Cyber-Terrorism Activities

Report No. 3

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

International Institute for Counter-Terrorism (ICT)

Additional ICT resources are available on ICT’s website: www.ict.org.il

Highlights

This 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:

- In a manifesto published by Al-Furqan in February, 2013, Sheikh Abu Sa'ad al-'Amili, a prominent Salafi-jihadist, discusses possible causes for lulls in the activity of several prominent jihadist Web forums, and proposes ways to increase the forums' activity.
- The Global Islamic Media Front (GIMF) publishes a new encoding program, Asrar Al-Dardasha [The Secrets of Chatting], for use in communications among mujahideen.
- Islamic legal scholar Abu Mundhir al-Shanqiti, the head of the Fatwa Committee of the Salafi-jihadist portal Minbar Al-Tawhid wal-Jihad, publishes a fatwa permitting hacking into US commercial Web sites, and offering a religious justification for cyber-attacks against the infidel.
- Several Palestinian groups issue guidelines for hackers.
- The international conglomerate of hackers known as "Anonymous" launches hostile cyber-operations against Israel, Palestine and Baluchistan – among other countries.
- An Egyptian telecommunications undersea cable is sabotaged, disrupting Internet service in that country and highlighting growing threats to international Internet service.
- The Web sites of AmericanExpress and other US financial institutions are hacked, temporarily disrupting their service.
- The Cyber-Desk Team extensively reviews phishing as a tool of cyber-attack, as illustrated by an analysis of a watering hole attack on the ICT's own Web site.
- This Newsletter's Case Study highlights a series of increasingly serious attacks on computer networks in South Korea, and compares the relative dangers of denial of service (DDoS) and "denial of computer" (DDoC) attacks.
- In this issue, Guest Contributor Swapnil Kishore reviews governments' use of "patriotic hackers" to counteract cyber crime.

Table of Contents

Electronic Jihad 1

Key Topics of Jihadist Discourse, February 2012.. 1

Jihadist Propaganda 2

Defensive Tactics 5

Offensive Tactics... 7

Cyber-Crime and Cyber-Terrorism, February-April 2012 9

Analysis of a Watering Hole Attack on the ICT Web Site 20

Case Study 24

From Preventing Service to Blocking Computers: Analysis of an Attack on South Korea......... 24

Guest Contributor... 30

An Act of Cyber Patriotism or an Act of Cyber Vengeance? 30

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 2012[1]

- In light of US President Barak Obama's promise to withdraw troops from Afghanistan in 2014, the Islamic Emirate of Afghanistan iterated that it would continue armed resistance until the end of the US occupation.
- Al-Qaeda in the Arabian Peninsula (AQAP) denounced France and its allies for waging war against jihadist groups in northern Mali, and insisted that every Muslim is obligated to engage in jihad, or to support it financially or through propaganda.
- During the latter half of February 2013, Muhammad al-Rubaish exhorted Muslims not to succumb to Western attempts to thwart efforts to impose Islamic law [shari'a]. Although implementing shari'a will exact many victims and martyrs from the Muslim Nation, said al-Rubaish, continued da'wa [missionary efforts] and jihad are guarantors of its implementation. Al-Rubaish also urged Sunnis in Arab lands who are directly threatened by Iran-backed Shi'ites to take up arms in self-defense and prepare for imminent battle.
- Boko Haram, a Nigerian jihadist group, took responsibility for abducting seven French citizens from Cameroon in protest against the French-led war against jihadist groups in northern Mali.

[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.

- A new Salafi-jihadist group has been established in Mauritania: Ansar Al-Sharia fi Bilad Sinqit.
- The Ibn Taymiyyah Media Center, which is affiliated with the Salafi-jihadist movement in the Gaza Strip, exhorted Muslims to focus on liberating brethren from prisons in Israel and the Palestinian Authority – for example by kidnapping Israeli soldiers and using them in negotiations, or by breaking into the prisons.
- The Global Islamic Media Front (GIMF), which is affiliated with Al-Qaeda and other jihadist groups, published a new computer encoding program: Asrar Al-Dardasha [The Secrets of Chatting].
- For a limited time only, the jihadist media center Fursan Al-Balagh welcomed new recruits interested in engaging in propaganda for the mujahideen and Islam.
- Two new jihadist portals were recently launched: The Islamic Caliphate, a Web forum; and Al-'Itisam, a media institution. Both will cover the Islamic State of Iraq.
- Sipah-e-Sahaba Pakistan (SSP), a Pakistani Salafi-jihadist group, launched a new magazine in English titled, *Al-Rashidun* [The Righteous].

Jihadist Propaganda

Fighting Jihad Online: In late December 2012, three prominent jihadist Web forums were taken down: Shumukh Al-Islam, Al-Fida, and Ansar Al-Mujahideen; they were up and running again by late January 2013. In response, on February 15, 2013, the jihadist propaganda center Al-Furqan published an article titled, "On the Lull in the Activity of Jihadist Web Forums: Causes and Solutions", by Sheikh Abu Sa'ad al-'Amili, a prominent Salafi-jihadist and frequent contributor to Web forums.[2]

Al-'Amili's article discussed the importance of jihadist Web Forums, whose multiple announcements, advertisements, articles, advice columns and opinion pieces have played a role in the awakening of the Muslim Nation. Moreover, these Web forums are a platform for jihadist organizations, which lack the actual and technical tools to develop official channels of communication. According to al-'Amili, even though the forums are the primary source of accurate, unbiased news for the enemies of Islam, these enemies are sore afraid because they recognize the forums' true significance.

Al-'Amili then cited possible reasons for the attrition of members from Web forums:

[2] http://www.as-ansar.com/vb/showthread.php?t=81504 (Arabic).

- The forced closure of certain jihadist Web forums, as in the case of the three prominent forums cited above (Shumukh Al-Islam, Al-Fida, and Ansar Al-Mujahideen), owing to deliberate sabotage by the enemy. This makes the forums seem vulnerable and unable to defend themselves; their takedown thus has a negative psychological effect, upsetting the security of certain members, who then flee in fear and choose other means of engaging in propaganda for the mujahideen. Conversely, many members of jihadist Web forums may ascribe the lull in their activity to concern with normative life, which "…is natural, because evil strains the psyche and Satan lures".

- Fear of being monitored by intelligence agents. Forum members fear that jihadist Web forums are under surveillance and are unsafe to visit.
- Going to fight jihad in the field. Members who choose this path are not actually "lost" to the jihadist Web forums. On the contrary, they serve as a role model for the brothers, demonstrating how important it is to fulfill the commandment of jihad. In fact, involvement on a Web forum is preparation for fighting jihad. Al-'Amili calls the Web forums "universities" that train fighters to enter arenas of jihad. Moreover, the forums themselves are an arena of jihad, though one that focuses on propaganda, which is no less important to jihad as a whole.
- The transition to social networks, particularly of prominent writers and analysts. Al-'Amili sees this as a fad that does not affect all Web forums. The upsurge in communication over social networks usually coincides with a hiatus in the activity of the Web forums. Use of the social networks to increase exposure to jihad is welcome, according to Al-'Amili, but is no substitute for the Web forums, which continue to be the primary source of news and analysis. In this context, al-'Amili urges writers and analysts to concentrate their activity on Web forums.
- A decline in the quantity of content on the forums. This is related to the previous matter: prominent writers "defect" to social media when they become disappointed in the small number of responses to their articles. According to al-'Amili, the threads posted on jihadist Web forums are meant to be disseminated widely.

Al-'Amili consequently proposed the following solutions:

- Reevaluate the importance of the jihadist Web forums as a deterrent to the enemy no less than an aid to Islam and the mujahideen. Participation in the forums should be recognized as a type of jihad, and every forum member should see himself as a mujahid who fights with words, and technical and technological skills.
- Quell forum members' fear for their personal safety, which is unjustified. Despite the forums' vulnerability, forum administrators do all they can to ensure members' safety – even more than they do their own. At the same time, members must take precautions when surfing jihadist Web forums; for example, if they do not camouflage their identity and IP, and save jihadist files on a separate computer, say, they expose themselves to danger. It is incumbent on every forum member to take safety precautions when surfing jihadist Web forums.
- Attract prominent writers and analysts to return to jihadist Web forums, which will benefit greatly from their return.
- Use social media as the last instance of propaganda. Social networks should not be used exclusively, since they have many disadvantages. For example, they cannot be controlled the way a Web forum can, and in fact may be controlled by the enemy, who may one day use them to damage supporters of jihad.
- Encourage tech-savvy people to contribute to jihadist Web forums, no less than journalists, analysts, designers, people who can transcribe or subtitle video clips and audio statements, and translators into multiple languages.

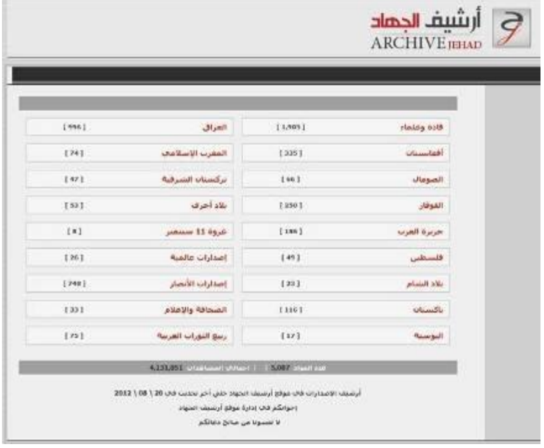
Using the Darknet: On February 4, 2013, Abu Abbas al-Qatari, the technical supervisor of the jihadist Web forum Shumukh Al-Islam, published a detailed explanation of how to use the computer program TOR to anonymously surf the Darknet,[3] a subliminal Web that exists "under" or "behind" the visible Internet, and which is home to extensive criminal activity, including the weapons trade, human organ sale, and terrorism. On February 6, 2013, al-Qatari published an index of threads uploaded during 2012 to the "computer and Internet room" – that is, a classified index of all of the threads on cyber activity, by topic. Among the topics indexed are help programs for a personal computer; safety and security when

[3] https://shamikh1.info/vb/showthread.php?t=190595 (Arabic).

surfing the Web; technical explanations of how to use various programs; and instruction in programming languages and hacking.[4]

Hacking: A member of Shumukh Al-Islam proposed a number of ways to hack into computers with an Internet connection, including circumventing anti-virus and security programs. He also listed the best hacking programs.[5]

Using the Web to Fight Jihad: Ansar Al-Mujahideen published a downloadable version of the Web site "ArchiveJihad". The archive contains video clips on jihad, which can be viewed even without an Internet connection.[6]



أرشيف الجهاد
ARCHIVE JEHAD

قادة وعلماء	[1,905]	العراق	[996]
أفغانستان	[335]	المغرب الإسلامي	[74]
الصومال	[66]	تركستان الشرقية	[47]
القوقاز	[250]	بلاد أخرى	[53]
جزيرة العرب	[186]	غزوة 11 سبتمبر	[8]
فلسطين	[49]	إصدارات عالمية	[26]
بلاد الشام	[23]	إصدارات الأنصار	[248]
باكستان	[116]	الصحافة والإعلام	[33]
البوسنة	[17]	ربيع الثورات العربية	[75]

عدد المواد 5,087 | اجمالي المشاهدات 4,131,851

أرشيف الإصدارات في موقع أرشيف الجهاد خلي أخر تحديث في 20 \ 08 \ 2012
إخوانكم في إدارة موقع أرشيف الجهاد
لا تنسونا من صالح دعائكم

The home page of the Archive of Jihad

A supervisor of the Web forum Ansar Al-Mujahideen who goes by the name Gharib published an introductory lesson in Photoshop, which can be used to design Web sites and banners promoting jihad. The lesson was part of the forum's online course, "From Zero to Break-in".[7]

Defensive Tactics

Encoding programs: On February 7, 2013, the Global Islamic Media Front (GIMF), which is affiliated with Al-Qaeda and other jihadist organizations, published a new computer encoding program named Asrar Al-Dardasha [The Secrets of Chatting]. The program provides several encoding options to ensure a secure connection. It is based on a previously-issued encoding program, Asrar Al-Mujahideen [The Secrets of the Mujahideen].

[4] https://shamikh1.info/vb/showthread.php?t=190738 (Arabic).
[5] https://shamikh1.info/vb/showthread.php?t=191177 (Arabic).
[6] http://al-fidaa.com/vb/showthread.php?t=56878 (Arabic).
[7] http://www.as-ansar.com/vb/showthread.php?t=82307 (Arabic).

Asrar Al-Dardasha is supported in multiple languages, including Arabic, English, Urdu, Pastho, Bengali and Indonesian. The program is easy and quick to use and is bsed on the RSA encoding algorithm, which requires the use of a double key: a public key allocated for encoding, and a personal key used to decipher the code. According to the GIMF, this is the only encoding program that is safe to use when contacting mujahideen and their supporters.

The GIMF added that electronic jihadist communications (e.g., Web forums and media centers) – the principal representative of the mujahideen worldwide – have developed and, despite the constant struggle against the West and traitorous Arab leaders, promote the mujahideen in a fair and balanced manner – something the media do not do. For example, the Soviet war in Afghanistan and the war in Bosnia suffered from biased reporting. However, the appearance of the Internet changed matters, prividing the mujahideen with a new and important means of self-expression, communication, and propaganda. Moreover, the Internent enables the mujahideen to transcend limitations of technology and resources, and to circumvent the persecution and legal travails imposed by tyrannical governments.

In fact, the mujahideen have won the media war against the West. Even Eric Clark, former spokesman for the US Central Command, admitted in 2006 that Al-Qaeda had won the media battle against the US. The GIMF concludes by reminding Muslims of their obligation to help the mujahideen, Islam and the Muslim Nation to win the Crusader campaign being waged by the US and its Muslim allies. The GIMF is proud to be the spearhead of this media war, and is determined to invest every effort on behalf of the mujahideen.[8]

ASRAR
الجبهة الإعلامية الإسلامية العالمية
القسم التقني
يقدم
ملحقة " أسرار الدردشة "
للتواصل الفوري المباشر المشفر
مميزات ملحقة "أسرار الدردشة":

- الملحقة لا تتطلب اي تقنية خاصة أو خبرة أو تركيب ملفات معقدة.
- الملحقة تقدم أعلى مستويات التشفير للاتصالات الآمن عبر التراسل الفوري
- الملحقة صغيرة الحجم وتنصب بثواني وسهلة الاستخدام مع برنامج "بدجن".
- هي أول ملحقة تشفير إسلامية تعتمد على برنامج التشفير الإسلامي "أسرار المجاهدين".
- الملحقة سهلة الاستعمال لا تحتاج إلا الى تبادل بصمة المفتاح للتأكد من صحة كل مفتاح عام.
- الملحقة موثوقة للاستخدام والاتصالات الآمنة نظراً لاعتمادها على برنامج التشفير "أسرار المجاهدين".
- تدعم معظم اللغات في العالم بواسطة الترميز الموحد "يونيكود" كالعربية والإنجليزية والأردية والبشتونية والبنغالية والأندونيسية.
- الملحقة يمكن استخدامها مع كثير من حسابات التواصل الفوري مثل YAHOO-MSN-GOOGLE TALK - AOL- JABBER

Based on an item in *The Guardian*, jihadist Web forum Al-Fida warned its readers that spyware, which can collect large quantities of personal data, is infesting Facebook, Twitter and other social networks. The spyware was allegedly developed by Raytheon (Rapid Information Overlay Technology), one of the largest military production companies in

[8] http://www.as-ansar.com/vb/showthread.php?p=480886 (Arabic); http://www.ansar1.info/showthread.php?p=164212 (English).

the world. Al-Fida noted that Raytheon had also developed technology for the US government in 2010, which was meant to maintain national security.[9]

Maintaining Internet Security: A visitor to the jihadist Web forum Ansar Al-Mujahideen uploaded a 156-page guidebook, first published in 2011 in the Gaza Strip, on how to maintain the security of your computer and your identity when surfing the Internet. The guidebook covers anti-spyware programs, programs for encoding files, and suggestions for safe surfing.[10]

Offensive Tactics

Religious Justification for Hacking: On February 2, 2013, the Islamic legal scholar Abu Mundhir al-Shanqiti, the head of the Fatwa Committee of the Salafi-jihadist portal Minbar Al-Tawhid wal-Jihad, published a fatwa [Islamic-legal ruling] about hacking into online US-based commercial sites. His fatwa was a response to the following set of questions, posed by one Abu Bakr al-Ansari:

> *Let us say that someone breaks into an American Internet store to "purchase" goods such as mobile telephones and computers for free. Let us say that he is paid 1,000 units of the local currency by someone who has asked him to buy a product online that has yet to reach the local market, or that is available locally but is being sold for the high price of, say, US$1,000:*
>
> - *What is the ruling regarding hacking into American online stores? What is the ruling regarding defrauding these stores by "purchasing" items without paying their estimated price? Is this theft, which is prohibited? Or is an infidel in dar al-harb [lit., the house of war – that is, someone living in a non-Muslim country] unworthy of protection?*
> - *What is the ruling regarding paying someone who is an expert in [hacking and defrauding] for his services? What if he charges 500 units of the local currency to obtain an item that costs US$500: Should he be paid this price for hacking into the site and obtaining the item?*

According to al-Shanqiti, it is legitimate to engage in any act meant to defraud and destroy the economy of a country that opposes Islam. Ergo, hacking and Internet

[9] http://al-fidaa.com/vb/showthread.php?t=56561 (Arabic).
[10] http://www.as-ansar.com/vb/showthread.php?t=82316 (Arabic)

fraud are completely legitimate, ergo it is permissible for someone to hire the services of a hacker to fraudulently obtain goods for him.[11]

Attacking Iraqi Targets: Recent months have seen rising tensions between Shi'ites and Sunnis in Iraq, reflected in countless protest rallies countrywide, at which Sunnis express their frustration at what they feel is the discrimination and oppression of government authorities. In this context, the jihadist Web forum Hanein reported that the Web site of Iraqi Prime Minister Nuri al-Maliki[12] had been hacked into twice, consecutively. The site's security was tightened as a result, to make it more difficult for hackers to attack it in the future. To date, investigations into these incidents have not borne fruit, and it is unclear whether the attacks were perpetrated by a hacker in or outside of Iraq.[13]

During the latter half of February 2013, the jihadist Web forum Hanein reported that Sunni Web sites in Iraq and Bahrain had been hacked. Among the sites attacked was that of the Iraqi Association [Al-Rabita Al-Iraqiyya],[14] a non-profit organization that promotes equality and nationalist sentiment among all citizens of Iraq. The ensuing discussion among site visitors indicated that attacks of this type were constantly being committed by a group of hackers known as Fariq 313, with which Hanein's contributors are apparently familiar.[15] It thus appears that the Internet is yet another arena of struggle between Sunnis and Shi'ites.[16]

Guidelines for Hackers: The Palestinian hackers' forum, gaza-hacker, published lesson 15 of its online course on hacking, titled "Symlink Bypass Software: nginx".[17]

Another Palestinian forum for hackers named Giants of Gaza [Amalikat Ghaza] launched an online, nine-lesson course in breaking into Web sites using distributed denial of service (DDoS) attacks.[18] In DDoS attacks, mass requests are made for

[11] http://tawhed.ws/FAQ/display_question?qid=7142&pageqa=1&i=&PHPSESSID=c63cbb77126fbdf6e8c242dc5630cc38 (Arabic).
[12] http://www.pmo.iq (Arabic).
[13] http://www.hanein.info/vb/showthread.php?t=312728 (Arabic).
[14] http://www.iraqirabita.org/index.php?do=intro&id=2 (Arabic).
[15] http://www.youtube.com/watch?v=EZE1FozIwEs (no longer available).
[16] http://hanein.info/vb/whowthread.php?t=313855 (Arabic).
[17] http://www.gaza-hacker.net/cc/showthread.php?p=316575 (Arabic).
[18] http://giant-gaza.com/vb/f121.html (Arabic).

service from a computer or network of computers, thereby overwhelming the computers' servers and causing them to crash.

Cyber-Crime and Cyber-Terrorism, February-April 2012

Recent years have seen increasing cyber attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations. These attacks, which are also, increasingly, receiving international attention, are perpetrated by states (which do not take responsibility for them); groups of hackers (such as Anonymous); criminal organizations; and lone hackers. The following information was culled from the visible (OSINT) and invisible ("dark Web")[19] Internet between February and April 2013.

Anonymous: During the period under review, several significant "operations" were perpetrated by Anonymous worldwide. Many of them targeted the official activity of states which Anonymous perceives as trammeling human rights, or as posing a danger to, or using violence against, their own citizens or the rest of the world. The following were among the acts committed by Anonymous:

- OpIran Menace: During the last week of March 2013, Anonymous hacked into the computers of several infrastructure providers and UN missions in Iran. Some 500 documents were leaked as a consequence of this act.[20]
- OpPalestine: Anonymous hacked into the servers of the Palestinian Foreign Ministry, leaking more than 150 extremely timely documents.[21]
- OpNorthKorea: In early April, Anonymous struck out against the government of North Korea, hacking into its official Flickr and Twitter sites[22] and leaking some 15,000 email accounts.[23]

[19] 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.

[20] Anonymous, "OP 'Iran Menace' UN Tehran and Iran Oil Companies Massive Leak", *CyberGuerrilla*, March 23, 2013, https://www.cyberguerrilla.org/blog/?p=10098.

[21] Anonymous, "OpPalestine_OpIranMenace: 29 Images", *Imgur*, http://imgur.com/a/ciyMJ#0.

[22] Lance Whitney, "Anonymous Hacks North Korea's Twitter and Flickr Accounts", *Cnet.com*, April 4, 2013, http://news.cnet.com/8301-1009_3-57577904-83/anonymous-hacks-north-koreas-twitter-and-flickr-accounts.

[23] "opNorthKorea NEW LEAK and Summary", *Pastebin.com*, April 5, 2013, http://pastebin.com/9WTyG00p.

- OpIsrael: On April 7, 2013, Anonymous carried out an attack against Israel, which had taken it more than one month to plan and whose aim was "to wipe Israel off the Internet map". Hackers from throughout the Middle East and the Muslim world – including Turkey,[24] Algeria,[25] Morocco,[26] Tunisia[27] and Indonesia[28] – participated in the attack. They defaced and attacked Israeli Web sites, and disseminated data purportedly about Israelis (which in most cases proved not to be). In other words, the attack was partly, perhaps primarily, an act of psychological warfare. For example, a pre-prepared page was identified, which made it possible to deploy a DDoS attack against seven Israeli government sites (ending in "gov.il").[29] When the attack was over, affiliates of Anonymous warned that Israel would face additional attacks in the coming months.[30]

  In response to this attack, Israeli hackers retaliated against a number of targets in the Middle East and the Muslim world. For example, a group of hackers calling itself the Israeli Elite Force hacked into several Pakistani sites and leaked their details.[31]
- OpBaluchistan: On April 9, 2013, persons identified with Anonymous announced an online attack on Pakistan, similar to the one perpetrated against Israel.[32]

As these "operations" indicate, Anonymous is involved in myriad issues and places around the world, motivated by a variety of different and sometimes contradictory interests. In the main it targets the online presence of government agencies and other representations of a state's sovereignty.

Governments and Essential Infrastructure: During the period under review, a number of actions were perpetrated which indicate the increasing vulnerability of essential, computer-based infrastructure to attack by hostile governments, groups of hackers, and "lone wolf" hackers.

[24] "Turkey Cyber Army Opisrael", *Pastebin.com*, April 9, 2013, http://pastebin.com/JFJaPQni.

[25] "#Op Israel Algerian to the Core Leaked Data Gov Emails", *Pastebin.com*, April 8, 2013, http://pastebin.com/ymSb26V0.

[26] Moroccan Ghosts, Untitled, *Pastebin.com*, April 8, 2013, http://pastebin.com/dMunDjV1.

[27] "بطاقات ائتمان اسرائيلية Tunisian_Hàckers Team", *Pastebin.com*, April 6, 2013, http://pastebin.com/Q2YPnbfy.

[28] Bapakagung, "H-1 Penghapusan Internet Israel #Anonymous #Hacker", *Kaskus*, March 21, 2013, http://www.kaskus.co.id/thread/515ffa3e7b12437e45000000/h-1-pernghapusan-internet-israel-anonymous-hacker.

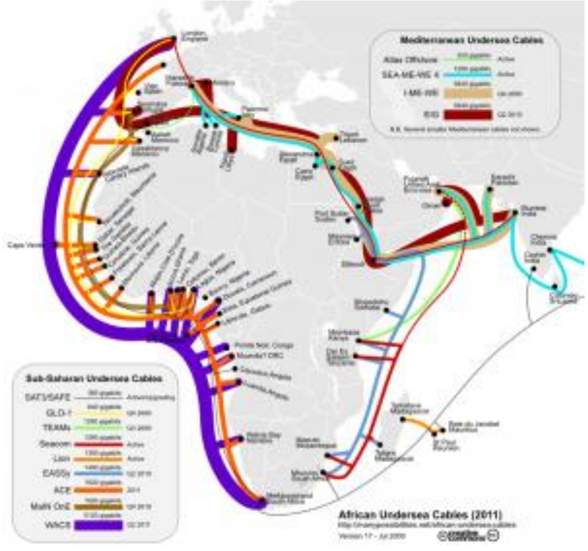
[29] Greget Hacking Team, "DDOS Attack by Greget Hacking Team – Indonesia", http://www.ddos-israel.blogspot.co.il.

[30] Untitled, *Pastebin.com*, April 9, 2013, http://pastebin.com/VMUhp5z5.

[31] Untitled, April 9, 2013, http://pastebin.com/32ZBnY8B.

[32] "Message to All Anonymous: #OpIsrael >> Next>> #OpBalochistanc", *Pastebin.com*, April 9, 2013, http://pastebin.com/fi29KrvQ.

For example, reports were recently received that an action was perpetrated against the US, which paralyzed the country's emergency telephone lines.[33] Like DDoS attacks against computer systems, the goal of this telecommunications denial of service (TDoS) attack was to overwhelm the targeted communications system and bring about its collapse. It should be noted that such attacks can be perpetrated by criminals wishing to extort money.


Mediterranean Undersea Cables
Atlas Offshore
SEA-ME-WE 4
I-ME-WE
EIG
Sub-Saharan Undersea Cables
SAT3/SAFE
GLO-1
TEAMs
Seacom
Lion
EASSy
ACE
MaIN OnE
WACS
African Undersea Cables (2011)

On March 27, 2013, the international media reported an extensive attack against an undersea communications cable, which caused Internet slow-downs throughout the world.[34] The attack was described as the largest of its kind in the history of the Internet;[35] some claim it was three times as powerful as the attack on the US banking system (see below).[36]
In fact, that day the world faced not only a slowdown of the Internet, but also the risk of a total blackout of the Internet in some locations. According to reports, an Egyptian coastal patrol stopped a fishing boat some 750 meters from the port of Alexandria.[37] Photographs of the three (unidentified) fishermen on deck were later posted on the Facebook page of the Egyptian Navy,[38] along with details of the incident, which began with

[33] Ted Samson, "Cyber Criminals Tying Up Emergency Phone Lines through TDoS Attacks", *InfoWorld*, April 1, 2013, http://m.infoworld.com/t/cyber-crime/cyber-criminals-tying-emergency-phone-lines-through-tdos-attacks-215585.
[34] "The DDoS That Almost Broke the Internet", *CloudFlare*, March 27, 2013, http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet.
[35] Siavash, "Massive DDoS Attacks Slows Internet Worldwide", *Cyberwarzone.com*, March 27, 2013, http://www.cyberwarzone.com/massive-ddos-attacks-slows-internet-worldwide-0.
[36] Michael Mimoso, "Spamhaus DDoS Attacks Triple Size Attacks US Banks", *Threatpost.com*, March 27, 2013, http://threatpost.com/spamhaus-ddos-attacks-triple-size-attacks-us-banks-032713/#.UVOVf8bfcPg.twitter.
[37] "Egypt Catches Divers Cutting Internet Cable Amid Disruptions", *Reuters.com*, March 27, 2013, http://www.reuters.com/article/2013/03/27/net-us-egypt-internet-idUSBRE92Q1AQ20130327.
[38] "صور المتهمين بقطع كابل الإنترنت والمضبوطات بحوزتهم," القوات البحرية المصرية, *Facebook.com,* March 27, 2013, https://www.facebook.com/media/set/?set=a.435169449900970.1073741825.146063395478245&type=1.

reports of trouble at 09:30 and ended with the arrest of the three fishermen at 13:10.[39]

The diagram above depicts the cable that serves Telecom Egypt, sole provider of telecommunications services in that country. According to a spokesman for the Egyptian Navy, the three fishermen were caught trying to detach or damage the undersea communications cable SEA-ME-WE-4,[40] which connects Europe to the Middle East and India as part of an international network of undersea cables.[41]

As of this writing, it is not clear what if any relationship this event has to an earlier incident, in which the communications cables of SEACOM, which connect Europe to Africa, the Middle East and Asia were damaged. It is a fact that Internet users in Egypt reported service slowdowns throughout this period.

According to the CEO of Telecom Egypt, the cable was indeed cut and damaged, causing a 60% decline in Internet service in Egypt.[42] Referring to both this and the previous incident, he added, "[Telecom Egypt] will bear the costs of this cable's repair and the other cable, which was cut on Friday". The Turkish Minister of Communications also addressed the issue, stating, "The crisis will be resolved gradually, within the next 20 hours".

Damage to a main undersea cable – which appears not to have been a one-time occurrence – is liable to have a swift, complete, and dire effect on the world. Although Internet service is delivered via a continuum of undersea cables, those that meet at strategic junctures, such as that in the vicinity of Suez, are particularly vulnerable to interference which, if effective, could "disconnect an entire continent" from the Internet.[43]

The TDoS attack on America's emergency communications system and the physical attack on Egypt's undersea Internet cable demonstrate how easy it can be to

[39] القوات المسلحة المصرية, *Facebook.com,* March 28, 2013, https://www.facebook.com/photo.php?fbid=509771315748409&set=a.151968161528728.31347.151949418197269&type=1&relevant_count=1.

[40] http://sphotos-b.ak.fbcdn.net/hphotos-ak-snc6/221658_509771315748409_2111527279_n.png.

[41] Submarine Cable Map 2013, TeleGeography, http://submarine-cable-map-2013.telegeography.com.

[42] *Al-Masry Al-Youm*, "Internet Saboteur Caught, says Telecom Egypt CEO", *Egypt Independent*, March 27, 2013, http://www.egyptindependent.com/news/internet-saboteur-caught-says-telecom-egypt-ceo.

[43] Leo Mirani, "How to Take an Entire Continent Offline", *Business Insider*, March 28, 2013, http://www.businessinsider.com/heres-how-to-take-an-entire-continent-offline-2013-3.

damage or even paralyze large numbers of Internet users – and Internet-dependent businesses, governments and infrastructure.

Mobile Phones: On March 24, 2013, Kaspersky, an Internet security company, reported that its experts had identified a unique online attack against Tibetan human rights activists. After hacking into the email account of a prominent activist, the attackers sent forged emails to the activist's contact list, with a contaminated attachment which, if opened on a mobile phone using the Android operating system, would activate malware that would document all of the written and verbal communication transacted on that mobile phone. These data were then transferred in an encoded form to a server in the US, which investigation indicates is actually operated by Chinese elements.[44]

Banking and Finance: At the end of March 2013, a report was received of a DDoS attack against the American Express Web site,[45] which succeeded in paralyzing the site for two hours. The Izz Al-Din Al-Qassam Cyber Warriors took responsibility for the attack, adding that it would continue until the film "Innocence of Muslims" had been completely removed from the Internet.[46]

> *"The Qassam group today has targeted its goals by powerful attacks. The Bank of America and American Express have gotten out of reach today due to Izz ad-Din al-Qassam group's attacks. The Qassam group's attacks to these Banks have caused the banks to be unable to offer service to their customers and this lead to their protests. The Qassam group has announced that till to complete removing of the film from internet, will continue its attacks to the U.S. Banks. The efforts of the authorities in order to prevent against the attacks have been ineffective until today".* [mistakes in the original]

In fact, the company's spokesperson, Amelia Woltering, allegedly admitted that an attack had been perpetrated against the site:[47]

[44] Costin Raiu, Kurt Baumgartner and Denis, " Android Trojan Found in Targeted Attack", *Securelist*, March 26, 2013, https://www.securelist.com/en/blog/208194186/Android_Trojan_Found_in_Targeted_Attack.

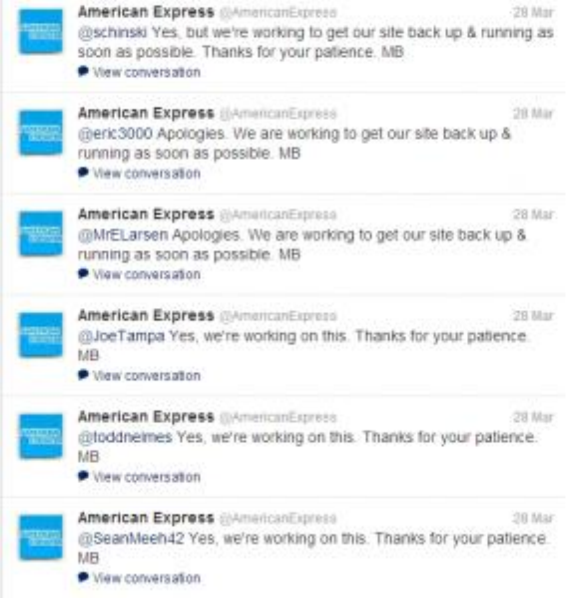
[45] Siavash, "American Express Hit by DDoS Attack", *Cyberwarzone.com*, March 30, 2013, http://cyberwarzone.com/american-express-hit-ddos-attack.

[46] Hilf-ol-Fozoul, "The Bank of America and American Express are Unable against Qassam Group's Attack", *The Global Movement of Hilf-ol-Fozoul*, March 28, 2013, http://hilf-ol-fozoul.blogspot.nl/2013/03/the-bank-of-america-and-american.html.

[47] Tracy Kitten, "DDoS Strikes American Express", *BankInfoSecurity.com*, March 29, 2013, http://www.bankinfosecurity.com/ddos-strikes-american-express-a-5645.

> *"Our site experienced a distributed-denial-of-service (DDoS) attack for about two hours on Thursday afternoon…We experienced intermittent slowing on our website that would have disrupted customers' ability to access their account information. We had a plan in place to defend against a potential attack and have taken steps to minimize ongoing customer impact".*

Interestingly, a Google search for Woltering's alleged comment came up empty;[48] the source of the statement could not be identified, even though it was repeatedly cited by various media. Moreover, no trace of a comment by Woltering addressing the incident could be found on the American Express Facebook[49] or Google+[50] pages. However, the official American Express Twitter feed did address difficulties accessing the Web site:[51]



American Express @AmericanExpress 28 Mar
@schinski Yes, but we're working to get our site back up & running as soon as possible. Thanks for your patience. MB
View conversation

American Express @AmericanExpress 28 Mar
@eric3000 Apologies. We are working to get our site back up & running as soon as possible. MB
View conversation

American Express @AmericanExpress 28 Mar
@MrELarsen Apologies. We are working to get our site back up & running as soon as possible. MB
View conversation

American Express @AmericanExpress 28 Mar
@JoeTampa Yes, we're working on this. Thanks for your patience. MB
View conversation

American Express @AmericanExpress 28 Mar
@toddneimes Yes, we're working on this. Thanks for your patience. MB
View conversation

American Express @AmericanExpress 28 Mar
@SeanMeeh42 Yes, we're working on this. Thanks for your patience. MB
View conversation

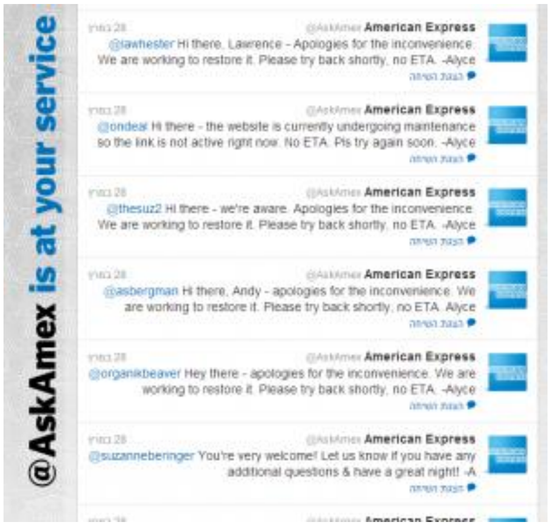
[48] https://www.google.co.il/search?q=Our+site+experienced+a+distributed-denial-of-service+(DDoS)+attack+for+about+two+hours+on+Thursday+afternoon&aq=f&oq=Our+site+experienced+a+distributed-denial-of-service+(DDoS)+attack+for+about+two+hours+on+Thursday+afternoon&aqs=chrome.0.57.1016&sourceid=chrome&ie=UTF-8#q=%22Our+site+experienced+a+distributed-denial-of-service+(DDoS)+attack+for+about+two+hours+on+Thursday+afternoon...We+experienced+intermittent+slowing+on+our+website+that+would+have+disrupted+customers%27+ability+to+access+their+account+information.+We+had+a+plan+in+place+to+defend+against+a+potential+attack+and+have+taken+steps+to+minimize+ongoing+customer+impact%22&hl=en&ei=cN5XUeeZF4HDPOvxgMAK&start=10&sa=N&fp=1&biw=1024&bih=667&bav=on.2,or.r_cp.r_qf.&cad=b&sei=wnFxUZSKCKX80QW6m4G4BA.

[49] American Express, *Facebook.com*, https://www.facebook.com/americanexpress.

[50] American Express, *Google+*, https://plus.google.com/114054690699015768556/posts.

[51] American Express, @AmericanExpress, *Twitter.com*, https://twitter.com/AmericanExpress/with_replies.

The American Express Twitter support site[52] featured a similar message, and an announcement mentioning "site maintenance":



@AskAmex is at your service

28 במרץ
American Express @AskAmex
@lawhester Hi there, Lawrence - Apologies for the inconvenience. We are working to restore it. Please try back shortly, no ETA. -Alyce
הצגת השיחה

28 במרץ
American Express @AskAmex
@ondeal Hi there - the website is currently undergoing maintenance so the link is not active right now. No ETA. Pls try again soon. -Alyce
הצגת השיחה

28 במרץ
American Express @AskAmex
@thesuz2 Hi there - we're aware. Apologies for the inconvenience. We are working to restore it. Please try back shortly, no ETA. -Alyce
הצגת השיחה

28 במרץ
American Express @AskAmex
@asbergman Hi there, Andy - apologies for the inconvenience. We are working to restore it. Please try back shortly, no ETA. Alyce
הצגת השיחה

28 במרץ
American Express @AskAmex
@organikbeaver Hey there - apologies for the inconvenience. We are working to restore it. Please try back shortly, no ETA. -Alyce
הצגת השיחה

28 במרץ
American Express @AskAmex
@suzanneberinger You're very welcome! Let us know if you have any additional questions & have a great night!! -A
הצגת השיחה

Some believe this incident was part of "the greatest attack in the history of the Internet" in late March (see above).[53]

This was not the first attack perpetrated by a group calling itself The Izz Al-Din Al-Qassam Cyber Warriors. In September 2012, Qassam Cyber Warriors caught the world's attention in an online attack, dubbed "Operation Ababil", against US financial industry targets. Ever since, the group has continued to attack the US financial sector in one way or another.

To illustrate: several days prior to the attack on American Express, online attacks were perpetrated against other American banks, including TD Bank and Keybank.[54] An announcement published on March 5, 2013, indicates that this was the start of the third phase of Operation Ababil.[55] During the second week of March 2013, an additional announcement was published, which stated, "the following banks and/or financial services were chosen as a target of attack:[56] PNC, Fifth Third Bancorp, J.M.Chase, U.S.Bank, UnionBank, Bank of America, Citibank, BB&T and Capitalone". In an announcement published during the third week of March 2013, the following

[52] American Express, @AskAmex, *Twitter.com*, https://twitter.com/AskAmex/with_replies.

[53] Adam Clark Estes, "A DDoS Attack Just Took Down AmEx.com", *Motherboard*, http://motherboard.vice.com/blog/a-ddos-attack-just-took-down-amexcom.

[54] Tracy Kitten, " TD Bank, KeyBank Confirm DDoS Attacks", *BankInfoSecurity.com*, March 26, 2013, http://www.bankinfosecurity.com/td-bank-keybank-confirm-ddos-attacks-a-5631.

[55] QASSAMCYBERFIGHTERS, "Phase 3, Operation Ababil", *Pastebin.com*, March 5, 2013, http://pastebin.com/kXSsVScS.

[56] QASSAMCYBERFIGHTERS, "Phase 3/W2, Operation Ababil", *Pastebin.com*, March 12, 2013. http://pastebin.com/YVhsSdLN.

targets were identified:[57] "BB&T, PNC, Chase, Citibank, U.S. Bancorp, Suntrust, Fifth Third Bancor, Wells Fargo, and some others". The announcement of March 26, 2013, which concerned the fourth phase of Operation Ababil, cited the following targets:[58] "BB&T, PNC, Chase, Citibank, U.S. Bancorp, Suntrust, Fifth Third Bancor, Wells Fargo, and some others". Lastly, an announcement on the blog Hilf-ol-Fozoul[59] cited the various US banks allegedly targeted by these attacks.[60]

Collecting Operative Intelligence: During the period under review, incidents were recorded in which sensitive government and security information was disseminated, which hostile entities could use to perpetrate online attacks. For example, on March 23, 2013, some 400 email addresses ostensibly belonging to US government and defense agencies were published;[61] it is not clear who was behind the publication of this information, which included 55 CIA email addresses, 21 Department of Defense addresses, 40 FBI addresses, 13 NATO addresses, 146 Department of Justice addresses, and 117 National Security Administration addresses.

The following email addresses, which were among those made public, were proven to be fake: gotsomerealproblems@cia.gov; spyguy26@cia.gov; bin_lad@cia.gov; fine@fbi gov; fine@fbi,gov; fine@fbi.gov; horny.pony@nato.int.

On March 24, 2013, the same source announced that it had hacked into 30 Chinese government Web sites, apparently as part of a struggle or competition among groups of hackers, and not necessarily as an assault on the Chinese government.[62]

A number of attempts were allegedly made to publicize the email addresses of Israeli government agencies, as well: on April 9, 2013, an announcement was made containing an email and password ostensibly belonging to someone in the Israel Police Force,[63] along with email addresses that supposedly belonged to employees of

[57] QASSAMCYBERFIGHTERS, "Phase 3/W3, Operation Ababil", *Pastebin.com*, March 19, 2013, http://pastebin.com/K98NaXWr.

[58] QASSAMCYBERFIGHTERS, "Phase 3/W4, Operation Ababil", *Pastebin.com*, March 26, 2013, http://pastebin.com/sumX4X8E.

[59] Hilf-ol-Fozoul, "The Bank of America and American Express Are Unable against Qassam Group's Attack", *The Global Movement of Hilf-ol-Fozoul*, March 28, 2013, http://hilf-ol-fozoul.blogspot.nl/2013/03/the-bank-of-america-and-american.html.

[60] Hilf-ol-Fozoul حلف الفضول, *Google+*, https://plus.google.com/103001647569797666354/posts.

[61] "FBI , CIA , NSA , Justice.gov Defense.gov Leaked Emails...", *Passtebin.com*, March 23, 2013, http://pastebin.com/PahwjTwj.

[62] "60 Website #Defaced by Charaf Anons", *Passtebin.com*, March 24, 2013, http://pastebin.com/8fPsA5Ng.

[63] "Israel Email Police HaCked By AnonGhost Team", *Passtebin.com*, April 9, 2013, http://pastebin.com/juiVPRnc.

the Ministry of Defense and the Mossad; however, these appear to be fake addresses. Similarly, a list of some 600 email addresses purportedly belonging to Israelis was made public in early April.[64] However, precise examination of this information reveals that most of the usernames and email addresses were generated automatically; only some 15 of them belong to "real" Israelis.

These incidents make clear that publicizing email addresses, like other online attacks and incidents, are in no small part a means of psychological warfare. Even though most of the email addresses publicized are fake, the product of an automatic mechanism that creates usernames and email addresses in bulk, they do create the illusion that a Web site has been infiltrated, leaving immense amounts of sensitive data vulnerable.

Phishing: Fraud is not a new phenomenon. Thanks to social engineering, anyone can exploit human nature and psychology to elicit cooperation with a fraudulent scheme. On the Internet as in the real world, the victim must cooperate if the defrauder is to succeed. If anything, the Internet has enabled fraud to flourish, thanks in part to its decreasing costs and the almost endless potential it provides to reach ever-increasing numbers of people worldwide. Most of the fraudulent schemes extant on the Internet are meant to generate financial gain, and are employed by criminals.

One of the older and more familiar types of Internet fraud is known as the "Nigerian sting". This involves broadly disseminating a lengthy email message ostensibly written by a high-ranking executive (e.g., a lawyer, accountant, CEO) at a respectable institution. The message usually offers the recipient the opportunity to earn a huge sum, for example by investing (via cash, checks, bank transfers, etc.) in a venture, or helping the institution that is purportedly behind the email to obtain drilling rights. In exchange, the victim is offered a nice profit of between 10% and 40% of the return on his investment – in cash or checks, gold, bank transfers, or diamonds. Invariably, the email contains a link to a malicious site of some sort.[65]

Other, more current fraudulent Internet schemes wield a variety of techniques to obtain one or another type of classified information from as many Internet users as possible. Internet fraud of this type, which may be used alone or in concert with the "Nigerian sting", is more commonly known as "phishing".

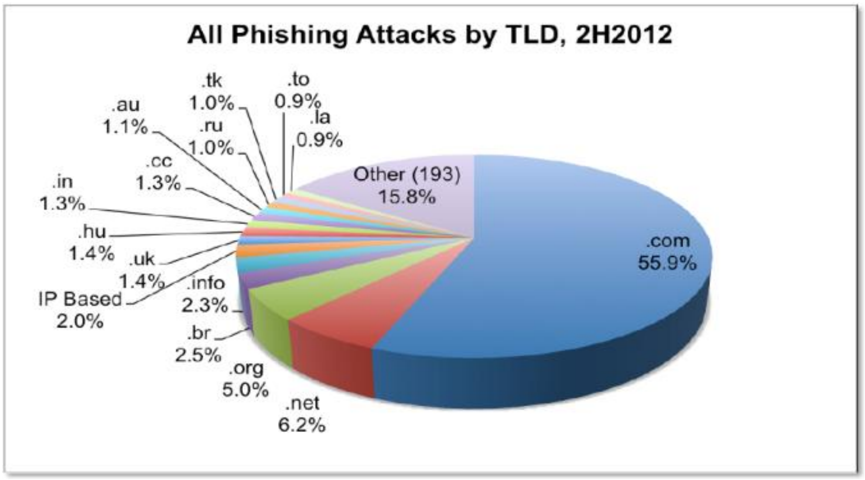
[64] "Email >>Hacked by Karamzaza", *Passtebin.com*, April 2, 2013, http://pastebin.com/1MMTWc3z.

[65] http://www.pcworld.com/article/192664/the_story_behind_the_nigerian_phishing_scam.html.

In the main, phishing is a method of fraudulently obtaining sensitive data such as passwords, the details of a bank account or credit card, and a social security or identity number. These may be elicited via email or through social networks. In either case, phishing involves the dissemination of a malicious code that "sucks out" the desired data, for future use or for sale on the black market.

The concept of phishing was first discussed in a 1987 article by Jerry Felix and Chris Hauck,[66] and the first documented case of phishing was the theft in the mid-1990s of the identifying details of clients who used the America Online (AOL) Web site.[67] According to the PhishTank Web site, active phishing sites have been documented since October 2006.[68]

RSA Security, Compliance, and Risk-Management Solutions recently estimated that the damage from phishing worldwide is $1.5 billion – an increase of 22% since 2011.[69] A breakdown of domain names attacked by phishing during the latter half of 2012 is provided by the Anti-Phishing Working Group (APWG).[70]



Not only is phishing on the rise, but its various methods are constantly evolving.[71] Today, several types of fishing are known: spear phishing, watering hole attacks, and whaling. Allied methods make use of systems other than computers, such as telephone systems, usually VoIP (vishing or voice phishing), and text messaging systems (SMiShing).

[66] Jerry Felix and Chris Hauck, "System Security: A Hacker's Perspective", *Interex Proceedings* 1: 6 (1987).

[67] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang and H. Deng, "A Survey of Cyber Crimes", *Security and Communication Networks* 5: 422-437 (2012). doi: 10.1002/sec.331

[68] http://www.phishtank.com/stats.php.

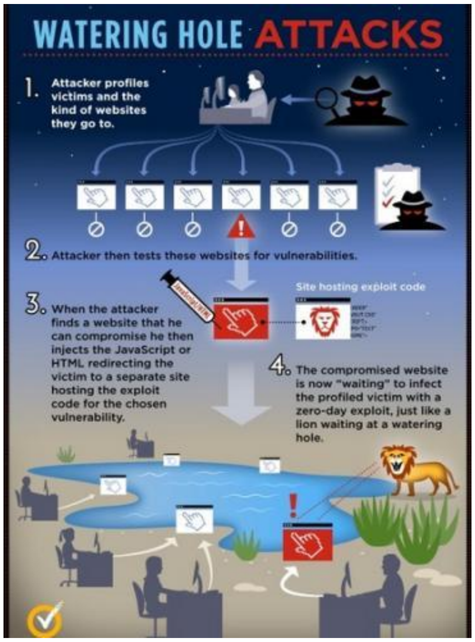
[69] http://blogs.rsa.com/laser-precision-phishing-are-you-on-the-bouncers-list-today/.

[70] http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf.

[71] http://resources.infosecinstitute.com/phishing-dangerous-cyber-threat/.

Among the types of phishing extant, one of the more prevalent forms of Internet fraud is “spear phishing”, which involves establishing a fake Web site – for example, one that pretends to be a bank or commercial entity like PayPal – which appeals to a distinct population. Once the site has been set up, an appeal is made to lure users to the fake site. Targeted users may be contacted by email or through (equally false) advertisements on Web forums, or fraudulent announcements from the fake Web site stating that it is necessary to click on a link to change your password, for example. The minute the user follows these instructions, his password is culled and preserved for future use by the “phisherman”. Although only a small percentage of spear phishing attacks succeeds, their potential for damage is on the rise.

In September 2012, Symantec warned of a new method of phishing: the watering hole attack. This method, which requires greater sophistication and more complex planning, is focused, and has four phases. During the first phase, the attacker identifies the Internet sites that his target audience uses. During the second phase, the attacker studies these sites to determine how they may be infiltrated. During the third phase, the attacker exploits breaches in the sites’ security to install a malicious code (such as a Trojan horse) – in other words, he co-opts a legitimate Web site to a fraudulent act. During the fourth and final stage, the attacker waits for his target audience to become ensnared by the malicious code. Since this entire process is invisible to the user and to site administrators, it can be difficult to discover that the site has been penetrated, such that the scam can continue for some time. Moreover, the watering hole attack can be used to hit an even larger number of victims if the attackers disseminate a malicious link to the impregnated site through a seemingly credible email, thereby improving the likelihood that the victims will cooperate with the scam.



WATERING HOLE ATTACKS

1. Attacker profiles victims and the kind of websites they go to.

2. Attacker then tests these websites for vulnerabilities.

3. When the attacker finds a website that he can compromise he then injects the JavaScript or HTML redirecting the victim to a separate site hosting the exploit code for the chosen vulnerability.

4. The compromised website is now “waiting” to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.

Another method of phishing is the “whaling attack”. In methodology similar to spear phishing, this type of attack targets people in key roles (CEOs, CFOs, etc.), with the aim of maximizing the efficacy of the data stolen. Like spear phishing and watering hole attacks, whaling can also be deployed through emails containing a link to a malicious code.

Although, as noted, much Internet fraud is deployed for criminal gain, it is easy to see how terrorist organizations[72] might also use it to obtain data openly or via the "dark Web" (see above) to serve their ends.

Analysis of a Watering Hole Attack on the ICT Web Site

In March 2013, Websense, which provides data monitoring and security, announced that there had been an attack on the Web site of the International Institute for Counter-Terrorism (ICT).[73] It estimated that the attack was perpetrated by a group calling itself The Elderwood which, since its 2006 inception, has had much success attacking Internet sites, Google's among them. The Elderwood appears to carefully plan most of its attacks,[74] and to favor the use of multiple zero day exploits or breaches;[75] their ability to do so indicates a high level of professionalism. To illustrate: while Stuxnet used four zero day breaches in security, The Elderwood has been known to use as many as eight in one attack.[76] In any case, the watering hole attack is protracted, and requires in-depth strategic thinking (see above).

The first reference to unidentified or unwanted files on the ICT Web site was made on January 23, 2013.[77] Apparently, the perpetrators embedded four files (three html files and one swf flash file) in a folder meant to contain JavaScripts. The files were difficult to identify for anyone not regularly monitoring the activity of the archive server and site. It is not possible to determine whether use was made of known breaches in security or of zero day exploits.

According to the Websense report, the goal of the attack was to introduce a Trojan horse into the computers of Web surfers visiting the ICT site. It must be stressed that, as of this writing, it appears that passive visitors to the ICT Web site were never in any danger; only those who clicked on the dedicated link

[72] http://www.fbi.gov/news/stories/2009/october/phishphry_100709.

[73] http://community.websense.com/blogs/securitylabs/archive/2013/03/12/israeli-website-for-international-institute-for-counter-terrorism-waterhole-serving-cve-2012-4969.aspx.

[74] http://www.huffingtonpost.co.uk/2012/09/07/zero-day-elderwood-hacking-group_n_1863602.html.

[75] "A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack." See http://searchsecurity.techtarget.com/definition/zero-day-exploit.

[76] http://www.symantec.com/connect/blogs/elderwood-project.

[77] http://jsunpack.jeek.org/dec/go/%3Flist%3D2?report=000fcf76178147a60c4326ba10efd0f5916c6c3f.

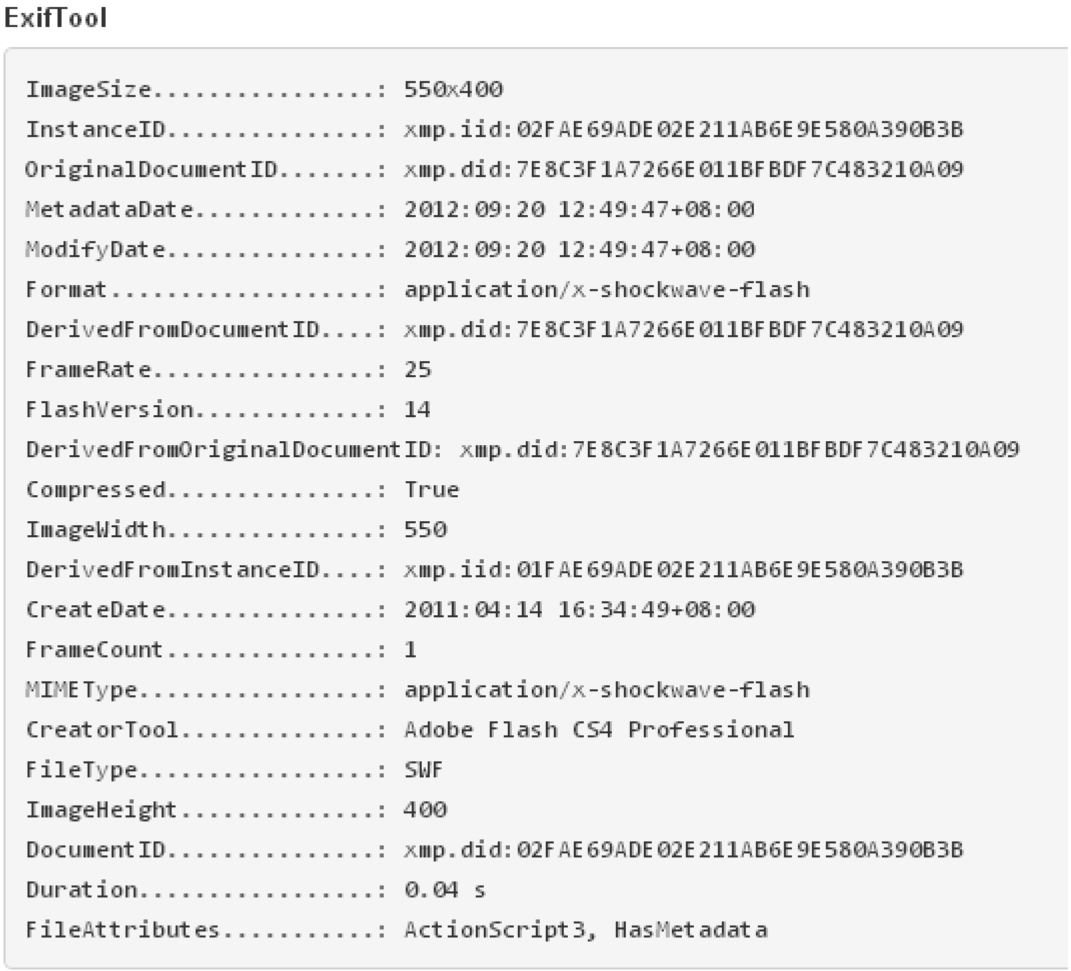
http://www.ict.org.il/js/1.html – which apparently activated the flash file in which the Trojan horse was embedded: Troj/SWFExp-BF,[78] EXP/FLASH.Carbul.Gen – may have been endangered. This spyware facilitates remote access to files; its estimated purpose is data theft. Moreover, this spyware automatically replicates itself, such that it is deliberately difficult to remove.[79] The dedicated server that activates the spyware is located in the US, but it is reasonable to assume that this server is connected to and operated by another server, in the attackers' country of origin.

It may be assumed that the attackers wanted to use the prestige of the ICT domain to disseminate this malicious link, by email, to persons active in security or decision making. It is possible that during infiltration, the ICT's database and the email addresses of users listed with the site were copied.

Analysis of the flash file revealed the date and time signature of its creation. Since the file was created in 2011, it may be surmised that the attack had been planned for some time. The time signature (+08) indicates the geographic location of the attackers – a time zone that includes China and Russia. It should be noted that a file's digital signature is derived from the date defined by the computer, which is easy to change; however, the likelihood that it will be changed is small.

[78] http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~SWFExp-BF.aspx.

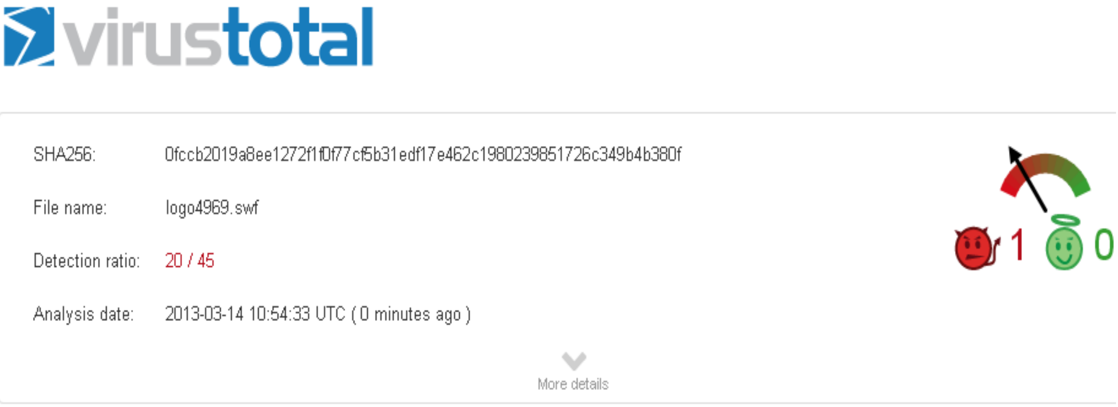
[79] http://www.zimbio.com/Latest+Computer+Threats/articles/18z94zb8ZqI/Troj+SWFExp+BF+Remove+Troj+SWFExp+BF+Automatically.



ExifTool

```
ImageSize................: 550x400
InstanceID...............: xmp.iid:02FAE69ADE02E211AB6E9E580A390B3B
OriginalDocumentID.......: xmp.did:7E8C3F1A7266E011BFBDF7C483210A09
MetadataDate.............: 2012:09:20 12:49:47+08:00
ModifyDate...............: 2012:09:20 12:49:47+08:00
Format...................: application/x-shockwave-flash
DerivedFromDocumentID....: xmp.did:7E8C3F1A7266E011BFBDF7C483210A09
FrameRate................: 25
FlashVersion.............: 14
DerivedFromOriginalDocumentID: xmp.did:7E8C3F1A7266E011BFBDF7C483210A09
Compressed...............: True
ImageWidth...............: 550
DerivedFromInstanceID....: xmp.iid:01FAE69ADE02E211AB6E9E580A390B3B
CreateDate...............: 2011:04:14 16:34:49+08:00
FrameCount...............: 1
MIMEType.................: application/x-shockwave-flash
CreatorTool..............: Adobe Flash CS4 Professional
FileType.................: SWF
ImageHeight..............: 400
DocumentID...............: xmp.did:02FAE69ADE02E211AB6E9E580A390B3B
Duration.................: 0.04 s
FileAttributes...........: ActionScript3, HasMetadata
```

Soon after this incident was discovered, an examination was made of the file using Virustotal, followed by a simultaneous examination of the file using 45 of the various tools currently available on the market to determine whether or not the malicious code embedded was known. Most of the tools could not identify the specific code, indicating that it is a new code not widely used in the past and so not identifiable.



SHA256: 0fccb2019a8ee1272f1f0f77cf5b31edf17e462c1980239851726c349b4b380f

File name: logo4969.swf

Detection ratio: 20 / 45

Analysis date: 2013-03-14 10:54:33 UTC (0 minutes ago)

In summary, timely discovery of an infiltration makes it possible to quickly remove spyware from the server, and prevent subsequent, significant stages of an attack. Was the embedding of a malicious code into the original code of the ICT’s Web site liable to automatically infect the computer of the random surfer? Since no fundamental change was found in the Web site’s code, it may be surmised that the average site user was not harmed. Moreover, an attack by a group like The Elderwood, which uses zero day exploits, raises the alarm for constant monitoring to detect changes. Because no visible damage was done in this case, it is possible that had Websense not reported the infiltration, the attack would have remained undetected for quite some time. Monitoring must include the examination of new files created on the server, especially any anomalous changes, like the addition of files by an unknown user with a strange IP. Updating components and monitoring security breaches in the server are essential to curtailing cybernetic attacks. However, the technology that will completely prevent such attacks is not yet available to the public.

Case Study

Each newsletter issued by the ICT's cyber-desk will discuss in greater detail a recent incident of cyber-attack. This issue highlights an extensive attack on South Korea.

From Preventing Service to Blocking Computers: Analysis of an Attack on South Korea[80]

Recent months have seen a reawakening of attacks on computers whose aim is to completely erase those computers. Such attacks target a large number of an organization's computers, in an attempt to significantly impair the organization's functioning. Since most organizations are almost totally dependent on computers, such attacks have significant implications for normal functioning and commerce. The severity of the damage from such attacks is commensurate with the organization's dependence on its computers. As related in a previous ICT Cyber-Desk Newsletter,[81] an attack of this type, known as Shamoon, erased some 30,000 of the computers of Saudi oil giant ARAMCO and caused similar damage to Qatari RasGas. Then-US Secretary of Defense Leon Panetta deemed it one of the most destructive attacks ever on the private sector.[82]

Also on the rise are denial of service or DDoS attacks (see above), which aim to prevent online service by overwhelming a communications server or occupying its data analysis functions to the point where they cannot serve legitimate users. But the topic of this case study is the recent resurgence in attacks that cause enough damage to necessitate the replacement of hardware or the reinstallation of damaged programs.[83] I have come to refer to such attacks as "denial of computers" (DDoC, a term that has yet to gain currency, to the best of my knowledge). Denial of computers attacks prevent an organization from using its computers because they

[80] This analysis was written by Ram Levi, Cyber-Security Advisor to the National Council for Research and Development and Senior Researcher at Tel Aviv University.

[81] See http://www.ict.org.il/LinkClick.aspx?fileticket=Mc6t6hF5Ug0%3d&tabid=492.

[82] See also Institute for Counter-Terrorism. *ICT Cyber-Desk Review*, January 24, 2013, http://www.ict.org.il/LinkClick.aspx?fileticket=Mc6t6hF5Ug0%3d&tabid=492 (accessed February 18, 2013).

[83] This type of attack has been deemed Permanent Denial of Service (PDoS). These are attacks that cause permanent damage physically to the computer or to computer and network equipment that require their replacement or reinstallation. Because of technological changes, the time it takes to recover from attacks that do not cause physical damage is shorter than in the past and can be done in concentrated form. Therefore this name does not accurately describe the new attacks that we are now witness to, as will be described in this analysis. See Sridhar Subramani, "Denial of Service Attacks and Mitigation Techniques: Real Time Implementation with Detailed Analysis", *SANS,* 2011, http://www.sans.org/reading_room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi_33764 (accessed April 17, 2013).

have been erased, or because the information they contain has been encoded by the attacker, who retains the key to the code. Such attacks cause more significant damage than do denial of service attacks, as is illustrated by what happened to South Korea this past March.

A Cyber Attack against South Korea

In March 2013, more than 48,000 computers in banks and television stations in South Korea simultaneously ceased functioning – in popular parlance, they "crashed". According to official police sources, the attack affected three television stations (KBS, MBC and YTN) and two banks (Shinhan Bank and NongHyup Bank), seriously disrupting their ability to function (even though the broadcasts of these TV stations were not impeded).[84] According to Symantec, this attack was related to cyber-attacks on South Korea in 2009 and 2011.

In 2009, a number of Web sites in South Korea and the US experienced a cyber-attack known as the "Fourth of July", which lasted for several days. The first wave of this attack began on July 4, 2009 and consisted primarily of denial of service (DDoS); it was not overly significant, but raised the suspicion that North Korea was behind the attack.[85] The second and third waves of the attack, which were a bit more sophisticated, began several days later. During this part of the attack, which lasted several days, email messages were sent with a logical bomb known as Trojan.Dozer, which was set to "detonate" on July 10, 2009, causing the erasure of a small – but essential – section of the hard disk (the MBR) of an infected computer,[86] rendering it unusable.[87]

On May 4, 2011, South Korea and the US again experienced a denial of service (DDoS) attack, this time perpetrated using a Trojan horse known as Trojan.Koredos,

[84] Laura Sciuto, "South Korea Hit Hard by Massive Cyber-Attack", April 1, 2013, http://www.pbs.org/newshour/extra/2013/04/south-korea-hit-hard-by-massive-cyber-attack/ (accessed April 1, 2013).

[85] John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea", July 9, 2009, http://www.nytimes.com/2009/07/10/technology/10cyber.html?_r=1& (accessed April 12, 2013).

[86] The most important part of the hard disk, when it is divided into partitions, is the partition that contains the master boot record (MBR), the hard disk signature, and the disk's partitions table. For more information about the Master Boot Code, see http://technet.microsoft.com/en-us/library/cc976786.aspx.

[87] Symantec. "Are the 2011 and 2013 South Korean Cyber Attacks Related?" April 2, 2012, http://www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyber-attacks-related (accessed April 4, 2012).

which carried a Bot network built by the attackers. This Trojan horse was fairly sophisticated, if only because it succeeded (by chance) in remaining undetected.[88]

A third attack, as noted, took place this March – specifically, on March 20, 2013. This time, a DDoS attack did not suffice. In what I am calling a "denial of computers" attack, the attackers went one step further, erasing 48,000 (forty-eight *thousand*) computers simultaneously. This attack is worthy of more in-depth attention, as it was far more sophisticated than its predecessors. First, the malware was attached at two vectors: (1) via email; and (2) via infiltration of the system administration for updating attributes. This is an extremely interesting case, because the patch management system[89] is meant to update security weaknesses in an organization's system. The importance of program updates to minimize potential attacks cannot be overstated; when a system like this serves as the basis for an attack, thorough examination is warranted, of the type that cannot be attempted here.

After positioning itself on the network, the malware, when activated, did two things: (1) it erased the MBR table, in effect removing the computer from service and, in most cases, necessitating reinstallation; (2) it sought mapped network disk drives, and tried to erase the information on them. Usually, most of an organization's material will not be on end-use computers but rather on network computers and the channels of access to them, through mapped network disk drives. Although it may be assumed that this material is backed up, restoring it from backup takes time, and may result in the loss of data.

China or North Korea?

Official sources in South Korea were quick to accuse Chinese agents of being behind the attack, in part because a number of Chinese IP addresses were identified. However, data protection groups, which included representatives from several government bodies, determined that the culprit was North Korea.

[88] Andrea Lelli, "Backdoor.Prioxer!inf: 'Accidentally' the Stealthiest File Infector Ever!" March 15, 2011, http://www.symantec.com/connect/blogs/backdoorprioxerinf-accidentally-stealthiest-file-infector-ever (accessed April 15, 2013).

[89] A patch is a section of code that a programming company disseminates to repair a problem found in one of its programs. A problem may be a security breach or weakness, which hackers can exploit to attack a computer containing the program. The difficulty performing program updates ensues from their interference with an organization's activities, primarily if the update necessitates rebooting computers or, in the case of mobile phones, using the entire data package purchased by the user.

> "The team, consisting of government, military and civilian organizations, also said that those responsible appeared to have implanted the codes used in the attack as many as eight months ago." [90]

In an official announcement by the Ministry of Information, Processing and Future Planning, North Korea was openly and officially blamed for the March 2013 attack.[91] According to the analysis conducted by a group of experts of the Ministry, 22 IP addresses were discovered which were linked to six North Korean computers that disseminated the malicious code for eight months (because the communication was routed via China, there was apparently confusion concerning who actually perpetrated the attack).[92]

South Korea's Response

As the above review indicates, South Korea has experienced a significant increase in cyber-attacks in recent years. At a government hearing, Nam Jae-Joon, who heads South Korea's security service (NIS), stated that in the past five years, South Korea had experienced more than 70,000 cyber-attacks, most of them emanating from North Korea. South Korea has difficulty coping effectively with the resolve and methodical nature of its rival to the north:

> "South Korea cannot cope with unpredictable and sophisticated provocations from North Korea with a bureaucratic, rigid mindset." [93]

In a visit to South Korea in April 2013, the NATO Secretary-General suggested increasing cooperation in the cyber field, in light of the recent cyber-attack:

> "The Minister explained the interim findings – announced on April 10 – of the ongoing investigation into the cyber terror that occurred on March 20. In

[90] He-suk, Choi, "Seoul Blames Pyongyang for Cyber Attacks", April 10, 2013, http://www.koreaherald.com/view.php?ud=20130410000766 (accessed April 12, 2013).

[91] Yonhap News Agency, "Gov't Confirms Pyongyang Link in March Cyber Attacks", April 10, 2013, http://english.yonhapnews.co.kr/northkorea/2013/04/10/49/0401000000AEN20130410007300320F.HTML (accessed April 12, 2013).

[92] Yonhap New Agency (Yonhap Editorial), "N. Korean Cyber Warfare Emerges as 'Existing Threat'", April 11, 2013,http://english.yonhapnews.co.kr/yhedit/2013/04/11/75/5100000000AEN20130411007500315F.HTML (accessed April 12, 2013).

[93] In-taek, Chae, "The Evolution of Provocation", March 28, 2013, http://koreajoongangdaily.joinsmsn.com/news/article/Article.aspx?aid=2969240 (accessed April 4, 2013).

> response, Secretary-General Rasmussen proposed that the two sides work together in cyber defense and various other fields."[94]

On April 2, 2013, the South Korean Ministry of Defense announced its intention to establish a new department dedicated to formulating policy governing the deterrence of cyber-attacks, and responsible for developing better methods of information security to confront developing threats.[95] The new department is meant to augment the work of the South Korean military cyber command established in 2010.

Analysis of the Attack

Several months of planning are required to conduct such an attack, during which intimate intelligence is acquired of the target network; a hold is placed on the network and it is studied to identify its weaknesses, including breaches through which it may be possible to pass a worm or a Trojan horse, which in the future will be deployed to erase the network's computers. As noted, while DDoS attacks target an organization's network but work from them outward, exploiting vulnerabilities in communications protocols, DDoC (denial of computers) attacks target an organization's network but exploit weaknesses in its computers – without being detected by antivirus software, IPS/IDS systems for detecting infiltrations and excesses, or additional means of security. In order for the attacker to know that the attack has begun, the Trojan horse must be able to covertly report its position in the network, and wait for the command to act. It is possible that, in order not to be detected, the attacker may program the malicious code to deploy at a certain time in the future – in other words, he may set up a time-released logical bomb – rather than trying to control or monitor the logical bomb. This choice puts the attacker at a significant disadvantage, because he will not be able to retreat from implementation if he changes his mind, nor will he have a clear idea of how many computers have been infected. Unless the attacker has a "mole" inside the organization, he will not be able to assess the likely outcome of his attack.

Furthermore, unlike DDoS attacks which damage the availability of online services, and which usually piggyback on "innocent" computers, DDoC attacks damage the very ability of a computer-dependent organization to function. DDoC attacks send multiple inputs into the computers of the targeted organization, which will ultimately

[94] Ministry of Foreign Affairs, "Foreign Minister Meets with the NATO Secretary-General", April 15, 2013, http://news.mofat.go.kr/enewspaper/articleview.php?master=&aid=5171&ssid=24&mvid=1498 (accessed April 17, 2013).

[95] Ibid.

necessitate their restoration – causing those computers to be “down” for a protracted time.

Why would anyone want to erase the computers of banks and television stations? Because doing so damages the functioning of the entire banking system, and of the entire television and radio network, and so has a marked psychological effect.

In summary, the attack on South Korea represents an escalation that should not be taken lightly. More destructive by far than a DDoS attack, the DDoC attack, which is complex to plan and implement and which requires more knowledge and resources, has a greater potential for harm over a longer period of time.

Guest Contributor

An Act of Cyber Patriotism or an Act of Cyber Vengeance?[96]

"Do you love your nation? Do you want to fight your nation's enemy? Join us and fight our enemy…" These slogans are enough to boost the adrenaline of any person who thinks about his or her nation. However, what if this mantra is just an incitement to committing nothing but a crime – either in the real world or in cyberspace?

Every day, cyberspace witnesses hundreds of cybercrimes, especially brawls among cyber hackers from around the world, all in the name of cyber patriotism. Who is authorized to call for people to act for such a noble cause as cyber patriotism?

Bangladesh, China, India, and Pakistan are among the countries that face the cyber patriotism dilemma. Are the hackers they confront really driven by "altruistic genes", or are they merely seeking revenge?

In the cyber-world, physical strength is insignificant; a hacker transcends a victim's defenses[97] not by summoning the combined efforts of 10 or 20 hackers, but by using

[96] This article was written by Swapnil Kishore, an ICT Research Intern who holds an MA in Government with a specialization in Counter Terrorism and Homeland Security from the IDC; he is also criminologist specializing in countering organized crime and terrorism, and a cyber security consultant, ethical hacker and cyber forensics expert.

[97] Perhaps the best example of this is the distributed denial of service (DDoS) attack. In February 2000, a 15-year-old Canadian known only as "Mafiaboy" used a distributed denial of service attack to shut down Web sites operated by CNN, eBay and Amazon.com, causing billions of dollars in damage. See "Mafiaboy's Pre-Trial Guilty Plea", *Wired News*, January 18, 2001, http://www.wired.com/news/politics/0,1283,41287,00.html and "Hacker Saga Continues: Mounties Nab 15-Year-Old Canadian", *IT World*, April 19, 2000, http://www.itworld.com/Sec/3834/ITW384/ (both are on file with the North Carolina Journal of Law & Technology). Mafiaboy acted alone, uzsing innocent computers – known as "zombies"

technology, automated techniques that enable him or her to bypass electronic defenses. An example of this is provided by the Honker Union of China (H.U.C.), whose Web site claims it is "a non-governmental patriotic organization". It states: "All our words and actions are based on patriotism and safeguarding China's dignity. Our voices and actions are the manifestation of China's national integrity". The Honker Union of China was formed after a group of computer hackers caused a stir in 2001 when they brought down thousands of US websites in response to the collision of a US spy plane and a Chinese fighter jet over the South China Sea. Since then, the group has developed into a highly organized network of more than 12,000 individuals who are at the cutting edge of the darkest arts of the information age.

Similarly, according to a top Philippine National Police official, that country has become a "haven" for transnational organized crime syndicates involved in cyber pornography, cyber sex dens, illegal online gambling, credit card fraud and identity theft due to weak laws against cyber crime and the poor technical know-how of law enforcement agencies.

The international legal community began showing its concern over cyber operations in the late 1990s. Most significantly, in 1999, the United States Naval War College convened the first major legal conference on the subject.[98] In the aftermath of the attacks of September 11, 2001, transnational terrorism and the ensuing armed conflicts diverted attention from this topic until the massive cyber operations by so-called "hacktivists" against Estonia in 2007; against Georgia during its war with the Russian Federation in 2008; and the targeting of the Iranian nuclear facilities by the Stuxnet worm in 2010.

The so-called "Tallinn Manual" on international law applicable to cyber warfare, written by an international group of independent experts, was the result of a three-

– to mount his attack; as in any DDoS attack, he used easily available programs to seize control of the computers he would use as zombies, often without the knowledge of their owners. See "What Is a Distributed Denial of Service (DDoS) Attack?", *Fox News*, June 15, 2002, http://www.foxnews.com/story/0,2933,55382,00.html and Eric J. Bowden, "DoS vs. DDoS Attacks", *ZD Net*, October 30, 2000, http://www.zdnet.com/products/stories/reviews/0,4161,2645417-2,00.html (both on file with the North Carolina Journal of Law & Technology). In 2001, a 13-year-old Wisconsin boy used a denial of service attack to shut down a California computer security site. In the real world, adolescents cannot mount solo attacks that cripple multimillion dollar businesses, but in the cyber world, it is not particularly difficult for them to do so. See Steve Gibson, "The Strange Tale of the Denial of Service Attacks against GRC.com", June 1, 2001, http://www.metafilter.com/8006/The-Strange-Tale-of-the-Denial-of-Service-Attacks-Aagainst-GRCCOM.

[98] For the proceedings see Michael N. Schmitt and Brian T. O'Donnell, eds., "Computer Network Attack and International Law", *Naval War College International Law Studies* 76 (2002).

year effort to examine how extant international law norms apply to this new form of warfare. However, the Tallinn Manual is not an official document, but an expression of the opinions of experts acting solely in a personal capacity.

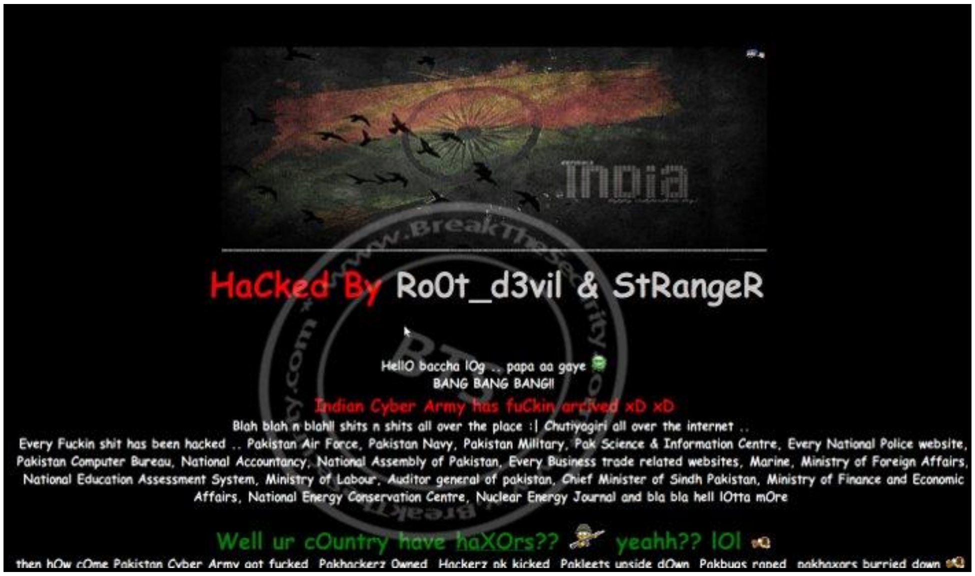
Spotlight on Cyber Attacks Emanating from the Indian Subcontinent

The rate of cyber attacks between India and Pakistan has grown to significant proportions. By some counts, Pakistani hackers attack 40-50 Indian Web sites a day, while Indian hackers attack some 10 Pakistani sites a day. Both countries have recognized the threat that these sub-state actors pose, and have responded by building both offensive and defensive cyber capabilities. The following is a chart of just some of the hackers active in Bangladesh, India and Pakistan:

Bangladesh	***India***	***Pakistan***
Bangladesh Anonymous Legion	Indishell	3xplore Cyber Army
Bangladesh Black Hat Hacker	Team Grey Hat	PAKBugs
Bangladesh Cyber Army	Team NUTS^{TM}	PakCyber Eaglez
Bangladesh Grey Hat Hackers (BGHH)	TOF (Team Open Fire)	P4k!$74n H4x0r$

Following are the banners of several of these hacker groups:

3xp1r3 Cyber Army
$\sqrt{3xp1r3} = \left(\frac{Hacking}{Security^2} \cdot \frac{Quality}{Quantity}\right)$
Proud of 3xp1r3 Cyber Army
we are waiting ..
w3 n3v3r G1v3 Up!
n3v3r f1ght w1th us!
n3v3r fl0w us!
Do n0t mak3 us c0m3 back aga1n!



HaCked By Ro0t_d3vil & StRangeR

HellO baccha lOg .. papa aa gaye
BANG BANG BANG!!

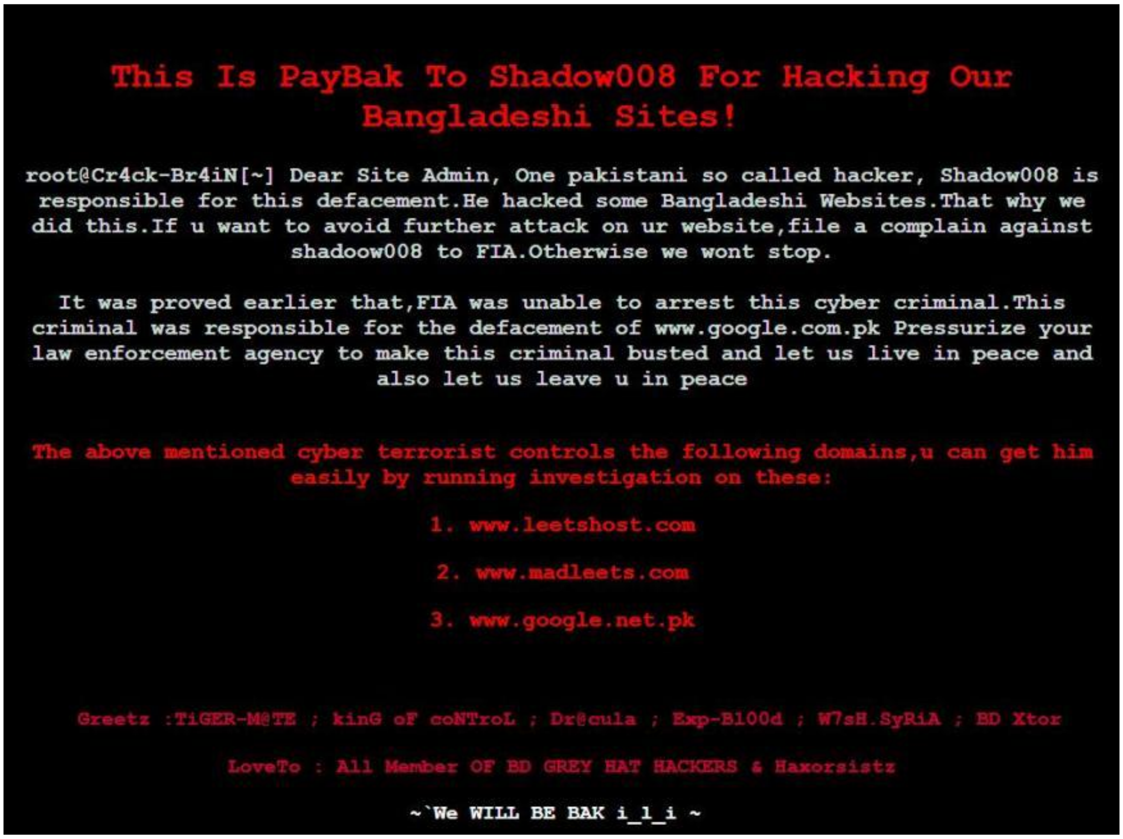
Indian Cyber Army has fuCkin arrived xD xD

Blah blah n blah!! shits n shits all over the place :| Chutiyagiri all over the internet ..

Every Fuckin shit has been hacked .. Pakistan Air Force, Pakistan Navy, Pakistan Military, Pak Science & Information Centre, Every National Police website, Pakistan Computer Bureau, National Accountancy, National Assembly of Pakistan, Every Business trade related websites, Marine, Ministry of Foreign Affairs, National Education Assessment System, Ministry of Labour, Auditor general of pakistan, Chief Minister of Sindh Pakistan, Ministry of Finance and Economic Affairs, National Energy Conservation Centre, Nuclear Energy Journal and bla bla hell lOtta mOre

Well ur cOuntry have haXOrs?? yeahh?? lOl

then hOw cOme Pakistan Cyber Army got fucked, Pakhackerz Owned, Hackerz pk kicked, Pakleets upside dOwn, Pakbugs raped, pakhaxors burried down



This Is PayBak To Shadow008 For Hacking Our Bangladeshi Sites!

root@Cr4ck-Br4iN[~] Dear Site Admin, One pakistani so called hacker, Shadow008 is responsible for this defacement.He hacked some Bangladeshi Websites.That why we did this.If u want to avoid further attack on ur website,file a complain against shadoow008 to FIA.Otherwise we wont stop.

It was proved earlier that,FIA was unable to arrest this cyber criminal.This criminal was responsible for the defacement of www.google.com.pk Pressurize your law enforcement agency to make this criminal busted and let us live in peace and also let us leave u in peace

The above mentioned cyber terrorist controls the following domains,u can get him easily by running investigation on these:

1. www.leetshost.com

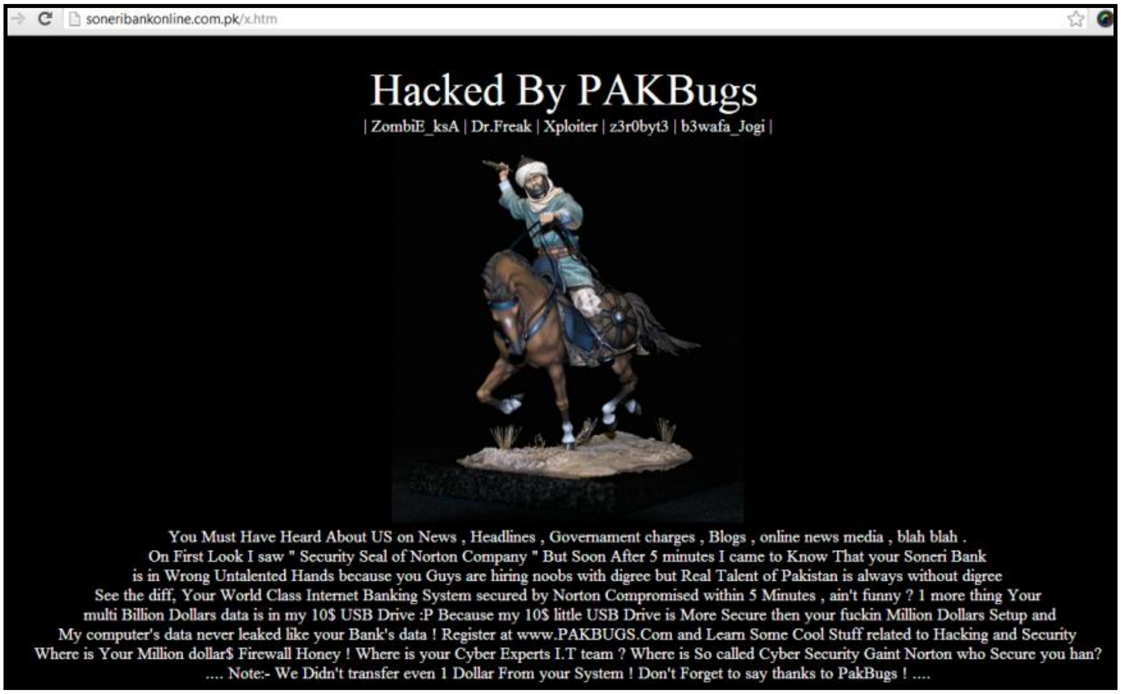
2. www.madleets.com

3. www.google.net.pk

Greetz :TiGER-M@TE ; kinG oF coNTroL ; Dr@cula ; Exp-B100d ; W7sH.SyRiA ; BD Xtor

LoveTo : All Member OF BD GREY HAT HACKERS & Haxorsistz

~`We WILL BE BAK i_l_i ~



Hacked By PAKBugs

| ZombiE_ksA | Dr.Freak | Xploiter | z3r0byt3 | b3wafa_Jogi |

You Must Have Heard About US on News , Headlines , Governament charges , Blogs , online news media , blah blah .
On First Look I saw " Security Seal of Norton Company " But Soon After 5 minutes I came to Know That your Soneri Bank
is in Wrong Untalented Hands because you Guys are hiring noobs with digree but Real Talent of Pakistan is always without digree
See the diff, Your World Class Internet Banking System secured by Norton Compromised within 5 Minutes , ain't funny ? 1 more thing Your
multi Billion Dollars data is in my 10$ USB Drive :P Because my 10$ little USB Drive is More Secure then your fuckin Million Dollars Setup and
My computer's data never leaked like your Bank's data ! Register at www.PAKBUGS.Com and Learn Some Cool Stuff related to Hacking and Security
Where is Your Million dollar$ Firewall Honey ! Where is your Cyber Experts I.T team ? Where is So called Cyber Security Gaint Norton who Secure you han?
.... Note:- We Didn't transfer even 1 Dollar From your System ! Don't Forget to say thanks to PakBugs ! ....

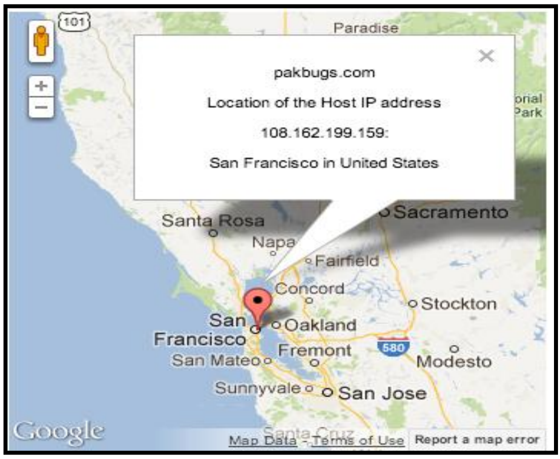
Pakistani hackers will always remember July 7, 2010 as the commencement of a dreadful period in their lives. Mr. Shahid Nadeem Baloch, the Director of Cyber Crime Investigations for the Federal Information Agency (FIA), Pakistan, announced the arrest of five ringleaders of the notorious hacker forum PAKBugs. They had become a bone of contention for the Pakistani government, due to their nefarious activities in cyber space. The following hackers were arrested or wanted:

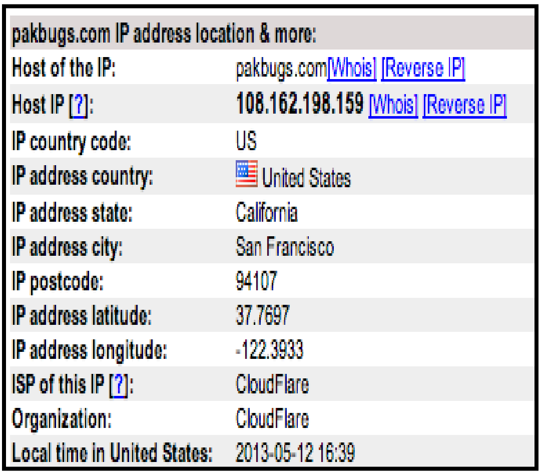
1. Jawad Ehsan (aka Humza, aka ZombiE_Ksa; mr.lonely420@hotmail.com), is still at large in Riyadh, Saudi Arabia. Jawad is the founder of PAKBugs, and probably the most famous of the PAKBugs hackers. He has been charged with 169 Web site defacements. Even India's Central Bureau of Investigation was hacked by Humza/ZombiE_Ksa.
2. Ahmad Hafeez (aka Vergil; hotpoint-001@hotmail.com) was arrested in Lahore. A moderator on the Web boards PAKBugs and Pakhaxorz, Ahmad Hafeez is charged with 480 Web site defacements.
3. Hassan Khan (aka x00mx00m; x00mx00m@gmail.com) was arrested in Peshawar. A co-founder of PAKBugs, he is charged with 8,697 Web site defacements.
4. Farman Ullah Khan (codename "Farman"; farmanullahkhan@gmail.com) was arrested in Bannu. Farman was a VIP-member of PAKBugs. The charges against Farman are not known.

5. Malik Hammad Khalid (goes by the hacker name inject0r; *lovedontcostapenny_1@live.com*) was arrested in Rawalpindi. Formerly a "super moderator" at PAKBugs, Malik Khan is charged with 134 Web site defacements.
6. Taimoor Zafar Bhatti (goes by the handler name h4v0c-; *amilliondollarsmile@hotmail.com*), was also arrested in Rawalpindi. Taimoor was a "super moderator" at PAKBugs; he is charged with 105 Web site defacements.

Hackers calling themselves BiG^Smoke (bigsmoke@loverzpoint.net), Cyb3r-Criminal (cyber-criminal420@loverzpoint.net), spo0feR (outlaw41@live.com) and [a] (ahmed.kamal29@gmail.com) are also wanted by the FIA Cyber Crimes Department, Pakistan.

The following are the server details of www.PAKBugs.com:



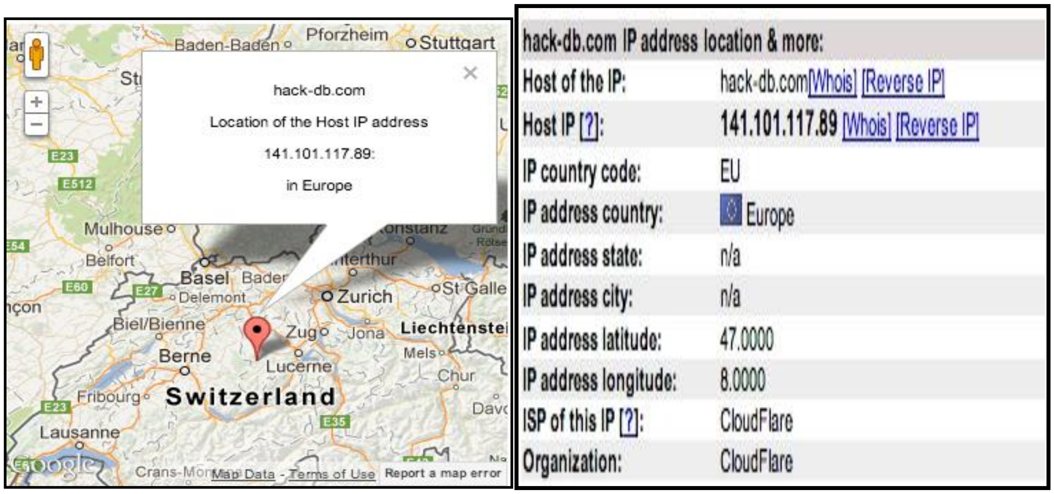


pakbugs.com IP address location & more:	
Host of the IP:	pakbugs.com[Whois] [Reverse IP]
Host IP [?]:	108.162.198.159 [Whois] [Reverse IP]
IP country code:	US
IP address country:	United States
IP address state:	California
IP address city:	San Francisco
IP postcode:	94107
IP address latitude:	37.7697
IP address longitude:	-122.3933
ISP of this IP [?]:	CloudFlare
Organization:	CloudFlare
Local time in United States:	2013-05-12 16:39

According to a press release, these individuals have expertise in the following techniques: Linux; SQL injection; Trojan horses; phishing; rooting; access to various servers; botnets; PHP scripts; stealers; ASP scripts (self writing); JSP scripts (self writing); key loggers; and credit card jacking and usage of stolen credit cards. The following are among the tools they may have used in their attacks: Ping of Death, HTTP Bomber 1.001b, EvilPing, FakeMail, Ping-Flood, MailBomber, Winsmurf, Attack 2.5.1, QuickFire, PutDown, and Defend.

According to the Web site www.hack-db.com, Pakistani hacker groups are maintaining databases for use by hackers and groups of hackers perpetrating cyber attacks in real time, all over the world. However, not all of these attacks are listed by country. It appears that only the allies of Pakistani hacker groups are cited on this Web site, which also provides cyber attack statistics on a weekly and a monthly basis. It is interesting to note that this Web site is acting as a sister to the Web site

3xplor Cyber Army (another Pakistani hacker group; http://www.3xp1r3.com/), thereby providing a place for hackers to participate actively and hold discussions. Both of these Web sites, along with PAKBugs, run under the CloudFlare ISP organization, in various regions of the US and Europe, as illustrated below.



hack-db.com

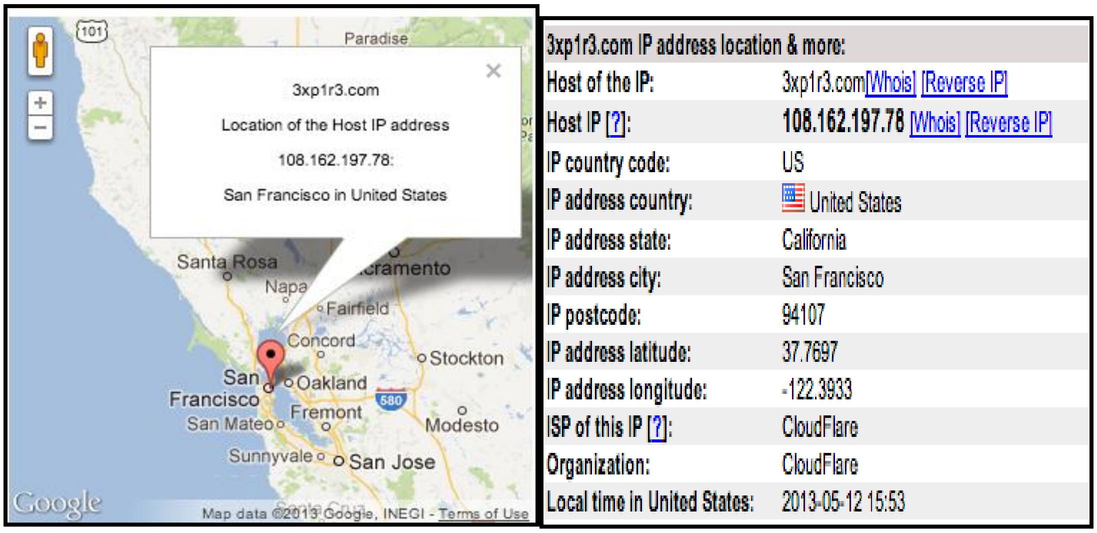
Location of the Host IP address

141.101.117.89:

in Europe

hack-db.com IP address location & more:	
Host of the IP:	hack-db.com[Whois] [Reverse IP]
Host IP [?]:	141.101.117.89 [Whois] [Reverse IP]
IP country code:	EU
IP address country:	Europe
IP address state:	n/a
IP address city:	n/a
IP address latitude:	47.0000
IP address longitude:	8.0000
ISP of this IP [?]:	CloudFlare
Organization:	CloudFlare

Server details of www.hack-db.com



3xp1r3.com

Location of the Host IP address

108.162.197.78:

San Francisco in United States

3xp1r3.com IP address location & more:	
Host of the IP:	3xp1r3.com[Whois] [Reverse IP]
Host IP [?]:	108.162.197.78 [Whois] [Reverse IP]
IP country code:	US
IP address country:	United States
IP address state:	California
IP address city:	San Francisco
IP postcode:	94107
IP address latitude:	37.7697
IP address longitude:	-122.3933
ISP of this IP [?]:	CloudFlare
Organization:	CloudFlare
Local time in United States:	2013-05-12 15:53

Server details of www.3xp1r3.com

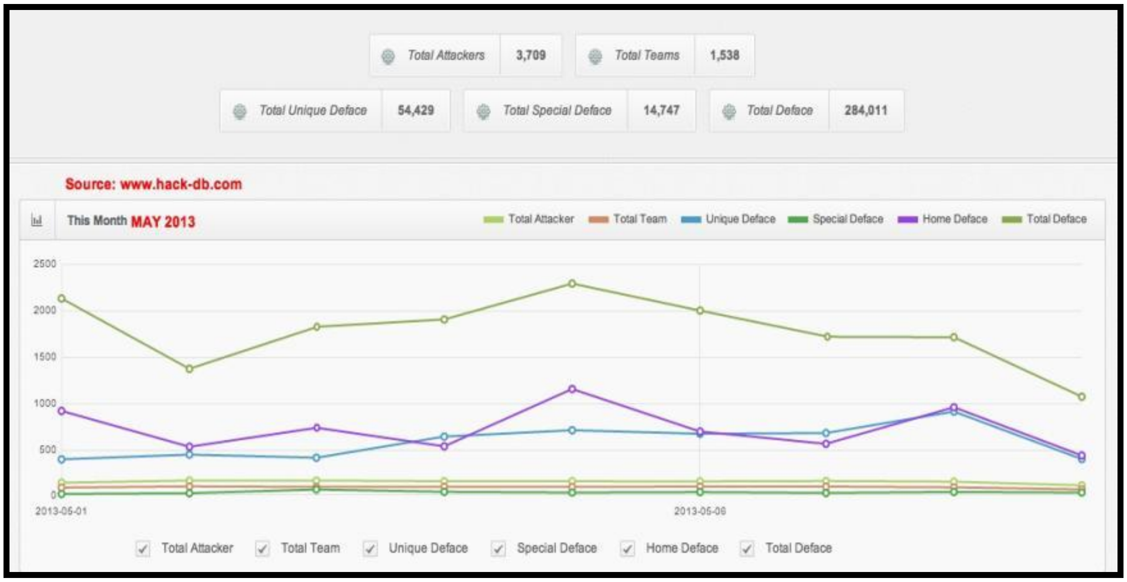
The Web site www.hack-db.com also showcases teams of what it calls the "top hackers", based on its analysis of how many Web sites have been defaced or disrupted by various hacker teams, as illustrated in the following chart:

Top Ten Cyber Hacker Teams **Date: 13/05/2013**

Source: www.hack-db.com

Position	Team	Total Member	Unique Deface	Home Deface	Special Deface	Total Deface
1.	3xp1r3 Cyber Army	49	10067	17291	1945	33256
2.	NinjaVirus	2	5712	28	213	8161
3.	Iran Security Team	13	5035	265	94	6564
4.	The Crows Crew	32	4868	15596	747	21962
5.	Hacker Newbie Community	49	2846	5393	393	7823
6.	Johor Hacking Crew	2	2563	1495	142	6482
7.	BD GREY HAT HACKERS	48	2557	14266	965z	15844
8.	Indonesian Cyber Army	59	2300	1774	131	4806
9.	BD BLACK HAT	42	2242	4910	356	9728
10.	Indonesian Security Down	76	2114	2058	366	6801

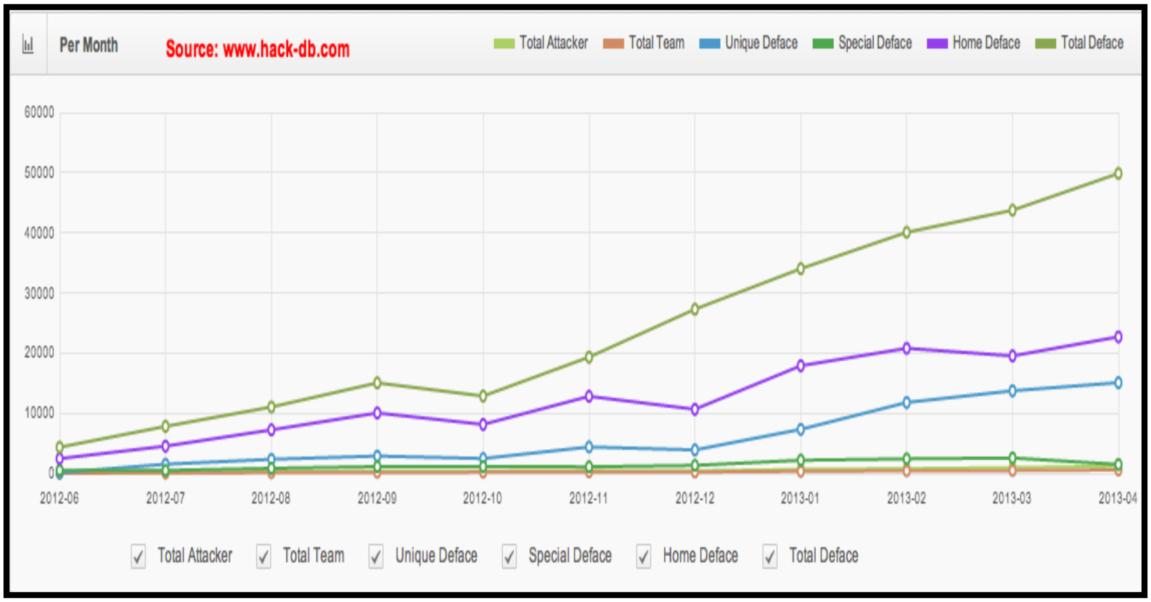
The following two graphs show the statistics for cyber attacks provided by www.hack-db.com:


Total Attackers 3,709 | Total Teams 1,538
Total Unique Deface 54,429 | Total Special Deface 14,747 | Total Deface 284,011

Source: www.hack-db.com

This Month MAY 2013

Cyber attacks in May 2013


Per Month

Source: www.hack-db.com

Cyber attacks by month, from June 2012 – April 2013

Governments have now realized the rewards and perils of cyber infiltration, and are mobilizing their resources and powers to pursue "politics by other means", as Clausewitz defined war, in the domain of cyber warfare. Today, administrations are actively harnessing hacker assets to augment their power in pursuing the traditional security goals of defending one's infrastructure, economy and assets, and establishing a counter-strike capability that can underpin deterrence as the bottom line of defense. In November 2011, Indian Information Technology Minister Kapil

Sibal urged the community of "ethical hackers" to help defend India's networks, since "the resource pool of them is very limited in the world". India has also reportedly been considering using "patriotic hackers" in offensive operations. The *Times of India* reported that a high-level meeting held in August 2010, which was chaired by National Security Adviser Shiv Shankar Menon and attended by the director of India's intelligence bureau as well as by senior officials from its telecom department and IT ministry, considered recruiting and providing legal protection to hackers who would be used to attack the computers of hostile nations. Several security experts in Delhi reported that National Technical Research Organization (NTRO) officials were soliciting hackers on Web sites and electronic bulletin boards.

China, of course, is widely suspected of using patriotic hackers and "cyber militias" as defense and offense. According to the *Financial Times*, Nanhao Group, a Web company near Beijing, has departments tasked with attack and defense. A Chinese report mentions cyber militias in Tianjin's Hexi District. Recent intelligence leaks and private security reports about cyber espionage suggest that the Chinese government backs or directs the majority of espionage attacks against Western and Japanese technology companies, with hackers clocking in and out between 9:00 a.m. and 5:00 p.m. local time.

Governments may see patriotic hackers as the answer to their cyber vulnerabilities, but they are not the solution, and using them will increasingly destabilize this and other regions. Rather, governments should start engaging in more stringent IT acts, as well as in international cooperation with other nations. These "geeks" or so-called "patriotic hackers" are nobody but a bunch of deviant cyber juveniles, who are injected with adrenaline for a certain period of time and who take every opportunity given by insubstantial laws to exploit technologies. Although by exploiting hacking, with the help of state or non-state actors, a nation may gain access to restricted and classified information, it is at the same time losing credibility, and exhibiting its inefficient strategies for apprehending such patriotic hackers.[99]

[99] The following Web sites were consulted in the writing of this article: www.hack-db.com; http://www.networkworld.com/news/2012/110812-chinese-ex-hacker-says-working-for-264074.html; http://www.scmp.com/article/703943/hacker-union-denies-hit-google; http://www.theepochtimes.com/n2/opinion/the-threat-of-chinas-patriotic-hacker-army-60695-all.html; and http://thediplomat.com/2012/02/29/the-danger-of-patriotic-geeks/?goback=%2Egde_41268_member_97962489.

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

Ram Levi, Cyber-Security Advisor to the National Council for Research and Development and Senior Researcher at Tel Aviv University

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

Nir Tordjman, Cyber Threats Researcher, ICT

Hila Oved, Special Project Manager, ICT