- On August 31, IBM's security investigators reported[80] a malware named "Shifu" that, according to estimates, was already active in April 2015. According to

[80] https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/

investigators, this malware mainly attacked banks in Japan - approximately 14 banks - and selected platforms of online banking throughout Europe, mostly Germany and Austria.

This malware is considered the most sophisticated Trojan horse for the banking sector, as it is based on and integrates software from known malware. It was also found that the malware comes in basic configuration to which additional components are added after establishing contact with the command and control server. This malware steals a broad spectrum of information that the victim uses for identification purposes in different ways. This enables the hackers to use the victim's confidential access information in order to take control of his bank accounts among the various service providers.

However, in addition to the hackers' desire to use the bank accounts of the victims to commit fraud, they also target various credit cards using POS. If the malware detects one, it collects the credit card details. In addition, it searches for digital signatures produced by the relevant authorities for bank users, especially in Italy, in order to commit bank fraud based on valid digital signatures. By attempting to hack bank applications rather than specific Web sites, the attack becomes more general and applicable to many more targets.

Nevertheless, it was reported that the bank's homepage is sometimes replaced in its entirety by the malware as part of a phishing attack in order to gather data about the users to be used at a later date.

An unusual characteristic of this malware is a tool to protect it from the installation of suspicious files in order to prevent other malware from penetrating the system and disrupting the hackers' activities.

Regarding the source of the malware, the investigators found notes in Russian, meaning that the malware's developers are either Russian speaker or residents of the Former Soviet Union. However, it is equally possible that the notes were designed to obscure the true origin of the developers.

- On September 2, it was reported that a group identifying itself as "Carbanak",[81] which was apparently responsible for one of the largest cyber thefts estimated at over one billion

[81] https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

dollars, had returned to operation.[82] This time it seemed that the goal of the malware was to attack large companies in Europe and the United States by hacking the svchost.exe process, which enables it to remain in the system's memory. The new malware was also found to be equipped with a designated protocol, and uses a preset IP address, folder and file names and "new geographical targets". Two additional plugins were also detected: wi.exe, klgconfig.plug. Despite the fact that this is the first new version of this malware, the study noted that at least four strains of the malware were discovered against "financial agents in large international companies". The study defines Carbanak as "financial" APT focused on small numbers and designed to slip under the radar.

Developments and Innovations in Cyber Fraud Methods

According to an FBI report on frauds carried out via business email compromise, approximately 8,200 victims were reported between October 2013 and August 2015, with damage in the amount of approximately 800 million dollars. The damage worldwide during that period was estimated at 1.2 billion dollars. It was also noted that there was a 270% increase in incidents reported since January 2015.[83] According to the report, one can see a trend towards an increase in phishing scams using fake email delivery posing as a source familiar to the victim, in which an email is sent with a link to the malware enabling access to the computer, including passwords and information about financial accounts. Another fraud method that was identified involves instances in which a fake email message is sent impersonating a lawyer or representative of a law firm on an issue requiring immediate attention. The email sender puts pressure on the victim to act quickly and transfer the required amount of money in order to take care of the issue, while some of the correspondence is sent under false pretenses to company officials, including CEO, CFO, etc.

- On August 4, the company, Ubiquiti Networks, published a message[84] to the United States Securities and Exchange Commission (SEC) according to which it was the victim of fraud in which the criminals impersonated a company employee and made fraudulent requests to an external entity from the company's financial department. This fraud led to the transfer of a

[82] https://www.csis.dk/en/csis/blog/4710/
[83] https://www.ic3.gov/media/2015/150827-1.aspx
[84] https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm

total of 46.7 million dollars from the company in Hong Kong to worldwide accounts held by third parties. When the fraud was discovered, the company took steps that led to the return of 8.1 million dollars from the total amount that was transferred. Another 6.8 million dollars is currently under legal injunction and is expected to be returned to the company, which is working on getting back the remaining 31.8 million dollars in cooperation with federal authorities in the US and other countries. In its announcement, the company stated that it was limited in the information that it could release since the incident was still under investigation. Nevertheless, the company reported that it concluded its probe on July 17 and did not find any evidence that the company's system had been breached or that its information – including financial information – had been accessed. Therefore, the company stated that it believed the fraud was an isolated incident, that its information systems were not hacked, and that it did not suspect the criminal involvement of its employees in the fraud.

- On August 11, it was published[85] that the communications company, Business Wire, announced that it was working together with the Justice Department to investigate a cyberattack that apparently enabled unauthorized access to information contained on its news distribution platform. An investigation by the SEC found that claims were filed against 32 people accused of taking part in an insider trading ring that profited from non-public information regarding company profits. It also stated that the group, which was headed by two Ukrainian citizens – Ivan Turchynov and Oleksandr Ieremenko – had hacked into two or more news service companies over a period of five years and stolen hundreds of messages regarding company profits before they were released to the general public. The stolen information was transmitted via a Web site for traders worldwide who were recruited through a video demonstration of their ability to obtain the information before its release to the general public. According to the SEC, the attack was a "global and sophisticated hacking program, unprecedented in terms of the scope of the hacking at issue, the number of traders involved the amount of profit", which provided the hackers with sensitive information and illegal profits in the amount of 100 million dollars by making trades based

[85] http://www.securityweek.com/business-wire-investigating-cyberattack

on the stolen information. For example, on May 1, 2013 the hackers took 36 minutes from the moment the company posted an announcement regarding a re-examination of its revenues and forecasts until the time of publication. Ten minutes after the company posted the announcement, which was still confidential, the hackers began to sell company shares and made a profit of 511,000 dollars before the announcement was published and the shares began to fall. This demonstrates the inherent value in obtaining sensitive information and/or internal information in order to make a profit through publicly traded investments.

Flight Disruption due to Computer Failure

- On the evening of September 17, 2015 it was reported[86] that "American Airlines flights were grounded nationwide: We are working to resolve technical issues impacting several airports as quickly as possible. We will provide updates and more information as they become available. We apologize to our customers for the inconvenience." It was later explained that incoming and outgoing flights in Chicago, Dallas and Miami airports were grounded due to "computer issues", as confirmed the Federal Aviation Administration.[87] The company later posted an announcement[88] according to which connectivity issues at the three airports had been fixed:

Whether this was a glitch that stemmed from software or hardware problems, the incident illustrates the potential danger that could result from damage to computer communications equipment. An attack on such equipment could disrupt aviation and cause significant economic damage to airline companies.

[86] http://breaking911.com/breaking-american-airlines-grounds-all-planes-nationwide/
[87] https://twitter.com/FAANews/status/644564704883535872
[88] https://twitter.com/AmericanAir/status/644575062482395136

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

Eli Amar, Expert on Cyber Security, EA Cyber

Dr. Michael Barak, Team Research Manager, ICT

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

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

Shuki Peleg, Information Security and Cyber-Security Consultant

Nir Tordjman, Cyber Desk Team Research Manager, ICT

ICT Interns

Chantelle Berman

Riana Goren

Kathryn Johnston

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.