IDC HERZLIYA

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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 6

October-November 2013

Highlights

- The new encryption software: Asrar Al-Ghuraba, "Secrets of foreigners", was published and distributed on the Snam Al-Islam Web forum. The Global Islamic Media Front jihadist media institution published a warning in Arabic and English not to use the software since it did not come from an official source.
- Various Web forums quoted and referenced the report by "60 Minutes" about the concern expressed by the personal physician of Dick Cheney, former Vice President of the United States, over an intentional attack [against Cheney] by terrorist organizations. His concern was due the fact that the Cheney's pacemaker could be controlled remotely.
- Officials from the "Anonymous" hackers groups continued their politically-motivated attacks around the world against targets in Arab countries, such as Syria and Morocco, and the United States in response to publications regarding activities by the National Security Agency (NSA). The Syrian Electronic Army continued its retaliatory attacks against elements that expressed opposition to the Assad regime.
- The Bitcoin gained momentum and crossed the $1,000 exchange rate mark. The Bitcoin's popularity has resulted in its acceptance as payment by an increasing number of establishments. In addition, an ATM machine was launched that enables the purchase and sale of the digital currency.
- A Web site designed to raise money for the Islamic struggle on the dark Web (Using TOR) was not successful with its goal as the site's credibility was in question.
- This report includes an in-depth analysis of "Ransomware", a type of malware that has returned to the scene with the advent of the Cryptolocker. Malware that struck hundreds of thousands of computers around the world and amassed tens of millions of dollars from victims. Such malwares were developed over time and make use of virtual and anonymous payment methods in order to extort money [from victims].

Table of Contents

Electronic Jihad

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

Key Topics of Jihadist Discourse, October-November 2013[1]

Escalation in Rhetoric and in Jihad Activities against the Egyptian Military

- In October 2013, Sheikh Ayman al-Zawahiri, leader of Al-Qaeda, criticized the Egyptian military for its policy of oppression against Islamists in Egypt, especially the Muslim Brotherhood. In light of this trend, al-Zawahiri called on Muslims to fight against the alliance formed between Egypt's military forces and secular camp, and the Zionist-Crusader forces, which he said was designed to damage the underlying strength of Islam. In addition, al-Zawahiri called on Muslims to prevent a similar situation from developing in Tunisia, and to thwart the anti-Islamic conspiracy being led by secular and Western elements in Tunisia.
- Abu Muhammad al-Maqdisi, a senior leader of the Salafi-jihadist movement in Jordan, echoed al-Zawahiri's call and wrote a letter from prison criticizing the campaign of oppression being carried out by the military regime in Egypt against Islamists and calling on Salafi-jihadist militants to help them. According to him, the Muslim Brotherhood is not a heretical party despite their differences of opinion.
- While sentiments against the Egyptian army and secular camp deteriorated, Salafi-jihadist

[1] For a more thorough review of jihadist life on the Web, see the ICT's Jihadi Website Monitoring Group's Periodic reports, at http://www.ict.org.il/ResearchPublications/JihadiWebsitesMonitoring/JWMGPeriodicalReviews/tabid/344/Default.aspx

militants in the Sinai Peninsula and in Egypt increased their efforts to attack Egyptian security forces in the Sinai Peninsula and to assassinate senior military officials in Egypt during October-November 2013. For instance, Ansar Bait Al-Maqdis, a Salafi-jihadist organization operating in the Sinai Peninsula, claimed responsibility for a terrorist attack that was carried out at an Egyptian intelligence building in Ismailia and for the assassination of Muhammad Mabruk, a senior Egyptian security official. The organization also threatened to harm officials in the Egyptian Ministry of Interior and Ministry of Defense.

Calls for Retaliatory Attacks against the United States

- The killing of Hakimullah Mehsud, leader of the Taliban-Pakistan, in October 2013 triggered a lively discourse on jihadist Web forums and social network sites. Jihad activists referred to Mehsud's contribution to the struggle against the enemies of Islam and called for retaliatory attacks against the United States.
- In November 2013, Sheikh Adam Yahiye Gadahn al-Amriki, a senior Al-Qaeda leader, called [on his followers] to harm U.S. interests in the Middle East in response to the kidnapping of Abu Mansour al-Libi, a member of Al-Qaeda responsible for the 1998 terrorist attacks against the U.S. Embassies in Kenya and Tanzania, by American forces. Al-Amriki called on Muslims in general, and Libyans in particular, to respond to American aggression.

Syria-Iraq

- Against the backdrop of rising tensions between the Al-Nusra Front, Al-Qaeda's official affiliate in Syria, and the Islamic State of Iraq and Al-Sham (ISIS), Sheikh Abu Muhammad al-Maqdisi, a senior member of the Salafi-jihadist movement in Jordan, and Abu Qatada al-Filistini, a former senior Al-Qaeda leader, sent letters to jihad activists in Syria calling on them to exercise discretion in pledging allegiance to Abu Bakr al-Baghdadi, the leader of the Islamic State of Iraq and Al-Sham.

Yemen

- During October-November 2013, Al-Qaeda in the Arabian Peninsula (AQAP) threatened to carry out retaliatory attacks against the Houthis, a Shi'ite minority in Yemen, in response to their

aggression towards Sunni Salafists in Dammaj. In addition, the organization promised to harm members of the Yemeni regime in response to prison guards' brutal oppression of Sunni inmates in prisons.

Defensive Tactics

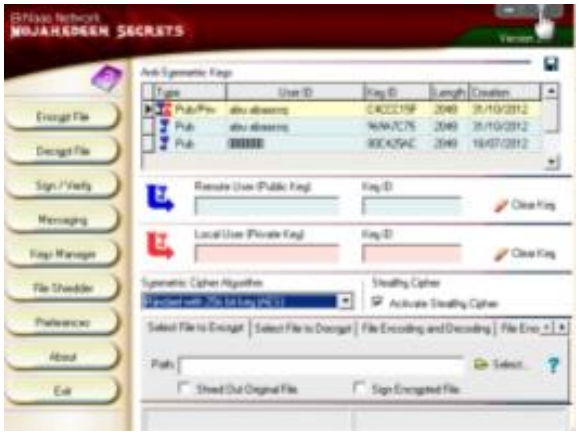
- A visitor to the jihadist forum for Assistance to the Al-Nusra Front published two videos about the rules of safe Internet surfing. The first video was titled, "How to Prevent Governments from Spying on You Via the Internet", and explained how to change the Domain Name System (DNS) – a protocol that translates verbal domain names to numerical IP addresses – and how to encrypt it in order to hide the computer details and location. For example, it recommended the dnscrypt software for DNS encryption. The second video was titled, "How the Police Can Discover Your Identity on the Internet". According to the video, Web browsing that is not secured or encrypted enables intelligence services to identify a computer's IP address and discover the user's identity.[2]

Photo of the two videos as they were uploaded to the Web forum

- The YouTube department administrator of the jihadist forum for Assistance to the Al-Nusra Front published a detailed explanation on how to install the Asrar al-Mujahideen ("Mujahideen Secrets") software on Macintosh computers, an encryption software for contacting various

[2] http://jalnosra.com/vb/showthread.php?t=2450

jihadist organizations.[3]



A snapshot of the software

- The administrator of the Snam al-Islam jihadist Web forum published an announcement about the launch of a new encryption software: Asrar Al- Ghurabaa ("Secrets of foreigners"). According to the announcement, the software is more advanced than the previous one, Asrar Al-Mujahideen, and is designed to offer a high level of protection for the mujahideen's correspondence. The announcement explained how the software can be used in order to encrypt files, to choose passwords that enable the reading of correspondence, and to generate keys to break the code. It also stated that members of the Islamic State of Iraq and Al-Sham were responsible for developing the software.[4]
- On December 5, 2013, the Global Islamic Media Front published an announcement in Arabic and English on various jihadist Web forums warning users not to use the Asrar Al-Ghurabaa software since it did not come from an official source:[5]

[3] http://jalnosra.com/vb/showthread.php?t=2588
[4] http://iraqsham.com/vb/showthread.php?2834 ; http://snamalislam.com/vb/showthread.php?t=22343
[5] http://alplatformmedia.com/vb/showthread.php?p=128338

"Global Islamic Media Front

Warning About the Use of the Program

"Asrar al-Ghurabaa"

Praise be to Allah, the Lord of the Universe, and may peace be upon our Prophet Muhammad and all of his family and companions. Thereafter:

We warn all the brothers using the new encryption program called "Asrar al-Ghurabaa" - the program is suspicious and its source is not trusted. Likewise, we confirm that there wasn't any relationship between the program "Asrar al-Ghurabaa" and the Front's encryption program "Asrar al-Mujahdeen," and therefore, we advise and warn the brothers not to use the program "Asrar al-Ghurabaa" entirely!

We also warn of using any encryption program which hasn't been published through the Global Islamic Media Front or Al-Fajr Center for Media.

And lastly, we remind that the sole source to download all of the technical programs for the Media Front:

Mobile Encryption Program

Asrar al-Dardashah Plugin

Asrar al-Mujahideen Program

The technical website for the Global Islamic Media Front

Direct link to the technical website for the Global Islamic Media Front"

Global Islamic Media Front

Warning About the Use of the Program
"Asrar al-Ghurabaa"

Praise be to Allah, the Lord of the Universe, and may peace be upon our Prophet Muhammad and all of his family and companions.
:Thereafter

We warn all the brothers using the new encryption program called "Asrar al-Ghurabaa" - the program is suspicious and its source is not .trusted

Likewise, we confirm that there wasn't any relationship between the program "Asrar al-Ghurabaa" and the Front's encryption program ,""Asrar al-Mujahdeen
!and therefore, we advise and warn the brothers not to use the program "Asrar al-Ghurabaa" entirely

We also warn of using any encryption program which hasn't been published through the Global Islamic Media Front or Al-Fajr Center for .Media

:And lastly, we remind that the sole source to download all of the technical programs for the Media Front
Mobile Encryption Program
Asrar al-Dardashah Plugin
Asrar al-Mujahideen Program

Is

The technical website for the Global Islamic Media Front

Direct link to the technical website for the Global Islamic Media Front

The announcement as it was published on jihadist Web forums

Ostensibly, the question arises as to how a jihadist Web forum could publish an official announcement about the launch of an encryption software for jihad activists and identify with the idea of global jihad, and a short while later publish an announcement warning others not to use it. The answer may have to do with the tension between the leadership of Al-Qaeda and the Islamic State of Iraq and Al-Sham. For the past year, the leadership of Al-Qaeda has tried, unsuccessfully, to impose its authority on ISIS in light of the latter's inclination to institute an independent policy in the field while ignoring instructions from the central leadership. The development of the above-mentioned software, attributed to ISIS, seems to be another component of this trend and, therefore, was viewed unfavourably by Al-Qaeda's leadership.

- A visitor to the Al-Minbar jihadist Web forum, Abu Sayf al-Ansar, posted several items on the topics of safe Web surfing and avoiding acts of fraud on the Internet, including:
    - Increased vigilance regarding the use of email addresses that are similar to a user's email address for the purpose of impersonating the user and stealing information from his contacts. For example, if the email address of a certain user is mo.arab@hotmail.com, then the impersonator's email address could be m0.arab@hotmail.com.[6]
    - A collection of tips for safe Web surfing on laptops, including: make sure to use a firewall, use passwords to protect personal computer files, and avoid making transactions or sending correspondence related to the transfer of funds.[7]
    - A warning against clicking on short links, such as wa9.la, tinyurl.com, bit.ly, out of concern that they will lead to Web sites that implant spyware on one's computer. According to the visitor, one can avoid this risk by using reliable browsers like Firefox and by updating the browsers in order to prevent breaches.[8]
    - Advice on how to surf anonymously on Google Chrome without Google being able to identify the Web sites that one visits.[9]
    - A collection of tips on how to make sure one's Gmail account is not compromised.[10]
    - A collection of tips on how to cope with security problems on iPads.[11]

[6] http://alplatformmedia.com/vb/showthread.php?t=30020
[7] http://alplatformmedia.com/vb/showthread.php?t=30025
[8] http://alplatformmedia.com/vb/showthread.php?t=30077
[9] http://alplatformmedia.com/vb/showthread.php?t=30318
[10] http://alplatformmedia.com/vb/showthread.php?t=30319

- Possible solutions for removing malware embedded in mobile phones. According to the visitor, most mobile phones have a secret software embedded in them called Carrier IQ, which tracks the user's location and registers the mobile phone's entire memory. One recommended solution to this issue is to install custom ROMs, the most well-known example being CyanogenMod, which provides mobile phone protection.[12]

- A recommendation to use the TCP View software in order to verify that spyware has not been implanted on one's computer, which would send computer files from one's personal computer to external agents.[13]
- A collection of tips on how to maintain privacy while using search engines such as Google, including: do not enter personal details, do not search for personal information using search engines, do not use personal emails, and change the settings in order to avoid having cookies sent to one's browser.[14]
- An explanation on how to encrypt emails on Gmail.[15]

Offensive Tactics

- Various Web forums quoted and referenced the report by "60 Minutes" that the personal physician of Dick Cheney, former Vice President of the United States, gave instructions on how to disable the remote login option on Cheney's pacemaker, which had allowed it to be accessed

---

[11] http://alplatformmedia.com/vb/showthread.php?t=30324
[12] http://alplatformmedia.com/vb/showthread.php?t=31201
[13] http://alplatformmedia.com/vb/showthread.php?t=30427
[14] http://alplatformmedia.com/vb/showthread.php?t=30430
[15] http://alplatformmedia.com/vb/showthread.php?t=30541

from a distance of approximately 90 meters. The instructions were given out of a concern that terrorist organizations could assassinate the former Vice President by hacking into his pacemaker and disrupting its proper operation.

- A visitor to the Al-Minbar jihadist Web forum, Abu Sayf al-Ansar, published information regarding the Spy Bubble spyware application for mobile phones.[16]

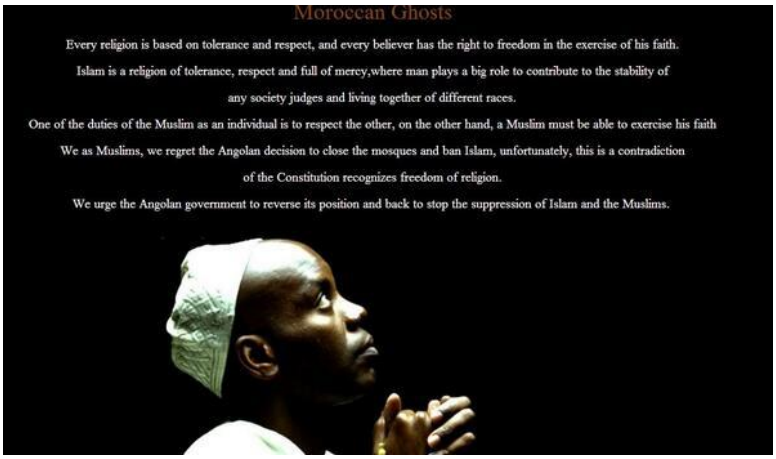
Moroccan Hackers

- In November 2013, the Moroccan hacker group, Moroccan Ghosts (Al-Ashbah al-Maghrebiyya), hacked into Web sites in countries including Algeria, Zambia and Nigeria, which had expressed support for Western Sahara's independence and criticized the Moroccan occupation of the region. For example, it attacked the Web site of the Nigerian Ministry of Defense (http://mod.gov.ng) and wrote [on its Web site] that the Western Sahara was Moroccan territory.[17]

The banner posted by the Moroccan Ghosts hacker group on the Web sites of countries that had expressed support for Western Sahara's independence

[16] http://alplatformmedia.com/vb/showthread.php?t=30520
[17] https://twitter.com/MoroccanGhosts

- Towards the end of November 2013, Muslim hacker groups focused on attacking Web sites of the Angolan government in response to the government's decision to illegalize Islam, close down mosques and ban any signs of the religion in Angola. The wave of attacks that began at the end of November and continued throughout December 2013 was given the name "OpAngola".
- Among the secular and Islamic hacker groups that claimed responsibility for hacking into and damaging dozens of Angolan Web sites were Anonghost, the Moroccan Islamic Electronic Association, and Moroccan Ghosts, which declared its intention to focus on Angolan Web sites.[18]



The banner posted by the Moroccan hacker group, Moroccan Ghosts, on Angolan Web sites

Attacks on Dutch Targets

- The AnonGhost hacker group claimed on its Twitter account that it had successfully hacked into and damaged over 100 Dutch Web sites.[19] The founder and leader of the group is a Muslim from Mauritania, and working alongside him are Muslims from Malaysia, Morocco, the United States, Ireland, and other countries.

Attacks on Turkish Targets

- The Marxist hacker group, RedHack, hacked into the official Web site of the Justice and Freedom Party (http://www.akpartiordu.org), Turkey's ruling party led by the Prime Minister of

[18] https://twitter.com/MIUM01
[19] https://twitter.com/An0nGhost

Turkey, Recep Tayyip Erdoğan. According to the group, the attack was carried out in response to the arrest of a 14-year-old boy named Taylan Kulaçoğlu by Turkish security forces, for his alleged membership in the RedHack hacker group. The group posted a banner on the Party's Web site, emphasizing that the teenager had no connection to the group and vehemently protesting the policies employed by the Turkish government to silence its citizens. According to the group, the Turkish government grossly tramples freedom of expression and, therefore, the group is obliged to protest any kind of dictatorship via additional cyber-attacks.[20]

From left to right : The introduction to a video that was published by the RedHack hacker group to demand the release of Taylan Kulaçoğlu; A photo of Taylan Kulaçoğlu

Guidance

- The Al-Batar jihadist media institution, which distributes materials on jihadist Web forums, announced on its Twitter account the launching of an online course on jihadist propaganda. The first class of the online course would focus on Photoshop, a software used for image processing.[21]

[20] https://twitter.com/TheRedHack
[21] https://twitter.com/AL_Bttaar/

The banner of the online course

- A visitor to the military section of the Al-Jihad Al-Alami jihadist Web forum, which focuses on hacking into Web sites, published a guidebook to computer hacking for beginners. The guidebook included comprehensive and in-depth explanations on how to use various hacking software, including sub7, and on how to use computer commands to hack into Web sites. The guidebook also included an explanation on how to cause a Web site to crash by creating an overload on the server on which it is stored. In addition, it included a great deal of information about various types of viruses and on the ways in which they can be built and programmed. At the end of guidebook there was a list of recommended software for hackers.[22]

Propaganda

- On November 23, 2013, the Al-Sham jihadist media institution, which focuses on the arena of jihad in Syria, published a propaganda campaign on its Twitter account. The campaign, which was titled "Help Them to Support the Residents of Al-Sham", was designed to raise funds for the mujahideen in Syria to continue the fight against the Syrian regime. The banner that was posted to the Twitter account included the contact details of those individuals responsible for the campaign, referred to as Abu al-Walid al-Muhajir and Al-Simbatik, including telephone numbers, PalTalk numbers and Twitter accounts.

  The following additional details were written in the text of the campaign banner:

[22] http://shabakataljahad.com/vb/showthread.php?t=34808

"A popular campaign for jihad with money [in other words, support jihad by making financial donations]. The campaign is being supervised by several mujahideen located in Al-Sham. The funds will be spent as the campaign supervisors see fit, from the supply of weapons and ammunition for the mujahideen, to clothing and food for the needy through dawah [the preaching of Islam] and education".

"The most important goals of the campaign are:

- Support and provision of military weapons and ammunition to the battlefronts.
- Care for the poor among the mujahideen.
- Care for the families of martyrs.
- Support for classes on the memorization of the Qur'an, Islamic institutes and madrasas [educational institutions].
- Medical assistance for the mujahideen".[23]

The campaign banner: "Help Them to Support the Residents of Al-Sham"

[23] https://twitter.com/alsham_1434/status/404329819154182144/photo/1

Review of Hacker Activity

Anonymous

Attacks against the Syrian Regime

In the afternoon hours of October 25, it was published[24] that members of "Anonymous" had successfully hacked into the government Web site of the Syrian Patent Office and leaked various documents.

The announcement referenced an article[25] on the subject, which included a link to a claim of responsibility[26] from October 24 and a referral to the file of documents that were leaked[27] in the incident. (At some point after it was posted the file was apparently removed. At present, it cannot

[24] https://twitter.com/ModusAnonymous/status/393749374276079616
[25] http://news.softpedia.com/news/OpSyria-Anonymous-Hackers-Leak-Data-from-Syrian-Patent-Office-394255.shtml
[26] http://pastebin.com/F62Ph1sU
[27] https://mega.co.nz/#!0BAHgRIC!eDfH2xYx8X1A8SDXxU8JOxXNMetCi_-yMXYro8ZTUWc

be downloaded from this address). The announcement ended with the message:

Anonymous: 4

Al-Assad: 0

This incident came on the heels of the group's breach of another Syrian government Web site, which took place a day earlier and in an identical manner; On October 24, a message was posted on Twitter[28] that referenced an article[29] taking responsibility[30] for the previous day's breach of the government Web site of Syria's Higher Commission[31] for Scientific Research (the third victory claimed by "Anonymous"[32]). This also included a reference to the leaked file,[33] which is also no longer available.

[28] https://twitter.com/AnonNewsIndo/status/393292379513294849

[29] http://news.softpedia.com/news/OpSyria-Anonymous-Hacks-Syria-s-Higher-Commission-for-Scientific-Research-393895.shtml

[30] http://pastebin.com/ghNpTi6W

[31] http://hcsr.gov.sy/

[32] https://twitter.com/Liberationtech/status/393200183137533952

[33] https://mega.co.nz/#!gVICBSiR!HM-TdmHPsSaKr93NFoDS3nTXJ7p7MEu-hY1sdA3TSTc

On October 25, a Twitter post called for attacks on all Syrian government Web sites[34] following an interview that was published[35] the previous day with someone who claimed to be involved in the attacks, who said that the attack had been carried out by three people and that the breach itself had only taken a few hours.

The above episodes followed the first two incidents in the series, which were carried out during the month of September: a breach of Syrian government Web sites[36] at the beginning of the month, and the apparent leak of the personal details of members of the Syrian Electronic Army[37] at the end of the month.

Attack against the Syrian Customs Web Site

On November 4, it was reported[38] that members of "Anonymous" had successfully hacked into the Syrian Customs Web site.[39] The report claimed that the operation itself had actually been carried out in September and that some of the information had been leaked at that time in order to prove that the breach had occurred. Now [in November] they leaked the entire contents of the Web site's

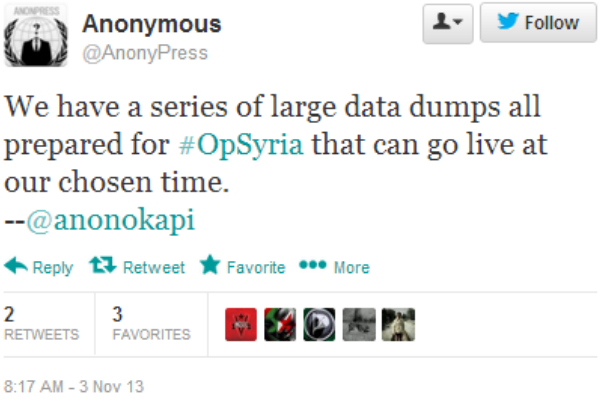
[34] https://twitter.com/YoungDashS/status/393704966860574720
[35] http://www.dailydot.com/news/opsyria-syrian-government-hack-interview/
[36] http://www.dailydot.com/news/anonymous-opsyria-assad-syria-sea/
[37] http://www.dailydot.com/politics/sea-syrian-electronic-army-globalpost-hacked/
[38] http://news.softpedia.com/news/Anonymous-Hackers-Leak-Data-Stolen-from-Syrian-Customs-Website-396729.shtml
[39] http://customs.gov.sy/

database, including the network structure and the security flaw through which they hacked into the site and which they claimed had not yet been fixed. This followed the breach of three other Syrian government Web sites at the beginning of the month,[40] as well as the breach of the Web sites belonging to the Syrian Patent Office[41] and to Syria's Higher Commission for Scientific Research.[42] All of the above-mentioned breaches were part of the "OpSyria" operation carried out by members of "Anonymous".

At the same time, these hackers continue to publish announcements warning of continued attacks against Syrian government Web sites. For example, the following message was posted on November 3 regarding the continuing operation:[43]

Another message was posted several minutes later in which "Anonymous" explicitly warned that they have many databases ready to be leaked:[44]

[40] http://news.softpedia.com/news/Three-Government-Websites-from-Syria-Hacked-and-Defaced-396126.shtml
[41] http://www.middleeast-internet-monitor.com/?p=4902
[42] http://pastebin.com/ghNpTi6W
[43] https://twitter.com/AnonyPress/status/396878101927297024
[44] https://twitter.com/AnonyPress/status/396883915832434689



Planned Global Demonstrations for November 5

November 5, which serves as an important date in both British history and in the history of the group "Anonymous", has been marked in recent years by online attacks and physical demonstrations. In this framework, there have been recent reports[45] of demonstrations planned by "Anonymous" members around the world. Reports[46] indicate that 430 demonstrations were planned for this date around the world and in our area, and were even mapped out.[47]

An examination revealed that several of these demonstrations (for which "events" were created on Facebook) were expected to take place in the Middle East, including Cairo[48] (131 registered); Antalya, Izmir, Ankara and Istanbul[49] (316 registered); Tunisia[50] (inactive event); Sfax[51] (339 registered); Tel Aviv[52] (390 registered); and even Socotra Island[53], which is under the control of Yemen[54] (8 registered).

Meanwhile, the Turkish "Red Hack" hacker group[55] called on its supporters to march alongside members of "Anonymous" on the same date as part of the Million Mask March;

[45] http://www.middleeast-internet-monitor.com/?p=4977
[46] http://millionmaskmarch.org/locations
[47] https://www.zeemaps.com/mobile?group=654291#mappage
[48] https://www.facebook.com/events/652256028117849
[49] https://www.facebook.com/events/358741054261719
[50] https://www.zeemaps.com/mobile?group=654291#entrypage
[51] https://www.facebook.com/events/172357496298759/
[52] https://www.facebook.com/events/498537740229520
[53] https://www.facebook.com/events/215866408562625
[54] http://he.wikipedia.org/wiki/%D7%A1%D7%95%D7%A7%D7%95%D7%98%D7%A8%D7%94
[55] https://twitter.com/RedHack_EN/status/396749809161605120

While mentioning the need for, and motive behind, the demonstrations;[56]

Attack against the National Security Agency (NSA)

After reports that the NSA's Web site had crashed for several hours[57] on October 26, speculation grew that it had been caused by a cyber-attack. The NSA claimed that there had been a glitch with

[56] https://twitter.com/RedHack_EN/status/396754091323715584

[57] http://www.theatlanticwire.com/technology/2013/10/no-one-knows-why-nsas-website-was-down-11-hours/70967/

the Web site but evidence[58] was found to suggest that there had indeed been an attack planned on that date.

The Twitter hashtag OpNSA,[59] next to another one called FuckTheNSA,[60] includes a collection of reports and videos against NSA activities[61], including one titled "Final Message to NSA",[62] dated September 10, calling for action. The videos against the NSA can be found in abundance. One video, dated June 25, was titled ""NSA – Anonymous. Enough, elite. You are FINISHED".[63] Another video, dated September 9 and titled "Anonymous – Call To Action OpNSA"[64], was posted by OfficialAnonymousTV1[65] and called for counter attacks. Towards the end of the video, it also mentioned the date of November 5 as a warning.

November 5 is an important date in British history and was adopted by these hackers as a date for protest and activities. Therefore, "Anonymous" has long been publishing videos and calls for action each and every year. On May 23, it published a video titled, "ANONYMOUS Declaration of Freedom Nov 5 2013"[66] as well as calls for practical action. On September 29, it published a video calling for a "Million Mask March"[67] throughout the world on November 5 (as well as another video containing the text of the announcement).[68]

At the same time, it became known that members of both "Anonymous" and the Turkish "Red Hack" group were planning acts of protest that did not include information leaks or Web site attacks, but rather "activism that does not include cyber-crime".[69]

[58] http://analysisintelligence.com/cyber-defense/nsa-website-hacked-nov-5-ddos/
[59] https://twitter.com/search?q=OPNSA
[60] https://twitter.com/search?q=%23FuckTheNSA
[61] http://www.youtube.com/watch?v=jh70i5Hig5o
[62] https://www.youtube.com/watch?v=td3-1-gAkK0
[63] http://youtu.be/eG5PUMDRfGI
[64] http://youtu.be/9yvNDRnYqwI
[65] http://www.youtube.com/user/OfficialAnonymousTV1?feature=watch
[66] http://youtu.be/_ZKEXK4ueFY
[67] http://youtu.be/HhAeWah-774
[68] http://www.liveleak.com/view?i=f2a_1383044424
[69] http://news.softpedia.com/news/RedHack-and-Anonymous-Team-Up-for-November-5-Protests-392990.shtml

Attacks against Governments around the World

On October 16, members of "Anonymous" reported[70] that they had hacked into the servers of the Polish Ministry of Economy in the framework of the OpGoldenDawn operation[71] against the Greek neo-Nazi movement, "Golden Dawn". Information from these servers was leaked online in a 384 MB compressed file that included hundreds of various government documents. Some of the documents, including passport photographs, were posted as photos on the Web site, Imgur.[72] The announcement stated that the email correspondence of the Italian government would be published during the end of the following week.

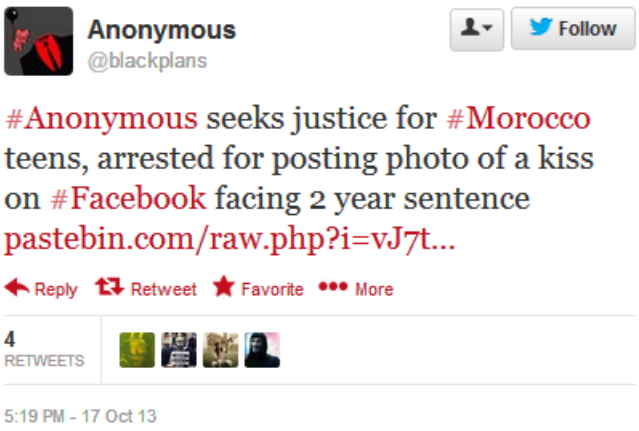
Two days earlier, thousands of documents from the Greek Foreign Ministry were leaked,[73] as were two compressed files at a volume of half a gigabyte, containing approximately 3,700 documents, from the Organization for Security and Co-operation in Europe (OSCE). The Greek Foreign Ministry admitted[74] that its systems were hacked. The reason for the attack stemmed from the activities of the neo-Nazi Golden Dawn Party in Greece.[75]

[70] https://twitter.com/AnonyInfo/status/390330749171154945
[71] https://twitter.com/search?q=%23OpGoldenDawn
[72] http://imgur.com/a/wJFQi#0
[73] https://www.cyberguerrilla.org/blog/?p=16040
[74] http://news.softpedia.com/news/Greek-Foreign-Ministry-Admits-Anonymous-Hacked-Email-Systems-391132.shtml
[75] http://news.softpedia.com/news/Anonymous-Leaks-3-700-Documents-Stolen-From-Greek-Government-and-OSCE-390752.shtml

This incident occurred several days after members of "Anonymous" had hacked into several Venezuelan government and military Web sites in protest against the Venezuelan government.[76]

Attack against the Moroccan Government

In the afternoon hours of October 17, activists affiliated with "Anonymous" posted an announcement on Twitter[77] that referred to a claim of responsibility[78] for the breach of the Web site belonging to the Department of Water in the Moroccan Ministry of Energy, Mines, Water and Environment. The announcement revealed a great deal of information from the Web site's database, and claimed that the breach had been carried out in revenge for the arrest of a young local couple on October 3 after a photo of them kissing outside of their school was posted on Facebook.[79] It was also reported that their trial would take place on November 22 and that, until then, "Anonymous" would be watching and ready to respond.



The announcement included an explicit warning to the Moroccan authorities:

"We intend to humiliate the Moroccan government the way that these youths have been humiliated. We intend to expose the Moroccan government, the way they have exposed the private

[76] http://news.softpedia.com/news/Venezuelan-Military-and-Government-Websites-Hacked-by-Anonymous-391564.shtml
[77] https://twitter.com/blackplans/status/390844489889095680
[78] http://pastebin.com/raw.php?i=vJ7t84jV
[79] http://www.rtbf.be/info/medias/detail_maroc-un-couple-d-adolescents-arrete-pour-un-baiser-sur-facebook?id=8105385

lives of these young teenagers. No matter what the eventual outcome of this case these young people will bear some burden from it, probably for the rest of their lives."

As well as:

"Continue down this road and we will rip through your government servers, leaking and deleting as we go. None of your systems will be safe. Our actions represent merely an opening volley, a warning."

The message also noted the abundance of material gained by the breach of the Web site:

"It seemed that the best place to sail in search of leaks would be the Moroccan Ministry of Energy, Mines, Water and Environment, specifically the Department of Water, What we got instead was a niagarous flood of data. We are sharing some of it with you here. Personnel files, bank transfer details, passwords, there is much, much more. This is merely a taste, we are holding back, hoping that leniency will be shown and our continued efforts will be unnecessary."

A demonstration was held even earlier, on October 12, in front of the Moroccan Parliament[80] during which dozens of demonstrators hugged and kissed in protest of the couple's arrest.

Attack against the Ukrainian Foreign Ministry

After reports surfaced[81] that members of "Anonymous" had successfully hacked into the computers of the Polish Ministry of Economy on October 16, and the computers of the Greek Foreign Ministry two days earlier from which they leaked thousands of documents, it was reported[82] on October 23 that they had also hacked into the computers of the Ukrainian Foreign Ministry. Partial screenshots were published[83] but the file and leaked documents are no longer available via the link that was published along with the claim of responsibility.[84]

---

[80] http://freearabs.com/index.php/society/85-video-gallery/730-jb-span-morocco-jb-span-kissing-freedom-goodbye

[81] http://www.middleeast-internet-monitor.com/?p=4850

[82] https://www.cyberguerrilla.org/blog/?p=16121

[83] http://imgur.com/a/zCKLB

[84] https://www.cyberguerrilla.org/blog/?p=16121

The "Syrian Electronic Army"

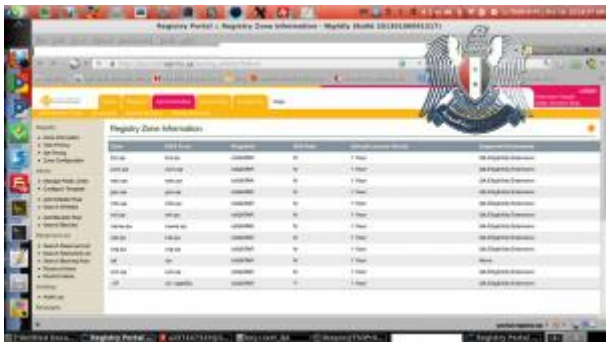
Attacks against the Government of Qatar

In the early hours of October 19, it was reported that the "Syrian Electronic Army" had returned to work after a long break, this time with an attack against Qatari government Web sites. The first announcement[85] was published at 01:54 and was general;

A few minutes later, three announcements were published listing the Web sites that they claimed to have attacked;

[85] https://twitter.com/Official_SEA16/status/391336620957257728

A screenshot[86] that was published[87] by Th3 Pr0, a self-described 19-year-old Syrian hacker and "Head of Special Operations Department"[88], revealed that the breach was of the local domain name registration site, Registry.qa;



Among the Web sites that were hacked were government and military sites, media and news company sites, and even the local Qatari Facebook and Google sites. To prove their claim, members later published[89] a screenshot[90] of the alleged breach of the Qatari Google Web site;

Nevertheless, the only reports of these attacks were made on the hacker group's Twitter account

[86] https://twitter.com/Official_SEA16/status/391339315562688513/photo/1
[87] https://twitter.com/Official_SEA16/status/391339315562688513
[88] http://blog.thepro.sy/who-am-i
[89] https://twitter.com/Official_SEA16/status/391411650655305728
[90] https://twitter.com/Official_SEA16/status/391411650655305728/photo/1

and by various media organizations.

This was not the first time that the "Syrian Electronic Army" carried out online attacks against the Qatari government; in the past they leaked details about the Qatari Royal Family,[91] its internal[92] and external[93] conduct, alongside various pieces of correspondence[94] and documents.[95]

The previous version of the Web site belonging to the "Syrian Electronic Army" even included a special poster that it had prepared, containing all of the information that it had stolen and leaked from Qatari government computers;

For now, some of the Web sites are again in working order but others, including the government Web sites and the Facebook sites, are unavailable.

Attack against President Obama

In the evening hours of October 28, it was reported that the "Syrian Electronic Army" had successfully hacked into several of the accounts representing President Obama on social network sites.

The first report was of a breach to the email account[96] belonging to Suzanne Snurpus, one of the administrators of the Web site, Organizing for Action,[97] which served Obama in his 2008 and 2012 election campaigns;

[91] http://www.sea.sy/article/id/1965/en
[92] http://www.sea.sy/article/id/1972/en
[93] http://www.sea.sy/article/id/1916/en
[94] http://www.sea.sy/article/id/1907/en
[95] http://www.sea.sy/article/id/1910
[96] https://twitter.com/Official_SEA16/status/394878079044055041
[97] http://www.barackobama.com/

The report included a screenshot of the Gmail account that was hacked;[98]

A few minutes later, another announcement was released[99] stating that the group had successfully hacked into the server of Blue State Digital (BSD), which provided strategic digital services in Obama's election campaigns;

[98] https://twitter.com/Official_SEA16/status/394878079044055041/photo/1/large
[99] https://twitter.com/Official_SEA16/status/394878677613162496

The message included a reference to a screenshot,[100] in which it mentioned the Web site on the address bar;

[100] https://twitter.com/Official_SEA16/status/394878677613162496/photo/1/large

Several minutes later, another announcement was posted,[101] indicating that a diversion had been created[102] whereby visitors to the Web page, donate.barackobama.com, were redirected to a pre-prepared page with the message "Hacked by SEA".[103]

Twenty minutes later, another announcement was posted,[104] stating the justification for the attack;

After another 15 minutes, it was reported[105] that the group had allegedly succeeded in getting

[101] https://twitter.com/Official_SEA16/status/394879792727601155
[102] http://thehackernews.com/2013/10/president-obamas-twitter-facebook.html
[103] http://www.zone-h.org/mirror/id/21091817
[104] https://twitter.com/Official_SEA16/status/394884772691865600

Twitter to block Obama's account;

It seems that members of the "Syrian Electronic Army" did not actually hack into the President's Web sites or various social network accounts, but rather successfully changed the links[106] that appeared in various posts on his Twitter and Facebook accounts, thereby redirecting users to the Web site of the hacker group. An announcement[107] regarding this was finally posted;

[105] https://twitter.com/Official_SEA16/status/394888463247343616
[106] http://mashable.com/2013/10/28/syrian-electronic-army-obama/
[107] https://twitter.com/Official_SEA16/status/394896676051103744

As was a screenshot[108] from the server on which the links were re-directed;

It seems that the pattern of attack was as follows: Members of the "Syrian Electronic Army" successfully hacked into the email account of Suzanne Snurpus, who was active on the site that served President Obama during his two presidential election campaigns. From the correspondence garnered on the breached account, they were able to hack into two accounts that served the Web

[108] https://twitter.com/Official_SEA16/status/394896676051103744/photo/1/large

site of the President – the Web site of the company that provided digital strategy and the Web site that shortens long links.

However, different sources confirm that the group did not actually hack into the Web site or Facebook and Twitter accounts, but rather it changed the links that appear in some of the announcements to redirect users to the previously-prepared video that presented "the truth about Syria".[109]

Cyber-Crime and Cyber-Terrorism, October-November 2013

Recent years have seen an increasing number of cyber-attacks on political targets, critical infrastructure, and the Web sites of commercial corporations. These attacks, which are also receiving increasing amounts of international attention, are perpetrated by states (which do not take responsibility for them), groups of hackers (such as Anonymous), criminal organizations and lone hackers. We believe that terrorist organizations are working in close collaboration with criminal organizations, are learning from their attempts [at cyber-crime], and may even be hiring their services. In light of this, it is important to examine and analyze cyber-crimes attributed to criminal organizations, as well as new development trends and patterns. The following information was culled from the visible (OSINT) and invisible ("dark Web")[110] Internet between October-November 2013.

Trends in Digital Currency (Bitcoin)

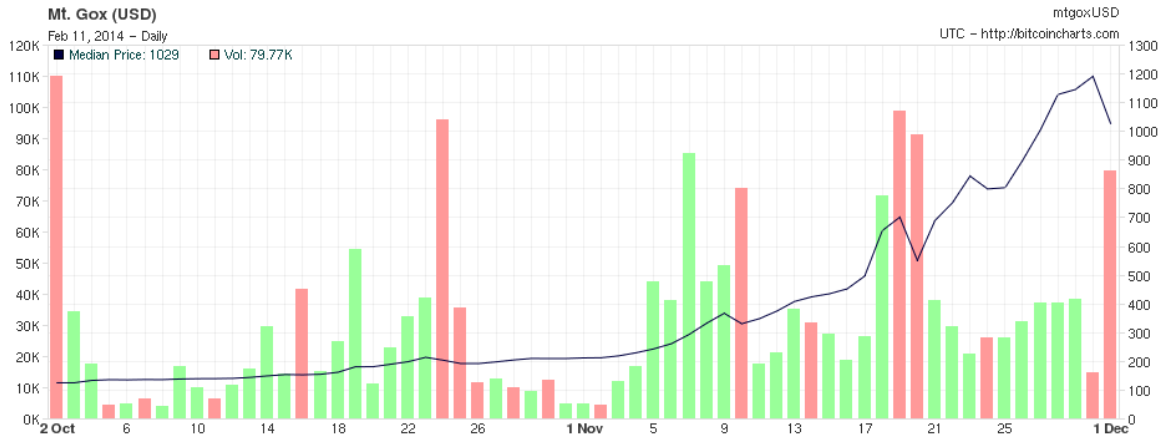
The Bitcoin currency gained significant momentum of over 1000% during October-November, when it reach an exchange rate of $1200. The following data reflects the median purchase price of the currency on the Mt. Gox Web site.[111]

---

[109] http://thehackernews.com/2013/10/president-obamas-twitter-facebook.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29

[110] 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.

[111] http://bitcoincharts.com/charts/mtgoxUSD#igDailyzczsg2013-10-01zeg2013-11-30ztgMzm1g10zm2g25zv



The data for October-November 2013 taken from the Mt. Gox Web site[112]

The negative effect of the currency following the closure of the illegal trading site, Silk Road, led to extreme fluctuations such that the exchange rate dropped from $140 to $109, and then rose again to $125.[113] During November, a hearing was held in the United States Senate about virtual currencies.[114] Opinions from various authorities in the United States were gathered in preparation for the hearing. One such authority was Ben Bernanke, Chairman of the Federal Reserve,[115] who noted that the Federal Reserve did not have the authority to monitor virtual currencies that were not issued by the U.S. government. The Senate hearing included positive opinions regarding virtual currencies and even claims that they constituted a legitimate means despite their risks and illegal uses, such as the Liberty Reserve and Silk Road.[116] Reports about the Senate hearing and its "apparent support" [for digital currency] led to a jump in the price of the currency, which reached $700.[117] Towards the end of November, the currency passed the $1000 mark in light of extensive demand from China.[118]

Several events influenced the legitimacy and options for Bitcoin use as an accepted and trade-able

[112] http://bitcoincharts.com/charts/mtgoxUSD#rg60zczsg2013-10-01zeg2013-11-30ztgMzm1g10zm2g25zv
[113] http://www.wired.com/wiredenterprise/2013/10/bitcoin-market-drops-600-million-on-silk-road-bust/
[114] http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies
[115] https://www.documentcloud.org/documents/835843-virtual-currency-hearings.html
[116] These cases were analyzed in previous issues of the Cyber Report (links)
[117] http://online.wsj.com/news/articles/SB10001424052702304439804579205740125297358
[118] http://www.wired.com/business/2013/11/bitcoin-one-thousand/

form of currency:

- At the end of October the first ATM machine for Bitcoins was launched in Vancouver, Canada.[119] The machine enables the quick purchase and sale of Bitcoins, and eases the process of trading and converting Bitcoins into a fluid currency. The Bitcoin ATM machine makes the process quick and accessible but does away with anonymity as the machine keeps a photo of the user and a scan of his handprint.
- At the end of November, Richard Branson, founder of the Virgin Group, which is marketing the first commercial flight into space, announced that it would be possible to pay for the flight using Bitcoins (the cost is $250,000).[120]
- The University of Nicosia in Cyrus announced that it would allow students to pay tuition using Bitcoins.[121]
- In mid-November, the Bitcoins Payment Solutions (BIPS) Web site, which serves as the central Bitcoin bank, was breached and 1,295 Bitcoins (worth an estimated one million dollars) was stolen.

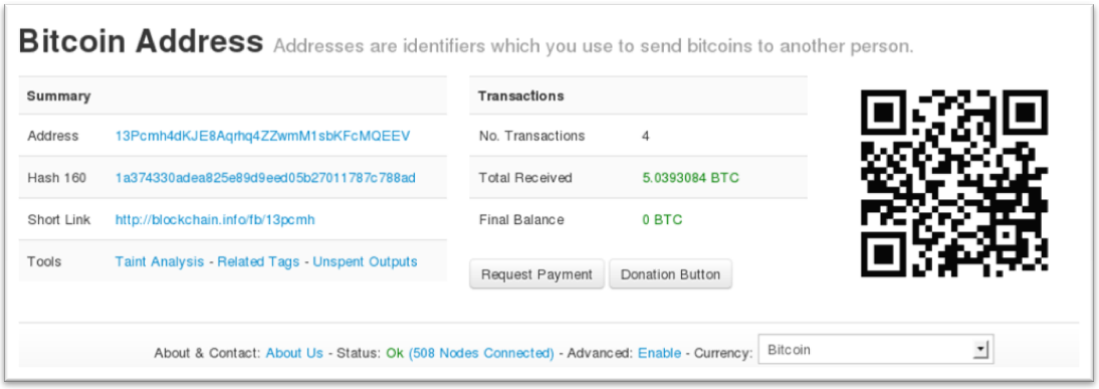
Raising Money for Terrorist Activity on the "Dark Web"

In September 2012, an anonymous Web site was uploaded to the "Dark Web" for the purpose of raising money anonymously (using Bitcoins) for the continuation of the Islamic struggle against the United States. The Web site includes a short text that explains the need to collect funds for the activities of Muslim youth and asks visitors to donate anonymously so as not to be detected. An email address to contact is listed at the end.

[119] http://mashable.com/2013/10/30/bitcoin-atm-2/
[120] http://www.theregister.co.uk/2013/11/22/when_hot_cash_meets_a_vacuum_virgin_galactic_takes_bitcoin/
[121] http://www.geekwire.com/2013/cyprusbased-school-university-accept-bitcoin-tuition/

A screenshot of the fundraising site

An examination of the virtual wallet that was published on the Web site showed that four transfers were made, two deposits and two withdrawals. The total amount deposited was approximately five BTC, in two transactions made in September 2012. During that time, the BTC exchange rate was around $10.



The virtual wallet details that were published

While it is difficult to know who is behind the Web site, and if it is indeed a fundraising site or a scam, for over a year the fundraising efforts were not successful. The reason for this may be due to users' mistrust in assuming that the site was is a scam or a trap set by the authorities, or due to the site's insufficient exposure.

Andrew Lewman, Executive Director of the Tor Project, denied that this is hard evidence to suggest that the Tor network is used by terrorist groups:

"Some teenager creates a site, which is just one page of brochureware, and now they're a

terrorist… Maybe it's run by terrorists who are hunting down IP addresses of press people… Maybe it's run by the mob... Maybe law enforcement".[122]

The Persian Gulf States as a Target for Cyber-Crime

On October 27 it was reported[123] that a study had shown that 65% of information systems specialists among the Gulf Cooperation Council (GCC) believe that the region is a worthy target for cyber-attacks. According to Kit Lloyd, an expert from Oman, cyber-criminals are exploiting the trusting nature of the people of the Middle East, including Oman. He noted that the issue of security in these countries has developed in recent years, especially due to the rise in cyber-crime. Companies are more aware of security-related problems in the fields of information systems and are expressing interest in taking preventative steps but they do not always take appropriate measures. Studies that were published a year ago revealed that the rate of contaminated work stations in Oman was double the global rate and the highest among the GCC.

The study revealed that 60% of companies in Oman devote up to 10% of their informational systems budget to information security. 34.4% of respondents confirmed that their companies had faced at least one security-related incident during the past year. In addition, 54.3% believed that they would continue to face more security-related incidents in the upcoming year.

Turkey's Military Unit to Combat Cyber-Crime

On October 11, the Turkish Minister of Transport, Maritime Affairs and Communications announced that the Turkish Army had established a unit to combat cyber-crime. According to him, cyber-crime has recently become the most-discussed topic in Turkey and poses a real threat to the country's security. He added that his office was working to pass a new law on the topic of cyber-crime.

In addition, on October 28[124], the Turkish Minister of Science, Industry and Technology announced that his country was working to strengthen its war against cyber-crime and would train professional experts in the field. He added that the training of experts was necessary to protect public establishments as well as financial business transactions made on the Internet.

---

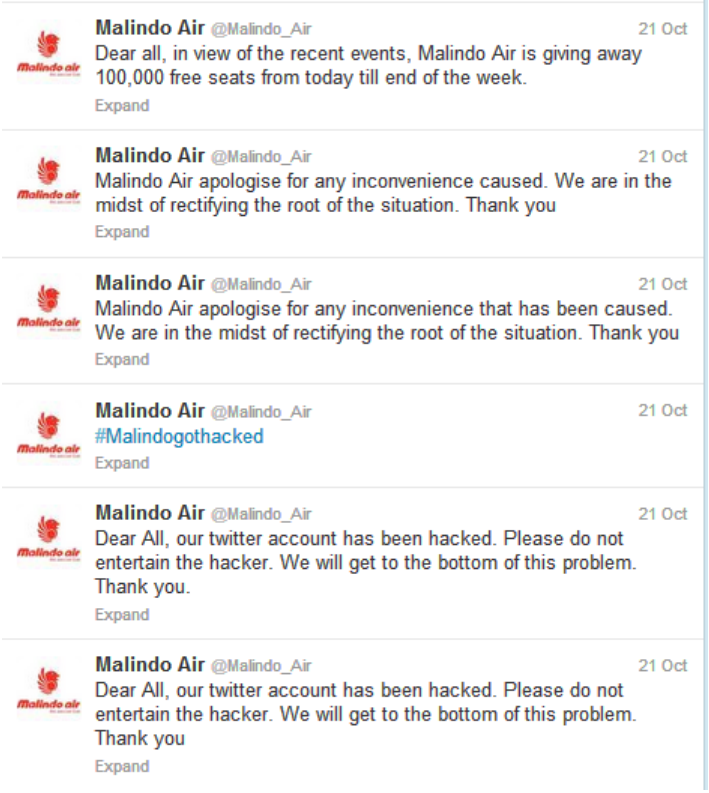
[122] http://freebeacon.com/anonymous-jihad/
[123] http://www.arabianbusiness.com/gcc-prime-target-for-cyber-crime-experts-524412.html
[124] http://en.trend.az/capital/it/2205267.html

In addition, a similar step was recently reported to have been taken in England. The British Minister of Defense[125] announced the establishment of a new reserve unit that will recruit hundreds of experts in the field of information systems to be tasked with the protection of critical infrastructure and valuable information in cyber-space, including protection from cyber-crime.

This unit was established following the publication of a British study[126] in January 2014, which claimed that a cyber-attack would cause a fatal blow to the army's ability to function since it is dependent on information system technology.

Twitter Account Hacked – Sometimes It's Not Just a Game

On October 21, the Twitter account of the Malaysian airline, Malindo Air, was hacked.[127] The hackers posted a message saying that the airline would provide 100,000 free plane tickets.



[125] http://news.softpedia.com/news/UK-to-Recruit-Hundreds-of-Cyber-Warriors-for-New-Joint-Cyber-Reserve-387125.shtml

[126] http://news.softpedia.com/news/Cyberattacks-Could-Compromise-Ability-of-UK-Armed-Forces-to-Operate-319783.shtml

[127] https://twitter.com/Malindo_Air

Company representatives immediately issued a denial on its Twitter account and Facebook page[128] but the hacker still seemed to have access[129] to the company's Twitter account; the original message was deleted but another one was posted - after the company's denial – in which it still offered 100,000 free plane tickers in light of the events.[130]

The incident illustrates the apparent ease with which Twitter accounts can be breached, sometimes just "for fun", but with the potential to cause a great deal of damage. Such was the case when the "Syrian Electronic Army" hacked into approximately 30 Twitter accounts[131] belonging to the Financial Times, and when it hacked into the Twitter account[132] of the Associated Press and posted an announcement that there had been explosions at the White House injuring President Obama. The post caused the Dow Jones to immediately plunge.

[128] https://www.facebook.com/malindoairmalaysia/posts/524309264319908
[129] http://news.softpedia.com/news/Malindo-Air-Twitter-Account-Hacked-Attacker-Promises-100-000-Free-Seats-392897.shtml
[130] https://twitter.com/Malindo_Air/status/392163893994196992
[131] http://www.middleeast-internet-monitor.com/?p=3652
[132] http://www.dailymail.co.uk/news/article-2313652/AP-Twitter-hackers-break-news-White-House-explosions-injured-Obama.html

Case Studies

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

Ransomware on an Upward Trend

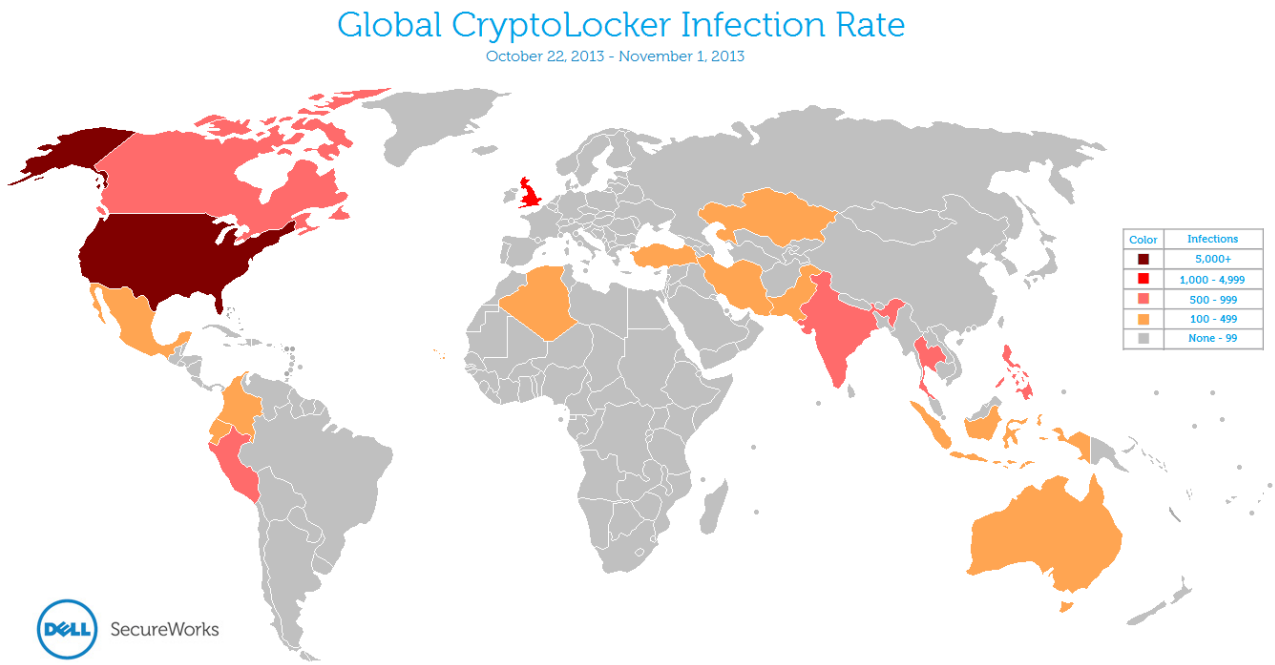
The phenomenon of ransomware is not new in the cyber-world and the first documented case of it happened back in the 1980's when it was possible to distinguish between malware that encrypts existing information on the computer and malware that prevents access to one's computer. Ransomware drew attention at the end of 2013 when Cryptolocker infected hundreds of thousands of computers around the world. In the beginning of September 2013, the first version of the Cryptolocker ransomware was documented,[133] a malware that encrypts all of the files on a computer and enables access at a cost of 100-300 dollars/Euros. Cryptolocker encrypts the computer files (photos, videos, documents, etc.) with the RSA-2048 encryption while the encryption key is saved on the server for a few days. If the user does not pay the ransom on time, the encryption key is deleted from the server and the chance of decrypting the files is nil.

[133] http://www.bbc.co.uk/news/technology-25506020

The CryptoLocker Screenshot

According to a report published by Dell SecureWorks,[134] the payment amount varies and adapts to the country in which the ransomware is operating so that payment can be made using a number of anonymous methods, including Bitcoin, Ukash,[135] CashU,[136] Paysafecard[137] or MoneyPak.[138] Researchers at Dell estimate that between 200,000-250,000 computers around the world were infected with malware. ZDnet's estimate after tracking four Bitcoin wallets was that between October 15-December 18, 2013, almost 42,000 BTC were paid (a value of tens of millions of dollars).[139] The following figure demonstrates the extent of the spread of malware around the world between October 22-November 1, 2013; it shows that damage to over 5,000 computers in North America, between 1,000-5,000 computers in England, and between 100-499 computers in Australia.

[134] http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/
[135] https://www.ukash.com/
[136] https://www.cashu.com/
[137] https://www.paysafecard.com/en-global/country-selection/
[138] https://www.moneypak.com/AboutMoneyPak.aspx
[139] http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/

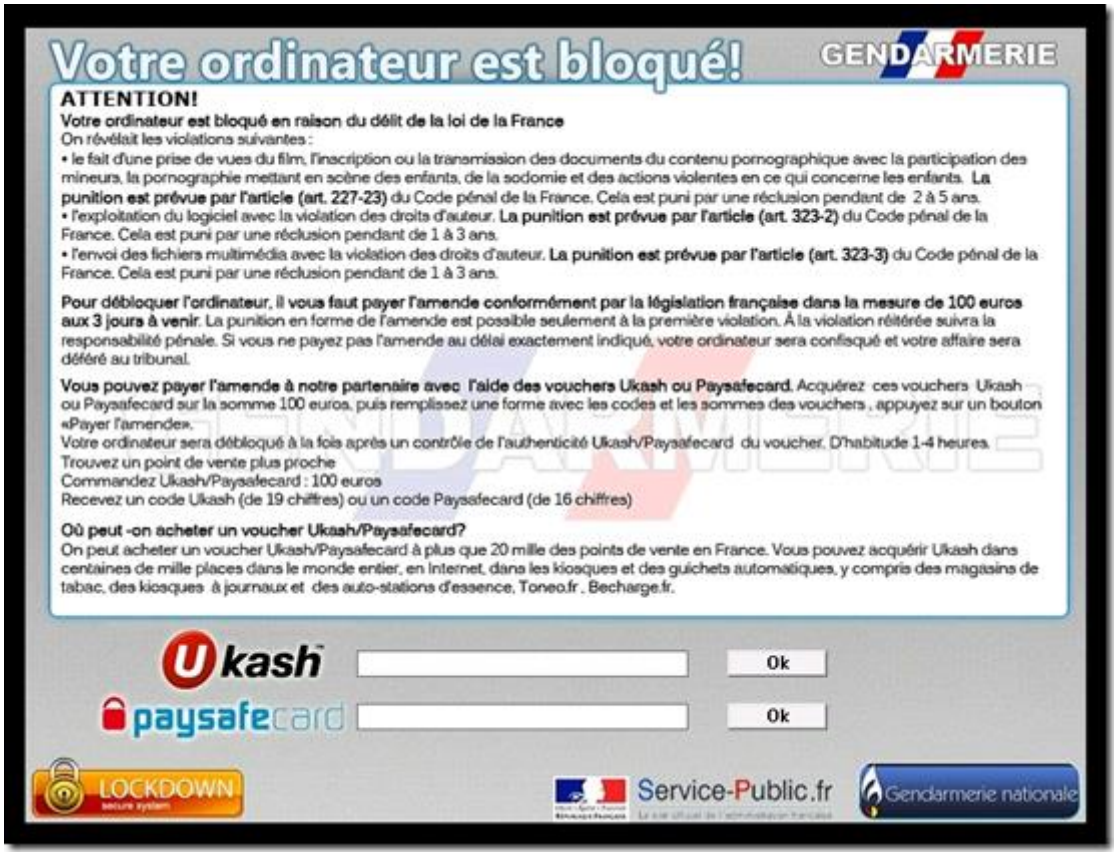


Global distribution of CryptoLocker infections between October 22 and November 1, 2013 (Source: Dell SecureWorks)

The first documented case of Ransomware is from the end of the 1980's when a Trojan Horse named PC CYBORG was spread by Joseph Popp via 20,000 floppy discs sent by mail. After encrypting the computer files, Popp demanded a ransom to decode the files.[140] Scareware was another type of ransomware, which used victim intimidation and a formal or informal demand for payment for the offense that was carried out.[141]

At the end of 2010, a malware was distributed that earned the name Virus Gendarmerie (police).[142] This malware impersonated an official action taken by French law enforcement against the distribution of pirated movies. The wording of the announcement accused the user of having acted illegally and requested a "fine" of 100 Euros to be pre-paid through virtual payments using Ukash[143] or Paysafecarde.[144]

[140] http://books.google.co.il/books?id=CWLyryduwMYC&lpg=PT232&ots=bZhToPBnBR&dq=PC%20CYBORG%20(AIDS)%20trojan%20horse%20popp&pg=PT232#v=onepage&q&f=false
[141] http://blogs.technet.com/b/markrussinovich/archive/2013/01/07/3543763.aspx
[142] http://www.commentcamarche.net/faq/33857-ransomware-virus-gendarmerie-votre-ordinateur-est-bloque
[143] https://www.ukash.com
[144] https://www.paysafecard.com



Virus Gendarmerie / Police / InterPol

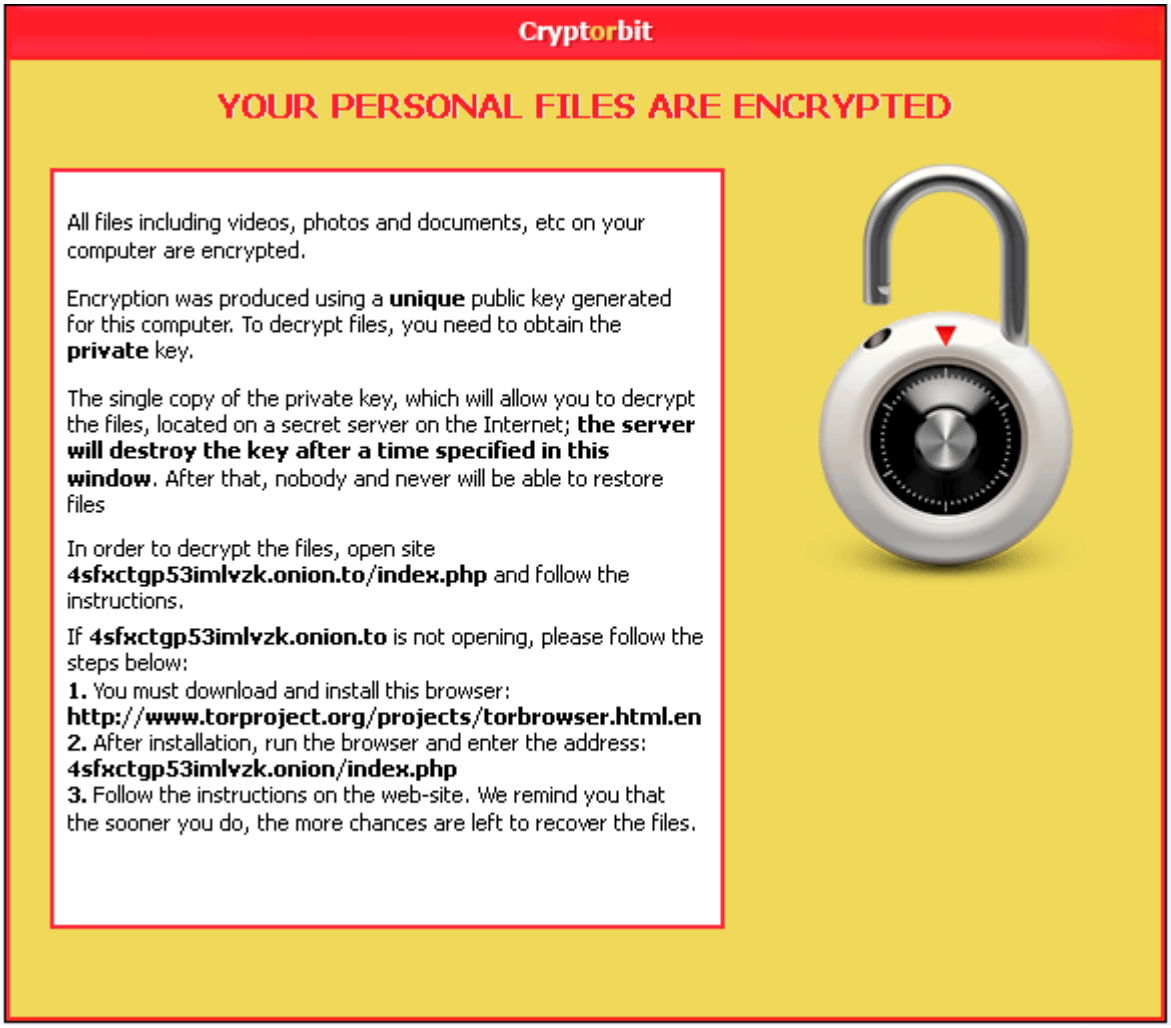
ESET reported on a malware that takes the form of an official announcement by the Anti-Cyber Crime Department of Federal Internet Security Agency with a report on the "Anti-Child Porn Spam Protection" Project.[145] After infecting the computer, a screen appears announcing that the computer had detected illegal span with pedophilic pornographic materials and that, in addition to encrypting the files with a 256bit code, access to the computer was also blocked. The ransom was set at $500 for the first 48 hours, after which the amount doubled. In addition to the threat against the user's personal computer and files, a threat was made should the user turn to the FBI.

[145] http://www.siliconrepublic.com/enterprise/item/34540-ransomware-nearly-doubles-i

Anti-Child Porn Spam Protection

The malware CryptorBit was first identified in the beginning of January 2014. It functions in a similar manner to Cryptolocker in that it encrypts all of the computer files and sends a ransom message for payment of 0.5 BTC via a designated Web site that can be accessed using TOR, but in this case it is a fraud and the user cannot access his files even after paying the ransom.[146] From an examination of the virtual wallet published on the darknet, it can be seen that three deposits were made, two of which were made in the amount of 0.5 BTC at the end of January 2014.

[146] http://thehackernews.com/2014/01/cryptorbit-ransoware-that-scam-for.html



Screenshot of CryptorBit

In the beginning of January 2014, a new malware called Prison Locker (Power Locker) was published on a Web forum. This malware will be sold on the black market for approximately $100[147] and was developed by 'gyx' and 'Porphyry'.[148] It enables anyone to carry out a ransomware cyber-attack, which increases the risk that the phenomenon will spread in the near future. It is reasonable to assume that the trend will develop along with "Internet of Things" such that, in the future, the ransom could be in oreder to "release" a car or the control to a "smart" home.

[147] http://malwaremustdie.blogspot.jp/2014/01/threat-intelligence-new-locker-prison.html
[148] http://pastebin.com/Dnhh0MWd

Guest Contributor

Countering Security Solutions – How Cyber-Criminals Easily Evade Detection (Part 2)[149]

Recap

In the first part of this article I discussed different methods used by cyber-criminals to evade various security systems. I mainly discussed device centric solutions as well as device ID evading techniques and tools. The second part of the article will take a closer look at profiling systems. Online financial profiling systems analyze multiple aspects of online banking sessions, such as the user's interaction with the Web site, login history, transactions history and more. Cyber-criminals have been fighting an uphill battle in this field but in recent months more and more solutions have been developed and deployed by cyber-criminals to address this "problem".

Evading cloud based profiling systems

Most of the techniques discussed in the first part of this article require manual work on the part of the cyber-criminals. When a username and password combination are stolen, a cyber-criminal must access the account and create a fraudulent transaction. If the cyber-criminal chooses to use RDP and VNC to circumvent a device ID solution, s/he will need to be in front of the computer and take over the session in real time. These types of manual operations are not cost effective and may require significant time and effort. As we already know, time is money! In an effort to save time, cyber-criminals developed automated scripts, which are implemented as part of a malware and spring into action to automatically create fraudulent transactions. The malware waits dormant until the victim logs in to his account. Once the username and password are validated and the online banking session begins, the script is executed and within a split second it (a) takes over the session, (b) initiates a money transfer to a mule account, and (c) releases the session back to the unsuspecting user with the only indication being that it took his bank account screen a couple of seconds longer to load. These systems, commonly referred to as ATS (Automatic Transfer Systems),

[149] This article was written by Etay Maor, an ICT Research Intern who holds an MA in Government with a specialization in Counter-Terrorism and Homeland Security from the IDC.
Part 1 was published in the ICT Cyber-Desk Review 5
http://www.ict.org.il/LinkClick.aspx?fileticket=QG0c9BKNLq0%3d&tabid=492

were a problem that banks had faced and to which they had found a solution. A rather simple analysis of the transaction page can be done, which would deny any transaction that was executed within less than one second. The reasoning is clear – humans cannot fill out a transaction page so fast and, therefore, any such transaction would be suspected of being malware. Once again, cyber-criminals were losing money and had to react quickly. One of the tools that they use today is a "slow fill" function. This function, which is implemented as part of the ATS script, and as its name suggests, "takes it time" when filling out the transaction page by inserting time delay intervals between charters that are used to fill out the form.

Some security solutions do not only look at the velocity of the user's actions but also at his clickstream. A user's clickstream is the analysis of where the user clicked on each screen while inside the online banking application. This generates behavior patterns that can be associated with a specific user, allowing the security application to identify abnormal behavior. To understand how users interact with a Web site, malware developers expanded on the existing, screen capturing capability. While screenshots can paint a picture of where users click, they are not a simple tool for this purpose and they do not show mouse movement or delays between clicks. To overcome this, a video screen capturing module was added to various malware families. Like other malware plugins, this module springs into action once the victim accesses his/her online banking session and creates a video file of everything the user did during the session. The file is later sent to the malware command and control server where the cyber-criminal can view it and analyze the interaction patterns of the specific user.

One recently identified criminal pattern aims to evade a cross between device ID systems and anomaly behavior systems. While access from a new device may not be indicative enough to mark the session as fraudulent, a new device that also performs a high risk action (high amount transaction or adding of a new payee to the system) is a combination that will raise red flags. To avoid this, cyber-criminals have been observed taking a more relaxed approach. Once a username and password are retrieved by the cyber-criminal's malware of phishing attack, the cybercriminal accesses the account from his device (which would be considered by device ID systems as a new device). However, instead of performing any high risk action, the cyber-criminal will just browse around and log off. This pattern continues over the course of a week during which the cybercriminal logs in but does not do much. After approximately one week, at which point the

device ID systems are already familiar with the new device, the cyber-criminal will start creating fraudulent transactions. This is by no means a foolproof technique but it does show that online criminals are constantly monitoring and learning the new security systems and their sensitivity threshold for suspicious actions. Intelligence gathering goes both ways, which is also evident in cyber-crime forums where criminals discuss these systems and their sensitivity levels, posting questions such as, "What is the max amount I can transfer in bank X before I hit a secondary authentication verification?"

The last counter security technique does not involve the online world directly. The cyber-crime forums mentioned in the previous paragraph offer various tools and services, such as creating fake IDs, driver licenses and passports. These services can be found mostly in Russian speaking forums as well as in darknet hidden services on the TOR network. Some packages offer a fake ID while others provide "the full package" – an ID, online credentials, physical credit card, etc. Using these credentials, a criminal can walk into a physical bank branch and open account or use the papers he obtained to authenticate his identity to a bank's call center or representative.

Summary

The cat and mouse game between cyber-criminals and security white hats will continue. Each side comes up with new tools and techniques, causing evolutions and a new wave of counter measures. What should we expect in the near future? As mobile devices open up to more features, and as mobile online banking adoption increases, we will continue to see a rise in attacks on mobile devices. Biometrics are striving to be frictionless authentication mechanisms and, indeed, they pose a challenge to cyber-criminals. Several POCs have already shown that some types of biometrics can already be dealt with. One more battlefield that is emerging involves digital currencies, particularly Bitcoins, which are used both to facilitate online fraudulent transactions as well as serve as a ripe target for cyber-criminals, but that is a topic for a different article. I will leave the reader with a quote by the famous Frank Abagnale: *"The police can't protect consumers. People need to be more aware and educated about identity theft. You need to be a little bit wiser, a little bit smarter and there's nothing wrong with being skeptical. We live in a time when if you make it easy for someone to steal from you, someone will."*

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

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

Shuki Peleg, Information Security and Cyber-Security Consultant

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

Nir Tordjman, Team Research Manager, ICT

ABOUT THE ICT

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

ABOUT ICT CYBER-DESK

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

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

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