IDC HERZLIYA

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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 8

February 2013 - March 2014

Highlights

This report covers the period of February - March 2014, the report covers two main subjets: 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:

- The Al-Platform Media Web forum published an announcement on the forum's technical department explaining how to disrupt the operation of unmanned aerial vehicles (UAV's). The guide described a method to disrupt the connection between the UAV and its control room and navigation systems, called GPS Spoofing.
- Several Islamist hacker groups published announcements about a combined cyber-attack against Israeli sites to take place on April 7, 2014 in protest against the establishment of the State of Israel. The participating hacker groups included: Fallaga Team, AnonGhost, Anonymous PS, Anonymous Arabe, Kalachinkov and Moroccan Agent Secret.
- The Syrian Electronic Army (SEA) continued its wave of attacks against opponents of the Assad regime in response to attacks recently carried out by a group identifying itself as the "European Cyber Army" against Syrian targets and the SEA.
- Following a report in February regarding the breach and theft of bitcoins from the large trading site, Mt.Gox, the company declared bankruptcy and the value of virtual currencies dropped significantly.
- The mining malware market has recently undergone rapid development. The malware exploits the device's resources for the purpose of mining Dogecoins and Mincoins.

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, February 2013 – March 2014[1]

Al-Qaeda's Internal Rift

- In the beginning of February 2014, Al-Qaeda's general leadership announced its rejection of the Islamic State of Iraq and Al-Sham (ISIS) and its cessation of ties with the organization against the backdrop of the latter's refusal to obey the dictates of Ayman al-Zawahiri, leader of Al-Qaeda. The announcement stirred up the discourse on jihadist Web forums and social networks, led to a wave of publications in favor of the ISIS and against the steps taken by the Al-Qaeda leadership, and increased the mutual accusations of responsibility for the failure of jihad in Syria. Several jihadist Web forums announced their support for the ISIS.
- Sheikh Abu Bakr al-Golani, leader of the Al-Nusra Front (an affiliate of Al-Qaeda in Syria), criticized the ISIS and accused it of the killing of Abu Khaled al-Suri, al-Zawahiri's representative in Syria who was sent to find a compromise to end the fighting between the ISIS and the Al-Nusra Front. With the failure to find a formula to stop the mutual clashes among jihadist factions, the hawkish argued, the enemy wins.

Syria-Lebanon

[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

- Salafi-jihadist organizations increased their attacks against Iranian and Hezbollah targets in Lebanon. The Abdullah Azzam Brigades claimed responsibility for a terrorist attack against the Iranian Cultural Center in Beirut. The Al-Nusra Front and the ISIS claimed responsibility for the launch of rockets towards Hezbollah targets in southern Lebanon.

The Maghreb

- Al-Qaeda in the Islamic Maghreb (AQIM) and the Nigerian Boko Haram threatened to attack French targets in response to France's military involvement in the Central African Republic. According to them, France excuses its military involvement in the region by claiming that it seeks to control the chaos in the country and return stability to the area, but in actuality it seeks to curb the power of Muslims in the region.

China and India

- During February-March 2014, there was an increase in jihadist calls for terrorist attacks against China and India. Sheikh Abu Dhar Azzam, a member of the Turkistan Islamic Party, called on Muslim residents of Turkistan to help the mujahideen financially and with its PR campaign against China. According to him, the Chinese and Buddhists will receive their punishment from the Muslims – an all-out war.

  Sheikh Abd al-Rahman al-Indi, a member of the Shari'a Council of Jama Ansar al-Tawhid in Hind, appealed to Muslims in India to act against the oppression, arrest and murder of Muslims by the Indian regime.

The Palestinians

- Palestinian jihadists generated discourse for the release of Muslim prisoners in Israeli and Palestinian Authority jails. Among the ways suggested to accomplish this was the abduction of Israeli soldiers as bargaining chips for prisoner exchanges, and the establishment of special units to be trained to carry out prison breaks modelled after the attempted prison breaks by members of the Islamic Emirate of Afghanistan, the Taliban in Pakistan and other jihadist groups.

Defensive Tactics

- A department administrator at the Al-Platform Media Web forum published an announcement on the forum's technical department regarding the ways in which the Syrian intelligence agency tracks people online using Skype (software used to carry out voice calls online) by intercepting email attachments and in other ways. The writer recommended downloading a software protection program such as Freegate and VPN, which allows the user to surf anonymously and more securely.[2]
- A visitor to the Hanein jihadist Web forum published an explanation, with illustrations, on how to install and use Tor, a browser plug-in that enables the user to surf the Internet anonymously and without being tracked. The visitor noted that the countries to be wary of include the Arab States (especially Syria), Israel and China.[3]

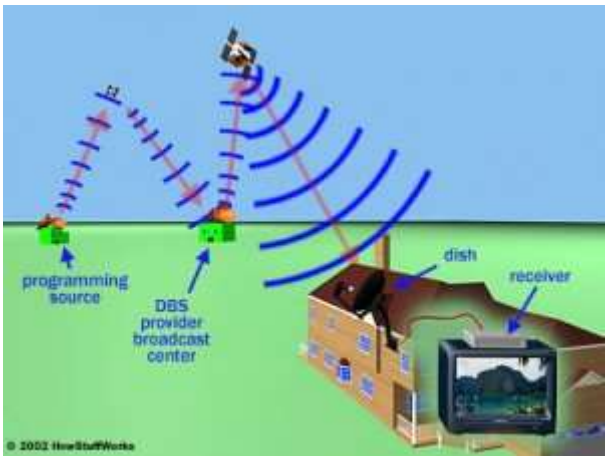
Guidance

- A visitor to the Hanein jihadist Web forum published an invitation to take part in a course on computer hacking to cover the following topics: methods of computer hacking, hiding one's identity using Remote Desktop Protocol (RDP) or a Virtual Private Server (VPS), and expertise in the BackTrack system, which includes computerized hacking and monitoring tools.[4]
- A visitor to the Snam al-Islam jihadist Web forum announced the opening of a chat room belonging to Ansar al-Mujahideen on the Paltalk software.[5] The chat room will be used to deliver reports about the organization's activities and can be accessed on the software by typing Middle East -- Islamic -- Ansar al-Moujahedin.[6]
- A department administrator at the Al-Platform Media Web forum published a warning on the forum's technical department about the ADNS 5020 computer mouse, claiming that hackers can remotely use this mouse as a camera and take photos of the user without his knowledge.[7]

---

[2] http://alplatformmedia.com/vb/showthread.php?t=39001,
[3] http://www.hanein.info/vb/showthread.php?p=2490606
[4] http://www.hanein.info/vb/showthread.php?t=351832
[5] http://www.paltalk.com (a free chat service)
[6] http://snamalislam.com/vb/showthread.php?t=22799
[7] http://alplatformmedia.com/vb/showthread.php?t=36324

- A department administrator at the Al-Platform Media Web forum published an explanation on the forum's technical department of the various steps taken by hackers to hack into computers - reconnaissance, scanning, exploitation and maintaining access – and suggested methods of defense against each one.[8]
- A visitor to the Al-Platform media Web forum reported that the Iranian infidel Web site, Ahbab Al-Hussein, had been hacked. The visitor signed the report, Marwan Al-Na'imi – "terrorist hacker".[9]
- A department administrator at the Al-Platform Media Web forum published a guide on the forum's technical department explaining how to disrupt the broadcast of television channels by detecting the frequencies through which the broadcasts are transmitted.[10]



[8] http://alplatformmedia.com/vb/showthread.php?t=36135
[9] http://alplatformmedia.com/vb/showthread.php?t=36728
[10] http://alplatformmedia.com/vb/showthread.php?t=37546

- An administrator at the Al-Platform Media Web forum published a guide on the forum's technical department explaining how to protect one's personal computer from the most powerful breach. The guide explains how to change the permissions settings via the Startup so that, in the event of a breach, the hacker will be unable to perform almost any action on the computer.[11]

- An administrator at the Al-Platform Media Web forum published a guide on the forum's technical department explaining how to hack into Facebook accounts using a method that relies on entering fake URL's similar to the real one, such as www.fecabook.com and www.faceb00k.com, in order to steal passwords.[12]
- An administrator at the Al-Platform Media Web forum published a guide on the forum's technical department explaining how to disrupt the operation of unmanned aerial vehicles (UAV's). The guide described a method to disrupt the connection between the UAV and its control room and navigation systems, called GPS Spoofing.[13]

[11] http://alplatformmedia.com/vb/showthread.php?t=38132
[12] http://alplatformmedia.com/vb/showthread.php?t=36526
[13] http://alplatformmedia.com/vb/showthread.php?t=37904

- A visitor to the Al-Minbar jihadist Web forum published the fourth instalment of the "Jihadist Encyclopedia", a collection of security directives for the mujahideen, including explanations on how to gather intelligence information, information on anti-take weapons, an explanation of military tactical communication, safety guidelines for forum users, and more.[14]

Social Networks

- On March 18, a Twitter account was opened under the name Al-Nusra al-Maqdisiyaa (Help from Jerusalem). The account is run by Palestinian Salafi-jihadist supporters affiliated with the ISIS.[15]

The banner of the Al-Nusra al-Maqdisiyaa Twitter account

- Palestinian Salafi-jihadist supporters of the ISIS used their Twitter account to call for help with their Twitter PR campaign to free Salafi-jihadist prisoners in Tunisia. The campaign began on April 27, 2014.[16]

[14] http://alplatformmedia.com/vb/showthread.php?t=42079
[15] https://twitter.com/dawlanoor
[16] https://twitter.com/dawlanoor/status/461233296425226240/photo/1, #أسرى_التوحيد_في_تونس

One of the banners posted to Twitter in the framework of the campaign, which reads:
The Lions of Tawhid in Islamic Tunisia: Help your Oppressed and Tortured Imprisoned Brothers, Free Them From Their Captivity

- Sheikh Anjem Choudary, a radical Islamist preacher in England, posted a request on his Twitter account for help with the PR campaign for the release of Sunni Muslims, including Sheikh Umar Bakri, from the hands of Lebanese security forces. Bakri, a radical Islamist preacher, founded the Al-Muhajirun organization in England in 1996 after leaving Hizb al-Tahrir. In 2005 he was expelled from Britain for incitement and found refuge in Lebanon.

One of the banners produced in the framework of the PR campaign on Twitter for Bakri's release

- On March 23, 2014 a Twitter account was opened by Palestinian Salafi-jihadist activists from the Gaza Strip who are fighting among the ranks of the ISIS in Syria, under the name: "The Mujahideen of Gaza in the ISIS: The Abu al-Nur al-Maqdisi Battalion". The account included praise for ISIS operations and focused on fighters of Palestinian origin among the ranks of the organization.[17] The battalion was named after Abu al-Nur al-Maqdisi, the leader of the Ibn Taymiyyah Mosque in Rafah and the spiritual leader of Jund Ansarallah fi Bayt al-Maqdis (The Army of Supporters of Allah in the Environs of Jerusalem), which is affiliated with Al-Qaeda. In June 2009, he was killed along with several of his supporters in the Ibn Taymiyyah Mosque in Rafah by members of Hamas after he announced the establishment of an Islamic Emirate in the Gaza Strip.

From left to right: The banner of the Twitter account; Mujahideen waving a sign on which it is written "Mujahideen from Gaza in the ISIS"

- Visitors to the Hanein jihadist Web forum held a discussion concerning the tens of thousands of fictitious followers of the ISIS's official Twitter account (https://twitter.com/wa3tasimu), an act that could cause it to be shut down. One visitor asked the other members of the forum to report the fictitious accounts while another visitor recommended re-tweeting announcements from the official account in order to confirm its credibility.[18]
- The Ansar al-Haqq jihadist media institution announced the launch of a new Facebook page and asked supporters of the mujahideen to show support for the page (the previous page was shut down three times after being reported to Facebook administrators).[19]

[17] https://twitter.com/dawla_gaza
[18] http://www.hanein.info/vb/showthread.php?t=358601
[19] http://www.hanein.info/vb/showthread.php?p=2491155

Cyber Attacks

- According to an article that was published[20] on February 28, a new study carried out by the company FireEye[21] showed that the average company is hit by a cyber-attack every 1.5 seconds, demonstrating an increase of 100% since the previous year. It also showed an increase in the number of countries in which malware was discovered, from 184 in 2012 to 206 in 2013. The attacks originated in the United States, Germany, South Korea, China, Holland, England and Russia.

  On the other hand, the main countries that served as targets of APT attacks were the United States, South Korea, Canada, Japan, England, Germany, Switzerland, Taiwan, Saudi Arabia and Israel.

- A news item from March 2, 2014 revealed[22] that, according to a study done by Kaspersky Lab, Russia topped the list of countries hit by attacks on mobile phones, with 40.34% of all attacks. India came in second with 7.9%. Most of the attacks were for phishing purposes as well for theft of banking details. Next on the list was Vietnam (3.96%), Ukraine (3.84%), England (3.42%), Germany (3.2%), Kazakhstan (2.88%), the United States (2.13%), Malaysia (2.12%) and Iran (2.01%).

  During 2013, approximately 100,000 new malware were diagnosed in the mobile field compared to 40,059 in 2012. 98.1% of all malware in this field in 2013 targeted Android devices, mainly due to the Android's architectural weaknesses and increasing popularity.

  Approximately 4 million malicious applications were used by cyber-criminals in order to create malware for Android device, most of which targeted users' money. The number of malware designed for phishing, theft of bank details and money from bank accounts increased 20-fold according to the study.

  Kaspersky Lab added that it had blocked 2,500 attempts to infect banking targets with Trojan Horses, defined as the most dangerous malware for users in the mobile field. At the start of 2013, the company identified 64 known banking Trojans but by the end of the year the number

[20] http://www.esecurityplanet.com/network-security/average-enterprise-is-hit-by-a-cyber-attack-every-1.5-seconds.html
[21] http://www2.fireeye.com/advanced-threat-report-2013.html
[22] http://indianexpress.com/article/india-others/india-second-on-cyber-attacks-on-mobile/

had stood at 1,321, and it is assumed that the number will grow, both in the countries surveyed as well as other in countries in 2014.

- A new study carried out by Arbor Networks, funded by the Economist Intelligence Unit, revealed[23] interesting data about the preparedness of businesses around the world for cyber-attacks. The study included 360 business leaders, 73% of whom held senior management positions around the world, including the Middle East.

  The study revealed that 76% of the companies suffered cyber-attacks during the past two years, 39% still do not have a plan of response to such events, and only 17% are fully prepared for cyber-security related events.

  A senior employee of a company responsible for its Middle East operations said that the region has experienced a steady rise in information leaks, attacks aimed to prevent service, and system errors that had a significant impact on business conduct, financial losses and damage to reputation. According to him, organizations in the region are beginning to wake up to the need to cope with such events. The better-prepared companies depend on their IT departments to lead the process but most of the companies use third-party services.

  The study's other findings show that the level of preparedness of the companies surveyed depended on an understanding of the various threats:

  - 40% felt that a better understanding of the threats would help them to better prepare;
  - The existence of an official plan or team has a significant influence on management's sense of preparedness;
  - Half of those surveyed felt that they cannot predict the business impact of information leaks;
  - The emphasis on damage to reputation prompts the implementation of processes and plans in the event of such incidents;
  - Two-thirds maintained that having a response to cyber-attacks can improve a company's reputation
  - Companies that experienced such attack during the past year were twice as likely to receive services from third party providers than companies that did not experience any

[23] http://www.bi-me.com/main.php?c=3&cg=2&t=1&id=64916

cyber-attacks;

- 57% of the companies do not independently report cyber-attacks if they are not legally required to do so;
- Only one-third of the companies share information about incidents with other organizations.

Russian Targets

- The hacker group, the Electronic Army of the Caucasus Emirate, published a video in which it declared:

  "To Russian Government and Russian citizenship! Anonymous kavkaz believes that Russia are the reason of injustice and nations genocide in the world so we decided to continue our cyber war till we see our victory destroying Russian economy and system. We fight for Islam and to return kavkaz to own people. We are all around the world. We are far and we are near to you. You can see us, listen us, finally you can fear us. We promise you to destroy your injustice system. We will not stop till you genocide Muslims in kavkaz till you imprison them, till you support Syrian and Iranian governments. We are your black mare. Count your last time. With each passing day we are becoming more and more. And one day will come for all Muslims in Caucasus when we will crush your system, and you will have such consequences, which Russia had not yet seen count your last breath".

  The group also claimed responsibility for hacking into several Russian banks, including Alpha Bank and VTB-24, and for the temporary shutdown of the banks' Web sites in revenge for Russia's war on Islam and in response to the hosting of the Olympic Games in the North Caucasus.[24]

[24] https://twitter.com/AnonsCaucasus;http://vdagestan.com/ar/archives/15618;https://www.youtube.com/watch?v=Fut8M_uwbGQ

The announcement on the vdagestan jihadist Web portal regarding the attack by Anonymous Caucasus against Russian banks

Israeli Targets

- Several Islamist hacker groups waged a combined cyber-attack against Israeli Web sites on April 7, 2014 in protest against the establishment of the State of Israel. The participating hacker groups include: Fallaga Team, AnonGhost, Anonymous PS, Anonymous Arabe, Kalachinkov and Moroccan Agent Secret.[25]

[25] #OpIsraelBirthday ; http://opisraelbirthday.blogspot.co.il/

The banners created in honor of the cyber-attack

USA Targets

- In an announcement from March 8, it was reported[26] that members of "Anonymous" had managed to hack into the computer systems of John Hopkins University, which admitted[27] to the breach the previous day.

  103 MB of information was stolen from the university's database, including the personal details of staff and students in the biomedical engineering department. A spokesperson for the university claimed that the FBI had informed the university of the breach a day after it received an extortion demand from an individual who identified himself with "Anonymous" and claimed that the stolen information would be published if he was not given the user name and password to access the university's network. ("The extortionist threatened to post stolen BME Department data if the university did not provide user ID and password credentials to access the university's network. The university did not and will not provide that access.")

  The spokesperson's message noted that the breach apparently took place sometime last year but was only discovered after an announcement was posted on Twitter that the department's server had been breached. According to the spokesperson, the code error that caused the breach of the database was identified and fixed but the information had already been leaked.

[26] http://news.softpedia.com/news/John-Hopkins-University-Breached-Blackmailed-by-Anonymous-Hackers-431189.shtml
[27] http://releases.jhu.edu/2014/03/07/server-breach/

He added that there was no proof that the leaked information included social security numbers, birth dates, credit card numbers, financial information or any other details that could be used to steal one's identity.

According to him, most of the stolen information belonged to employees and was available on the department's Web site. Nevertheless, he added that it was brought to their attention that week that the database also included information about 848 students in one of the department's design courses who were registered between 2006-2013, not including grades but including student assessments of the course and their colleagues.

The spokesperson declared that the university was working to reclaim the information that was stolen and remove it from the Internet, and informed those affected both within and outside of the university.

- An announcement published on March 8 stated[28] that electrical installations in the United States had become a popular target for hackers as they pose a danger to America's ability to supply the required power needs. Last year the energy sector in the United States was subject to over 150 cyber-attacks, according to a report[29] titled, "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat", which was published in February by the Bipartisan Policy Center.

  The report noted that the two-day shut-down that took place in 2003 caused an estimated six billion dollars in damage. Although this was not the result of a cyber-attack, the incident illustrated the necessity of the continuous operation of the power grid. The report also determined that, in order to protect the electric grid from attack, the private sector must take the necessary steps to minimize weakness in the networks that operate and connect electricity providers with distributors. The report also included a recommendation to establish an organization for the electricity sector to protect the grid from hackers - an "Institute for Electric Grid Cybersecurity". It was recommended that participation in this institute be free but that the government should encourage companies to join by offering a series of incentives such as the guarantee of insurance against financial losses in the event of a cyber-attack.

[28] http://www.allgov.com/news/controversies/153-cyber-attacks-on-us-energy-grid-in-one-year-140308?news=852631

[29] http://bipartisanpolicy.org/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf

The energy industry[30] is the top target for cyber-attacks. If you want to disrupt anything, attack the electricity infrastructure. Another factor that places the energy sector at the highest risk is the range of attackers who are interested in targeting this industry. A report titled, "Targeted Attacks Against the Energy Sector",[31] claimed that attackers include youths, business competitors, political activists, hostile elements with companies, cyber-criminals and even countries – all of which are interested in stealing information or damaging the electric grid.

The study determined that between July 2012 and June 2013, 74 cyber-attacks were registered on average per day, 16.3% of which targeted the energy industry, placing it second only to the government and public sector, which was hit with 25.4% of the attacks. The Department of Homeland Security in the United States reported last year that that the ICT-CERT team[32] had responded to over 200 incidents between October 2012 and May 2013, 53% of which were directed at the energy industry, but stated that no attack had succeeded in causing catastrophic damage to the energy grid. However, opinions are divided regarding the degree of danger; there are experts who believe that while the dangers are real and should raise concern, they are unlikely to cause catastrophic or long-term damage. Others believe that that country's economy could be paralyzed for several months and even more than one year until the critical infrastructure systems can be re-built.

Nevertheless, the study determined that the increasing number of systems connected to the grid, coupled with the centralized control of Industrial Control Systems (ICS), mean that the risk of future attacks will increase. Companies in the energy field must be aware of the risks and plan accordingly to protect their sensitive data as well as their ICS or SCADA networks. Therefore, some ICS experts have been warning for years about the risks involved not only in using a central control system but also in the fact that they are all the product of a single

[30] http://www.csoonline.com/article/748580/energy-sector-a-prime-target-for-cyber-attacks?page=1

[31] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

[32] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

company – Siemens – which adds to its vulnerability. Not to mention the sheer number of devices connected to the electric grid, whether via small power plants such as windmills or solar stations, or smartphones in private homes that exponentially increase potential areas of attack. The assumption is that the number of "smart sensors" connected to the grid will increase from 3.5 billion today to over a trillion in the next decade.

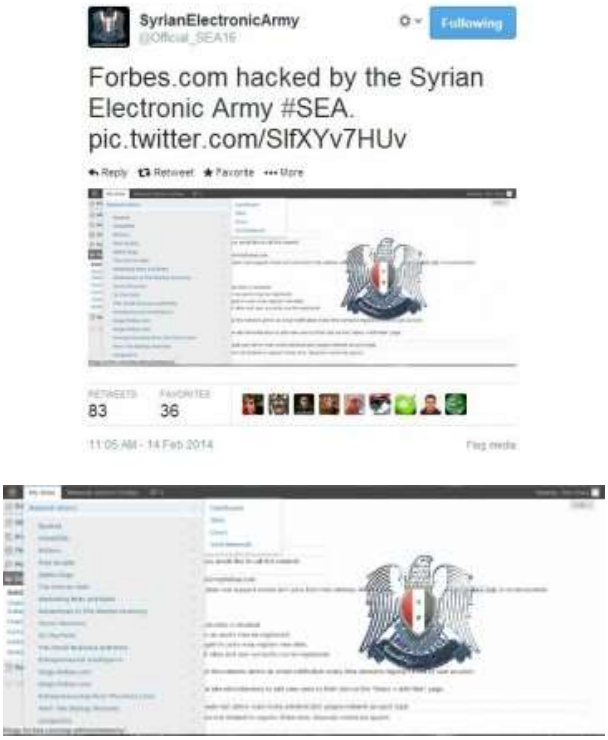
ICS-CERT reported last year about a series of Brute Force attacks on gas compression station operators, which is significant because these systems were connected to the Internet, despite the recommendation by ICT-CERT to avoid this.

On March 24, it was published[33] that in 2013 the American FBI had informed thousands of companies that they had fallen victim to cyber-attacks. Lisa Monaco, the Homeland-Security and Counterterrorism Adviser to the White House, announced that over 3,000 companies had received such a warning. Most of these updates (approximately 2,000) were made with a telephone call or a visit by an FBI representative, while FBI agents simultaneously tried to provide useful information for dealing with the attack. This publication illustrated the U.S. government's involvement in protecting the private sector from cyber-attacks.

The Syrian Electronic Army

- On February 14, members of the Syrian Electronic Army announced[34] that they had managed to hack into the Web site of Forbes Magazine and included a screenshot[35] that apparently proved their claim. The announcement also stated that the site had been built using the WordPress platform;

[33] http://www.washingtonpost.com/world/national-security/us-notified-3000-companies-in-2013-about-cyberattacks/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html
[34] https://twitter.com/Official_SEA16/status/434252085597466624
[35] https://twitter.com/Official_SEA16/status/434252085597466624/photo/1/large



Another announcement was published[36] that mocked the ease with which they had hacked into the Forbes website administrator account;

An article regarding the incident[37] included a screenshot[38] of the Web page that was apparently damaged by the hackers;

[36] https://twitter.com/Official_SEA16/status/434290687832375296
[37] http://hackread.com/syria-electronic-army-hacks-forbes-site-twitter/
[38] http://hackread.com/middleeasternet/wp-content/uploads/2014/02/the-frobe-magzine-website-and-twitter-account-hacked-by-syrian-electronic-army.jpg

It seems that they also managed to hack[39] into several Twitter accounts associated with the magazine - @ForbesTech, @samsharf, @TheAlexKnapp.

After they published several announcements on February 28 in which they warned of the imminent breach of CENTCOM computers, in the afternoon hours of March 14 members of the Syrian Electronic Army posted[40] on the group's Twitter account that they had successfully hacked into CENTCOM's computers in response to President Obama's decision to launch an electronic attack on Syria.

Four minutes after the initial announcement was published, they published a second

[39] http://www.ibtimes.co.uk/forbes-com-hacked-by-syrian-electronic-army-because-hate-syria-1436415
[40] https://twitter.com/Official_SEA16/status/444506846989402112

announcement that included a screenshot[41] of the system after it was hacked.

The announcement claimed that it was part of a continuous operation and that they had managed to hack into many systems. They claimed to have gotten their hands on a file that contained 21,866 classified documents.[42] Indeed, three minutes later, another announcement was published[43] that stated that they would provide additional details in the coming days regarding the hundreds of documents that they allegedly obtained during this breach;

[41] https://twitter.com/Official_SEA16/status/444507843475955712
[42] http://www.scmagazine.com/syrian-electronic-army-claims-it-obtained-us-central-command-docs-via-hack/article/338371/
[43] https://twitter.com/Official_SEA16/status/444508595615711232

A short while later, an announcement was published[44] in which a spokesperson for CENTCOM claimed that the announcement was "an absolute fake". In response, members of the Syrian Electronic Army published an announcement[45] in which they retorted that they still have not published all of the information at their disposal and that the operation is still underway as far as they are concerned.

In the evening hours of March 15, members of the Syrian Electronic Army published an announcement[46] on Twitter according to which they had managed to hack into the Web site of the Syrian Opposition Coalition (http://etilaf.org).

Several minutes later, they published another announcement[47] in which they provided alleged proof of the breach.[48]

[44] http://tbo.com/list/military-news/centcom-denies-claims-its-computers-were-hacked-20140314/
[45] https://twitter.com/Official_SEA16/status/444560581119705088
[46] https://twitter.com/Official_SEA16/status/444903639153643520
[47] https://twitter.com/Official_SEA16/status/444906503489986563
[48] http://www.zone-h.org/mirror/id/22015751

It also published an announcement on the group's Web site[49] in which it claimed to have hacked into two more sites.

[49] http://www.sea.sy/article/id/2033/en

The "European Cyber Army" Versus the "Syrian Electronic Army"

- In response to the frequent cyber-attacks carried out by the Syrian Electronic Army,[50] a group identifying itself as the "European Cyber Army" attacked Syrian targets in recent days. A look at its Twitter account[51] revealed that the group has been active since January 12, 2014 and has posted 670 tweets to date, some of which were even in Russian, French and Arabic.

On March 12, the Syrian Electronic Army published warnings not to continue attacking the Western media or else Syrian government targets would be attacked;

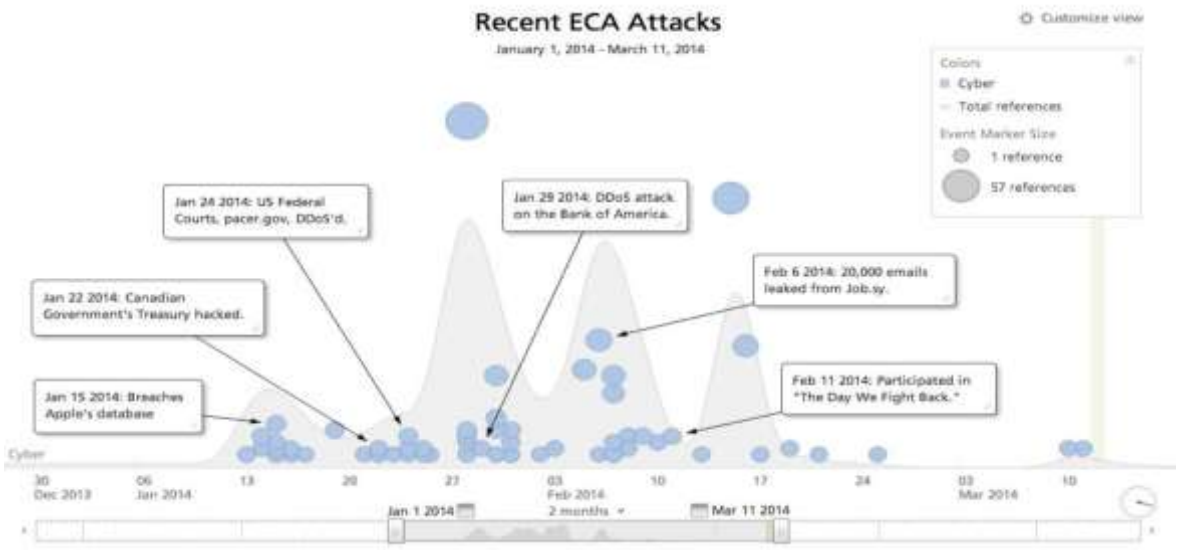
[50] https://twitter.com/ECA_Legion/status/444915981056761858/photo/1
[51] https://twitter.com/ECA_Legion

On March 15, several announcements were published regarding the attack that was allegedly carried out against the Syrian Customs Authority (http://www.customs.gov.sy) in response to news of the CENTCOM breach,[52] including a warning to "stay away from the West".[53]

[52] https://twitter.com/ECA_Legion/status/444874956313493504
[53] https://twitter.com/ECA_Legion/status/444877018573053953

The announcement included a link to a separate announcement[54] containing information about the breach of the Syrian Customs database, the database structure and the information that was leaked. Another announcement[55] included links to seven announcements (all of which are no longer available) that allegedly included over 20,000 Syrian email addresses and passwords.

The following is a comprehensive analysis[56] of ECA operations and an overview of attacks:



An analysis of attacks published by Recorded Future

[54] http://pastebin.com/cf2a02dM
[55] http://paste.meowstars.org/?71869c6789a860ff#4SvaJyYQEllP4jv0LXBpsZ2cgpbCHNjBckj3RYKB9fA
[56] https://www.recordedfuture.com/european-cyber-army-analysis

In the framework of its overall operations, and as part of its cyber-attacks against Syria, the European Cyber Army took focused action against the Syrian Electronic Army during the month of March in several arenas:

Exposure of Syrian Electronic Army Members – an announcement was published[57] on March 21 that supposedly included the names of Syrian Electronic Army members, and was followed by another announcement[58] about Victor, the founder of the Syrian Electronic Army, who they claim was captured by the rebels.

Internet Shutdown in Syria – the group claimed[59] that the Internet shutdown in Syria, which took place on March 20, was the result of the European Cyber Army's cyber-attack as revenge for Syrian Electronic Army attacks against the West.

Database Breaches and Leaks – the breach[60] of the Web site belonging to the Syrian Center for Documentation (http://www.documents.sy) and the leak of the site's database.[61]

[57] http://pastebin.com/ANbFZFzp
[58] http://pastebin.com/QyVhG5BD
[59] https://twitter.com/ECA_Legion/status/446660424969093121
[60] https://twitter.com/ECA_Legion/status/447209444846608384
[61] http://pastebin.com/b6iTUsM0

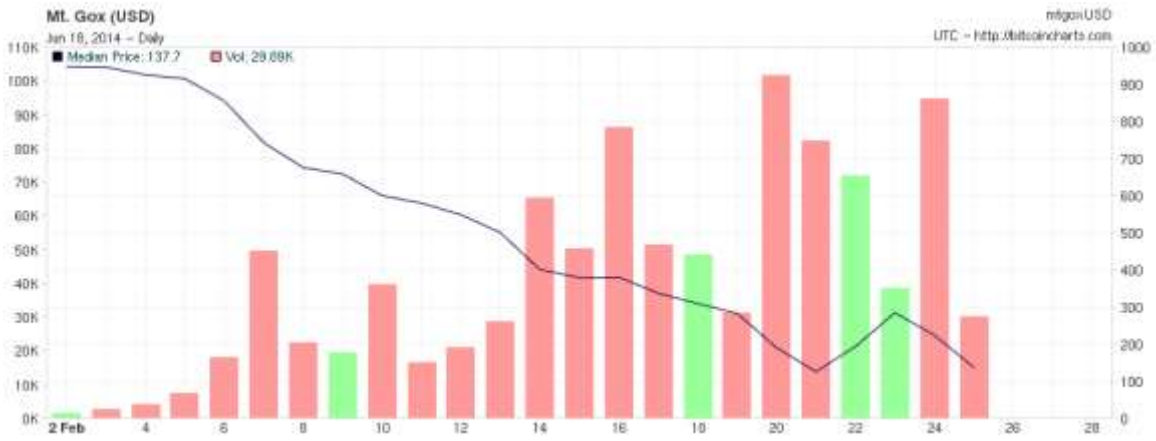
Cyber-Crime and Cyber-Terrorism, February - March 2014

Recent years have seen an increasing number of cyber-attacks on political targets, critical infrastructure, and the Web sites of commercial corporations. These attacks, which are also receiving increasing amounts of international attention, are perpetrated by states (which do not take responsibility for them), groups of hackers (such as Anonymous), criminal organizations and lone hackers. We believe that terrorist organizations are working in close collaboration with criminal organizations, are learning from their attempts [at cyber-crime], and may even be hiring their services. In light of this, it is important to examine and analyze cyber-crimes attributed to criminal organizations, as well as new development trends and patterns. The following information was culled from the visible (OSINT) and invisible ("dark Web")[62] Internet between February - March 2014.

Virtual Currency – Bitcoin Updates

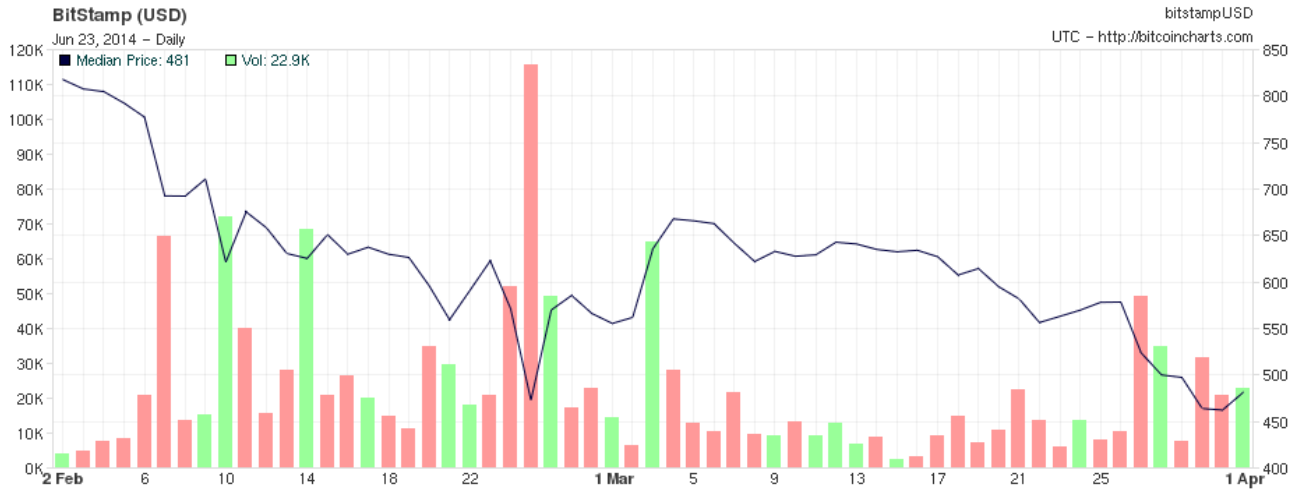
- The following diagram shows the bitcoin price chart on the exchange site, Mt. Gox, in February 2014. The columns refer to the volume of the currency and the median price in USD. In the beginning of February, the exchange rate stood at $1,000 for one bitcoin but over the course of the month it dropped to $200 following reports of breaches and the theft of bitcoins from the Web site, which led to its bankruptcy as will be seen below.

[62] 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.



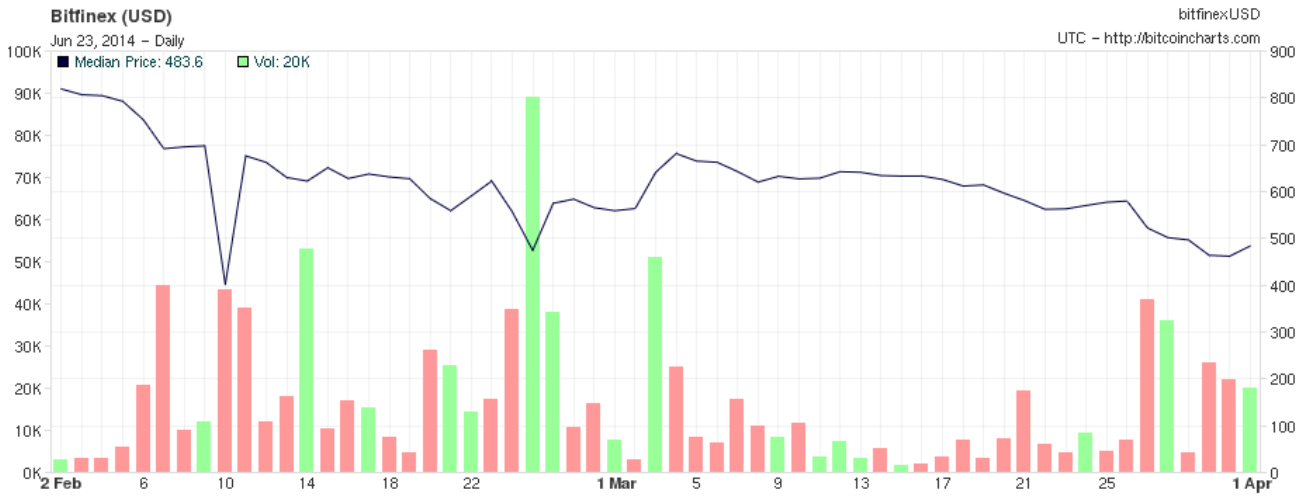
Bitcoin price chart in Mt. Gox for February 2014[63]

- The bitcoin experienced several significant events when a number of trading sites were breached, including Mt. Gox, a leading trading site at the time, which led to the collapse of the currency on the site itself and to a decrease in the currency value on other sites. There are almost 100 different trading sites on the market[64], each of which trades independently, leading to different prices. Sometimes a significant arbitrage gap exists between the various Web sites. The following diagrams illustrate the bitcoin price chart for two leading trading sites:



Bitcoin price chart in BitStamp for February - March 2014[65]

[63] http://bitcoincharts.com/charts/mtgoxUSD#rg60zczsg2014-02-01zeg2014-02-28ztgMzm1g10zm2g25zv
[64] http://bitcoincharts.com/markets/
[65] http://bitcoincharts.com/charts/bitstampUSD#czsg2014-02-01zeg2014-03-31ztgMzm1g10zm2g25zv



Bitcoin price chart in BitFinex for February - March 2014[66]

Regulations around the World

- Towards the end of January 2014, the Central Bank of Russia published[67] a statement asserting that virtual currency should be avoided. It addition, it warned against converting the national currency (ruble) into virtual currency as such action may be considered suspicious activity (money laundering or terrorism financing).
- Towards the end of February, Janet Yellen, the Chair of the Board of Governors of the Federal Reserve System, testified that the Federal Reserve has no authority to supervise the bitcoin and appealed to Congress to examine the legality of the issue:

  "Bitcoin is a payment innovation that's taking place outside the banking industry. To the best of my knowledge there's no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate. So the Fed doesn't have authority to supervise or regulate Bitcoin in anyway... But certainly it would be appropriate for Congress to ask questions about what the right legal structure would be for digital currencies."
- In the beginning of March, the Japanese government declared that it does not recognize the bitcoin as tradable currency but stated that bitcoin transactions could be taxable.[68]

[66] http://bitcoincharts.com/charts/bitfinexUSD#rg60zczsg2014-02-01zeg2014-03-31ztgMzm1g10zm2g25zv
[67] http://techcrunch.com/2014/02/07/russia-bans-bitcoin
[68] http://www.globalpost.com/dispatch/news/afp/140307/japan-says-bitcoin-not-currency-taxable

The Collapse of the Mt. Gox Trading Site

- Evidence[69] of theft and fraud involving the bitcoin currency existed back in 2011 but nothing like the collapse of Mt. Gox, a trading site in Japan considered to be one of the largest in the world. It was reported in the beginning of February that, as a result of problems with the site, users would be unable to redeem their money from the site. Despite declarations by Mark Karpeles, the CEO of Mt. Gox, in an interview with the Wall Street Journal,[70] the currency suffered a drastic drop in value to approximately $120 while the median price on other trading sites stood at $570.[71]

  Towards the end of February, a document was leaked that claimed that the site had been compromised for a long period of time and approximately 750,000 coins (with an estimated value of hundreds of millions of dollars) had been stolen over the years. On February 28, the site filed for bankruptcy after confirming the leak and claiming that in addition to the 750,000 coins "whose location is unknown", 100,000 coins belonging to the company itself were also missing.[72]

  The collapse of the site led to several developments in the world of virtual currency. As a result of several class action lawsuits, the company transferred information about clients that could reveal the details of users and the identity of virtual wallet holders who used the site.

The Development of Malware in the World of Virtual Currency

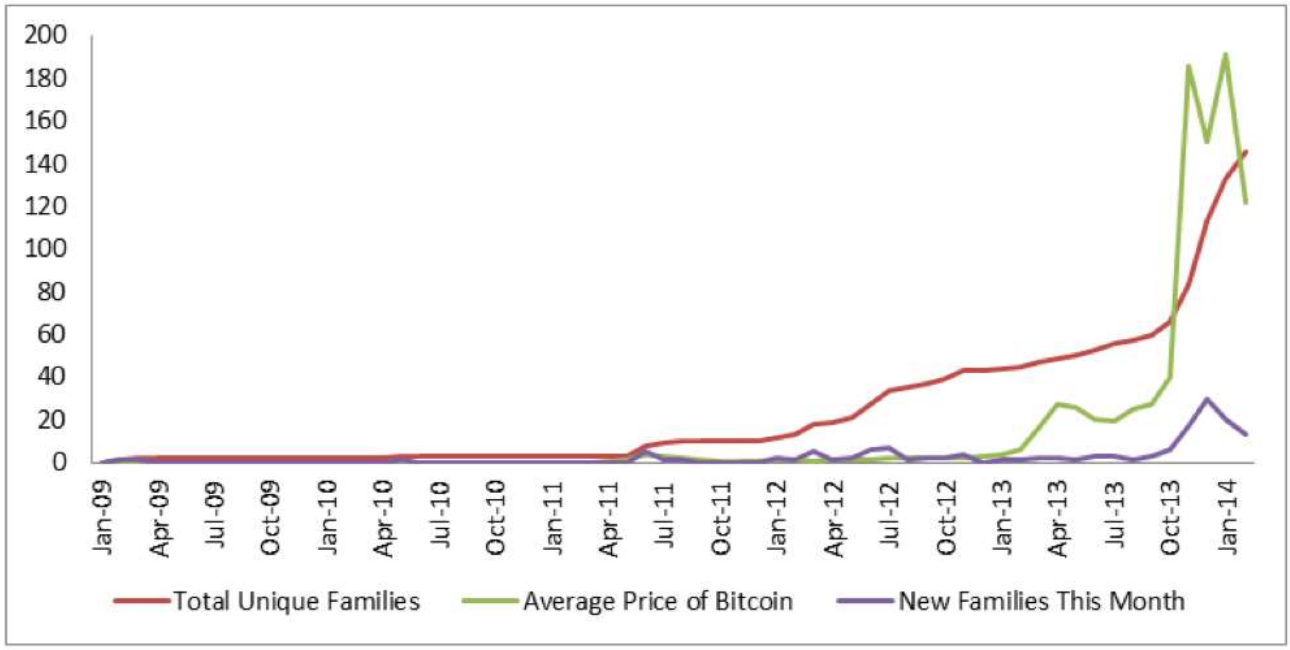
- Symantec published[73] an announcement regarding a new malware called Linux.Darlloz[74] that attacks ARM and MIPS processor-based computers, as well as Intel-processors popular in laptops and desktop computers. ARM processors are common in various devices, including smart phones, Android TV tablets, etc. According to the report, the malware was found in approximately 31,000 devices.

  The malware exploits the device for the purpose of mining virtual currencies such as Dogecoins

[69] http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency
[70] http://online.wsj.com/article/BT-CO-20140217-702655.html
[71] http://money.cnn.com/2014/02/20/technology/innovation/bitcoin-mtgox/index.html?iid=EL
[72] http://newslines.org/mt-gox
[73] http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency
[74] http://www.symantec.com/security_response/writeup.jsp?docid=2013-112710-1612-99

and Mincoins. The assessment that the malware is not intended for the common virtual currency, the Bitcoin, stems from the fact that the mining process of Dogecoins and Mincoins is still not advanced and requires extensive resources since they are new.

- A study published by Dell's SecureWorks security division found that there are about 150 different malware.[75]



SecureWorks' chart showing the correlation between Bitcoin's price increases and the creation of new Bitcoin-targeting malware.

Silk Road 2 Hacked

- In the beginning of October, it was reported[76] that the illegal trading site, Silk Road, which operated on the darknet using TOR protocol, had been shut down. New trading sites were opened, including one that went by the same name and even earned the nickname, "Silk Road 2". In February 2014, the site administrator published an announcement that the site had been

[75] http://www.forbes.com/sites/andygreenberg/2014/02/26/nearly-150-breeds-of-bitcoin-stealing-malware-in-the-wild-researchers-say/?ss=cio-network

[76] An in-depth analysis was published in cyber report 5: http://www.ict.org.il/Article/63/ICT-Cyber-Desk-Review-Report-5

breached and that all of the bitcoins – an estimated 4,500 BTC - had been stolen.[77] Another report by the site administrator of Defcon stated that 26% of the site's regular users had lost all of their money. The administrator denied rumors that the breach had been carried out by an employee or was embezzled. In addition, he promised to repay the stolen funds.[78] A user named Oracle published[79] a post in which he revealed the details of the alleged hacker, named DOXX, who lives in Chechnya and was responsible for the breach and theft.

The Theft of Medical Information

- The medical records of 55,900 patients in the public health system in San Francisco were stolen[80] from an external collections company. The breach, which apparently took place on February 5, resulted in the disclosure of names, collection details, birth dates and, in some instances, the social security numbers of patients in San Francisco General Hospital as well as several public health clinics in the city. Most of the records belonged to uninsured patients who were treated between August-November 2012. The head of the public health department announced that they were working to inform all of those affected by the breach. According to senior officials, there was no evidence at the time that the stolen data had been misused. The authorities, including the Attorney General of California, provided an update about additional breach, claiming that it included 169,000 records of public health patients in Los Angeles. This incident was one of many security breaches in hospitals in northern California or in hospital systems in recent years.

Saudi Arabia: A Flourishing Trade in Illegal SIM Cards

- An article from March 11 described[81] the phenomenon of trafficking in illegal SIM cards in the kingdom, which led police in Jeddah to raid vendors selling on the streets of the city while warning that punitive measures will be taken for violation of local laws. The phenomenon

[77] http://www.deepdotweb.com/2014/02/13/silk-road-2-hacked-bitcoins-stolen-unknown-amount
[78] http://www.deepdotweb.com/2014/02/16/defcons-latest-post-we-will-repay-the-stolen-funds
[79] http://www.deepdotweb.com/2014/02/18/alleged-silk-road-2-0-hacker-doxxed
[80] http://www.bizjournals.com/sanfrancisco/blog/2014/03/data-torrance-55-900-san-francisco-public-health.html
[81] http://www.arabnews.com/news/538256

continues despite recent raids by the authorities due to, among other things, the large number of illegal workers in Saudi Arabia who turned the trafficking of illegal SIM cards into the most profitable business for vendors.

The above measures were taken by the authorities due to concern that these cards could be used for suspicious activities since the owner's user ID number is not known. Therefore, despite strict guidelines, these cards – designed for devices by most major telephone manufacturers - continue to be sold in the kingdom without customers having to present proof of their identity. The vendors are taking advantage of loopholes in the regulations in order to get cards and sell them illegally, with some phone store owners helping the vendors for a fee.

The Saudi Communications and Information Technology Commission (CITC) announced back in 2012 that users would be required to enter their ID number along with the card number in order to charge mobile phone credits or transfer money to another user, in order to put an end to the misuse of SIM cards by anonymous users. In addition, the CITC determined that only legal residents of the kingdom would be able to purchase SIM cards by presenting proof of their residency.

Meanwhile, there is also a thriving trade in legal SIM cards whose owners sell them in the black market while others sell them to cell phone stores that, in turn, transfer them to street vendors. A source in Telecom who chose not to be identified explained that a customer cannot purchase more than ten SIM cards with one ID number. The option to purchase more is only give to private companies that have approved commercial listings by the Chambers of Industry and Commerce or to private companies that purchase these cards for their employees.

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 Cyber@ict.org.il.