Triangle of
Middle East Cyber Warfare
"Egypt – Israel – Iran"

By: Ebrahim Hegazy

Agenda

1- What is Cyber Warfare
2- Fields of Cyber Warfare:
A) Critical web sites
B) Computers and Networks

3- Middle East and Cyber warfare motivations
4- Hacking Groups and individuals in: Egypt - Israel – Iran
5- Famous Web Defacements and Computer Attacks
6- Responsible authorities for cyber security in:
A) Egypt
B) Iran
C) Israel
7- Comparison & Comments

What is Cyber Warfare?

- Cyber Warfare, cyber spying, and cyber terrorism & “cyber warfare” can consist of any type of aggressive or malicious action taken against a corporation, private citizen, or government agency that occurs in cyberspace.

- There are a number of different forms of cyber attacks that can be perpetrated against a person, business, or government and these different attacks typically build on each other toward a single goal.

- Espionage is a common form of “cyber warfare”, often referred to as cyber espionage, and typically consists of attempting to learn secret or private information about a person, business, or government.

Fields of Cyber Warfare

Critical Web Sites

Mentioned are the websites that are related to government, military, economy and others that affect the country, which mean that any attack on this websites will cause problems to country government or like.

Computers and Networks

Referred to Computers and Networks used in important institutions, such as: Military institution, Government institutions, Oil industries & Banks.
It also includes personal computers for employees in these institutions.

Motivations for Cyber warfare in the Middle East

- To collect intelligence information.
- Electronic Jihad
- Sabotage operations to inflict losses to other countries
- To stand against the electronic arms systems owned by opponent
- The political repercussions in the Middle East

Hacking Groups

Israel

- Hannibal
- IDF-Team
- Nuclear-Group
- SaNTi12
- Hencohen
- NickNiTRo

Iran

- Ashiyane Digital Security Team
- Digital Boys Underground Team
- Mafia Hacking Team
- Persian Boys Hacking Team
- ISCN
- !nf3rN.4lL
- Iran Cyber Army
- Hacker.web9

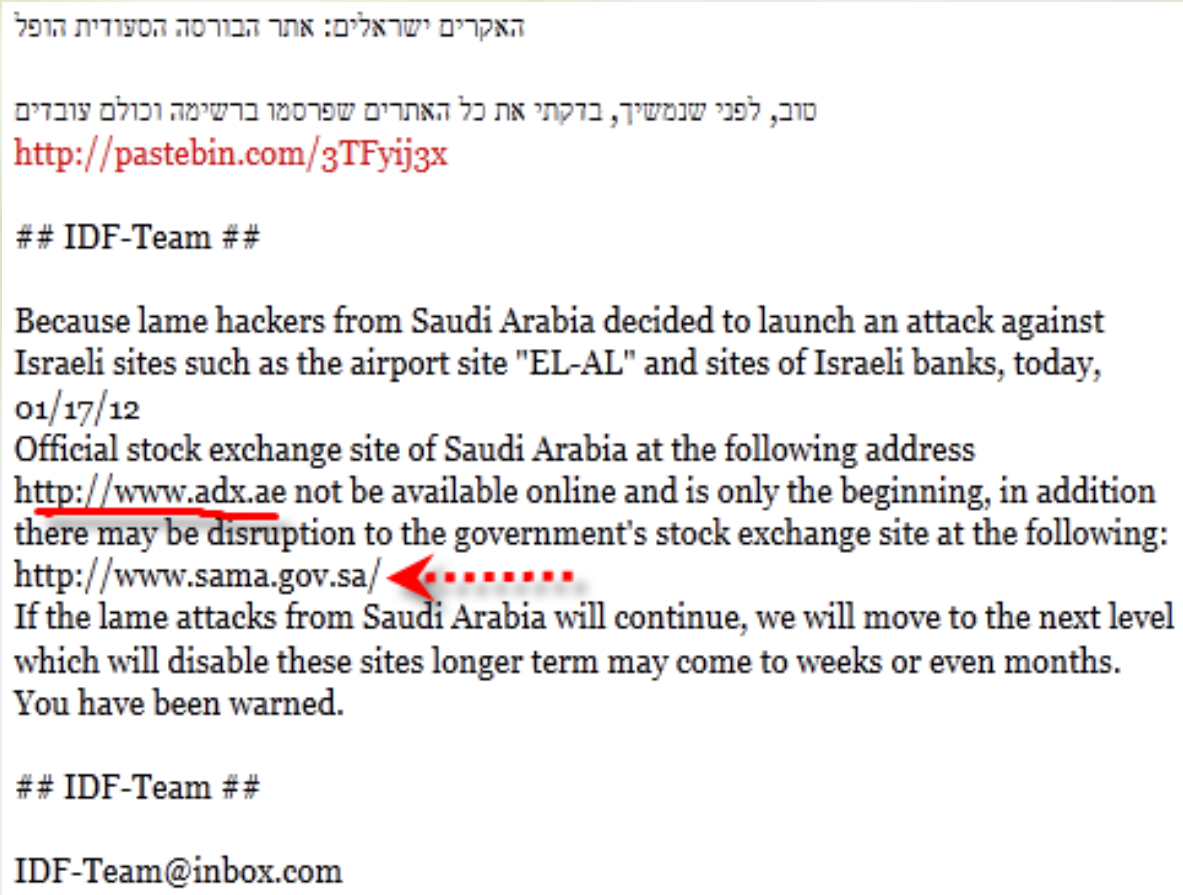
Egypt & co.

- Team Evil
- Erhabe007
- S4udi-S3cur1ty-T3rror
- Gaza Hacker Team
- Group-XP
- 0xomar
- DZ-Team
- Eg-r1z Team
- Egyption H4x0rz
- Egy-Virus Team
- CapoO TunisiAno
- Cold Zero

Israel Hacking Teams

Israel Hacking Teams Review

IDF Team:



האקרים ישראלים: אתר הבורסה הסעודית הופל

טוב, לפני שנמשיך, בדקתי את כל האתרים שפרסמו ברשימה וכולם עובדים
http://pastebin.com/3TFyij3x

IDF-Team

Because lame hackers from Saudi Arabia decided to launch an attack against Israeli sites such as the airport site "EL-AL" and sites of Israeli banks, today, 01/17/12
Official stock exchange site of Saudi Arabia at the following address http://www.adx.ae not be available online and is only the beginning, in addition there may be disruption to the government's stock exchange site at the following: http://www.sama.gov.sa/
If the lame attacks from Saudi Arabia will continue, we will move to the next level which will disable these sites longer term may come to weeks or even months.
You have been warned.

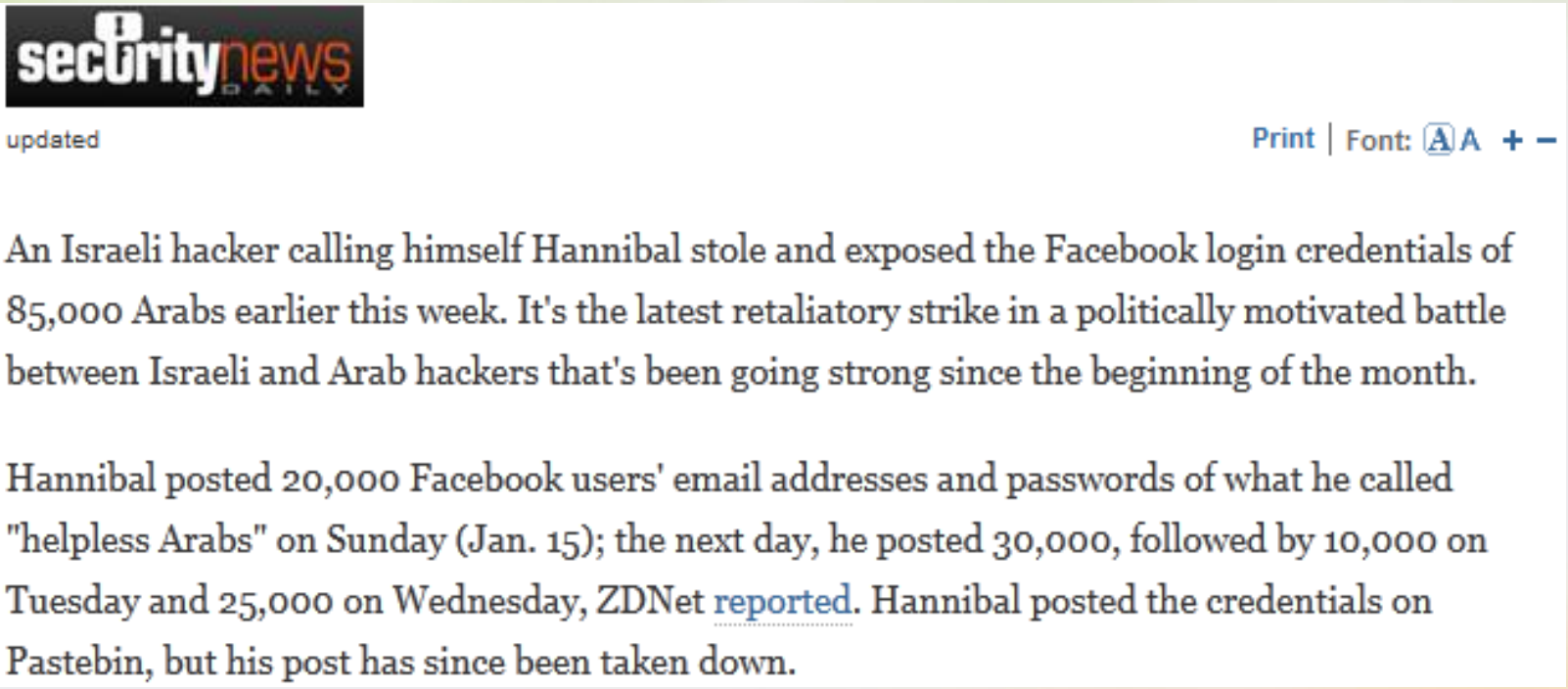
IDF-Team

IDF-Team@inbox.com

- Taken down Stock Exchange websites in Saudi and UAE with DDOS Attack.
- Taken down Hamas website with DDOS Attack.

Israel Hacking Teams Review

Hannibal:



securitynews DAILY

updated

Print | Font: A A + −

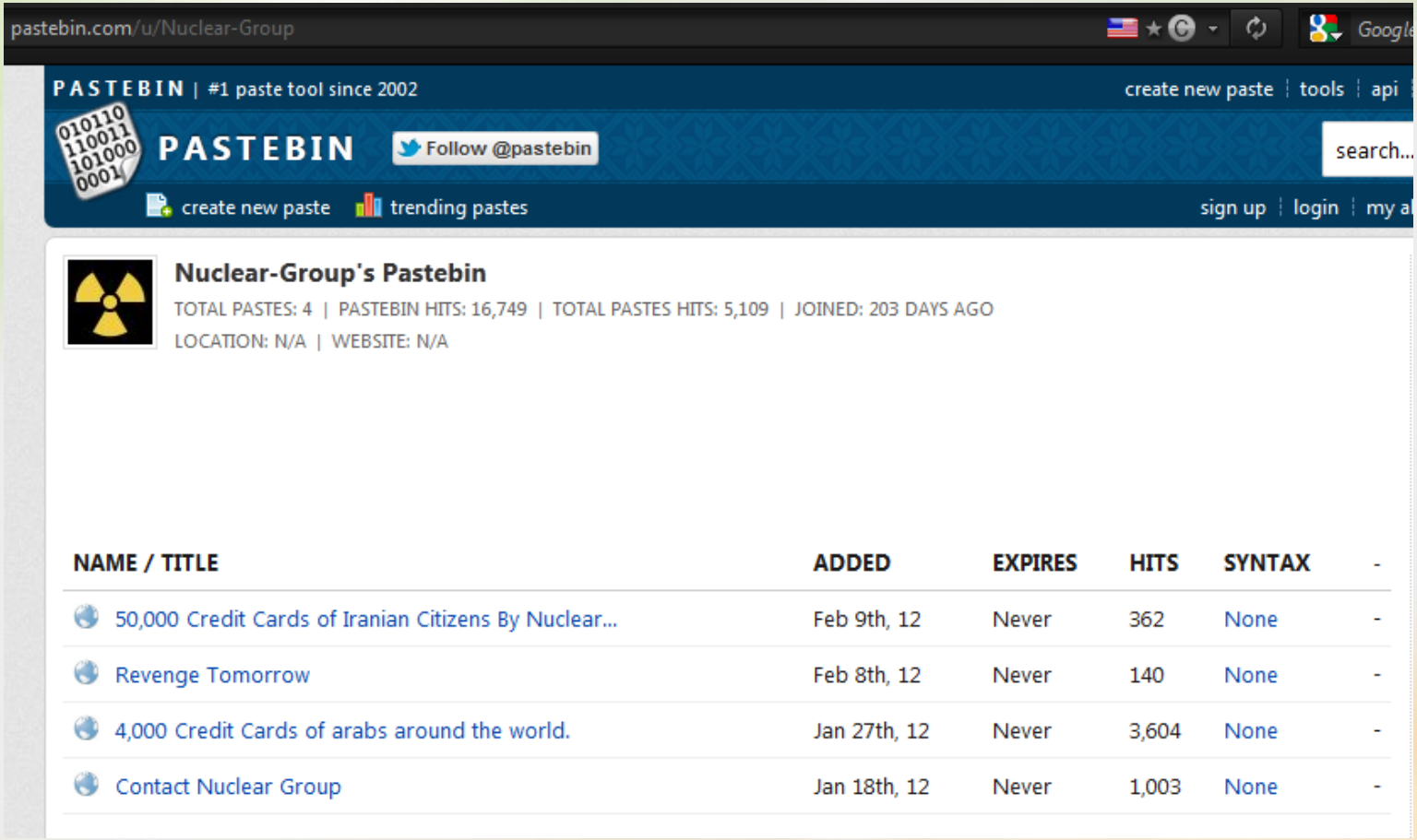
An Israeli hacker calling himself Hannibal stole and exposed the Facebook login credentials of 85,000 Arabs earlier this week. It's the latest retaliatory strike in a politically motivated battle between Israeli and Arab hackers that's been going strong since the beginning of the month.

Hannibal posted 20,000 Facebook users' email addresses and passwords of what he called "helpless Arabs" on Sunday (Jan. 15); the next day, he posted 30,000, followed by 10,000 on Tuesday and 25,000 on Wednesday, ZDNet reported. Hannibal posted the credentials on Pastebin, but his post has since been taken down.

- Known with his leaks for thousands of Emails and password for Arab users.

Israel Hacking Teams Review

Nuclear-Group:



- Leaked 50,000 Credit Cards of Iranian Citizens.
- Leaked 4,000 Credit Cards of Arabs around the world.

Israel Hacking Teams Review

SaNTi12:

NAME / TITLE	ADDED	EXPIRES	HITS	SYNTAX
1500 Facebook users of the Arabs Part 3	Feb 9th, 12	Never	299	None
900 Facebook users of the Arabs Part 2	Jan 26th, 12	Never	614	None
370 Facebook users of the Arabs Part 1	Jan 25th, 12	Never	489	None
Arab sites were broken into	Jan 21st, 12	Never	281	None

- Leaked 2500 Facebook Arab users.

Hencohen

He is an Israeli spammer used to spam bank accounts in UAE and Qatar.

Israel Hacking Teams Review

NickNiTRo:

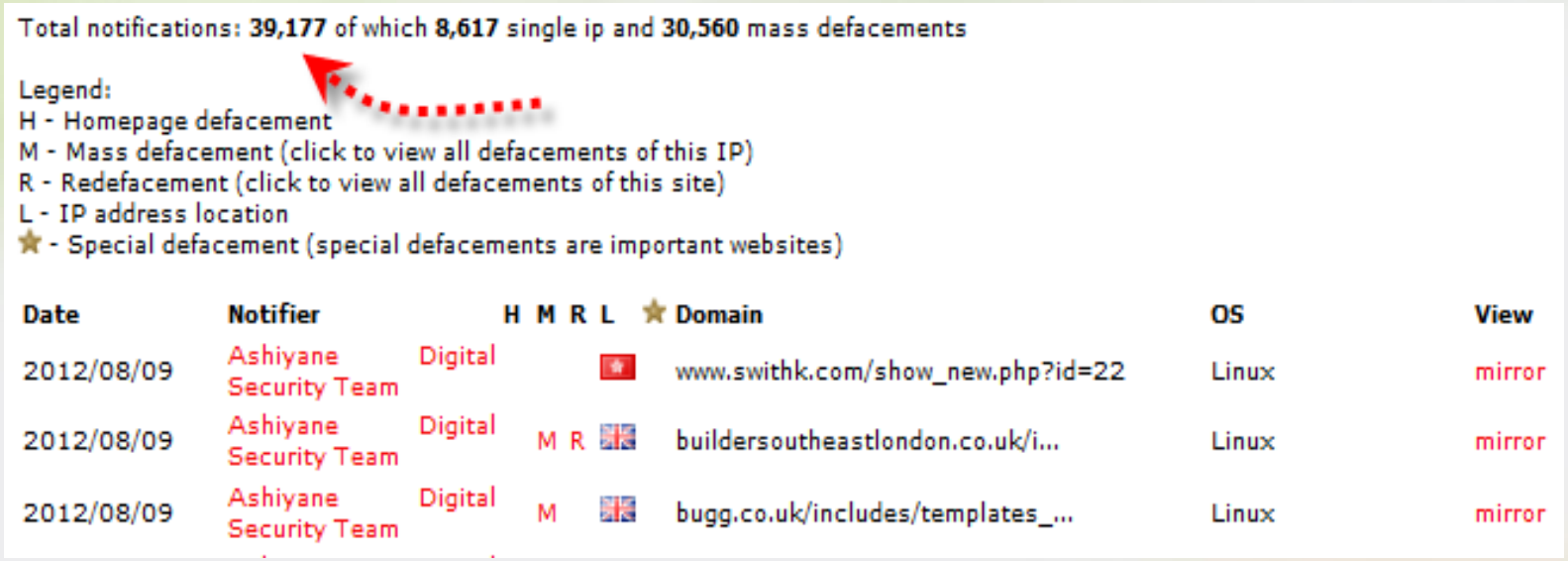
NAME / TITLE	ADDED	EXPIRES	HITS	SYNTAX
FREE Facebook Accounts [By NickNiTRo]	Jun 1st, 12	Never	101	None
New Arabian Credit Cards	Jan 18th, 12	Never	885	None
Part 10 | 40,000+ Arabs Facebook Accounts [By Nick...	Jan 16th, 12	Never	1,473	None
Part 9 | 40,000+ Arabs Facebook Accounts [By NickN...	Jan 16th, 12	Never	583	None
Part 8 | 40,000+ Arabs Facebook Accounts [By NickN...	Jan 16th, 12	Never	717	None
Part 7 | 40,000+ Arabs Facebook Accounts [By NickN...	Jan 16th, 12	Never	542	None
Part 6 | 40,000+ Arabs Facebook Accounts [By NickN...	Jan 16th, 12	Never	448	None
Part 5 | 40,000+ Arabs Facebook Accounts [By NickN...	Jan 16th, 12	Never	750	None
Part 4| 40,000+ Arabs Facebook Accounts [By NickNi...	Jan 16th, 12	Never	345	None
Part 3| 40,000+ Arabs Facebook Accounts [By NickNi...	Jan 16th, 12	Never	422	None
Part 2| 40,000+ Arabs Facebook Accounts [By NickNi...	Jan 16th, 12	Never	436	None
part 1| 40,000+ Arabs Facebook Accounts [By NickNi...	Jan 15th, 12	Never	859	None

- Leaked about 40k Emails & passwords of Arab users with some credit cards data.

Iran Hacking Teams

Iran Hacking Teams Review

Ashiyane Digital Security Team:



Total notifications: **39,177** of which **8,617** single ip and **30,560** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2012/08/09	Ashiyane Digital Security Team						www.swithk.com/show_new.php?id=22	Linux	mirror
2012/08/09	Ashiyane Digital Security Team		M	R			buildersoutheastlondon.co.uk/i...	Linux	mirror
2012/08/09	Ashiyane Digital Security Team		M				bugg.co.uk/includes/templates_...	Linux	mirror

- The Iranian Fars News Agency reported that the Ashiyane Security Group Hacked 400 Israeli websites, including the websites of the Mossad and Israeli Defense Minister EhudBarak.
- The team manage and moderate one of the best Iran Hacking communities called: http://ashiyane.org/forums

Iran Hacking Teams Review

Mafia Hacking Team

Date	Notifier	H	M	R	L		Domain	OS	View
2009/04/18	Mafia Hacking Team			R		★	www.presidency.gov.eg/darkl0rd...	Win 2003	mirror
2009/04/18	Mafia Hacking Team			R		★	library.idsc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/18	Mafia Hacking Team		M				www.investinalexandria.gov.eg/...	Win 2003	mirror
2009/04/18	Mafia Hacking Team		M	R			www.goief.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/18	Mafia Hacking Team		M	R			www.moi.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/18	Mafia Hacking Team		M			★	www.mdci.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.pbc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.alex-cic.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.assiuttp.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R		★	www.egsma.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.observatory.gov.eg/darkl0r...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.eitpfollow.gov.eg/darkl0rd...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.fayoum.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R		★	www.ngisc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	preview.idsc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R		★	www.cairobiennale.gov.eg/darkl...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.alexmuseum.gov.eg/darkl0rd...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.mop.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team						conference.idsc.gov.eg/darkl0r...	Win 2003	mirror
2009/04/17	Persian Boys Hacking Team		M	R			www.gem.gov.eg/d.htm	Win 2003	mirror
2009/04/17	Persian Boys Hacking Team		M			★	www.suez.gov.eg/d.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M				www.scc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R			www.grm.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M				www.tanmia-mosharka.gov.eg/dar...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R			www.gocp.gov.eg/darkl0rd.htm	Win 2003	mirror

➢ They are one of the active teams in attacking Egyptian web sites with archive of many ".gov.eg" Hacked web sites.

Iran Hacking Teams Review

ISCN

Is an Iranian team consists of 2 Iranian Hackers named as: Mormoroth, M49icBoy.

!nf3rN.4lL

Is an Individual Iranian Hacker used to Hack into Arabs web sites.

Date	Notifier	H	M	R	L	Domain	OS	View
2011/08/02	Digital Boys Underground Team					www.nct.gov.eg/db.htm	Win 2003	mirror
2011/07/12	Mr-AdeL			R		www.esa.gov.eg/dz.txt	Win 2003	mirror
2011/06/28	Hmei7					www.tobacco-control.mohealth.g...	Win 2003	mirror
2011/06/27	red virus	H	M	R		www.housing-portsaid.gov.eg	Linux	mirror
2011/06/07	the_storm					www.dpa.gov.eg/training/file.p...	Linux	mirror
2011/04/05	!nf3rN.4lL		M	R		www.egyinfo.gov.eg/Love.htm	Win 2008	mirror
2011/04/05	!nf3rN.4lL					1000qarya.gov.eg/Love.htm	Win 2008	mirror
2011/02/14	Mafia Hacking Team					mfti.gov.eg/images/	Win 2003	mirror
2011/02/14	Mafia Hacking Team		M			www.mti.gov.eg/images/	Win 2003	mirror
2011/02/07	stupid					www.aswan-sun.gov.eg/me.php	Win 2003	mirror
2011/02/04	Ma3sTr0-Dz					www.nmi.gov.eg/mdz.htm	Win 2003	mirror
2011/01/21	ISCN					maadicity.gov.eg/Default.aspx	Win 2003	mirror
2011/01/20	ISCN		M			msd.afmic.gov.eg/iscn.htm	Win 2003	mirror
2011/01/19	ISCN			R		www.elshoura.gov.eg/hits/	Win 2003	mirror
2011/01/19	ISCN					www.mmc.gov.eg/index.html	Win 2003	mirror
2010/12/16	Hmei7					eaea.gov.eg/indonesia.htm	Win 2003	mirror
2010/11/19	OmiDeR	H	M	R		sme.gov.eg	Win 2003	mirror
2010/11/11	Hmei7					www.monofeya.gov.eg/indonesia.htm	Win 2003	mirror
2010/11/11	TacticiaN					www.assiut.gov.eg/newnewnewall...	Win 2003	mirror
2010/11/09	TNT-PoweR	H	M			ewra.gov.eg	Win 2003	mirror
2010/11/08	1923Turk		M			services.monofeya.gov.eg/image...	Win 2003	mirror
2010/11/08	1923Turk		M			services.ismaelya.gov.eg/image...	Win 2003	mirror
2010/10/18	3n_byt3	H				www.gizaedu.gov.eg	Win 2003	mirror
2010/10/14	Hmei7			R		www.mcit.gov.eg/indonesia.htm	Win 2003	mirror
2010/10/06	iskorpitx	H				www.egtheatre.gov.eg	Linux	mirror

Iran Hacking Teams Review

Digital Boys Underground Team
Persian Boys Hacking Team

Both teams is Iranian teams, they used to Hack into .gov. any extension just to get Stars for a special defacements in zone-h.org web sites which will help them to be ranked in zone-H stats.

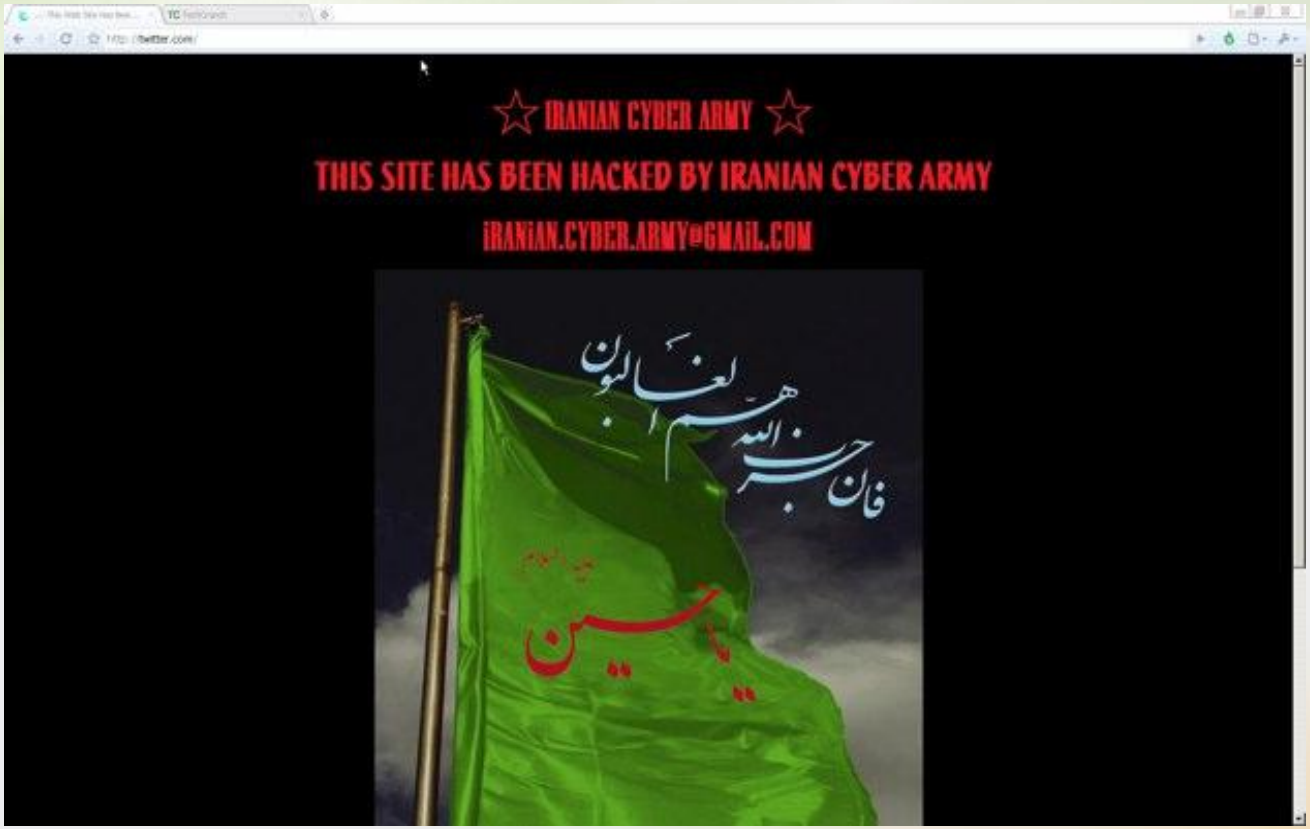
Total notifications: **7,874** of which **1,017** single ip and **6,857** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2012/08/01	Digital Boys Underground Team	H				★	interrior.ospjn.gob.ar	Win 2003	mirror
2012/07/30	Digital Boys Underground Team		M	R		★	www.e-ca.iaa.csic.es/db.htm	Linux	mirror
2012/07/30	Digital Boys Underground Team			R		★	e-ca.iaa.es/db.htm	Linux	mirror
2012/07/30	Digital Boys Underground Team			R		★	skhcn.bacgiang.gov.vn/db.htm	Win 2003	mirror
2012/07/30	Digital Boys Underground Team			R		★	danguybinhthuan.gov.vn/db.htm	Win 2003	mirror
2012/07/25	Digital Boys Underground Team	H		R			blog.irist.ir	Linux	mirror
2012/07/24	Digital Boys Underground Team	H				★	jieqi.scripts.mit.edu	Linux	mirror
2012/07/23	Digital Boys Underground Team	H				★	swib.stanford.edu	F5 Big-IP	mirror
2012/07/23	Digital Boys Underground Team					★	www05.stanford.edu/group/swib/...	Linux	mirror
2012/07/23	Digital Boys Underground Team					★	www01.stanford.edu/group/swib/...	Win 2003	mirror
2012/07/19	Digital Boys Underground Team			R		★	www.nongnghiepsoctrang.gov.vn/...	Win 2003	mirror

Iran Hacking Teams Review

Iran Cyber Army:



➢ Is the most experienced Iranian Hacking teams, as they successfully Defaced Twitter.com and baidu.com in 2009, both sites are high ranked sites and from the top 50 sites around the world, they claimed to Hack into that sites using DNS exploit privately found and exploited by the team.

Iran Hacking Teams Review

Hacker.web9:

- Known with his attacks against "Sunnah" web sites and Arab Hacking web sites, he had exploit in godaddy.com domains registrar and been very active in the cyber war between Sunnah and Shiaa in 2008, he used that exploit to Hack into alarabiya.net the Arabian news agency, as he did Hacked xp10.com the first Arabian Hacking web site.

Arab Hacking Teams

Arab Hacking Teams Review

Team-Evil:

Date	Notifier	H	M	R	L	Domain	OS	View
2008/08/26	Team-evil					www.toyota.co.il/news1.asp	Win 2000	mirror
2006/11/28	Team-Evil	H		R		www.fiat.co.il	Win 2003	mirror
2006/11/13	Team-Evil	H				crossword.msn.co.il	Win 2003	mirror
2006/11/09	Team-Evil					www.kereni.gov.il/db	Win 2003	mirror
2006/10/22	Team-Evil	H				i-travel.msn.co.il	Win 2003	mirror
2006/10/07	Team-Evil	H				habama.msn.co.il	Win 2000	mirror
2006/09/18	Team-Evil		M			www.antidrugs.gov.il/news/defa...	Win 2000	mirror
2006/09/15	Team-Evil	H	M			www.renault.co.il	Win 2003	mirror
2006/09/09	Team-Evil	H				www.nissan.co.il	Win 2003	mirror
2006/08/07	Team-Evil	H	M			www.mazda.co.il	Win 2003	mirror
2006/08/05	Team-Evil	H				www.ford.co.il	Win 2003	mirror
2006/07/03	Team-Evil	H	M			www.eGov.co.il	Linux	mirror
2006/07/03	Team-Evil	H	M			www.FirstGov.co.il	Linux	mirror
2006/07/03	Team-Evil	H	M			www.Government.co.il	Linux	mirror
2006/06/28	Team-Evil	H	M			www.citroen.co.il	Win 2003	mirror
2006/06/28	Team-Evil	H	M			tarbut-hadiur.gov.il	Win 2003	mirror
2006/06/28	Team-evil	H	M			www.bmw.co.il	Win 2003	mirror
2006/04/12	Team-evil	H				www.iibr.gov.il	Win 2003	mirror
2006/04/09	Team-evil					www.mcdonalds.co.il/index.htm	Win 2003	mirror
2006/02/06	Team-Evil					jsis.washington.edu/ma.htm	Win 2003	mirror
2005/09/07	Team-evil					www.export.gov.il/_Uploads/531...	Win 2000	mirror
2005/09/07	Team-evil		M	R		www.orianit.edu-negev.gov.il/f...	Win 2000	mirror
2005/08/30	Team-evil					www.ci.st-charles.il.us/news/s...	Win 2000	mirror
2005/08/28	Team-evil					www.sinaloa.gob.mx/fpdb/galeri...	Win 2000	mirror

➢ In June of 2006, around 750 Israeli websites were Hacked in one day in a coordinated campaign. The sites were taken down and replaced with a screen displaying the message: "Hacked by Team-Evil Arab hackers u KILL Palestine people we KILL Israeli servers." Among the targeted sites were those of Bank Hapoalim, a Haifa-area hospital, the Israeli representatives of international car manufacturers BMW, Subaru and Citroen, and of the Kadima party.

Arab Hacking Teams Review

S4udi-S3curity-T3rror:

Total notifications: **323** of which **174** single ip and **149** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2012/08/09	S4udi-S3curity-T3rror	H		R		★	www.iranembassy.org.za	Linux	mirror
2012/02/24	S4udi-S3curity-T3rror	H		R		★	forum2.msi.com.tw	FreeBSD	mirror
2012/02/24	S4udi-S3curity-T3rror	H	M	R		★	forum-tc.msi.com	FreeBSD	mirror
2011/11/28	S4udi-S3curity-T3rror	H	M			★	nio.org	Linux	mirror
2011/11/21	s4udi-S3curity-T3rror	H	M			★	blog.nlconsulateorlando.org	Linux	mirror
2011/10/24	S4udi-S3curity-T3rror	H				★	iranembassyjp.org	Win 2003	mirror
2011/10/24	S4udi-S3curity-T3rror	H				★	iran-embassy-oslo.org	Linux	mirror
2011/10/17	S4udi-S3curity-T3rror	H				★	shia.iranembassy.co.zw	Linux	mirror
2011/10/14	S4udi-S3curity-T3rror	H				★	www2.ijrood.gov.ir	Linux	mirror
2011/10/14	S4udi-S3curity-T3rror	H		R		★	survey.msi.com	FreeBSD	mirror
2011/10/04	S4udi-S3curity-T3rror	H				★	www.rma.packardbell.cl	Linux	mirror
2011/09/15	S4udi-S3curity-T3rror	H				★	moc.gov.sy	Linux	mirror
2011/09/09	s4udi-S3curity-t3rror	H		R		★	mod.ir	Linux	mirror

➢ Known with his attacks against Iranian government and embassies web sites, one of his famous attacks was against Iranian Ministry of Defense: http://www.mod.ir

Arab Hacking Teams Review

Gaza Hacker Team:

Total notifications: **1,482** of which **247** single ip and **1,235** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain	OS	View
2012/07/28	Gaza Hacker Team	H	M	R		www.ybcreative.co.il	Win 2003	mirror
2012/07/28	Gaza Hacker Team	H	M	R		www.mymed.co.il	Win 2003	mirror
2012/07/28	Gaza Hacker Team	H	M	R		www.ruderman.co.il	Win 2003	mirror
2012/07/28	Gaza Hacker Team	H	M	R		www.silverpro.co.il	Win 2003	mirror
2012/07/28	Gaza Hacker Team	H	M	R		www.kitchenstudio.co.il	Win 2003	mirror
2012/07/28	Gaza Hacker Team	H	M	R		trb.co.il	Win 2003	mirror
2012/07/28	Gaza Hacker Team	H	M	R		animalvet.co.il	Win 2003	mirror
2012/07/28	Gaza Hacker Team	H		R		www.eldangroup.co.il	Win 2003	mirror
2012/07/27	Gaza Hacker Team	H	M			www.edelstein.org.il	Linux	mirror
2012/07/26	Gaza Hacker Team	H				www.smartcash.co.il	Win 2003	mirror
2012/07/26	Gaza Hacker Team	H	M			www.levi-mp.co.il	Win 2003	mirror
2012/07/26	Gaza Hacker Team	H	M			www.mantraspa.co.il	Win 2003	mirror
2012/07/26	Gaza Hacker Team	H	M			www.backlife.com	Win 2003	mirror
2012/07/26	Gaza Hacker Team	H	M			morag.artvision.co.il	Win 2003	mirror

- Team runs the website of the same name. It is responsible for defacing the Kadima party website on February 13, 2009. they also Hacked into the Knesset web site, Haaretz daily, and Israel's Deputy Foreign Minister Danny Ayalon's website.
- Team Members: Mr.Le0n & Claw & Casper

Arab Hacking Teams Review

DZ Team:

- It first made headlines in April 2008 when it Hacked the Bank of Israel website over Passover weekend. DZ Team defaced several Israeli websites during Operation Cast Lead, including the Israeli portals of Volkswagen, Burger King, and Pepsi, the website of Israeli defense contractor BVR systems, the Kadima party website, and the Hillel Yaffe hospital website.
- Team Members : The Moorish - Kader11000 - His0k4 - maxi32 - L4st-H4ck3r - Oxide

Arab Hacking Teams Review

0xomar:

- The Saudi Hacker who is constantly causing trouble for Israeli's, he also known with his huge leaks of Israeli people credit cards, emails and password and personal data on the internet,.
- 0xomar started a cyber war against Israel by leaking over 400k of Israeli credit cards on the internet and DDosing on big Israeli sites also defacing some ".gov.il" web sites.

Arab Hacking Teams Review

XP-Group A.K.A Alm3refa Group:

GROUP-XP Warns of more Israel Information Leaks

By Lee J

Published January 4th, 2012

This week we seen thousands of Israeli's attacked via cyberspace in the form of data breaches and credit card and personal detail leaking and now In what's become so far one of the biggest hacks of information in some time, has made major headlines and really got a lot of blood boiling has now released another statement that warns of more attacks to come over the coming weeks

The messages which was put as a link on to the one of the last dump paste on pastebin.com by GROUP-XP.

The message from GROUP-XP.

Response to some comments:
a) It's not only One, we used One to reach our message to people, we havecked larger networks to gather those information, it's not single source
b) That isn't a single file, see 40,000 file with fresh cards, look at 27000, etc.
c) It's first part of our release of files, wait for the next in couple weeks

- Known with them huge attacks against Shiaa web sites which caused a cyber war between Iranian Hackers and Saudi Hackers in 2008 as the Saudi Hacker 0xomar is one of the XP-Team.

Arab Hacking Teams Review

CapoO_TunisiAno:

Total notifications: **4,250** of which **298** single ip and **3,952** mass defacements

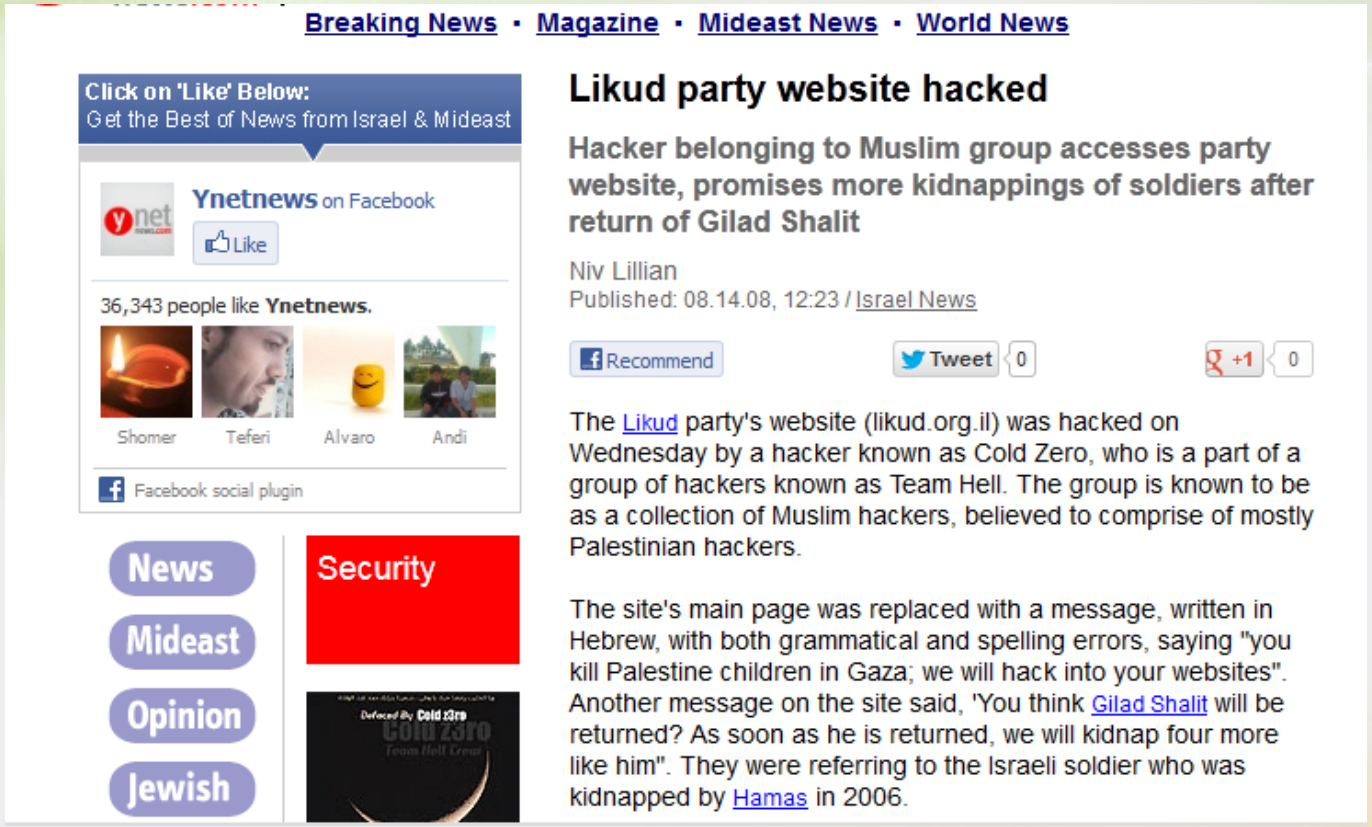
Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2012/05/31	CapoO_TunisiAnoO	H	M				ambassadorisrael.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				ambulance.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				aroma.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				adifim.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				quality.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				babylon.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				aviv-hitech.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				ats.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				astrology.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				carspa.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				coaching.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				cognito-con.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				cv-pool.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				dayan.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				funtaziko.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				eranron.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				electrosupply.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				dyslexia.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				duna.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				dogscenter.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				di1.allbiz.co.il	Win 2003	mirror
2012/05/31	CapoO_TunisiAnoO	H	M				gina.allbiz.co.il	Win 2003	mirror

➢Is an Tunisian hacker known with his attacks against many Israeli web sites for Gaza Attacks by Israel army.

Arab Hacking Teams Review

Cold Zero:



➢Is an Palestine Hacker, He first gained notoriety for an attack on the Likud Party website in August 2008. He has since claimed responsibility for 5,000 website defacements, according to Gary Warner, an expert in computer forensics. He has a profile on the Arabic Mirror website, which lists 2,485 of these defacements. According to the Arabic Mirror site,779 of these are related to the Gaza crisis.

Arab Hacking Teams Review

Erhabe007:

- He is an Tunisian hacker, and he is the first known Arabian electronic jihadist, erhabe007 used to hack into computers and web sites for critical computer systems in USA, he was the advertising campaigns leader for Al-Qaida in Iraq between 2004-2006 till the British police raided him in 2006 and he is now into the jail.
- Real Name: Yunis Tesuli

Arab Hacking Teams Review

Egyption.H4x0rz:

«هاكرز مصريون» يخترقون موقع «نتنياهو» ويكتبون شعارات «مناهضة للصهيونية»

أحمد بلال
Tue, 23/08/2011 - 18:00

57 Tweet 781 Like Send 0 +1 ShareThis

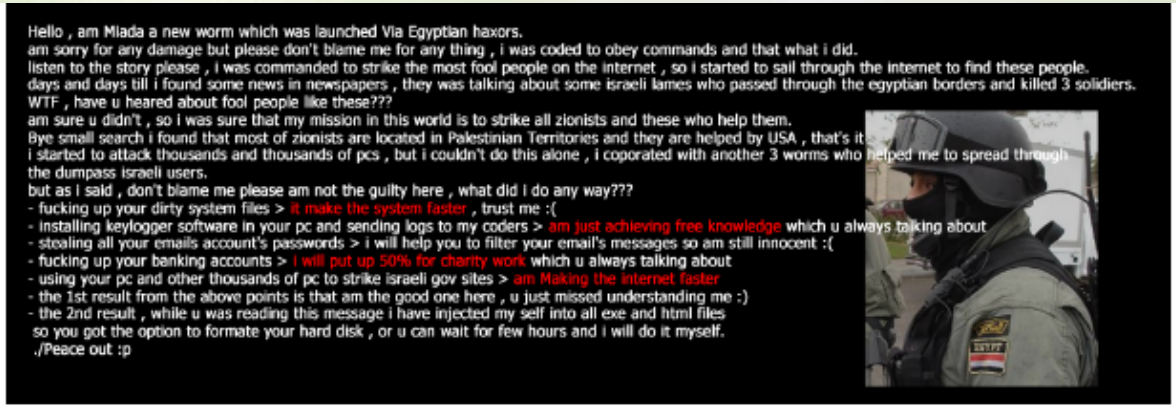
تصوير أ.ف.ب

قالت مجلة «زا ماركر» الملحق الاقتصادي لصحيفة «هآرتس»، إن قراصنة إليكترونيين «هاكرز»، مؤيدين للفلسطينيين، دمروا مساء الأحد موقع رئيس الوزراء الإسرائيلي، بنيامين نتنياهو، وكتبوا عليه رسائل مناهضة للصهيونية، وأشارت «زا ماركر» أنه «في السنوات الأخيرة، وفي أعقاب كل حدث يتصل بالصراع الإسرائيلي – الفلسطيني، تزداد حدة المحاولات الرامية لاختراق المواقع الإليكترونية الإسرائيلية».

- Known with them attacks against critical Israel web sites such as Likud party web site and Israeli prime minister Netanyahu, Radio of Israel web site & more.
- Team Members: Hcj, Cyb3r.1st, Egyption.H4x0rz, ISM

Arab Hacking Teams Review

Eg-r1z Team:



In Sudden escalation for the attack level , an Egyptian group launched computer worm which infected about 50000 personal computer in Israel and united states. Despite of my virtual machine security level , it was also infected by the same worm. I (Reuben Rayner) didn't notice that am infected till the attackers launched an exe file which viewed message in the full screen mode.

- Known with them botnet mass spreading in Israel that helped them to a successfully hack into 50000 of Israel and US computers.
- Team Members: i-Hmx, H3ll C0d3, Str1k3r

Arab Hacking Teams Review

Egy-Virus Team:

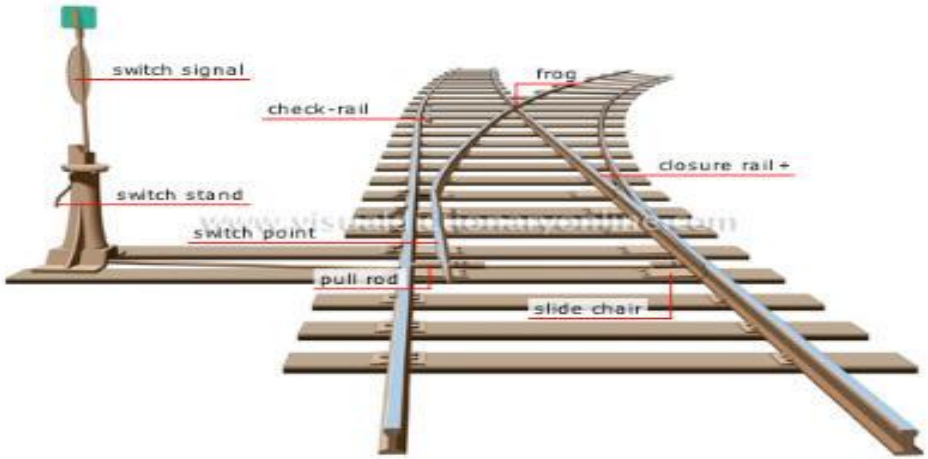
- Known with them attacks against big Israeli web sites & botnet spreading in Israel.
- Team's famous attacks: Hacking into more than 800 Israeli computers, hacking into Channel Two of Israeli television, Israeli Ministry of Foreign Affairs, Adobe and more.
- Team Members: Virus_Hima, RedVirus

Famous Web Defacements & Computer Attacks

Reviews:

أجهزة التحكم بمسارات القطارات تستطيع توقيفها بهجمات حجب الخدمة

نشر بـ الخميس, ديسمبر 29, 2011 من طرف **Admin**. تحت تصنيف **أخبار الإختراقات**



الإعتقاد السائد لدى الهكرز عن هجمات حجب الخدمة اعتقد انه سيتغير بعد أن ذكر البروفسور الألماني ستيفن كيتزينبسير أن بإمكان القراصنة إستهداف أجهزة الكمبيوتر والأنظمة التي تقوم بتحويل مسارات القطارات مما يدق ناقوس الخطر لدى رحلات القطارات السريعة التي تعتمد على هذه الأنظمة حيث قد تشكل خطر في حال معرفة المخربين باستغلال هذه الهجمات ستنتج كوارث بلا شك قد تتسبب في حوادث تصادم وكذلك تغيير مسار قطار من منطقة إلى اخرى حيث لن يكون النظام قابلا للاستجابة عند تعرضه لهجمات حجب الخدمة

Reviews:

ففي ديسمبر/كانون الأول من العام 2009، أوردت الحكومة الكورية الجنوبية تقريرا عن تعرضها لهجوم نفّذه قراصنة كوريين شماليين بهدف سرقة خطط دفاعية سريّة تتضمن معلومات عن شكل التحرّك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية.**(5)**

وفي يوليو/ تموز 2010، أعلنت ألمانيا أنّها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات الصناعية والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة.**(6)**

ويجمع الخبراء على أنّ الهجوم الإلكتروني الذي استهدف أستونيا في العام 2007، يكاد يكون الهجوم الإلكتروني الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والإعلامية مسببا خسائر بعشرات الملايين من الدولارات إضافة إلى شلل البلاد. وعلى الرغم من ان الشكوك كانت تحوم حول موسكو على اعتبار أن الهجوم جاء بعد فترة قصيرة من خلاف أستوني-روسي كبير،**(7)** إلا أنّ أحدا لم يستطع تحديد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم، وهي من المصاعب والمشاكل التي ترتبط بحروب الإنترنيت إلى الآن.

تقرير قناة الجزيرة حول الحرب الإلكترونية

Reviews:

'Iran set to build first cyber army'

Director of Iran's Passive Defense Organization has announced plans to build the first Iranian cyber army following the successful launch of the cyber defense headquarters, Press TV reports.

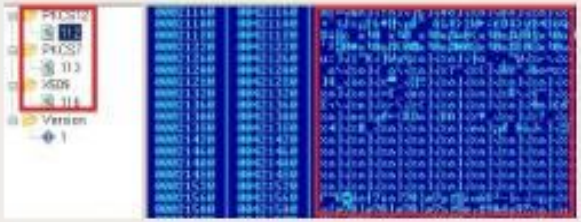
Mon Feb 20, 2012 7:15PM

Famous web Defacements and Computer attacks against **Iran**

Shamon:

Shamoon Malware, cyber espionage tool, cyber weapon or …

by paganinip on August 19th, 2012



The cyberspace has no peace, every time a **malware** or a **botnet** is detected and decapitated a new cyber threat is coming, this time a new agent scare security experts, its name is Shamoon and is able to destroy files on victim's pc and overwrite the master boot record of its disks.

In different way respect all the malware **isolated in the last months**, this agent hasn't been developed only to spy on victims but its purpose it destroy them making the machine unusable. The malware attacks Windows 95, Windows 98, Windows XP, Windows 200, Windows Vista, Windows NT, Windows ME, Windows 7, Windows Server 2003 and Windows Server 2008.

Some experts are convinced that there is a relationship between the agent and the malware Wiper, but other researchers deny the hypothesis.

The virus that hit the petroleum sector, Aramco and RasGas

Reviews:

أدوات الموضوع | انواع عرض الموضوع

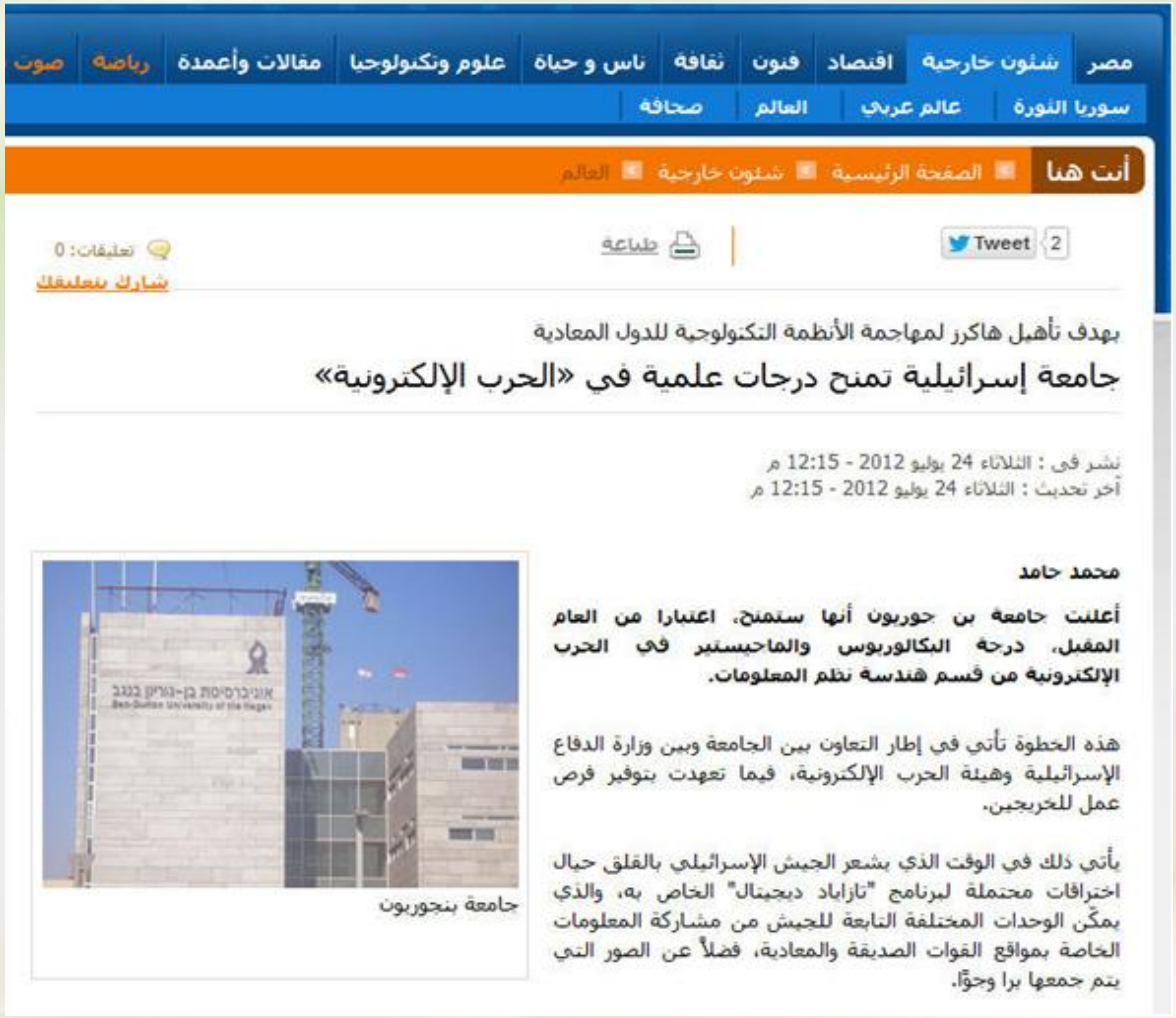
#1

مليار دولار خسائر البنوك السعودية بسبب الجرائم الإلكترونية ..

مليار دولار خسائر البنوك السعودية بسبب الجرائم الإلكترونية
الجمعة 27, يناير 2012

لجينيات : كشف عضو مجلس الشورى نائب رئيس لجنة النقل والاتصالات وتقنية المعلومات الدكتور جبريل العريشي، أن خسائر البنوك السعودية جراء الجرائم الإلكترونية بلغت أكثر من مليار دولار في غضون عامين فقط، مؤكدا على أن سنة 2012 ستكون عام الجرائم المعلوماتية.

Reviews:



مصر | شئون خارجية | اقتصاد | فنون | ثقافة | ناس و حياة | علوم وتكنولوجيا | مقالات وأعمدة | رياضة | صوت

سوريا الثورة | عالم عربي | العالم | صحافة

أنت هنا ■ الصفحة الرئيسية ■ شئون خارجية ■ العالم

Tweet 2 | طباعة | تعليقات: 0 | شارك بتعليقك

بهدف تأهيل هاكرز لمهاجمة الأنظمة التكنولوجية للدول المعادية

جامعة إسرائيلية تمنح درجات علمية في «الحرب الإلكترونية»

نشر في : الثلاثاء 24 يوليو 2012 - 12:15 م
آخر تحديث : الثلاثاء 24 يوليو 2012 - 12:15 م

جامعة بنجوريون

محمد حامد

أعلنت جامعة بن جوريون أنها ستمنح، اعتبارا من العام المقبل، درجة البكالوريوس والماجيستير في الحرب الإلكترونية من قسم هندسة نظم المعلومات.

هذه الخطوة تأتي في إطار التعاون بين الجامعة وبين وزارة الدفاع الإسرائيلية وهيئة الحرب الإلكترونية، فيما تعهدت بتوفير فرص عمل للخريجين.

يأتي ذلك في الوقت الذي يشعر الجيش الإسرائيلي بالقلق حيال اختراقات محتملة لبرنامج "تازاباد ديجيتال" الخاص به، والذي يمكّن الوحدات المختلفة التابعة للجيش من مشاركة المعلومات الخاصة بمواقع القوات الصديقة والمعادية، فضلاً عن الصور التي يتم جمعها برا وجوًا.

Reviews:

باراك خلال محاضرته بجامعة تل أبيب حول الحرب الإلكترونية (الجزيرة)

وديع عواودة - حيفا

اعترف وزير الدفاع الإسرائيلي إيهود باراك للمرة الأولى بخوض إسرائيل معركة إلكترونية على عدة جبهات, وسعيها لاحتلال الريادة في هذا المجال على المستوى العالمي.

وقال باراك خلال يوم دراسي حول "حرب السايبر" نظمته جامعة تل أبيب إن إسرائيل "تستعد لأن تكون في الواجهة العالمية في الحرب الإلكترونية على المستويين المدني والأمني".

وأضاف أنه "مقابل تطوير العدو لسلاح الصواريخ فإن السايبر "يسّجل تطورا غير مسبوق", مشيرا إلى أنه بوسع "هاكر" (قرصان إنترنت) واحد إلحاق ضرر فادح بالأنظمة الاقتصادية والقومية.

وكان رئيس الوزراء الإسرائيلي بنيامين نتانياهو اعتبر -في محاضرة نظمها معهد دراسات الأمن القومي قبل أيام- أن "السايبر" خطر إستراتيجي يتهدد إسرائيل" مشيرا إلى تخصيص ميزانيات وطاقات بشرية ضخمة للدفاع الإلكتروني.

Reviews:

ما هي شبكة إيكيلون Echelon

[عدل]

إيكيلون (ECHELON بالإنجليزية) هو نظام عالمي لرصد البيانات، واعتراضها، ونقلها، يتم تشغيله من قبل مؤسسات استخبارية في خمس دول هي: الولايات المتحدة، والمملكة المتحدة، وكندا، وأستراليا، ونيوزلندا. ومن المعتقد أن الاسم إيكيلون هو التسمية الخاصة بجزء من النظام يقوم باعتراض الاتصالات التي تتم عبر الأقمار الاصطناعية. وتقوم هذه المؤسسات الاستخبارية بالتنسيق بين جهودها استنادا إلى اتفاقية UKUSA والتي تم توقيعها في العام 1947، ولكن نظام إيكيلون المستخدم حاليا ابتدأ العمل منذ عام 1941، وقد توسعت طاقاته وقدراته ومستوى شموليته كثيرا منذ ذلك الحين، ومن المعتقد أن عملياته تغطي كافة أنحاء العالم. وطبقا للتقارير، ومنها التقرير الذي أعدته اللجنة الأوروبية، فإن بإمكان إيكيلون اعتراض وتعقب أكثر من ثلاثة مليارات عمليات اتصال يوميا (تشمل كل شيء من المكالمة الهاتفية العادية، والجوالة، واتصالات إنترنت، وانتهاء بالاتصالات التي تتم عبر الأقمار الاصطناعية). ويقوم نظام إيكيلون بجمع كافة هذه الاتصالات دون تمييز ومن ثم تصفيتها وفلترتها باستخدام برامج الذكاء الاصطناعي لإنشاء تقارير استخبارية. وتقول بعض المصادر لأن إيكيلون يقوم بالتجسس على 90% من المعلومات المتداولة عبر إنترنت، وتبقى هذه مجرد إشاعة حيث أنه لا يوجد مصادر يمكنها أن تشير بدقة إلى قدرة النظام.

كيف يعمل إيكيلون؟

[عدل]

يقوم نظام إيكيلون بجمع البيانات بطرق متعددة؛ حيث تشير التقارير إلى أن الوكالات الاستخبارية قامت بتثبيت هوائيات راديوية عملاقة في مواقع مختلفة من الكرة الأرضية، وذلك لاعتراض البث المرسل من وإلى الأقمار الاصطناعية، كما أن هنالك بعض المواقع المتخصصة في تعقب الاتصالات الأرضية. وتوجد هذه الهوائيات حسب التقارير في الولايات المتحدة، وإيطاليا، وإنجلترا، وتركيا، ونيوزلندا، وكندا، وأستراليا، ومجموعة من المواقع الأخرى. كما أن إيكيلون يستخدم مجموعة من الأقمار الاصطناعية الخاصة التي تقوم بمراقبة البيانات "الفائضة Spillover" بين الأقمار الاصطناعية، ومن ثم إرسال هذه البيانات إلى مواقع معالجة خاصة على الأرض تتمركز في الولايات المتحدة بالقرب من مدينة دنفر بولاية كولورادو، وفي بريطانيا (منويث هيل)، وأستراليا، وألمانيا. كما أن نظام إيكيلون يقوم بشكل روتيني بمراقبة عمليات الإرسال التي تتم عبر إنترنت، حيث قامت المؤسسة بتثبيت عدد من برمجيات وأدوات "تعقب" الحزم شبيهة بكارنيفور ولكن دون المحددات المفروضة عليه. وإضافة إلى ذلك فإن إيكيلون يستخدم عددا من برمجيات البحث للتنقيب في المعلومات الموجودة في مواقع إنترنت مختارة. وأُشيع أيضا بأن إيكيلون استخدم معدات تحتمائية خاصة، يمكن تركيبها على الكوابل التي تحمل المكالمات الهاتفية، وقد تم اكتشاف إحدى هذه الأدوات في عام 1982. ومن غير المعروف حاليا إذا ما كان بإمكان إيكيلون رصد المكالمات المتداولة عبر كوابل الألياف الضوئية. وإضافة إلى جميع الوسائل المذكورة أعلاه، والتي تتم عادة عن بعد، دون الاحتكاك مع الجهات المشبوه بها، فإن الوكالات المشاركة في إيكيلون تقوم باستخدام عملاء سريين مدربين خصيصا يقومون بتثبيت أدوات للتصنت وجمع المعلومات في المواقع التي ترغب بها الوكالة. وبعد جمع البيانات الخام، يقوم نظام إيكيلون بالتنقيب في هذه البيانات والبحث بها باستخدام نظام اسمه DICTIONARY، والذي يتكون من مجموعة من أجهزة الكمبيوتر الفائقة، والتي تعثر على المعلومات المفيدة للتقارير الاستخبارية بالبحث عن كلمات مفتاحية، وعناوين، وما إلى ذلك. وبفضل برمجيات البحث المتقدمة هذه، يمكن الاستفادة بشكل جيد من الكميات المهولة من البيانات التي تمر عبر النظام يوميا، كما يبدو أنها تسمح للعملاء بتركيز بحثهم على المعلومات الضرورية فقط.

Reviews:

القدرات الإسرائيلية في الحرب الإلكترونية

في أواخر التسعينات نجح خبير في مجال الحواسيب يعمل في جهاز الأمن الداخلي الإسرائيلي (شين بيت) من خلال تقنيات القرصنة في اقتحام نظام الكمبيوتر الخاص بمستودع (بي جالوت) للوقود شمالي تل أبيب. كان الهدف إجراء اختبار روتيني لتدابير الحماية بالموقع الاستراتيجي، لكن هذه العملية نبهت الإسرائيليين أيضا إلى الإمكانية التي توفرها هذه التسللات عالية التقنية للقيام بأعمال تخريبية حقيقية، وأدركوا حينها أنه بخلاف الاطلاع على البيانات السرية، فإنهم يستطيعون أيضا تنفيذ تفجيرات متعمدة بمجرد برمجة تغيير في مسار خطوط الأنابيب".**(34)**

ومنذ ذلك الوقت تبلورت الحرب الإلكترونية شيئا فشيئا لتصبح ركنا رئيسيا في التخطيط الاستراتيجي لإسرائيل. وتعتبر الوحدة 8200 في الجيش الإسرائيلي أكثر الوحدات تطورا من الناحية التقنية والتكنولوجية ولها نشاطات واسعة في حروب الإنترنيت والشبكات، وقد انضم إليها الالاف من العقول الإسرائيلية منذ إنشائها نظرا لشهرتها الواسعة حيث تعمل على ضمان التفوق النوعي لإسرائيل من خلال عمليات دفاعية أو هجومية في الفضاء الإلكتروني.**(35)**

وعلى الرغم من أنّه قد تمّ تصنيف الوحدة 8200 من قبل بعض المؤسسات المعنيّة بأنها أكبر سادس مطلق لهجمات الإنترنيت في العالم**(36)**، فان هذه الوحدة ليست الوحيدة التي تتمتع بهذه القدرات التقنية العالية في إسرائيل، فهناك العديد من الوحدات الأخرى التي تتمتع بقدرات متطورة جدا في مجال تكنولوجيا المعلومات في جميع التخصصات. ويتم استقطاب وتجنيد الأطفال الإسرائيليين من النخبة حتى قبل إنهائهم دراستهم الثانوية، عندما يبلغ هؤلاء سن الـ25 عاما، يكون لديهم اكثر من 7 سنوات خبرة عملية في مجال التكنولوجيا**(37)**.

ولا يقتصر الأمر على الجيش الإسرائيلي في توظيف الأدمغة وبناء قدرات عالية في مجال الحروب الإلكترونية وإنشاء وحدات قوات نخبة خاصة كوماندوس بحروب الإنترنيت وتكون مهمتها التعامل مع أصعب وأخطر وأعقد الحالات المتعلقة بهذه الحروب، وإنما تدخل الاستخبارات الشين بيت على الخط أيضا للقيام بنفس المهمة، ويتم الاستفادة في هذا الإطار من العناصر المخضرمة ايضا، ومن المؤسسات التقنية والمعلوماتية الإسرائيلية ومن العاملين فيها كرافد مهم.**(38)**

Reviews:

واستند معد التقرير إلى مجندة بالاستخبارات العسكرية الإسرائيلية في الكشف عن أكبر قاعدة أكبر وأضخم قاعدة من نوعها في العالم، والتي تتمثل مهمتها في اعتراض المكالمات التليفونية والرسائل والبيانات الإلكترونية، التي يتم إرسالها عبر الأقمار الصناعية وكابلات الاتصالات البحرية الموجودة في البحر الأبيض المتوسط، كما أن لديها القدرة على جمع المعلومات الإلكترونية، ورصد اتصالات الحكومات والمنظمات والشركات والأفراد على حد سواء.

ونقل عن المجندة السابقة بوحدة 8200 التابعة للمخابرات العسكرية الإسرائيلية، دون أن يكشف عن اسمها، إن القاعدة تتجسس على عدد من الدول من بينها دول معادية لإسرائيل وأخرى تعتبر صديقة لها، وذكرت أن القاعدة التي تقع بمنطقة (أوريم) بجنوب إسرائيل على بعد 30 كيلومترا من سجن مدينة بئر السبع، تعترض الاتصالات الصادرة من الشرق الأوسط وأوروبا وأفريقيا وآسيا، وتشرف على تشغيلها وحدة 8200.

جريدة الفتح الفلسطينية

وقالت إن المعلومات التي تجمعها القاعدة ترسل للوحدة 8200، وإن القاعدة تخضع لحماية أمنية مشددة، فتبدو أسوارها عالية، وبواباتها كبيرة ومحمية بالعديد من كلاب الحراسة، معتبرةً أن أهم الإنجازات التي قامت بها الوحدة المسئولة عن تلك القاعدة هو اعتراض الاتصال الهاتفي بين الرئيس المصري جمال عبد الناصر والعاهل الأردني الراحل الملك حسين خلال اليوم الأول من حرب يونيو 1967، واعتراض الاتصال الهاتفي بين الرئيس الفلسطيني الراحل ياسر عرفات و بين المجموعة التي اختطفت السفينة (أكيلي لاورو) في العام 1995.

Famous web Defacements & Computer attacks in:

Iran

Famous web Defacements and Computer attacks against **Iran**

Computers and Networks Attacks:
Stuxnet
Duqu
Flame A.K.A Sky Wiper
Cyber attack on Iran's Internet system

Web Sites Attacks:
S4udi-S3cur1ty-T3rror
XP-Group Attacks
Other Individual Attacks.

Famous web Defacements and Computer attacks against **Iran**

Stuxnet:

Famous web Defacements and Computer attacks against **Iran**

Stuxnet:

"ستكسنت" أحدث أسلحة الحرب الإلكترونية

في 25 سبتمبر/أيلول 2010، أكدت إيران أن العديد من وحداتها الصناعية وقعت ضحية إرهاب إلكتروني بعد إصابتها بفيروس "ستكسنت" ويعد هذا الفيروس وفق العديد من التقارير التي صدرت مؤخرا واحد من أعقد الأدوات التي تم استخدامها إلى الآن.

فـ"ستكسنت" عبارة عن برنامج كومبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا. وكان الخبراء بداية يعتقدون أنّ مهمّة البرنامج هي التجسس الصناعي ونقل المعلومات التي تساعد على تقليد المنتجات.**(21)**

لكن تبيّن لخبراء الهندسة العكسيّة فيما بعد أنّ الأمر مختلف كليّا. فالبرنامج -وعلى عكس الكثير من البرامج المعروفة إلى الآن- ليس مخصصا للتجسس وسرقة المعلومات الصناعية لمحاولة كسب المال أو لسرقة الملكية الفكرية. فبعد حوالي أربعة أشهر من العمل، ظهر أن الأمر أكثر تعقيدا مما كان متصورا، وأننا نقف اليوم أمام نوع جديد من البرامج التي من الممكن أن تتحول إلى نموذج للأطراف التي تنوي إطلاق هجمات إلكترونية تؤدي إلى دمار حقيقي واقعي في البلد المستهدف حتى دون الحاجة إلى الإنترنيت.**(22)**

فالبرنامج لا يعمل بشكل عشوائي كما هي العادة وإنما بشكل محدد جدا. إذ يقوم بعد اختراق الأجهزة والحواسيب بالتفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة "سيمنز الألمانية"، فإذا ما وجدها يقوم عندها بتفعيل نفسه ويبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة من خلال العبث بأنظمة التحكم وقد تتعدد المنشآت التي يستطيع مهاجمتها من خطوط نقل النفط إلى محطات توليد الكهرباء وحتى المفاعلات النووية وغيرها من المنشآت الإستراتيجية الحسّاسة، أمّا إذا لم يجدها، فيترك الحاسوب وشأنه.**(23)**

"

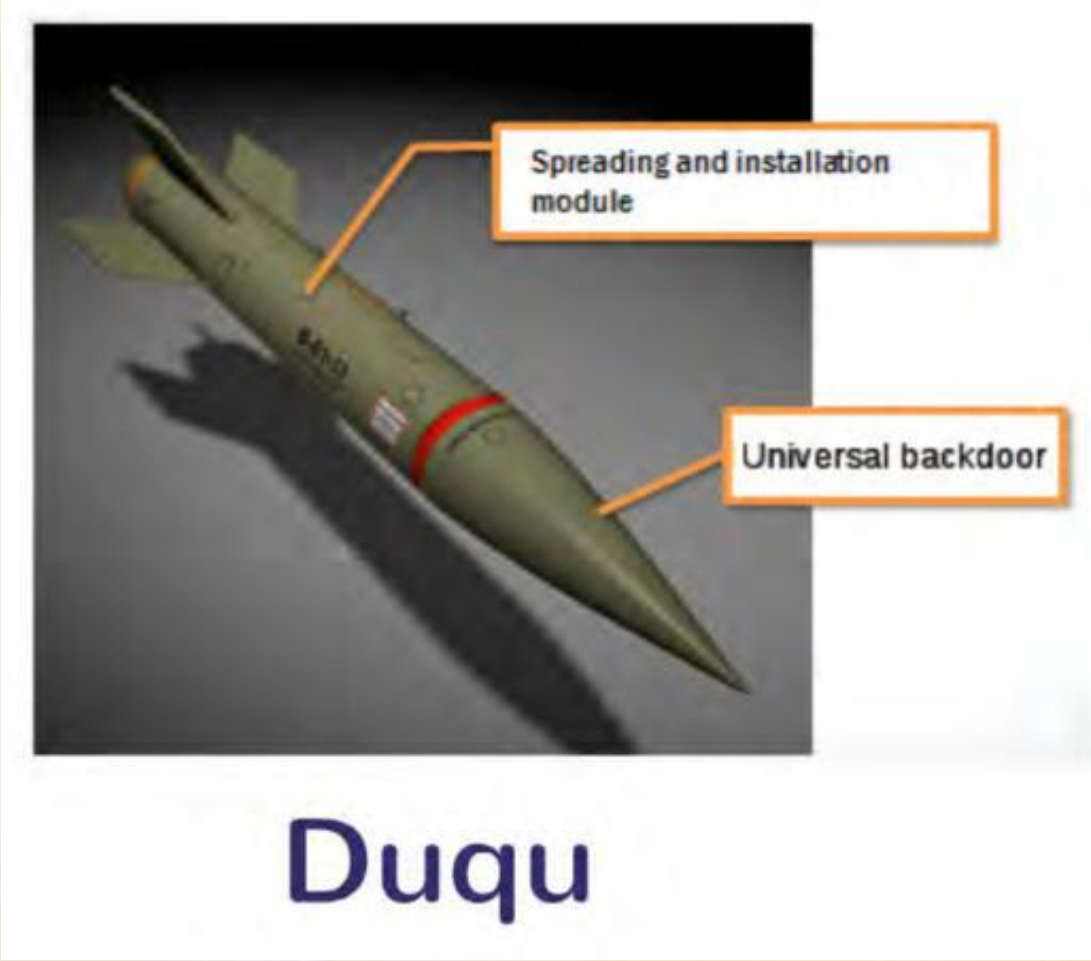
أشارت شركة "سيمناتيك" التي تعمل في مجال برامج الأمن الإلكتروني والبرامج المضادة للفيروسات أنّ إيران تأتي في طليعة الدول المستهدفة من ناحية الإصابات التي حققها برنامج "ستكسنت" وأنّ ما يقارب 60% من أجهزة الكمبيوتر التي تعرضت لهجوم من هذا التطبيق الخبيث كانت في إيران

"

تقرير قناة الجزيرة عن الحرب الإلكترونية

Famous web Defacements and Computer attacks against **Iran**

Duqu:



Famous web Defacements and Computer attacks against **Iran**

Duqu:

دودة جديدة تضرب إيران والسّودان

الكاتب: بشار | يوم: 30 أكتوبر, 2011 | التصنيف: الأخبار, الحوادث الأمنية, المقالات الرئيسية | التعليقات: 3 | القراءات: - عدد المشاهدات 1,768

في منتصف الشهر الحالي ظهرت تقارير تتحدث عن ظهور دودة جديدة مشابهة لدودة Stuxnet والتي ضربت المفاعلات النووية الإيرانيّة في منتصف 2010. وبعيداً عن الجدل الدّائر حول إذا ما كان الفريق الذي طوّر Stuxnet هو نفسه الذي قام بتطوير الدودة الجديدة والتي اطلق عليها Duqu، أمّ أنّه فريق مختلف، فإن الأمر المؤكد هو أنّ هذه الدّودة متطورة بشكل كبير جدّاً. فمختبرات شركة الحماية كاسبيرسكي قد أظهرت وجود أربع إصدارات من هذه الدودة حتى اللحظة، ثلاثة منها في إيران والرابع في السودان.

كل نوع من هذه الأنواع (او التعديلات) للدّودة تستخدم آلية إصابة للنظام مختلفة. ففي حالة استخدمت موجّه يستخدم شهادة رقميّة مزيفة، وفي حالات أخرى لم يستخدم الموجّه أي شهادة. وفي بعض الحالات كان هناك مؤشرات على وجود إصابة بالدودة ولكن لم يعثر على الملفات أثناء دراستها. هذا اعطى إنطباع للباحثين أنّ الدودة تغير من هدفها والذي لا زال معروفاً حتى الآن تبعاً للحاسوب أو النّظام الذي قامت بإصابته.

أحد الدراسات التفصليّة لهذه الدودة قامت بها شركة سيمانتك، والتي ذكرت أنّها حصلت على عيّنة مخبريّة لهذه الدودة في الرابع عشر من الشهر الحالي (اكتوبر تشرين اول). حيث ذكرت الدّراسة أن العيّنة التي تمّت دراستها أظهرت العديد من أوجه الشبه بين هذه الدودة و Stuxnet إلى الحدّ الذي دفع القائمين عليها للقول بأن Duqu هي ابنة (أو ابن) Stuxnet، أو Stuxnet 2.0.

Famous web Defacements and Computer attacks against **Iran**

Duqu:

ما نعرفه عن الدّودة حتى الآن؟

الدودة اطلق عليها اسم Duqu لأنّها تقوم بإنشاء ملفات مسبوقة بالأحرف DQ. العينة التي حصلت عليها شركة Symantec مصدرها هو مؤسسة أوروبيّة. الهدف الظاهر للدودة وفقاً ل Symantec هو جمع المعلومات (وإن كان الهدف الحقيق غير معلوم لغاية الآن) من شركات صناعيّ وغيرها من أجل استخدامها في هجمات مستقبلية. Duqu لا تحتوي على اكواد متعلقة بأنظمة التحكم الصناعي وفقاً ل Symantec، فهي بدرجة أساسية مشابهة لتروجانات التحكم عن بعد (المعروفة ب RAT)، والتي تسمح للمهاجم بالتحكم عن بعد بحاسوب الضحية. الدودة تقوم بتحميل برنامج لسرقة المعلومات والذي يقوم بتسجيل جميع المفاتيح التي قام الضحيّة بضغطها في لوحة مفاتيحه بالإضافة إلى معلومات أخرى وارسالها للمهاجم.

Duqu تستخدم كلاً من HTTP و HTTPS للاتصال بخادم التحكم والاتصال وعنوانه 206.1830.111.97 وهو موجود في الهند. السلطات الهندية قامت اليوم (29-10) بمصادرة بعض العتاد من هذا الخادم ضمن إطار التحقيق في هذه الدودة. Duqu استخدمت هذا الخادم في تثبيت البرنامج الذي يقوم بسرقة المعلومات. حيث تقوم الدودة بتشفير البيانات التي تمّ جمعها تمهيداً لإرسالها.

Famous web Defacements and Computer attacks against **Iran**

Flame:

كتشفت معامل كاسبرسكاي عن فيروس Flame (اللهب) الذكي جداً القادر على التجسس على كل ماتقوم به وإرساله إلى المخترقين لكن طريقة عمل هذا الفيروس تدل على أن هناك جهة كبرى تقف وراءه ويظن خبراء كاسبرسكاي أن حكومة ما تقف وراء هذا الفيروس.

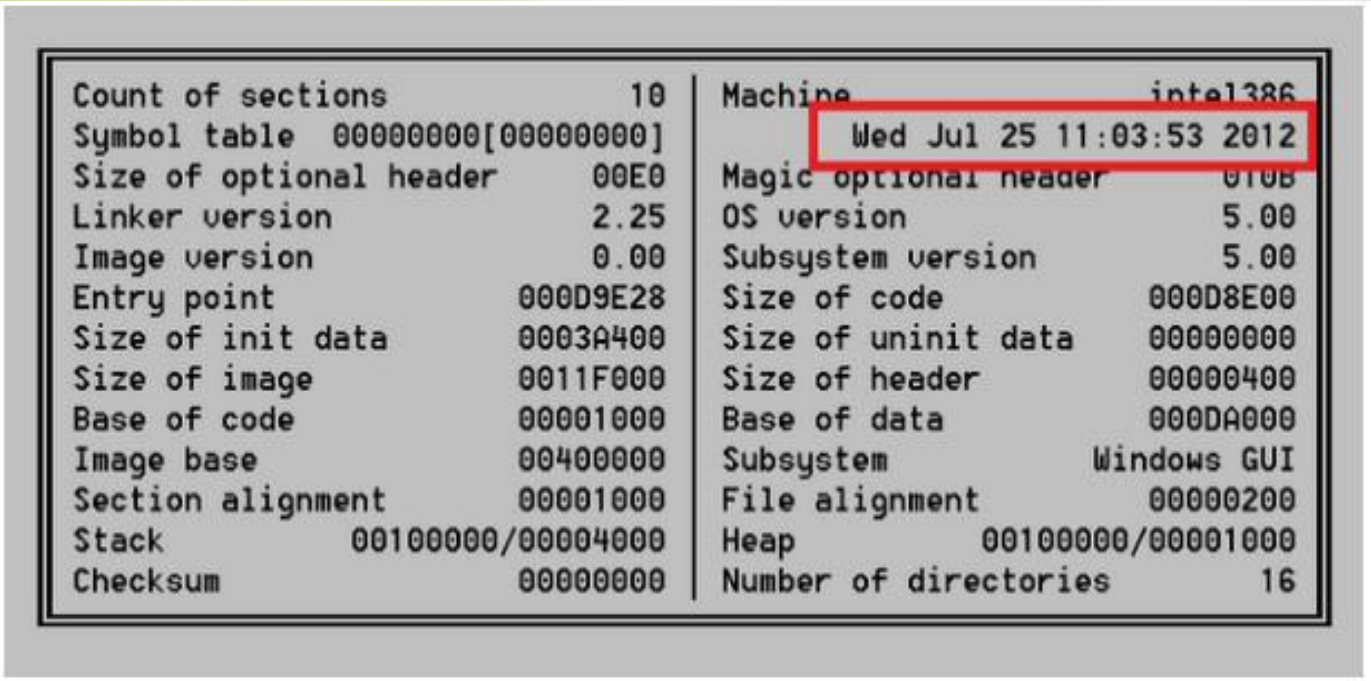
Flame الذي يبلغ من الحجم 20 ميجابايت كان يعمل في الخفاء منذ تم إكتشافه من قبل كاسبرسكاي في 2010 لايقوم بحذف الملفات أو الإضرار بنظام التشغيل بل يعمل على جمع البيانات والمعلومات بشكل صامت، فهو يراقب حركة بيانات الشبكة ويقوم بإستخدام المايكروفون وتسجيل الصوت وضغطه وإرساله وهو قادر على إستشعار البرامج المهمة من أجل أن يأخذ بعض الصور للأمور التي تقوم بالعمل عليها.

الأمر المثير للريبة هو أن هذا الفيروس يستهدف العديد من المنظمات المنتشرة في العديد من دول الشرق الأوسط وإيران على رأس هذه القائمة يليها الكيان الصهيوني ومن ثم سوريا والسودان، لبنان، السعودية ومصر دون إستهداف أي دولة أخرى ممايجعلك تشك بأن هناك جهداً مخابراتياً وراء هذا الفيروس، لأن الهدف منه هو التجسس فقط فهو لن يقوم بإرسال أي بيانات عبر بريدك او سرقة أي حسابات.

Flame قادر على التكاثر عبر الشبكة وإصابة العديد من الأجهزة عبر الشبكة ومن الصعب معرفة مقدار تغلغل هذا الفيروس في أنظمة وأجهزة الدول المستهدفة ولكن قدرة الفيروس التجسسية العالية مخيفة جداً، ومن يدري لعلك مراقب الأن من قبلهم.

Famous web Defacements and Computer attacks against **Iran**

Mehdi:



Count of sections	10	Machine	intel386
Symbol table	00000000[00000000]		Wed Jul 25 11:03:53 2012
Size of optional header	00E0	Magic optional header	010B
Linker version	2.25	OS version	5.00
Image version	0.00	Subsystem version	5.00
Entry point	000D9E28	Size of code	000D8E00
Size of init data	0003A400	Size of uninit data	00000000
Size of image	0011F000	Size of header	00000400
Base of code	00001000	Base of data	000DA000
Image base	00400000	Subsystem	Windows GUI
Section alignment	00001000	File alignment	00000200
Stack	00100000/00004000	Heap	00100000/00001000
Checksum	00000000	Number of directories	16

The majority of the victims were in Iran, and many were found to be businesspeople working on Iranian and Israeli critical-infrastructure projects, Israeli financial institutions, Middle East engineering students or various government agencies in the region. All totaled, multiple gigabytes of data are believed to have been uploaded from victims' computers, researchers have said.

Seculert and Kaspersky dubbed the campaign Mahdi after a term referring to the prophesied redeemer of Islam because evidence suggests the attackers used a folder with that name as they developed the software to run the project.

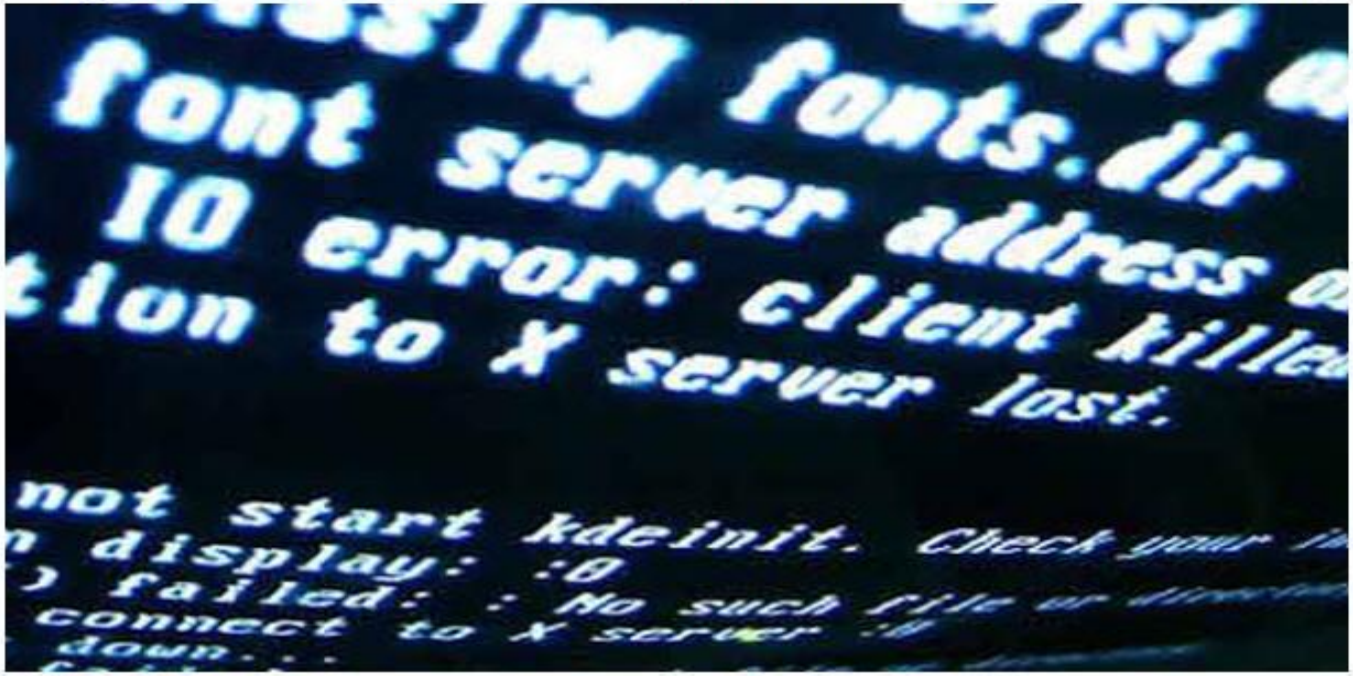
Famous web Defacements and Computer attacks against **Iran**

Cyber attack on Iran's Internet system.

Cyber attack on Iran's Internet system Disrupts Iran Internet

POSTED BY MOHIT KUMAR on 10/04/2012 10:40:00 PM

IRAN state official has said that Cyber attackers have targeted Iranian infrastructure and communications companies, disrupting the Internet across the country. "***Yesterday we had a heavy attack against the country's infrastructure and communications companies which has forced us to limit the Internet,***"



Famous web Defacements and Computer attacks against **Iran**

Iran Web Sites Attacks by S4udi-S3curity-T3rror:

www.qom.gov.ir
www.atf.gov.ir
www.press.gov.ir
www.iranembassy.org.za
www.iranembassyjp.org
www.shia.iranembassy.co.zw
www.iran-embassy-oslo.org
www.iran.iranembassy.co.zw
www.mod.ir
www2.ijrood.gov.ir
www.arak.gov.ir
www.nikshahr.gov.ir
www.kggo.gov.ir
www.ea.gov.ir
www.awqaf-hr.gov.ir
www.iran.qom.gov.ir
www.forum.ea.gov.ir

Famous web Defacements and Computer attacks against **Iran**

Iran Web Sites Attacks by XP-Group:

➢ XP-Group Hacked into over 300 Iranian web sites in the cyber war between Sunni and Shiiaas in 2008, the most famous sites of this list was Alkawthar TV channel, and the Ministry of Industry web site, here is a sample list of the some hacked web sites:

picshop.ir	popular.ir	nooshabe.ir
poya-sanat.ir	practice.ir	notice-ht.ir
pyrogen.ir	radio-parsa.ir	oep.ir
rahasepehr.ir	rahbari2.ir	manaka.ir
rahgoshaa.ir	ramiz.ir	pvcpipeandfittingasoo.ir
netspeed.ir	nikmobile.ir	pvcpipeandfittingasso.ir

Famous web Defacements and Computer attacks against **Iran**

Iran Web Sites Attacks by Individuals:

Famous web Defacements and Computer attacks against **Iran**

Iran Web Sites Attacks by Individuals:

قام اتحاد القراصنة الاحرار باختراق موقع منظمة التجارة الايرانية ردا على دعم ايران لنظام بشار

http://en.tpo.ir/Default.html

http://fa.tpo.ir/Default.html

http://iraq.tpo.ir/Default.html

http://portal-stat.tpo.ir/Default.html

http://portal-export.tpo.ir/Default.html

Famous web Defacements & Computer attacks in:

Egypt

Famous web Defacements and Computer attacks against **Egypt**

Computers and Networks Attacks:

There is no known mass spreading cases or targeting a computer systems happen before in Egypt, but it seems that there is few number of computers Hacked by: Duqu and Flame.

Web Sites Attacks:

- Iran Hackers Attacks
- Israel Hackers Attacks
- DDOS attacks against Link.net DNS
- DDOS attacks against Egyptian government web portals.

Famous web Defacements and Computer attacks against **Egypt**

Attacks on Egyptian Web Sites by Iranian Hackers:

Date	Notifier	H	M	R	L	★	Domain	OS	View
2009/04/18	Mafia Hacking Team			R		★	www.presidency.gov.eg/darkl0rd...	Win 2003	mirror
2009/04/18	Mafia Hacking Team			R		★	library.idsc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/18	Mafia Hacking Team		M				www.investinalexandria.gov.eg/...	Win 2003	mirror
2009/04/18	Mafia Hacking Team		M	R			www.goief.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/18	Mafia Hacking Team		M	R			www.moi.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/18	Mafia Hacking Team		M			★	www.mdci.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.pbc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.alex-cic.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.assiuttp.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R		★	www.egsma.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.observatory.gov.eg/darkl0r...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.eitpfollow.gov.eg/darkl0rd...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.fayoum.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R		★	www.ngisc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	preview.idsc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R		★	www.cairobiennale.gov.eg/darkl...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.alexmuseum.gov.eg/darkl0rd...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M			★	www.mop.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team						conference.idsc.gov.eg/darkl0r...	Win 2003	mirror
2009/04/17	Persian Boys Hacking Team		M	R			www.gem.gov.eg/d.htm	Win 2003	mirror
2009/04/17	Persian Boys Hacking Team		M			★	www.suez.gov.eg/d.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M				www.scc.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R			www.grm.gov.eg/darkl0rd.htm	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M				www.tanmia-mosharka.gov.eg/dar...	Win 2003	mirror
2009/04/17	Mafia Hacking Team		M	R			www.gocp.gov.eg/darkl0rd.htm	Win 2003	mirror

Famous web Defacements and Computer attacks against **Egypt**

Attacks on Egyptian Web Sites by Israeli hackers:

جزء من الازمة الموجوده بين مصر و اسرائيل الان هى قيام عدد كبير من الهاكر العربى باختراق مواقع الكيان الصهيونى على الانترنت و ذلك ردا على ما فعلته من قتل الجنود المصريين على الحدود لذلك رد الهاكر الاسرائيلى باختراق مواقع مصرية و لاسف استطاع اخترق اكبر صفحة على الفيس بوك لمحافظة الاسكندرية و ترك رسالة بالعبرية **אנחנו שולטים בעולם** تعنى " اسرائيل تحكم العالم " فى رسالة تحدى واضح لمصر و كل الدول العربية يذكر ان هذه الازمة بدأت بعد قايم اسرائيل بقتل الجنود المصريين على الحدود مع مصر و ردت بعدها اسرائيل بانها تأسف لما حدث و لكنها رفضت الاعتذار

نقلا عن بوابه الفجر الالكترونيه

Famous web Defacements and Computer attacks against **Egypt**

Attacks on Egyptian Web Sites by Israeli hackers:

Total notifications: **196** of which **89** single ip and **107** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2010/06/04	g0x	H	M				www.iccs-x.org.eg	Win 2003	mirror
2010/06/04	g0x		M				www.epdi.org.eg/index.aspx	Win 2003	mirror
2010/06/04	g0x		M	R			www.tourismnet.com.eg/g0x.htm	Win 2003	mirror
2010/06/04	g0x		M	R			www.tourism.egnet.net/g0x.htm	Win 2003	mirror
2010/06/04	g0x		M	R		★	www.cicpo.gov.eg/g0x.htm	Win 2003	mirror
2010/06/04	g0x		M				www.egyptlib.net.eg/g0x.htm	Win 2003	mirror
2010/06/04	g0x		M				www.fepsalumni.org.eg/g0x.htm	Win 2003	mirror
2010/06/04	g0x		M	R			www.netegypt.egnet.net/WebDire...	Win 2003	mirror
2010/06/04	g0x	H	M	R			www.ics.org.eg	Win 2003	mirror

Famous web Defacements and Computer attacks against **Egypt**

DDOS attacks against Link.net DNS

In June 2011, Naguib Sawiris the famous Egyptian business man published an image on his twitter account, that image Raised a lot of hate towards him, which caused some Hackers to start a huge DDOS attack against Link.net DNS servers, that DDOS attacks taken down all the web sites used link.net DNS, such as:
Mobinil.com, Masrawy.com, Yallakora.com and other web sites related to link DNS.

Famous web Defacements and Computer attacks against **Egypt**

DDOS attacks against Egyptian Government portals.

In 2011, During the Egyptian revolution, Anonymous group started huge DDOS attack against government portals, that DDOS attacks taken down most of the .gov.eg web sites, They tried to mass DDOS against mcit.gov.eg web site but without success!

Famous web Defacements & Computer attacks in:

Israel

Famous web Defacements and Computer attacks against **Israel**

Computers and Networks Attacks:

- Attacks by 0xomar
- Attacks by Eg-R1z Team
- Attacks by Egy-Virus Team
- Attacks by Iranian Hackers
- Attacks by Un-known Hackers

Web Sites Attacks:

- Iranian Hackers Attacks
- Arab Hackers Attacks
- World Hackers Attacks

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli web sites by 0xomar:

هارتس: اختراق موقعي "العال" وبورصة تل أبيب بأجهزة كمبيوتر إسرائيلية

نشر بـ الثلاثاء يناير 17, 2012 من طرف **Admin** تحت تصنيف **أخبار القراصنة العرب**

كد خبير إسرائيلي رفيع المستوى في مجال أمن برامج الحاسب أن سلسلة هجمات الإنترنت التي حدثت أخيرا ضد شركات بطاقات الائتمان والبنوك والمواقع الحكومية في إسرائيل تمت الاستعانة في تنفيذها بآلاف الحواسب التي قام بتشغيلها أشخاص مهاجمون عن بعد.

ونقلت صحيفة "هآرتس"الإسرائيلية اليوم الثلاثاء – في تقرير أوردته على موقعها الإلكتروني على شبكة الإنترنت – عن الخبير الإسرائيلي جيل شويد قوله " عندما ننظر للهجوم الذي وقع بالأمس، فإنه لا يعد ضربة من جهاز كمبيوتر في السعودية. إنها آلاف من الحواسب حول العالم".

وأضاف شويد، مؤسس وقائد شركة أمن الحواسب الكبرى (تشيك بوينت للتقنيات البرمجية) " أن جزءا كبيرا من الحواسب التي هاجمتنا موجودة في إسرائيل. فهذا بشكل دقيق يفسر ما هو البوت".

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Anonymous:

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Un-known Hackers :

Gauss

Country	Unique users
Lebanon	1660
Israel	483
Palestinian Territory	261
United States	43
United Arab Emirates	11
Germany	5
Egypt	4
Qatar	4
Jordan	4
Saudi Arabia	4
Syria	4

Gauss has attacked over 2,500 personal computers in the Middle East.

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Eg-R1z Team:

In Sudden escalation for the attack level , an Egyptian group launched computer worm which infected about 50000 personal computer in Israel and united states. Despite of my virtual machine security level , it was also infected by the same worm. I (Reuben Rayner) didn't notice that am infected till the attackers launched an exe file which viewed message in the full screen mode.

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Eg-R1z Team:

viewed Israel gov sites yesterday? Try pinging mossad.gov.il for example

The pinging result

C:\>ping mossad.gov.il -ttl

Pinging mossad.gov.il [147.237.72.71] with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

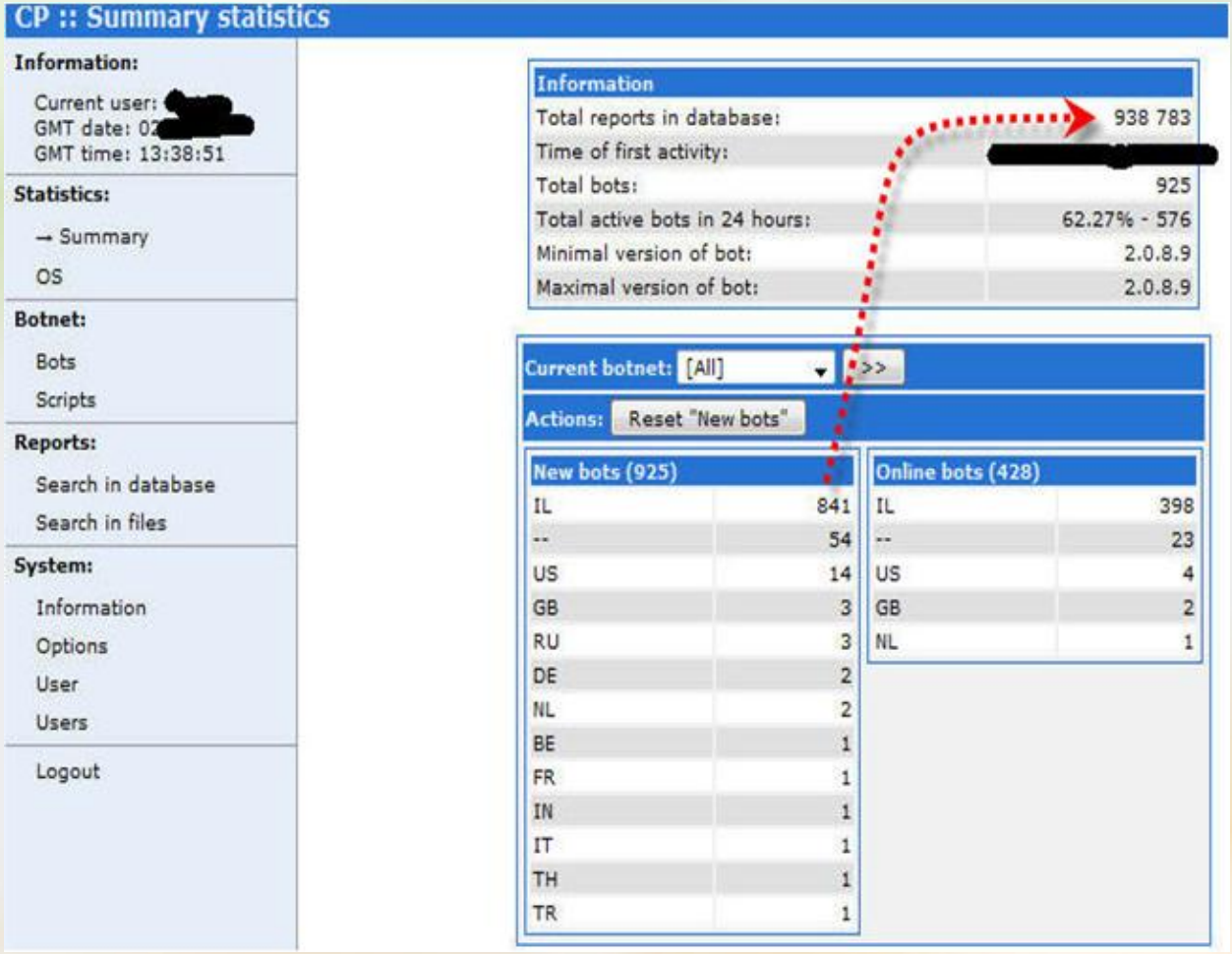
What's the point??

If the attackers used the same massive bots to attack sensitive gov sites , this will probably cause a disaster.

If they did it and dumped the banking accounts of thousands and thousands of users they got , this will also cause disaster.

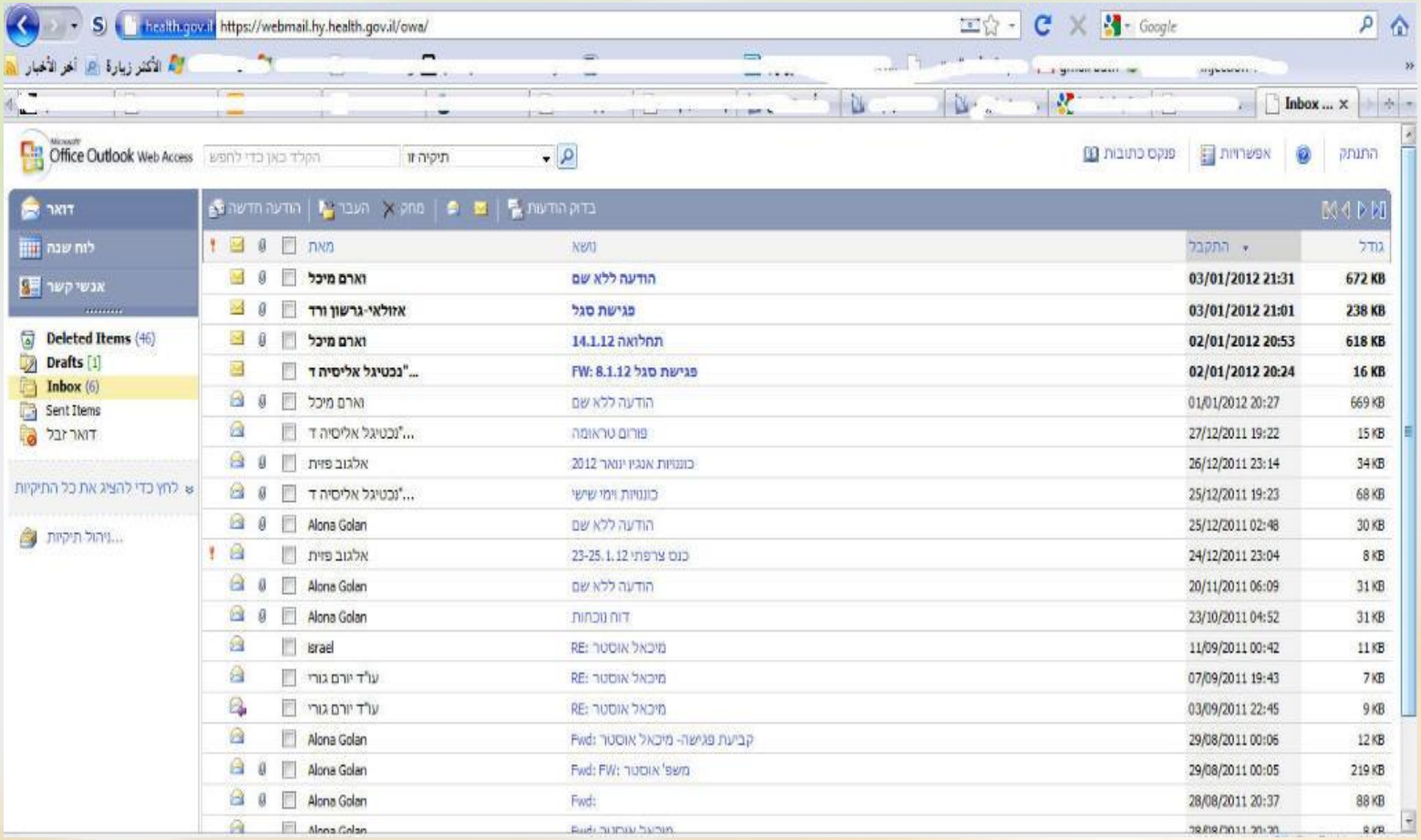
Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Egy-Virus Team:



Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Egy-Virus Team:



Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Anonymous:

Israeli SCADA Systems Hacked by Anonymous

By Lee J

Published January 12th, 2012


```
#fuckisrael - trend this.

ISRAELI #SCADA SYSTEMS:
http://95.35.29.236/
http://62.219.7.27/
http://193.104.44.37/
http://212.143.97.144/
http://79.181.197.213/
http://82.102.153.52/login
http://213.57.132.28/
http://84.106.144.158
http://82.80.232.37/en-US.htm
http://81.218.206.85/notsecure.asp

Find their systems. Login using default logins. ("100" being the password)
```

In what is turning out to be a full on attack on Israeli systems has taken another turn now, with one of the more well known anonymous twitter account announced for everyone to go follow @FuryOfAnon for upcoming release's.

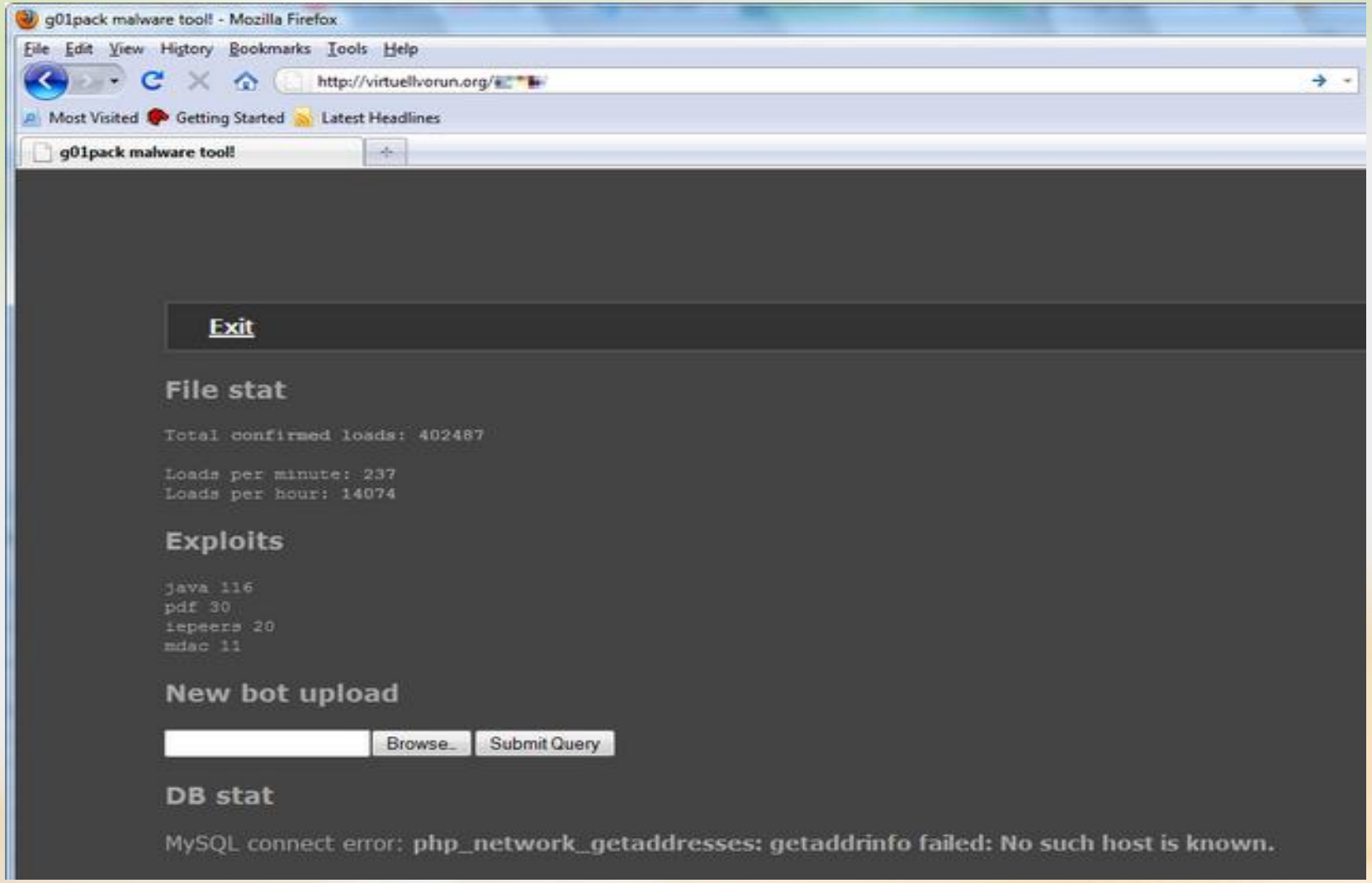
From this came the following tweet.

@FuryOfAnon
Furyoku

Who wanna have some fun with israeli scada systems... pastebin.com/ZyEzJnFB #Anonymous #Antisec #OWS

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Iranian hackers:



Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Iranian hackers:

```
<h3>Exploits</h3>
<pre>
java 106
pdf 39
iepeers 20
mdac 10</pre>

<h3>New bot upload</h3>
<form method="post" enctype="multipart/form-data"><input type='file' name='botfile' /><input type='submit' /></form>


<h3>DB stat</h3>

MySQL connect error: <b>php_network_getaddresses: getaddrinfo failed: No such host is known.</b>

</body>
<!-- Iranian Cyber Army -->
</html>
```

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli web sites by 0xomar:

www.israeltoday.co.il/NewsItem/tabid/178/nid/23111/language/en-US/Default.aspx

Israel Today hacked; Israeli army jumps into cyber war

Thursday, February 09, 2012 | Ryan Jones

| Share

Many of our readers will have noticed that our online services have been sporadic at best over the past few days. Many will also be aware that Israel is in the midst of an escalating cyber war with pro-Palestinian activists around the world. Our latest server problems are related to that war.

Over the past few days, an unknown hacker or group of hackers pounded the israeltoday.co.il domain with so many requests that it repeatedly crashed. We weren't the only ones affected. Hundreds of Israeli sites were targeted and briefly brought down, including the Hebrew and English-language news sites of Israel's best-selling newspaper, *Yediot Ahronot*.

As the cyber war between Israel and pro-Palestinian hackers intensifies, the Israeli army is taking an increasingly prominent role in defending the nation on this new battlefield.

The IDF Spokesperson reported this week that 27-year-old Daniel, a recent immigrant from Mexico, had been recruited by the army for is "creative" computer skills.

Related Stories

- Flytilla activists scrawl swastika at Israel airport
- Israel works to shrink Arab unemployment
- IDF gearing up to invade Gaza

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Iranian hackers:

نشر بتاريخ 27-07-2012 :: 09:30 AM

SHARE

مصادر ايرانية: هكرز ايراني يخترقون 220 موقعاً اسرائيلياً

وطن للانباء/ قالت وكالة "مهر" الإيرانية للأنباء، امس الخميس، إن مجموعة من الشباب الإيراني اخترقت 220 موقعاً إسرائيلياً على شبكة الإنترنت، وذلك بالذكرى السنوية لاغتيال العالم النووي الإيراني داريوش رضائي نجاد.

وأضافت أن مجموعة من الشبان في ايران تدعى "مجموعة أمن الإنترنت" استطاعت اختراق المواقع الأساسية في"الكيان الصهيوني" وتعطيلها.

ونقلت الوكالة عن أحد افراد المجموعة قوله إنه بالذكرى السنوية لإغتيال العالم النووي الايراني داريوش رضائي نجاد، قامت المجموعة "بشن هجوم على المواقع الإلكترونية التابعة للكيان الصهيوني ونجحت في تعطيل 220 موقعاً منها".

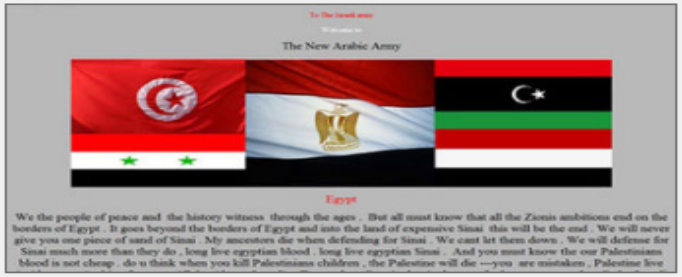
واضاف انه تم الوصول "الى اكثر المواقع حساسية في الكيان الصهيوني وتعطيل الخوادم مثل موقع مركز تدريب قوات الأمن الإسرائيلي وموقع منتدى اسرائيل الأساسي وموقع تجاري مصرفي يقوم بحماية البطاقات المصرفية للإسرائيليين".

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Arab hackers:

هاكرز مصرى يخترق موقعا تابعا لوزارة الدفاع الإسرائيلية

الإثنين، 22 أغسطس 2011 - 15:10



دماء شهدائنا ليس رخيصا.. سنقاتل من أجل سيناء

كتب هاشم القفراتى

ذكرت صحيفة "هآرتس" الإسرائيلية أن مجموعة من "الهاكرز " المصرى اخترق صباح اليوم الموقع الإلكترونى الخاص بالجنود الإسرائيليين وهو army.co.il، المعنى بنشر أخبار الجنود ويقدم لغير المجندين الاستشارات ومعلومات عن الجيش الإسرائيلى.

وأضافت الصحيفة أن مخترقى الموقع الذى تم تأسيسه فى عام 2003 ويتبع وزارة الدفاع الإسرائيلية، كتبوا على الموقع الإلكترونى الإسرائيلى "دماء شهدائنا ليس رخيصا.. سنقاتل من أجل سيناء"، ووضعوا صور أعلام مصر وسوريا وليبيا وتونس، وأعلى الأعلام كتب "الجيش العربى الجديد" باللغة الإنجليزية.

ونقلت الصحيفة عن "يائير كوتفيتش" مدير تحرير الموقع، أنه فى تمام الساعة 11 صباح اليوم، فوجئ العاملون بالموقع بهذه الصورة التى عليها الأعلام العربية ويتوسطها العلم المصرى.

يذكر أن مجموعة من الهاكرز المصرى اخترقوا أمس الموقع الإلكترونى لرئيس الحكومة الإسرائيلية بنيامين نتانياهو، ووضعوا عليه صورة جندى يرفع العلم المصرى، بالإضافة إلى اختراق موقع الليكود، بالإضافة إلى اختراق موقع هيئة الأرصاد الجوية الإسرائيلية التابع لمجلس الوزراء الإسرائيلى.

أخبار المحافظات
أخبار عربية
أخبار عالمية
اقتصاد
بورصة وبنوك
أخبار الرياضة
فن
تليفزيون وتوك شو
ثقافة
منوعات ومجتمع
صحة وطب
مقالات القراء
ألبومات اليوم السابع
مقالات
صحافة محلية
صحافة عالمية
صحافة إسرائيلية
بقلم رئيس التحرير
دورة الألعاب الأوليمبية
كاريكاتير اليوم
توك شو

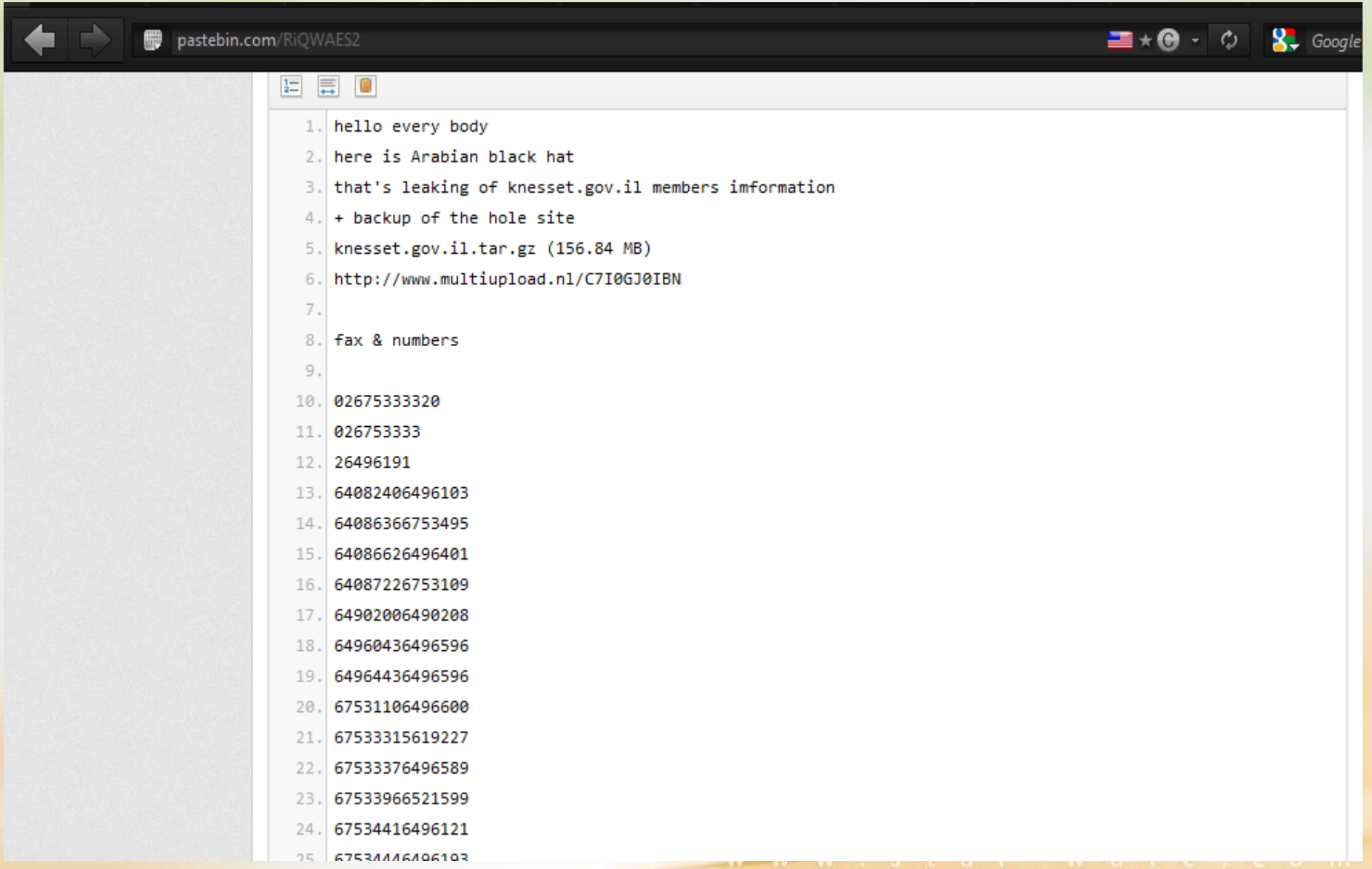
Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Arab hackers:

??????? ?? ???? ???????-???????? ????????? ????????? ?? ????????? 40 ???????? ? ????????: "?? ?????????? ?????????? ??????????? ?????? ???????? ???????????? ?? ????????? ????? ? ????????, ???????????, ???????????? ????? ? ????????? ???????????????? ????????????????? ????????, ? ????? ??? ?????? ...

Famous web Defacements and Computer attacks against Egypt

Attacking on Israeli Web Sites by Arab Hackers:



Famous web Defacements and Computer attacks against Egypt

Attacking on Israeli Web Sites by Arab Hackers:

www.usatoday.com/news/world/story/2012-01-16/hackers-israel-airline-stocks/52601712/1

Hackers disrupt Israel airline, stock market

Updated

Comment

JERUSALEM (AP) – A hacker network that claims to be based in Saudi Arabia paralyzed the websites of Israel's stock exchange and national airline on Monday, escalating an international cyber war that has jolted this security-obsessed country.

By Ariel Schalit, A

A security guard, right, stands at the entrance o the national Israeli air carrier El Al sales offices ir Tel Aviv, Israel, on Monday.

Neither website contains sensitive information and trading and flights were not affected. But the ongoing salvos by hackers who use anti-Israel language in their posts has revealed how vulnerable Israel is to cyber warfare, despite its sophisticated computer security units in the military and advanced high-tech sector.

The attacks began earlier this month when hackers identifying themselves as group-xp, a known Saudi hacking group, claimed on an Israeli sports website to have gained access to 400,000 Israeli credit card accounts. The group called it a "gift to the world for the

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Arab hackers:

Date	Notifier	H	M	R	L	Domain	OS	View
2008/08/26	Team-evil					www.toyota.co.il/news1.asp	Win 2000	mirror
2006/11/28	Team-Evil	H		R		www.fiat.co.il	Win 2003	mirror
2006/11/13	Team-Evil	H				crossword.msn.co.il	Win 2003	mirror
2006/11/09	Team-Evil					www.kereni.gov.il/db	Win 2003	mirror
2006/10/22	Team-Evil	H				i-travel.msn.co.il	Win 2003	mirror
2006/10/07	Team-Evil	H				habama.msn.co.il	Win 2000	mirror
2006/09/18	Team-Evil		M			www.antidrugs.gov.il/news/defa...	Win 2000	mirror
2006/09/15	Team-Evil	H	M			www.renault.co.il	Win 2003	mirror
2006/09/09	Team-Evil	H				www.nissan.co.il	Win 2003	mirror
2006/08/07	Team-Evil	H	M			www.mazda.co.il	Win 2003	mirror
2006/08/05	Team-Evil	H				www.ford.co.il	Win 2003	mirror
2006/07/03	Team-Evil	H	M			www.eGov.co.il	Linux	mirror
2006/07/03	Team-Evil	H	M			www.FirstGov.co.il	Linux	mirror
2006/07/03	Team-Evil	H	M			www.Government.co.il	Linux	mirror
2006/06/28	Team-Evil	H	M			www.citroen.co.il	Win 2003	mirror
2006/06/28	Team-Evil	H	M			tarbut-hadiur.gov.il	Win 2003	mirror
2006/06/28	Team-evil	H	M			www.bmw.co.il	Win 2003	mirror
2006/04/12	Team-evil	H				www.iibr.gov.il	Win 2003	mirror
2006/04/09	Team-evil					www.mcdonalds.co.il/index.htm	Win 2003	mirror
2006/02/06	Team-Evil					jsis.washington.edu/ma.htm	Win 2003	mirror
2005/09/07	Team-evil					www.export.gov.il/_Uploads/531...	Win 2000	mirror
2005/09/07	Team-evil		M	R		www.orianit.edu-negev.gov.il/f...	Win 2000	mirror
2005/08/30	Team-evil					www.ci.st-charles.il.us/news/s...	Win 2000	mirror
2005/08/28	Team-evil					www.sinaloa.gob.mx/fpdb/galeri...	Win 2000	mirror

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Arab hackers:

OrderID	PaymentMethod	CreditCard	ExpDate	email	phone
071222082859	Visa	4580120712975727	02\10	israelor@nonstop.net.il	0526450819
071222172244	Mastercard	5326100308877095	11/09	levi.yavin@gmail.com	0506500559
071222173115	Visa	4580031180150646	09/10	rubido@walla.com	0507776235
071222174007					
071223164635	Isracard	29858518	01/10	efratfenig@gmail.com	097920312
071224185243	Check/Money Order			eilamsher@gmail.com	097493042
071221132045	Isracard	test	test	sales@music4you.co.il	test
071221133911	Check/Money Order			tamir36@gmail.com	057-8166714
080122170625	Visa	4580160007224811	11.10	lockstock@walla.co.il	0504206535
080124075723	Isracard	57853991	07/08	boazho@netvision.net.il	052-3640414
080224211106	Visa	4580120774324228	12/2010	ruti.sharon@gmail.com	052-5611220
080224180219					
080224191443	Isracard	59578246	01/09	eddietheone@walla.co.il	0524712148
080224065709	Visa	4580-1600-0963-3308	11/2010	maly3443@bezeqint.net	052-7687655
080221224351	Isracard	64841944	02/11	soofzam@gmail.com	0578899801
080218191150	Mastercard	5326100321014783	02/10	talgaldanyam@walla.com	0524643576
080217151406	Visa	4580121112236124	12/09	georgeabdalla1@gmail.com	052-3568242
080217193950					
080217151350	Visa	4580121112236124	12/09	georgeabdalla1@gmail.com	052-3568242
080216190111	Mastercard	5326100321014783	02/10	talgaldanyam@walla.com	0524643576
080214194142	Check/Money Order			michael.hefetz.spam@gmail.com	0504460481
080214143108	Visa	4580030787725743	10/2008	ty@maaganm.co.il	0522272917
080214155837	Mastercard	5326100351116409	08/10	caspi_nili@hotmail.com	052-3413559
080210174019	Check/Money Order			galihuss@yahoo.com	0547595918
080210143543	Visa	4580100707922991	08/09	ehonen@gmail.com	054-4470601
08029235401	Isracard	64027562	05/10	no_zahavi1@walla.com	054-7520026
08029224311	Visa	4580030792984442	4/2010	ori.marmari@gmail.com	0542558322
08029185102	Isracard	66087449	01/11	galit_pe@hotmail.com	0546747586
08027232538	Visa	4580160108769656	0508	lihi.lasslo@gmail.com	0547623662

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by European hackers:

فريق كوسوفي ينضم للإنتفاضة ويسحب 7000 بطاقة بنكية اسرائيلية ويقوم بنشرها

نشر بـ الخميس, يناير 19, 2012 من طرف **Admin**، تحت تصنيف **أخبار الإختراقات**

قام فريق Kosova Hacker's Security من كوسوفو بالانضمام للإنتفاضة وقام باستهداف مؤسسة اسرائيلية للتسوق وسحب قاعدة بياناتها التي تحتوي على ما يقارب 7000 بطاقة بنكية سارية المفعول ولا يوجد اي منها منتهي الصلاحيه باذن الله

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Turkish Hackers:

Date	Notifier	H	M	R	L	★	Domain	OS	View
2010/08/26	turkguvenligi.info	H	M			★	cokezero.co.kr	Linux	mirror
2010/08/24	turkguvenligi.info	H				★	interpol.com	Linux	mirror
2010/07/31	TurkGuvenligi.Info	H				★	www.privacyprotect.org	Linux	mirror
2010/07/31	TurkGuvenligi.Info	H				★	www.resellerclub.com	Linux	mirror
2010/07/31	Turkguvenligi.Info	H					domainer.logicboxes.com	Linux	mirror
2010/07/31	Turkguvenligi.Info	H	M				directihosting.com	Linux	mirror
2010/07/31	TurkGuvenligi.Info	H				★	www.directi.com	Linux	mirror
2010/07/31	TurkGuvenligi.Info	H	M				gtldinfo.com	Linux	mirror
2010/07/31	TurkGuvenligi.Info	H					www.web.in	Linux	mirror
2010/07/07	TurkGuvenligi.Info					★	www.kaspersky.co.id/Presscente...	Win 2008	mirror
2010/06/16	TurkGuvenligi.info	H	M			★	admin.ci.waterville.mn.us	Linux	mirror
2010/06/10	turkguvenligi.info	H	M				travian.co.il	Unknown	mirror
2010/06/10	turkguvenligi.info	H	M	R		★	blogs.microsoft.co.il	Linux	mirror
2010/06/10	turkguvenligi.info	H	M			★	microsoft.co.il	Linux	mirror
2010/06/10	turkguvenligi.info	H	M			★	cocacola.co.il	Linux	mirror
2010/06/10	turkguvenligi.info	H	M			★	hotmail.co.il	Linux	mirror
2010/06/10	turkguvenligi.info	H				★	live.co.il	Linux	mirror
2010/06/10	turkguvenligi.info	H	M	R		★	msn.co.il	Linux	mirror
2010/06/10	turkguvenligi.info	H	M			★	bing.co.il	Linux	mirror
2010/06/10	turkguvenligi.info	H	M			★	coca-cola.co.il	Linux	mirror
2010/06/10	turkguvenligi.info	H	M			★	coke.co.il	Linux	mirror
2010/06/08	TurkGuvenligi.Info						www.tapuz.co.il/softwares/	Win 2003	mirror
2010/06/03	TurkGuvenligi.info	H	M				halkinkurtuluspartisi.org	FreeBSD	mirror
2010/06/03	TurkGuvenligi.Info	H					www.doingzionism.org	Win 2003	mirror
2010/06/03	turkguvenligi.info	H	M				www.doingzionism.org.il	Win 2003	mirror

Famous web Defacements and Computer attacks against **Israel**

Attacks on Israeli Computers and Networks by Turkish Hackers:

Date	Notifier	H	M	R	L	Domain	OS	View
2012/11/19	1337	H	M			blog.sprite.co.il	Linux	mirror
2012/11/19	1337	H	M			pm.parliament.co.il	Linux	mirror
2012/11/19	1337	H	M			blog.fanta.co.il	Linux	mirror
2012/11/19	1337	H	M			sprite.org.il	Linux	mirror
2012/11/19	1337	H	M			www.microsoftstore.co.il	Linux	mirror
2012/11/19	1337	H	M			intelatom.co.il	Linux	mirror
2012/11/19	1337	H	M	R		www.opel.co.il	Linux	mirror
2012/11/19	1337	H	M			philips.co.il	Linux	mirror
2012/11/19	1337	H	M	R		bing.co.il	Linux	mirror
2012/11/19	1337	H	M			bbc.org.il	Linux	mirror
2012/11/19	1337	H	M			pantene.co.il	Linux	mirror
2012/11/19	1337	H	M			paypass.co.il	Linux	mirror
2012/11/19	1337	H	M			amazonunbox.co.il	Linux	mirror
2012/11/19	1337	H	M			windowslive.co.il	Linux	mirror
2012/11/19	1337	H	M			windows.co.il	Linux	mirror
2012/11/19	1337	H	M			www.nbcuni.co.il	Linux	mirror
2012/11/19	1337	H	M			citibank.co.il	Linux	mirror
2012/11/19	1337	H	M			xbox360.co.il	Linux	mirror
2012/11/19	1337	H	M			www.xboxfusion.co.il	Linux	mirror
2012/11/19	1337	H	M	R		cocacola.co.il	Linux	mirror
2012/11/19	1337	H	M	R		coke.co.il	Linux	mirror
2012/11/19	1337	H	M			www.xboxignite.co.il	Linux	mirror
2012/11/19	1337	H	M			www.intelappup.co.il	Linux	mirror
2012/11/19	1337	H	M			www.intel.co.il	Linux	mirror
2012/11/19	1337	H	M	R		live.co.il	Linux	mirror

1 2 3 4 5 6 7

Responsible Authorities for Cyber Security

Israel

- Il-CERT
- CERT-GOVIL
- ILAN-CERT
- Mamram Unit

Iran

- IrCERT
- APA-SUcert
- APA-SharifCERT
- MAHER center

Egypt

- EG-CERT
- Cyber crime investigation department

Comparison and Recommendations

Comparison and Recommendations

وكانت الولايات المتحدة قد أقرت استراتيجية جديدة في العام 2010 تحضر لامكانية خوض حرب إلكترونية، وتعتبر العالم الافتراضي ميدانا حقيقيا لحرب محتملة لا يقل أهمية عن المجال الجوي والبري والبحري، وجهز البنتاغون لذلك 15 ألف شبكة حاسوب يعمل على ادارتها 90 ألف خبير في الكمبيوتر، إضافة إلى نحو ألف خبير عسكري في القرصنه والجاسوسيه الإلكترونيه.

وتنحصر المهمة الرئيسية للجيش الكبير من المختصين بالتجسس في المجال الإلكتروني، والتصدي للهجمات السبرنيتيكية على الولايات المتحدة، وتسديد الضربات الإستباقية الى الجهات التي تحضر تلك الهجمات.

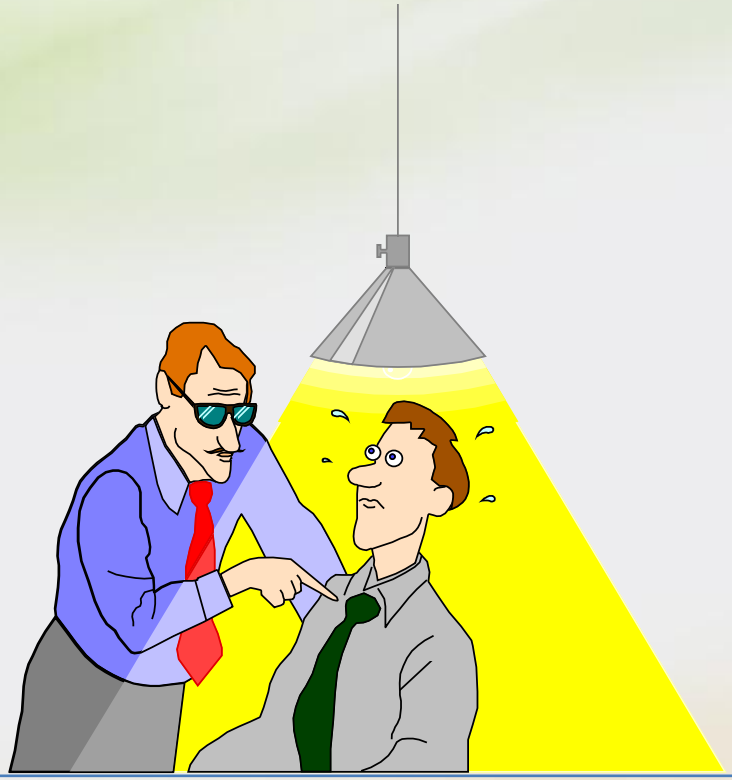
من جانبه حدد رئيس الوزراء الإسرائيلي بنيامين نتنياهو السايبر كأحد أهم المجالات التى تسعى بلاده لتطويرها، وشدد في مؤتمر مركز دراسات الامن القومي في جامعة تل ابيب، منذ ايام على انه يعتبر من التحديات المهمة التي تواجه الدولة العبرية، وقال إن "قدرات السايبر التي نطورها تزيد من قدرات إسرائيل الدفاعية. ونحن نستثمر في ذلك رأسمالا هائلاً، بشرياً ومالياً، وأنا أتوقع أن يزداد هذا الاستثمار. لقد شكلت هيئة السايبر القومية وحددت لها هدفاً: أن تغدو إسرائيل واحدة من القوى العظمى الخمس الرائدة في هذا المجال، وأنا أؤمن أننا سنحافظ على هذا الهدف".

وفيما حملت إيران واشنطن وتل أبيب المسؤولية عن نشر الفيروس الالكتروني الحالي، فإن تقارير عدة تشير إلى أن طهران تستعد لخوض حرب إلكترونية مع البلدين، وأنها أعدت جيشا من قراصنة الإنترنت لاستهداف شبكات الكهرباء والمياه الأمريكية والإسرائيلية والعديد من منشآت البنية التحتية انتقاما للهجمات الالكترونية التي تعرضت لها في السنتين الأخيرتين.

وتحدثت تقارير سابقة عن تخصيص إيران نحو مليار دولار لقراصنة مختصين من أجل توجيه هذه الضربات، ويوضح المهندس سامر سفاريني لموقع "روسيا اليوم" انه على الرغم من التفاوت بين قدرات إيران والولايات المتحدة فإن "جمع جيش إلكتروني وأسلحة سيبرنيتيكية ليس بالأمر الصعب في حال توافرت الرغبة والامكانات المادية"، ورغم أن الخبير في الاتصالات وبرامج الكمبيوتر يعتقد بأنه "لا يوجد حتى الآن فيروس جاهز في العالم يستطيع تعطيل خدمات حكومة بأكملها، وأن معظمها يستخدم لأغراض التجسس" فإنه يتفق مع الرأي بأن "العالم في القرن الحادي والعشرين يواجه خطر كوارث كبيرة قد تصل إلى تدمير معظم منجزات الحضارة الإنسانية في حال انتشار وباء بيولوجي نعجز عن إيجاد علاج له، أو فيروس إلكتروني يؤثر في شبكات الخدمات المدنية ويصل إلى الشبكات العسكرية..."

Comparison and Recommendations

- We have experts and specialists, but as individuals and not participated in teams.
- Our government is not supporting the Egyptian hackers.
- Curriculum in computer studies universities is too old and not up to date!
- Do we have a team or unit that can launch and manage a Cyber Warfare?
- In Iran and Israel there is a CERT in the biggest country universities that works as CERT for the university and to help the main country CERT, why don't we have such things in Egypt?
- There is no security awareness in the real form in our countries.
- Why there is no legislation and laws to curb sabotage operations through the Internet?
- Responsible Authorities in Egypt doesn't have enough permissions to force ISP's, critical sites, etc to apply a security policy or to patch a vulnerability.



Questions

Thanks for your time

Starware Security Team
By: Ebrahim Hegazy