i DEFENSE

Intelligence Services Report

Israeli-Palestinian Cyber Conflict (IPCC)

VERSION 2.0PR
PUBLIC RELEASE

Jan. 3, 2001 – 15:41 GMT

ATTENTION: The IPCC report is dynamic document subject to frequent revision and changes. It contains placeholders and areas that have yet to be fleshed out. The IPCC report is being provided to you in the interest of speed so that you have the best information available at this time. The Public Release (PR) version is a sanitized version of the report released by iDEFENSE to its clients and government agencies. Due to the sensitivity of sources and methods some content has been reduced or removed. The PR version provides the clearest picture possible of an ongoing conflict in a public release format. All inquiries regarding information contained in this report can be directed to iDEFENSE Director of Corporate Communications Jerry Irvine at cell 703-622-3058 or email at press@idefense.com.

Table of Contents

VIII. Pro-Israeli Sites Hosting Live Attack Tools 37

IX. Pro-Palestinian Sites Hosting Live Attack Tools 38

X. Pro-Palestinian Sites Supporting the Campaign...............................39

XI. Pro-Israeli Targets 40

XII. Pro-Palestinian Targets..42

XIII. Other Targeted Sites...49

XIV. Tools...50

XV. Palestinian/Israeli Conflict Timeline 56

I. Executive Summary

iDEFENSE Intelligence Services continues to monitor escalating cyber attacks between pro-Palestinian and pro-Israeli groups. This activity parallels the increase in tensions and violence on the ground. So far, pro-Palestinian attackers hit more than 166 web sites and pro-Israeli attackers struck more than 34 sites. Targets are not limited to web sites. They also include real-time chat rooms and critical infrastructure such as domain name servers. One pro-Palestinian hacker threatened distributed denial of service attacks against "Zionist" sites similar to the assaults in Feb. 2000 that disrupted Yahoo.com, CNN.com and several others.

iDEFENSE expects cyber activity to intensify and become increasingly sophisticated as attackers on both sides have time to prepare and launch more intricate assaults. High-profile web sites will continue to rank highly among potential targets. Should either side successfully deploy a self-propagating virus or Trojan horse, iDEFENSE expects damage to spread beyond their intended targets.

Information on Cyber Incidents to Date

- Number of Sites/Targets Attacked by pro-Palestinian Supporters: 166+

- Number of Sites/Targets Attacked by pro-Israeli Supporters: 34+

- Government Targets Attacked (Eight Governments): Iran, Israel, Lebanon, Malaysia, Palestine, Qatar, United Arab Emirates, US

- Geographical Ties (23 Countries): Belgium, Brazil, China, Egypt, Germany, India, Iran, Israel, Italy, Japan, Lebanon, Malaysia, Mexico, Netherlands, Pakistan, Palestine, Peru, Qatar, South Korea, Taiwan, United Arab Emirates, UK, US

- Targets Include: Web sites, e-commerce servers, email servers, Internet relay chat (IRC) servers, domain name servers (DNS), Internet service provider infrastructure, file transfer protocol (FTP) sites

- Languages Used: English, Arabic, Hebrew, Portuguese

- Attack Tools Used: 16+

Pro-Palestinian Attackers – Percent of Targeted Sites within a top-level domain
(does not include every attack or take into consideration repeat attacks)

- .il (Israel): **42 percent**
  .co.il (59 percent)
  .ac.il (21 percent)
  .gov.il (13 percent)
  .org.il (4 percent)
  .k12.il (2 percent)
  .idf.il (1 percent)
- .com (commercial): **19 percent**
- .org (organizations): **9 percent**
- .in (India): **5 percent**
- .us (United States) and .sk (Slovak Republic): **3 percent each**
- .edu (education), .net (network), .gov (US government) and .my (Mylasia): **2 percent each**
- .eg (Egypt) and .cn (China): **1 percent each**
- .br (Brazil), it (Italy), .de (Germany), .jp (Japan), .qa (Qatar), tw (Taiwan), .cz (Czech Republic), .si (Slovenia), .pe (Peru), .be (Belgium), .nl (Netherlands) and .mx (Mexico): **0.7 percent each**

Pro-Palestinian Attacks by Top-level Domains

Legend:
- .il (Israel)
- .com (commercial)
- .org (organizations)
- .in (India)
- .us (United States)
- .net (network)
- .gov (US government)
- .edu (education)
- Other countries

Pro-Israeli Attacks by Top-level Domains

Legend:
- .com (commercial)
- .org (organization)
- .net (network)
- .ir (Iran)
- .pk (Pakistan)
- .ps (Palestinian Territories)
- .edu (educational)
- Other countries
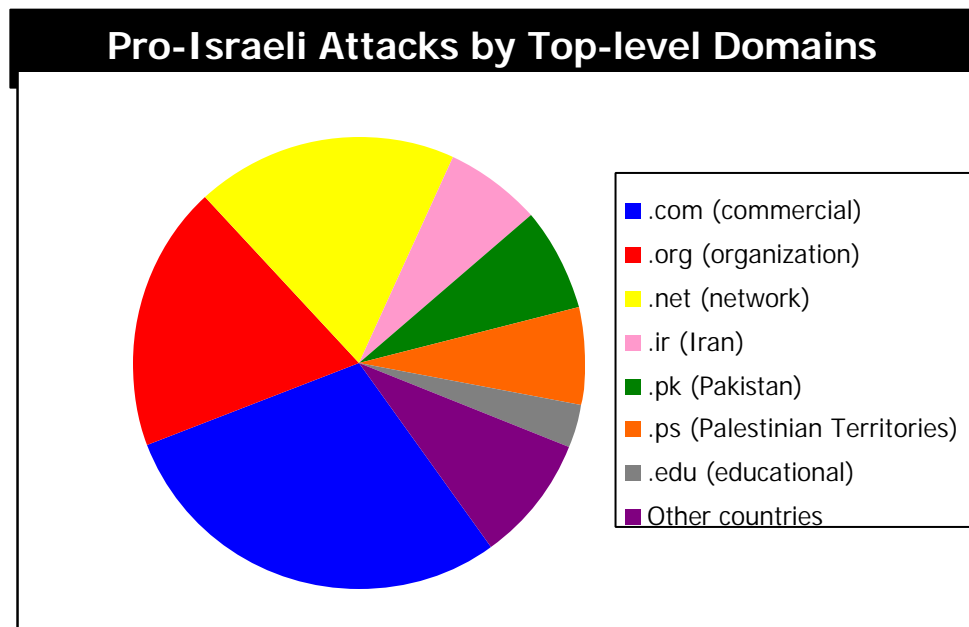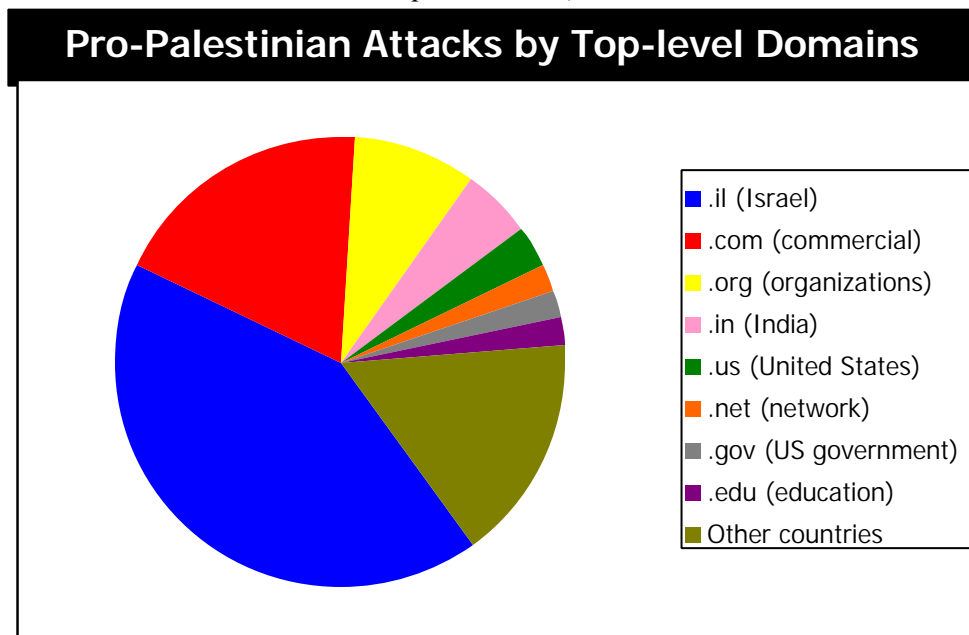
Pro-Israeli Attackers –
Percent of Targeted Sites within a TLD
(does not include every attack or take into consideration repeat attacks)
- .com (commercial): **29 percent**
- .org (organization) and .net (network): **19 percent each**

- .ir (Iran), .pk (Pakistan) and .ps (Palestinian Territories): **7 percent each**
- .lb (Lebanon), .qa (Qatar), .edu (US education) and .ae (United Arab Emirates): **3 percent each**

Pro-Palestinian Attackers – Targets by Sector

(does not include every attack or take into consideration repeat attacks)

- Corporate: **51 percent**
  Technology (49 percent)
  Telecommunications (23 percent)
  Other (6 percent)
  Media (3 percent)
  Financial, Entertainment, Health (2 percent each)
  Fashion (1 percent)
- Educational: **21 percent**
- Government: **10 percent**
- Other: **7 percent**
- Religious: **4 percent**
- Organizations/Associations, Institutes/Scientific: **3 percent each**
- Political: **1 percent**

Pro-Palestinian Attacks by Sector

Legend:
- Corporate
- Education
- Government
- Religious
- Organizations/Associations
- Institutes/Scientific
- Other
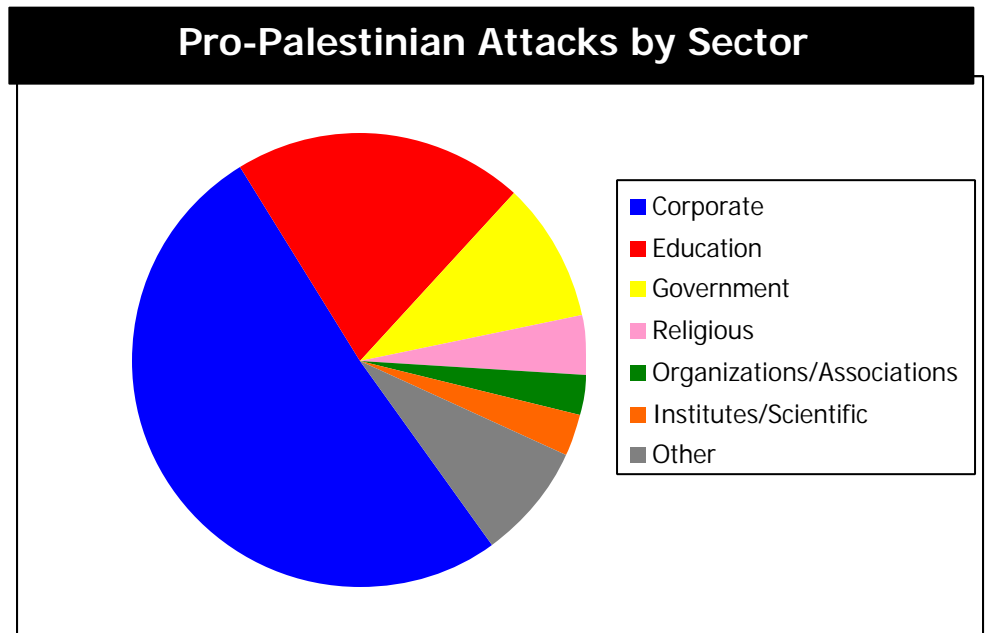
Pro-Israeli Attackers – Targets by Sector

(does not include every attack or take into consideration repeat attacks)

- Terrorist/Extremist: **39 percent**
- Government: **26 percent**
- Corporate: **16 percent**
- Religious: **9 percent**
- Educational: **3 percent**
- Other: **7 percent**

Pro-Israeli Attacks by Sector

Legend:
- Terrorist/Extremist
- Government
- Corporate
- Religious
- Education
- Other
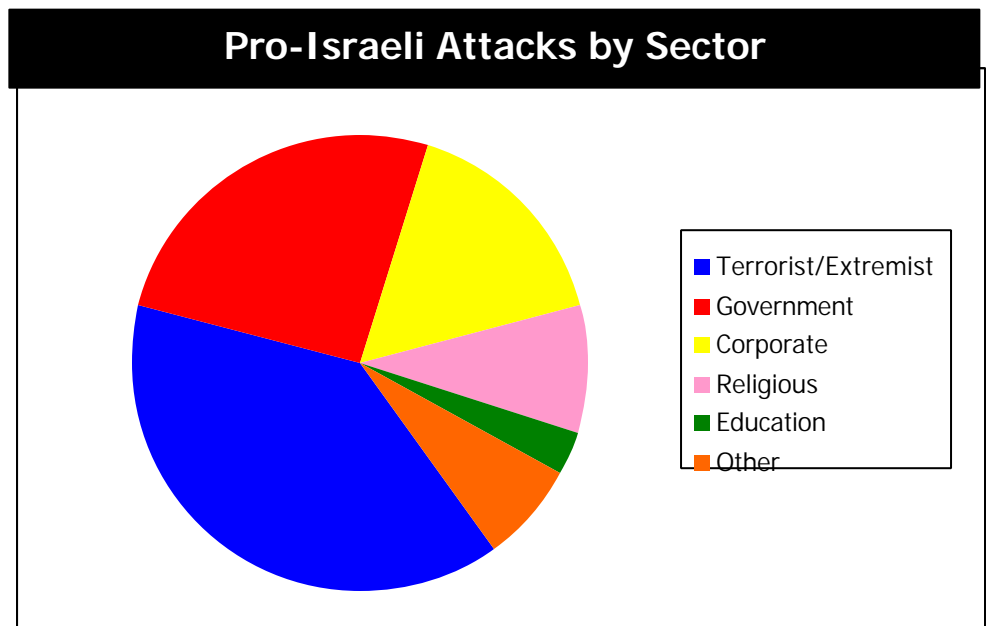
II. Overview

Despite 3 months of relentless cyber attacks by pro-Israeli and pro-Palestinian attackers, the conflict shows no sign of abating. New targets, tools, tactics and actors continue to appear almost daily.

The current Israeli-Palestinian Cyber Conflict moved into full swing shortly after pro-Israeli attackers placed FloodNet-type denial of service attack tools on a web site called Wizel.com on Oct. 6, 2000. The attack tools targeted six different Hezbollah sites as well as Hamas.org, PNA.org, Palestine-info.net and Moqawama.org.

Pro-Palestinian attackers quickly retaliated by attacking Wizel.com and a wide range of other Israeli sites. As of Dec. 27, 2000, iDEFENSE identified pro-Palestinian attacks against more than 166 web sites and pro-Israeli attacks on more than 34 sites. This activity parallels the increase of tensions and violence on the ground.

Attacks by the pro-Palestinian supporters have been the most numerous and pervasive with targets in more than 19 countries. Sites within Israel's assigned .il top-level domain extension have been the hardest hit, accounting for 42 percent of the attacked sites. Of the attacks on .il sites, 59 percent have been on .co.il sites, 21 percent on .ac.il, and 13 percent on .gov.il. The second most attacked top-level domain extension is .com, accounting for 19 percent of the attacks. Sites with the .org top-level domain accounted for 9 percent of the targets and .in sites accounted for 5 percent.

Attacks by pro-Israeli supporters began to reach out beyond the terrorist/extremist and Palestinian government sites around mid-November. While the number of attacked sites is climbing, it remains significantly lower than the number of sites hit by the pro-Palestinian attackers. Twenty-nine percent of the sites attacked by the pro-Israelis have been within the .com commercial top-level domain name. Sites with the .org top-level domain accounted for 19 percent of the targets. Iran's .ir and Pakistan's .pk sites accounted for 6 percent each.

The commercial sector is bearing the brunt of the pro-Palestinian cyber assault. Fifty-one percent of the attacks have been against corporate sites as of Dec. 28, 2000. The technology and telecommunication industries have been hit hardest so far, at 49 percent and 23 percent respectively. Financial, media, health and other industries were also hit, but to a much lesser extent. Educational sites followed commercial targets, accounting for 21 percent of the attacked sites. Government targets ranked third on the list at 10 percent, but this does not account for repeat attacks, such as those experienced by Israeli government sites. Religious, scientific, associations and political sectors all came in below 5 percent. Ten percent of the sites attacked were "American."

This same type of target demographic can be expected in a campaign directed against the US, should attentions move in that direction. If the US were to become involved in activity in the region which generates a significant level of outrage in the Muslim extremist community, there is a distinct possibility that US government and commercial organizations will face cyber attacks

much like those hitting Israeli sites today. One event that would generate such a response is a US attack on terrorist targets in Afghanistan in response to the bombing of the USS Cole. Concentrated cyber attacks could begin within 24-48 hours of such an event. As in the current conflict, these attacks will run the full range from denial of service attacks to defacements to malicious system penetrations.

The pro-Israeli attackers focused their campaign in the beginning of the conflict on terrorist/extremist sites, hitting many of the Hamas and Hezbollah mirror sites. Thirty-nine percent of the sites attacked by the pro-Israelis falls into this category. Government sites accounted for 26 percent of the attacked sites and religious targets came to 9 percent. So far attacks have targeted sites in more than eight countries.

Both sides have also taken to attacking each other's web pages, IRC channels and email addresses.

The coordinated and more sophisticated attacks by the pro-Palestinians are focused on government sites, high-profile sites and those that are believed to be able to cause either financial loss or damage to the Israeli communications infrastructure. The majority of the sites hit by defacements have been more targets of opportunity (e.g., a web site with a known vulnerability) than the result of dedicated efforts on those specific sites.

One pro-Palestinian hacker, ReALiST, threatened distributed denial of service (DDoS) attacks against "Zionist" sites. Similar DDoS assaults in Feb. 2000 that disrupted Yahoo.com, CNN.com and several others. Since the beginning of the conflict, iDEFENSE has monitored a full range of cyber attacks and threatened tactics including web site defacements, FloodNet-class attacks, system penetrations, SYN flood attacks, time-delayed malicious code, ping attacks, disinformation campaigns, allegations of virus use, and a variety of others.

Analysis by iDEFENSE identified a number of key players and organizations involved in the attacks. Pro-Israeli individuals and groups include Wizel.com, a.israforce.com, SmallMistake, Hizballa - No More, Nir M, lion&type_o ha k'eil, Israel Hackers Unite and Mike Buzaglo. Pro-Palestinian individuals and groups include ReALiST, PROJECTGAMMA, dodi, UNITY, Xegypt, Hezbollah, Ummah.net, Arab Hax0rs, GForce Pakistan, World's Fantabulous Defacers (WFD) and al-Muhajiroun. The active support by al-Muhajiroun for the current cyber activity is significant due to the group's well-known history of supporting traditional terrorist actions as well as its ties to Osama bin Laden.

Headquartered in London, the leader of al-Muhajiroun in the UK is Anjem Choudary. Al-Muhajiroun boasts chapters in Pakistan, the US and other countries. Sheikh Omar Bakri Mohammed is a key leader in the group.

Al-Muhajiroun hosted a 1998 conference in which Hamas and Hezbollah—as well as Egyptian and Algerian fundamentalist groups—took part. Al-Muhajiroun has continued to be a major player in the jihad movement by trying to unify the "jihad" campaign against the US and Israel. Group representatives said the US, Israel, Russia and Britain have declared war on Islam. The

British Charity Commission reportedly withdrew al-Muhajiroun's charity license around Nov. 1999. The licenses for the Sharia Court of the UK and the London School of Sharia were also revoked. Sheikh Omar Bakri Mohammed supervises all three organizations.

ReALiST claimed responsibility for the pro-Palestinian web page defacements against Egynile.com and Cairo.eun.eg/hacked.asp. He is a member of the Xegypt hacker group. In a message posted to an Arab hacker bulletin board, ReALiST said, *"I'm thinking of something like DDoS, on major Israel networks and sites, and sending emails helping all Arab ISP's and sites for more security, we will just tell them what we know... I'm thinking of installing TFN3K servers and doing the cnn.com and Yahoo.com thing again any one in, mail me quick."*

iDEFENSE has confirmed the existence of TFN3K but has not yet confirmed ReALiST's possession of or ability to deploy the tool effectively.

A FloodNet-type tool known as "defend" is being used by a number of pro-Palestinian groups to attack a dozen different targets. At least three different versions of the tool exist, with each successive version adding sites to its target list. The tool is simple in nature and its effectiveness depends on the number of participants simultaneously engaged in the attack. It uses a new method to defeat caching problems experienced by cyber activists in the past. During an attack, defend requests non-existent pages on targeted sites by calling for URLs that include the current date and time. The pro-Palestinians have mirrored the attack tool on Angelfire.com, Tripod.com, Ummah.net, Jumpfun.com and other hosting sites.

Despite the fact that Wizel.com was eventually forced offline, apparently by a pro-Palestinian counterattack, pro-Israeli attackers have managed to sustain FloodNet-type attacks as well. Using a slightly different version of "defend," attacks were running at one point against at least six different pro-Palestinian sites. The tool has been mirrored on Nana.co.il, Online.no and some .to hosting sites.

One pro-Palestinian protester has called the current actions an "e-jihad." The term "cyber jihad" has also appeared on mainstream fundamentalist bulletin boards and email lists.

Pro-Israeli attackers effectively incorporated a disinformation element into their cyber campaign by registering and setting up a series of web pages similar in name to actual Hezbollah sites. These imposter sites—hizballa.org and hizballa.com—present decidedly pro-Israeli messages to the visitor rather than the expected Hezbollah message.

In a noteworthy escalation of the campaign, a group of Pakistani defacers known as GForce Pakistan entered the fray on Nov. 3. The group wasted little time, defacing six sites in one day and maintaining a high level of activity in the following days. The Pakistan Hackerz Club (PHC) and the duo m0r0n and nightman also became actively involved.

Pro-Israeli defacers lion&type_o ha k'eil responded by defacing the web site of the Iranian Agriculture Ministry and posting a message threatening to launch attacks against Lebanese,

Iranian and Pakistani sites if GForce Pakistan did not back down. In the following days, other pro-Israeli groups attacked official Iranian sites as well, further broadening the conflict.

Current attacks could affect not only those targeted, but also other sites and services that rely on the same connections, bandwidth and DNS servers to access the Internet. NetVision reportedly hosts and provides connectivity to 70 percent of Israel's Internet users. The Israeli ISP reported significant difficulties in servicing its customers due to the heavy traffic sent to the targets hosted on its servers. Inconet, an ISP in Lebanon, has also reported bandwidth problems due to attacks against some of the Hezbollah sites located on its servers.

iDEFENSE Intelligence Services has confirmed that a pro-Palestinian attack site is making available the LoveLetter, CIH and Melissa viruses, along with 12 Microsoft Word macro viruses, for use in attacks against Israelis. Visitors to the site are greeted with the message, "I swear that I will not use these programs on anyone but Jews and Israelis." This marks the first confirmed distribution of viruses for use in the current cyber conflict by either side.

Sixteen different attack tools are in active distribution among the attackers with many others being discussed or suspected of already being deployed. Tools identified include EvilPing, WinSmurf, HTTP Bomber 1.001b, FakeMail, MailBomber, Attack 2.5.1, defend, PutDown and QuickFire. iDEFENSE is also monitoring a coordinated effort to identify vulnerable Israeli systems and gain root access to them.

The pro-Palestinian group UNITY has divided its "public" attack strategy into a series of phases. Phase 1 was focused on official Israeli government sites. Phase 2 added such financial targets as the Bank of Israel and Tel Aviv Stock Exchange. Phase 3, beginning in late October, shifted to the telecommunications industry, naming Lucent and a number of Israeli ISPs as targets. The group announced the intent of Phase 4 when Phase 3 was initiated, but has yet to launch it. Phase 4 is designed to target "Zionist" e-commerce sites in order to cause as much of a financial loss as possible to affect their ability to support the Israeli security forces on the ground.

Taking their own initiative, pro-Palestinian defacers m0r0n and nightman of the World's Fantabulous Defacers (WFD) group announced on Dec. 27 the beginning of Phase 5. This latest phase is designed to promote "global awareness" of Israel's actions through web page defacements and other cyber attacks. It is not yet clear when UNITY intends to launch Phase 4 e-commerce attacks.

In addition to the obvious risk to sites perceived to support any one side of the conflict, high-profile web sites may find themselves targeted simply because attackers find them an effective means to garner attention for their causes. The likelihood that pro-Palestinian attackers will step-up attacks against US government sites is also high.

The cyber conflict will intensify as political tensions in the region heighten. Support for the cyber campaign will also grow among other high-profile Muslim extremist groups, many of which have a strong presence on the Internet. Attacks used by one side against the other are

likely to be turned around in a matter of hours, depending upon the amount of customization and set-up time required.

The sophistication of attacks is expected to increase as attackers on both sides have time to prepare and launch more intricate actions. In the event that either side deploys viruses or Trojan horses, infections will not remain confined to their intended targets. Such cyber assaults will likely spread to the Internet as a whole, infecting systems worldwide.

III. Points for Consideration

- The current Israeli-Palestinian cyber conflict is pulling "ethical" Arab and Israeli hackers into the fight, primarily because each side perceives their efforts to be defensive actions rather than offensive or "unethical."

- Sympathetic hackers and others around the world have begun to offer their services and enter the fray as the profile of the conflict continues to grow.

- Tactics used by either side could quickly be targeted against any government, corporation or organization, should their profile rise high enough in the attack group circles. Warning before such an attack is unlikely.

- In the event that either side successfully deploys self-propagating viruses or Trojan horses, infections will not remain confined to their intended targets. Such tactics could pose problems for users around the world.

- The current campaign will help preexisting, as well as newly formed groups, with recruiting and fundraising.

- Muslim extremist groups are believed to be identifying particular pro-Palestinian attackers or groups and provide them with funding and/or resources.

- The cyber conflict is serving as a proof of concept for rebel, terrorist, activists and other disenfranchised groups around the world. It is at the same time serving as a test bed for both offensive and defensive tactics that are likely to be used or built upon during the next similar conflict.

IV. Pro-Israeli Actors

Digibrain & haboshnik

Posted in a message on Oct. 16, 2000: *"we are working on a softwhear that will give you control on the hizzballa's ftp with out a password. FUCK HIZZBALLA!!! sincerly digibrain & haboshanik (we are the domain masters)."*

Hackers of Israel Unite

Hackers of Israel Unite is believed to be a new group formed in response to pro-Palestinian attacks against Israeli sites. The group said on its site on Nov. 6, 2000, *"Ok all my israely hackers We are now becoming an army Of the israely Soldiers on the net Our Troopers Canot Die Just Their Computers can burn! Or a site is going to crash! We Are the Israely Soldiers of The internet Our goal is to search and destroy All Of the Arab's Sites on the net! Or to Del as many of the arabs Computers To kill their Chats and icq's. I need help on the web… So if you can send me javas Source I need a java That Does A ping! AnyOne that can help will become a member AnyOne that wants Can Become a Soldier we don't have tests but you need tools to fight! All you need to have is a computer and a shell And revenge! (or a fast modem at home)"*

The group called for attacks against www.pna.gov.ps, www.almanar.com.lb, www.sis.gov.ps, www.irna.com, and www.albawaba.com. Hackers of Israel Unite is the first group on either side to call for attacks against chat rooms and ICQ. Around Nov. 12, the group began distributing WinSmurf through its www.israelhackers.clb.net site. The group claimed that is was successfully able to down one Arab site with WinSmurf using only a 56K dial-up connection and an ADSL line.
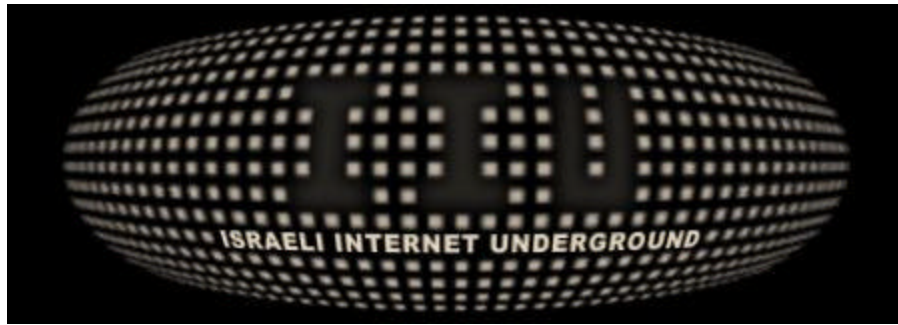
Hizballa - No More

Runs an Israeli attack site advocating ping flood attacks against Hezbollah, Hamas and other pro-Palestinian sites.

Israeli Internet Underground (IIU)

Site: http://www.iiu.org.il

The Israeli Internet Underground was formed by a group of "white hat" hackers in response to attacks by pro-Palestinian attackers. The group is working to identify vulnerabilities in Israeli sites and secure them through its SODA Project, in conjunction with Israeli computer security company, 2XS.

israforce

An Israeli attack site advocating ping flood attacks against Hezbollah, Hamas and other pro-Palestinian sites.

lion&type_o ha k'eil

On Nov. 4, 2000, lion&type_o ha k'eil defaced the site of the Iranian Ministry of Agriculture at www.moa.or.ir in support of the Israelis. lion&type_o ha k'eil threatens to take down .ir and .lb sites and then .pk sites if Gforce Pakistan keeps defacing .il sites.

Mike Buzaglo

A 21-year old Israeli took credit in an interview on Israel TV for first sabotaging the Hezbollah site. He said that he and some of his friends broke into the site and replaced its content with the Israeli flag and the Star of David. In an interview with CNN, Buzaglo said, *"We, the Israeli hackers, need to show the right pictures and we will not give a chance, for example, to a Hezbollah site that will show propaganda against Israel. So this is the reason why I decided to attack a couple of Hezbollah sites."*

In earlier interviews Buzaglo said, *"You cannot be perfectly safe. Any system can be infiltrated. There is a war of brains going on here."*

On Nov. 3, 2000, Buzaglo said that he stopped hacking anti-Israeli web sites but will continue his war of words on his own site.

m0sad

On Dec. 3, 2000, m0sad defaced the Ministry of Awqaf and Islamic Affairs, Qatar site at http://www.islam.gov.qa in support of the Israelis. m0sad wrote in the defacement, *"Now only information has real cost. And it cannot be guarded by armed squad or even by the goverment special forces. One man can destroy an whole company with one click. Remember about it..."*

Nir M

Claimed credit for defacing the al-Manar site on Oct. 29, 2000.

Polo0

Polo0 reportedly posted the following on the Internet: Several Palestinian officials' cell phone numbers, instructions on how to access Palestinian fax, telephone systems, 24 web sites, 15 Internet relay chat (IRC) channels and the IRC server.

Wizel.com

Site was used by pro-Israeli supporters to host a FloodNet class attack tool, beginning on Oct. 6, 2000. The site's main logo says, *"ATTACK & DESTROY HiZBALLAH."* The site eventually went down after a pro-Palestinian counterattack. The site contained pages both in English and Hebrew. Wizel.com initially targeted six Hezbollah sites, Hamas.org, the Palestinian National Authority at pna.org, Palestine-info.net and Moqawama.org through a FloodNet type tool. The site is hosted by host4u.net in the US. The site claimed to have received 21,800 visitors between Oct. 6 and Oct. 24, 2000.

V. Pro-Palestinian Actors

al-Muhajiroun

Site: http://www.almuhajiroun.com

A Muslim extremist group headquartered in London. The leader of al-Muhajiroun in the UK is Anjem Choudary. The group has chapters in Pakistan, the US and other countries around the world. Sheikh Omar Bakri Mohammed is a key leadership figure in the group. The group is tied to a number of Muslim terrorist organizations and has contact with Osama bin Laden.

The group hosted a conference in 1998 in which Hamas, Hezbollah, and Egyptian and Algerian fundamentalist groups took part and has continued to be a major player in terms of trying to unify the "jihad" campaign against the US and Israel. The group has stated that the US, Israel, Russia and Britain have declared war on Islam.

The British Charity Commission reportedly withdrew al-Muhajiroun's charity license around Nov. 1999. The licenses for the Sharia Court of the UK and the London School of Sharia were also revoked. All three organizations are supervised by Sheikh Omar Bakri Mohammed. Commenting on the loss of the licenses Sheikh Omar Bakri Mohammed said, "the withdrawal of the Sharia Court's license is part of the attempt to tighten the noose on Islamists in Britain." He added that "in the past, we used to work within the legal limits, but it seems that from now on we have no other option but to work outside the allowed limits."

The following message was issued to the members of al-Muhajiroun: *We urge you to participate in Phase II of the counterattack against Israeli sites attacking the Moqawama (Islamic Resistance) sites. Enter these web pages and press 'defend the resistance'. A file will start attacking the Israeli Websites as long as you are connected to the net. Open as much windows as you can. http://members.tripod.com/irsa2001, http://www.angelfire.com/oh4/irsa2000, http://irsa2000.jumpfun.com*"

Arab Hax0rs

In a message posted to the Arab Hackers Organization bulletin board on Oct. 22, 2000, Arab Hax0rs claimed responsibility for downing the site at www.gilo.jlm.k12.il. It is not clear at this point if Arab Hax0rs is an individual or group.

Boss

Associates: tR|cky, KUCAU

On Nov. 8, 2000 tR|cky, Boss and KUCAU defaced www.order-click.co.il and www.dilim.co.il in support of the Palestinians.

BrakeOff

BrakeOff began defacing sites in support of the Palestinians on Dec. 19, 2000. BrakeOff is a member of the World's Fantabulous Defacers (WFD).

core Hackers (cH)

Members: tR|cky, xoid

tR|cky has carried out a number of defacements in support of the Palestinians.

[^CyBeRpUnK^]

On Dec. 2, 2000, [^CyBeRpUnK^] defaced the Hebrew University of Jerusalem, Israel site at http://shemesh.fiz.huji.ac.il and the www.as.huji.ac.il site with a pro-peace message. Since then, [^CyBeRpUnK^] -- a member of the World's Fantabulous Defacers (WFD) -- has begun to deface sites with pro-Palestinian messages. The change in [^CyBeRpUnK^]'s messages began to occur after m0r0n and nightman joined the WFD.

DevilSoul

Members: NiTR8

Suspected of entering the conflict on the pro-Palestinian side on Nov. 12, 2000. NiTR8 defaced two Iranian sites on the first day. It is not clear why the Iranian sites were targeted as opposed to more traditional pro-Palestinian targets.

Doctor Nuker

Associations: Member of the Pakistan Hackerz Club (PHC)

On Nov. 2, 2000, Doctor Nuker broke into the American Israel Public Affairs Committee site at www.aipac.org and posted pro-Palestinian messages in addition to the credit card numbers and contact information of those who purchased items through the site, member contact information, and thousands of email addresses of individuals who signed up to receive email alerts. On the defaced site Doctor Nuker said, *"This is to inform you that the www.aipac.org web site server is hacked..the web site defaced and all of their users database is compromised. Yes, that includes not only users personal information but their credit card numbers too (that implies to people who have subscribed to their services)... I've put all the email addresses in a file so that you can have an nice mailing list of 3500+ people... The hack is to protest against the attrocities in Palestine by the barbarian Israeli soldiers and their constant support by the US government."*

dodi

dodi has claimed responsibility for defacing three sites and has threatened to take down NetVision's entire network. In his defacement of the Ebrick Inc. web site at http://lotus.ebrick.com, dodi wrote, *"The time is Sat Oct 21 20:04:22 2000 all of Israels NetVision backbone is offline as of this minute. For those of you who don't know NetVision is the largest internet provider is israel and is host to most of Israels government/comercial networks. NetVision is also the largest public isp in israel and has many dialup access pads and even an dsl network. I think my point is clear... if an islamic site is attacked I down/drop all of israel :)."*

dodi's first defacement in the current conflict occurred Oct. 12, 2000 when he defaced the Israeli Academic Sub-Domain at www.netanya.ac.il. On Oct 20, 2000, dodi defaced www.jmjservices.com, www.watersportsworld.com and lab.cvdds.com with the same anti-Israeli message.

On Nov. 3, 2000, in a web page defacement of the COGNIFIT site at www.cognifit.co.il, pro-Palestinian hacker dodi recommended all wanting to carry out attacks against Israeli sites to launch SYN flood attacks using the "juno" or "slice" SYN flooder tools against two Domain Name System (DNS) servers run by the NetVision ISP.

dodi wrote, *"For people wanting a method to easily disable jewish government web pages try hitting dns.netvision.net.il & nypop.elron.net on port 53 with a SYN flooder (I recommend juno or slice) 300 k/sec on each port should see both boxes offline. Doing this ensures no one can resolve any web sites these two nameservers are authoritative to unless they are already cached of course."*

An attack of this type against NetVision, which reportedly hosts 70 percent of all the web sites in Israel, could have serious consequences on sites in the region. dodi also wrote, *"this isn't just a war against 'israel' for the perpatrators of the attrocities in palestine are US backed. Its America which has blood on its hands the blood of innocent women and children."*

ISPs should be prepared for this type of attack over the coming days and weeks. Governments, corporations and other organizations should understand their critical dependencies on their ISPs and make sure the proper contingency plans are in place should any domain name or other problems arise.

iDEFENSE has also examined a portion of shell code that was posted on the COGNIFIT defacement. Preliminary analysis of the code indicates that if placed onto a system it would, at a specified time, delete essentially all files on the computer except the operating system. It would then execute an attack tool, if it is located in the local directory, and begin to attack a targeted site. The code examined by iDEFENSE executes the "juno" SYN flooder and begins an attack against the www.idf.il site on port 80. This could easily be modified, however, to utilize a different tool and target any site the attacker wished.

dodi and other attackers may have installed such code on previously compromised sites or may begin to do so. Organizations whose sites have been targeted or are victims of attacks connected to the current Israeli/Palestinian cyber conflict are advised to immediately search for a file called "isat." Companies are also advised to examine all "cron" and "at" jobs to see if anything unusual is set to run.

dodi has made claims of being able to shut down NetVision. dodi also said in the COGNIFIT defacement, *"Netvision.net.il's backbone was held down for another hour leaving many .gov.il web sites inacessible. Expect more in the coming weeks. This time even the uunet peering router was badly lagged. As for www.idf.il I don't care where you move your propaganda machine I will continue to take it out."*

While iDEFENSE has not confirmed dodi's technical abilities, dodi's threat against the US is of concern. NetVision has confirmed that it has had difficulty dealing with the heavy loads of incoming traffic targeting official Israeli web sites. It is not clear if this is the result of efforts by dodi, other pro-Palestinian attackers, or some combination of both.

In the COGNIFIT defacement, dodi gave "shouts" to Pakistan Hackerz Club (PHC), GForce Pakistan, Hamas, Hezbollah and Osama bin Laden.

EDGE

Associates: KARTOOS.AK.47

EDGE began defacing sites in support of the Palestinians on Dec. 21, 2000 along with KARTOOS.AK.47. The two have hit sites in both Germany and Japan so far. In December 2000, EDGE and KARTOOS.AK.47 formed a group called THE SCYTHE.

Kala

On Oct. 30, 2000, Kala defaced the Netanya Academic College site at mars.netanya.ac.il in support of the Palestinians. Kala claims to be from Hungary.

KARTOOS.AK.47

Associates: EDGE

KARTOOS.AK.47 began defacing sites in support of the Palestinians on Dec. 21, 2000 along with EDGE. The two have hit sites in both Germany and Japan so far. In Dec. 2000, EDGE and KARTOOS.AK.47 formed a group called THE SCYTHE.

Kr4kr0k Industries

On Dec. 20, 2000, Kr4kr0k Industries defaced Arttalk.com at http://www.arttalk.com in support of the Palestinians, stating *"The situation in the middle east has gone on for long enough. Palestinians are dying at Israeli hands and the world just lets the whole thing go in one in ear and out the other. Jews are not Gods holy people, nor are they special. What gives them any right to take an innocents life anymore than the next guy. Nothing! That is why Israel needs to stop now. The stage has been set for many years now for the Israelis to have a peacefull resolution, and they have answered yet again with bullets, explosives, and hate. Is this really a holy people? I don't think so. Nuff said."* The group also said in the defacement, *"security and html provided by antibi0sis."*

KUCAU

Associates: tR|cky, Boss

On Nov. 8, 2000 tR|cky, Boss and KUCAU deface www.order-click.co.il and www.dilim.co.il in support of the Palestinians.

GForce Pakistan

Site: www9.50megs.com/gforce/mirror.htm
Members: sniper, heataz, Rsnake, instinct, miller, rave, nicks xtremist

On Nov. 3, 2000, Pakistani hacker group GForce Pakistan joined the fray on the pro-Palestinian side. It began defacing Israeli sites: *"GForce Declares a War against Israel?.… Ok, GForce Pakistan is back. We really planned not to come back to the defacing scene again, but once again our Muslim brothers needed us."* This is likely to sizably increase the number of web page defacements and is also likely to contribute to other attack efforts.

On Nov. 4, the group defaced the sites of Jen Communications at www.jen.co.il, Health Infosystems Association Israel at www.healthinfonet.co.il, Visiting Israel Students Association at www.visa.org.il, Jewish Bible Association at www.jewishbible.org, and shemayisrael.co.il.

The addition of nicks xtremist to the group was announced in the Nov. 8, 2000 defacement of the Ornetix site at ntserver.ornetix.co.il and in the defacement of the Radwiz (IL) site at www.radwiz.co.il. Also on the same day, GForce Pakistan threatened to launch attacks against DNS servers and NetVision. The threat was made in a defacement of the Terminal-Computers & Multimedia site at www.terminal.co.il and a defacement of the Rooster site at mail.rooster.co.il.

Hezbollah

Hezbollah, or Party of God, was formed in reaction to the Israeli invasion of Lebanon by the IDF in 1982. They are seen as a radical Shia group dedicated to the "creation of Iranian-style Islamic republic in Lebanon and the removal of all non-Islamic influences from the area." Sheik Rafheb was seen as the leader of Hezbollah until his slaying in 1984. His successor, Sayyid Abbas al-Musawi, lead the group in its "liquidation of Israel" until his killing in Feb. 1992. Sheik Hassan Nasrallah, Mussawi's successor expressed, "The only way to achieve a lasting peace in the Middle East is to return all the Jewish occupiers to the lands from which they originally came."

Strongly anti-West and anti-Israel, Hezbollah is closely allied with, and often directed by, Iran. Hezbollah has created its own influence within Lebanon, politically, militarily, and socially. Hezbollah believed to have several thousand members, operating in the Bekaa Valley, the southern suburbs of Beirut, and southern Lebanon. They also have established operations in Europe, Africa, South America, North America, and Asia. Hezbollah receives substantial amounts of financial, training, weapons, political, and organizational aid from Iran and Syria. In recent years, they have used the Internet to successfully advocate their beliefs.

Hezbollah's web site provides detailed information and news on the group's policies and its web site is widely used for its campaign against Israel. Ali Ayoub, Hezbollah's webmaster stated, *"We will never give up the Internet."*

On Oct. 7, 2000, Hezbollah stated that its web site at www.hizbollah.org and www.hizballah.org crashed after allegedly receiving millions of hits from Israel and the US. Ayoub, stated *"We have names of 8,521 servers mainly in these two countries that have been hitting our web site regularly and sending us simultaneously tens of thousands of hostile emails, some of them carrying viruses to sabotage our server."*

In addition, pro-Israel individuals have allegedly set up several decoy sites, attempting to take advantage of misspellings. One site, www.hizballa.org, contains an Israeli flag with the word "WAR" displayed in flames above, while pro-Israeli music is played in the background. In addition, hizballa.com reads, *"The Official Site of The God's Party, We are sorry to say Israel was write. The land of Israel belongs to the people of Israel."*

Iron Guards

Group organized and recruited for by UNITY. Began its first announced action during early Nov. 2000. The group is the result of an organized recruiting campaign by UNITY for skilled hackers

and crackers. It is involved in more technically sophisticated attacks that may or may not follow the publicly announced cyber attack plan by UNITY.

Kuds

Distributor of HTTP Bomber 1.0 and HTTP Bomber 1.001b. The kuds.8k.com site was taken down and they relocated the main page to kuds.8m.com. The group continued to utilize the admin@kuds.8k.com email address however. The kuds.8k.com site was taken offline sometime on or before Nov. 7 and the kuds.8m.com site was confirmed as being live by iDEFENSE on Nov. 7. As of late Dec. 2000, the kuds.8m.com site was down. It is not clear where or if the group relocated site again.

lovenectar

Sites: http://www.fightisrael.com

Runs the attack site, FightIsrael.com. Site is a distribution point for EvilPing, WinSmurf and HTTP Bomber 1.01.

m0r0n

Associates: nightman

On Oct 31, 2000, m0r0n and nightman defaced two MBA International School of Business Administration Management sites at www.eiba.biu.ac.il and www.mba.biu.ac.il in support of the Palestinians. On Nov. 2, m0r0n and nightman defaced the Shenkar College site at www.shenkar.ac.il. On Nov. 3, m0r0n and nightman defaced the site of the Yizrael Valley College (Mihlelet Emek Yizrael) at www.yvc.ac.il and Israeli Academic site at www.yvc.ac.il. On Nov. 4, m0r0n and nightman defaced the sites of www.bayan.co.il and www.caspit.co.il. On Dec. 1, 2000, m0r0n and nightman defaced the site of the SOMA Gallery in Northport, NY, at http://www.somagalleries.com. The defacement marked an announcement that m0r0n and nightman are joining with the "World's fantabulous defacers" (WFD). The hack, which include Macromedia Flash animation, stated: *"we will be defacing for them because they are helping us spread the word. Anyone interested in helping us spreading the word is most welcome."*

On Dec. 27, 2000, m0r0n, nightman, and fighter4Isl@m announced the beginning of Phase 5 for the pro-Palestinian side in a defacement of the www.order-click.co.il site. The message read, *"Note to All Pro-Palestinian Hackers Involved in the Cyber-War: Just a few weeks ago, you will recall that Unity was leading this war. Unity's voice apparently was silenced by the Zionists and their supporters and their site as a result was taken down. Their needs to be unity among us, for we are indeed one brotherhood, and whether we are Pakistani, Arab, African, Brazilian, or any other nationality, we are fighting for the one and the same purpose. Their needs to be a leader in this fight, and we are going to try to take a leading role in this war. Phase 4 by Unity was originally planned to cause Israeli companies and organizations immense economic losses. Whether or not this phase actually went forward or not, we need to move on with Phase 5. Phase 5 'Global Awareness' involves exactly what the name implies, awarness in every sector and realm of the Internet about the truth about what is occuring in Palestine. After an anonymous*

Israeli hacker defaced Hizballah on December 26, we decided to move forward with this phase. Global Awareness constitutes everything from email bombs to message board postings to defacements. Defacement is the weapon of choice. Email us at wfd2000@hushmail.com at tell us what you feel about it.

The cyberwar has not ended. It has just begun. The cyberwar will never end as long as the furious, unforgiving rockets, bullets, and missiles of Zionism fire upon the innocent Muslim and Christian children of Palestine.

Signed,

- World's Fantabalous Defacers

P.S. - Phase 5 'Global Awareness' has now been initiated. Please note that Phase 5 is planned to be a very benevolent phase, so you geezers at IDefense don't need to feel the urgency to monitor our every move. Our policy is not to destroy, but to deface. Oh yes, and if Hizballah's website is attacked again in anyway, it will be met immediately with swift retribution.

TO ADMIN: Your database has remained unharmed and untouched as have those of all our other 'victims', but if we are provoked by you or your ally organizations in any way, matter, shape, or form, we will certainly not hesitate to go beyond defacements, because we certainly have the ability to."

Murtaza Baloch aka EdGe

On Nov. 15, 2000, Murtaza Baloch (aka EdGe) defaced the www.karate.org.il site in support of the Palestinians. It has not been confirmed as to whether or not EdGe is the same EDGE that has been working with KARTOOS.AK.47.

nightman

Associates: m0r0n

On Oct 31, 2000, m0r0n and nightman defaced two MBA International School of Business Administration Management sites at www.eiba.biu.ac.il and www.mba.biu.ac.il in support of the Palestinians. On Nov. 2, m0r0n and nightman defaced the Shenkar College site at www.shenkar.ac.il. On Nov. 3, m0r0n and nightman defaced the site of the Yizrael Valley College (Mihlelet Emek Yizrael) at www.yvc.ac.il and Israeli Academic site at www.yvc.ac.il. On Nov. 4, m0r0n and nightman defaced the site of www.bayan.co.il and www.caspit.co.il. On Dec. 1, 2000, m0r0n and nightman defaced the site of the SOMA Gallery in Northport, NY, at http://www.somagalleries.com. The defacement marked an announcement that m0r0n and nightman are joining with the "World's fantabulous defacers" (WFD). The hack, which include Macromedia Flash animation, stated: *"we will be defacing for them because they are helping us spread the word. Anyone interested in helping us spreading the word is most welcome."*

On Dec. 27, 2000, m0r0n, nightman, and fighter4Isl@m announced the beginning of Phase 5 for the pro-Palestinian side in a defacement of the www.order-click.co.il site. The message read, *"Note to All Pro-Palestinian Hackers Involved in the Cyber-War: Just a few weeks ago, you will recall that Unity was leading this war. Unity's voice apparently was silenced by the Zionists and their supporters and their site as a result was taken down. Their needs to be unity among us, for we are indeed one brotherhood, and whether we are Pakistani, Arab, African, Brazilian, or any other nationality, we are fighting for the one and the same purpose. Their needs to be a leader in this fight, and we are going to try to take a leading role in this war. Phase 4 by Unity was originally planned to cause Israeli companies and organizations immense economic losses. Whether or not this phase actually went forward or not, we need to move on with Phase 5. Phase 5 'Global Awareness' involves exactly what the name implies, awarness in every sector and realm of the Internet about the truth about what is occuring in Palestine. After an anonymous Israeli hacker defaced Hizballah on December 26, we decided to move forward with this phase. Global Awareness constitutes everything from email bombs to message board postings to defacements. Defacement is the weapon of choice. Email us at wfd2000@hushmail.com at tell us what you feel about it.*

The cyberwar has not ended. It has just begun. The cyberwar will never end as long as the furious, unforgiving rockets, bullets, and missiles of Zionism fire upon the innocent Muslim and Christian children of Palestine.

Signed,

 - World's Fantabalous Defacers

P.S. - Phase 5 'Global Awareness' has now been initiated. Please note that Phase 5 is planned to be a very benevolent phase, so you geezers at IDefense don't need to feel the urgency to monitor our every move. Our policy is not to destroy, but to deface. Oh yes, and if Hizballah's website is attacked again in anyway, it will be met immediately with swift retribution.

TO ADMIN: Your database has remained unharmed and untouched as have those of all our other 'victims', but if we are provoked by you or your ally organizations in any way, matter, shape, or form, we will certainly not hesitate to go beyond defacements, because we certainly have the ability to."

Pakistan Hackerz Club (PHC)

Members: Doctor Nuker

On Nov. 2, 2000, PHC joined the fray on the pro-Palestinian side and began defacing Israeli sites.

ReALiST

ReALiST has claimed responsibility for web page defacements against egynile.com and cairo.eun.eg/hacked.asp. He is a member of the Xegypt hacker group. In a message posted to an Arab hacker bulletin board, ReALiST wrote, *"I'm thinking of something like DDoS, on major Israel networks and sites, and sending emails helping all Arab ISP's and sites for more security, we will just tell them what we know... I'm thinking of installing TFN3K servers and doing the cnn.com and Yahoo.com thing again any one in, mail me quick."*

ReALiST, along with PROJECTGAMMA, also claimed responsibility for the defacement of www.aucegypt.edu/hi.htm. When the defacement occurred is uncertain. The defaced page read: *"ReAlist+ProjectGamma Defaced This Sie,Cyber Jihad Has Begun,MicroSoft Was Hacked Why Dont You?"*

On Sept. 2, 2000, on the bulletin board of the Arab Hackers Association, ReALiST posted a message stating, *" salam y'all its really an annoying matter when i ever think of it,all the IT Rise all over the world and we are now sure electronic WAR wont be underestimated , so will there ever be arab cyber warriors to attack,defend..when it is really needed. when i see arab cyber users ,i only see Chatting,MP3's,Pornography and other trivial stuff,And Tim Is So Critical in that case,i myself will never save any piece of info or help for any wannabe or beginner,and thats what every one do... thx"*

tR|cky

Associates: Boss, KUCAU, petite_lourve, xoid

On Nov. 8, 2000, tR|cky, Boss and KUCAU deface www.order-click.co.il and www.dilim.co.il in support of the Palestinians. tR|cky is a member of core Hackers (cH). On Nov. 18, tR|cky and petite_lourve defaced the Open University-Jerusalem site at http://online.achva.ac.il.

Ummah.net

Ummah.net is a web hosting and Islamic Gateway based in the UK. The company hosts the web sites for the Muslim Hackers Club (MHC), the MHC's Houston Chapter, UNITY and other Muslim extremist sites. The site was also once home to the web pages of al-Muhajiroun and Supporters of Sharia.

UNITY

UNITY, a Muslim extremist group with ties to Hezbollah and other terrorist organizations, began "Phase 3 of its Cyber War" on Oct. 31, 2000. Phase 3 targets the Israeli ISP infrastructure through the use of the "defend" tool (Phase 3 release) and through other more sophisticated methods. Initial targets include www.lucent.com, www.webstyle2000.com, www.goldenlines.co.il and www.comsec.co.il. Other ISPs or telecommunications companies either operating in Israel or with a visible business presence in the region are also at risk. Phase 1 targeted predominately official government sites, while Phase 2 expanded the scope to include such targets as the Tel Aviv Stock Exchange and Bank of Israel.

On Oct. 31, 2000, UNITY also announced its intention to launch Phase 4 in the near future, *"we warn the Zionist and their supports that any attempt to touch any Anti-Zionist site, will be faced by phase 4 of the cyber war, which will be: 'Attacking Zionist E-Commerce' sites with millions of dollars of losses in transactions."*

UNITY has also been responsible for forming the Iron Guards group, which has been active in carrying out more sophisticated cyber attacks against Israeli sites.

Walid

Walid was quoted in the Oct. 26, 2000 edition of the Lebanese Daily Star as saying that he intended to hack into the Knesset server late on Oct 25. Walid said, *"We'll target and hack Israeli websites one by one. This will continue."* He added that the attacks may get fiercer, with an email war between Israel and Arabs seeing an exchange of viruses designed to crash systems.

World's Fantabulous Defacers (WFD)

Pro-Palestinian cracker group World Fantabulous Defacers intensified its cyber campaign since Dec. 1, 2000, when the duo m0r0n and nightman joined the ranks of the WFD. At least 64 sites were defaced in varying degrees since the beginning of the month, but all defacements called for "global awareness" in the Israeli-Palestinian conflict. WFD joined the cyber side of the conflict around Nov. 20, 2000, defacing with pro-Palestinian or anti-war content. Some content-especially the defacements from m0r0n and nightman-contained gruesome photographs. Of the 64 sites defaced since the beginning of December, a dozen were US educational institutions including kindergarten through 12th grade schools as well as colleges and universities. Six sites were governmental sites including the federal government and local municipalities. The US

Centers for Disease Control site at http://phil.cdc.gov was defaced on Dec. 23 by WFD. Most of the sites defaced—56 out of 64—were running Windows NT 4.0 with Internet Information Server 4.0. However, WFD defaced four sites running Unix: three servers running Silicon Graphic Inc.'s Irix and one running IBM Corp.'s AIX. The operating systems of the remaining servers is uncertain.

At least 11 people claim membership in WFD. Here's the current breakdown for the defacement campaign based on WFD's members:

- B_Real defaced four sites alone, but paired with Brake^Off for two defacements and CyBeRpUnK for one other defacement.

- b1n4ry c0d3 defaced only one site on Dec. 3, 2000. This defacement was the only one to refer to the WFD as the "World's Fuck Defacers."

- Brake^Off, by far, has been the most active in the defacement campaign, hitting 25 sites. Brake^Off's defacements tend to be text-only. Brake^Off's email is elbarto224@usa.net.

- CyBeRpUnK hit five sites alone. CyBeRpUnK also worked with nightman on two defacements and B_Real on one. CyBeRpUnK's email address is cyberpunk_2000@hushmail.com.

- fighter4isl@m has authored the Macromedia Flash content for some of m0r0n and nightman's defacements. On Dec. 26 and 27, fighter4isl@m was listed as an equal partner with m0r0n and nightman on two defacements.

- h3ll rais3r always works with laughing 3y3s, hitting five sites since Dec. 16.

- laughing 3y3s always defaces with h3ll rais3r, hitting five sites since Dec. 16.

- m0r0n always works with nightman. Since Dec. 1, m0r0n and nightman defaced 10 sites under the name of WFD and three sites without any mention of WFD. m0r0n and nightman's defacements have gotten more sophisticated, incorporating Macromedia Flash objects written by fighter4isl@m. Two sites—one defaced on Dec. 26 and the other on Dec. 27—added full credit to fighter4isl@m for the defacement. The email address for nightman and m0r0n is m0r0nandnightman@hushmail.com.

- nightman normally works with m0r0n, completing 10 site defacements. However, nightman executed two defacements with CyBeRpUnK. The email address for nightman and m0r0n is m0r0nandnightman@hushmail.com.

- SoFh hacked only one site and uses the email address sofh@nightmail.com.

- Tå|{ê Ñø £Øgîç defaced three sites in the campaign.

- Three defacements mention WFD and are unsigned.

WFD's attention on US institutions is cause for concern. Generally, the defacements have not been destructive, leaving original content untouched. However, defacements include content from WFD with plans for increasing defacements as 2000 ends and 2001 begins. Administrators are urged to assure all web server software has been patched and monitors throughout the holiday period and into 2001.

Xegypt

Members: ReALiST, m0h

While Xegypt itself has not formally claimed any attacks against Israeli sites, group member ReALiST has been active in support of the Palestinians. Sometime in October or November, the group's web site was forced offline. It is not clear if this was because of involvement with the cyber conflict or other unrelated issues.

xoid

Associates: tR|cky

On Nov. 19, 2000, tR|cky and xoid defaced the Open University-Jerusalem site at http://www.jccopenu.ac.il in support of the Palestinians. xoid is a member of core Hackers (cH).

VI. Other Actors

AnIcLaToR

AnIcLaToR is responsible for the first defacement of a US government web site since this cyber conflict began. AnIcLaToR defaced the site at mrdata.usgs.gov. Rather than supporting a side, this attacker advocates an end to the Israeli-Palestinian ground conflict altogether. AnIcLaToR's work appears to be non-destructive in nature. AnIcLaTor is believed to be based in Brazil.. On Nov. 7, 2000, AnIcLaToR defaced the SofTech Tecnologia em Informatica LTDA site at www.stn.com.br. AnIcLaToR is a member of prime suspectz.

DeTH 'Sauron

Group:	DeTH Crew or DeTH Brotherhood
Members:	DeTH`Watice, DeTH`Flameboy, DeTH`Angelus, DeTH`Arcrass, DeTH`Milenko, DeTH`Altered, DeTH`Digital, DeTH`Monarch, DeTH`Romeo, DeTH`Overide and DeTH`Xanor. Star/Yung/Yungsta and Havokator.

On Nov. 1, 2000, DeTH 'Sauron defaced the web site of the Jarvis Entertainment Group at http://www.gamingrevolution.com. The site was overwritten with a message regarding the current Israeli-Palestinian conflict, deriding both sides: *"Not many people realise the severity of the constant religious warfare and other CRAP that goes on in the middle east between Jews and arabs."*

The site was backed up as index1.html and nothing on the site was damaged, DeTH 'Sauron said.

VII. Incidents

al-Manar Site (almanar.com.lb)

On Oct. 29, 2000, a pro-Israeli attacker going by Nir M defaced Hezbollah's al-Manar site. The attacker uploaded an animated Israeli flag to the site and a link to information about Palestinian rioters and photographs of the lynching of two Israeli soldiers in Ramallah.

American Israel Public Affairs Committee (www.aipac.org)

On Nov. 2, 2000, Doctor Nuker broke into the American Israel Public Affairs Committee site (www.aipac.org) and posted pro-Palestinian messages in addition to the credit card numbers and contact information of those who made purchases through the site, member contact information and the email addresses of thousands who signed up to receive email alerts.

Bank of Israel

The Bank of Israel has been under attack by pre-configured FloodNet type tools since at least Oct. 25, 2000.

al-Bawaba Portal

This Arab portal site, based in Jordan, was attacked by pro-Israeli supporters in early Oct. 2000. According to a Nov. 5 Jerusalem Post report, *"The attack, called denial of service... flooded the portal's political forum chat room with heavy graphics files insulting Islam, the Prophet Mohammed, Yasser Arafat, and the Palestinian Authority, forcing it to shut down. The assault was apparently taking the forum's hot debates one step further, said Ramzy Khoury, Al-Bawaba's editor in chief, who added that the attack was the first in a series; the last of them came this week on the site's e-mail server. The first few attacks have already been traced to an organized Israeli effort to attack the Arab portal, with Web pages posted on Israeli sites automatically starting an assault when opened."*

Bayan.co.il

On Nov. 4, 2000, m0r0n and nightman defaced the site of bayan.co.il. In this defacement, the duo continued its attacks against Israeli sites claiming *"Anything anti-muslim will be hacked!"* *"Our motto is simple and clear and that is to CREATE GLOBAL AWARENESS AMONGST the world so that everyone would come to know of the attrocities done to Muslims all round the world. And shouts to DoctorNuker for his hack...too!"*

Cairo.eun.eg/hacked.asp

On Oct. 25, 2000, pro-Palestinian hackers ReALiST and PROJECTGAMMA, defaced the site of www.cairo.eun.eg. A message posted to the site said, *"PALESTINE CHILDEREN IN DANGER."*

COGNIFIT (www.cognifit.co.il)

dodi defaced the site of www.cognifit.co.il on Nov. 4, 2000. dodi continued to express his pro-Palestinian statement: *"this isn't just a war against 'israel' for the perpatrators of the attrocities in palestine are US backed. Its America which has blood on its hands the blood of innocent women and children."*

In this defacement, dodi recommended all wanting to carry out attacks against Israeli sites to launch SYN flood attacks using the "juno" or "slice" SYN flooder tools against two Domain Name System (DNS) servers run by the NetVision ISP.

www.caspit.co.il

On Nov. 4, 2000, m0r0n and nightman defaced the Automated Transaction System at www.caspit.co.il in support of the Palestinians. The two stated, *"You have been hacked by m0r0n and nightman of Pakistan and there is only one reason behind this defacement and that is the WAR OF ISRAEL with PALESTINIANS! Stop the violence and STOP killing Muslims(that includes children and women!)."*

The two also expressed *"Greetz to GFORCE Pakistan,DoctorNuker,Anti Security, Aniclator and all those who support us by their heart rending emails of which we are planning to quote a few of them in our upcoming HACKS!"*

Ebrick Inc.

On Oct. 21, 2000, pro-Palestinian attacker dodi defaced the lotus.ebrick.com site of Ebrick. See the appendix for the text of the defacement.

Health Infosystems Association, Israel (www.healthinfonet.co.il)

On Nov. 3, 2000 GForce Pakistan defaced the site of Health Infosystems Association, Israel in support of the Palestinians.

Gega Net ISP

Gega Net is a branch of the Egyptian German Telecommunications Industries (EGTI) and is one of the most popular ISPs in Egypt. PROJECTGAMMA claimed responsibility for the defacement.

Gilo.jlm.k12.il

A high school in Jerusalem hosted by NetVision. As of Nov. 6, 2000, the site is still down. PROJECTGAMMA claimed responsibility for attacking the site.

Hamas.org

Hezbollah Site (hezbollah.com, 207.222.197.194, 216.147.45.137)

Hezbollah webmaster Ali Ayoub said, *"We have names of 8,521 servers mainly in these two countries* [US and Israel] *that have been hitting our Web site regularly and sending us simultaneously tens of thousands of hostile emails, some of them carrying viruses to sabotage our server."*

Inconet

Inconet is an ISP that hosts a number of the Hezbollah sites. According to Inconet's Mahasen Ajam, the company was targeted by sources that *"originated in Israel from five different sites, four of them official. This is a new way of fighting and just like they used to attack our infrastructures with planes, now they might attack our Internet and technological capacities. We have to be ready."*

Iranian Ministry of Agriculture

On Nov. 4, 2000, lion&type_o ha k'eil defaced the site of the Iranian Ministry of Agriculture at www.moa.or.ir in support of the Israelis. Lion&type_o ha k'eil threatens to take down .ir and .lb sites and then .pk sites if GForce keeps defacing .il sites.

Israeli Academic (www.yvc.ac.il)

On Nov. 3, 2000, m0r0n and nightman defaced the Israeli Academic site at www.yvc.ac.il in support of the Palestinians.

Israeli Defense Forces (IDF) Site

According to UNITY on Oct. 28, 2000, *"Although the IDF cooperated with AT&T to provide an advanced security to its web site, the site was disabled for couple of hours last night due to a Cyber attack."*

The site has been under attack by a number of sites deploying FloodNet type tools since at least Oct. 25, 2000 and possibly earlier. It is highly likely that the site has been under additional types of attack as well.

Israeli Foreign Ministry Site

Due to attacks, the Israeli Foreign Ministry site went down for more than three days. The site reportedly first went down of Oct. 25, 2000.

Israeli Government (israel.org)

The site has been under attack by a number of sites deploying FloodNet type tools since at least Oct. 25, 2000 and possibly earlier. It is highly likely that the site has been under additional types of attacks as well.

Israeli Knesset Site

Knesset Spokesman Giora Pordes said attackers broke into the site and tampered with its files. Pordes said the attack may have come from Saudi Arabia.

Israeli Prime Minister's Office Site

The site has been under attack by a number of sites deploying FloodNet type tools since at least Oct. 25, 2000 and possibly earlier. It is highly likely that the site has been under additional types of attacks as well.

UNITY issued a statement on Oct. 28, 2000 that said, *"After discovering the trick that made the Zionist Prime Minster Office site revive, the site was sent down last night, it is still down till the moments of writing this report (www.pmo.gov.il), and our greetings to the staff of Tehila Security tem for their bad job in protecting the main governmental sever in the Zionist entity."*

Jen Communications (www.jen.co.il)

On Nov. 3, 2000, Jen Communications' site was defaced by GForce Pakistan in support of the Palestinians.

Jerusalem Post

During the week of Oct. 23, suspected pro-Palestinian attackers attempted to overload the servers hosting the Jerusalem Post, which uses NetVision to host its site.

Jewish Bible Association (www.jewishbible.org)

On Nov. 3, 2000, the site of the Jewish Bible Association at www.jewishbible.org was defaced by GForce Pakistan in support of the Palestinians.

MBA International School of Business Administration Management (www.eiba.biu.ac.il and www.mba.biu.ac.il)

On Oct. 31, 2000, m0r0n and nightman defaced the MBA International School of Business Administration Management sites at www.eiba.biu.ac.il and www.mba.biu.ac.il in support of the Palestinians.

Netanya Academic College (mars.netanya.ac.il)

On Oct. 30, 2000, Kala defaced the Netanya Academic College site at mars.netanya.ac.il in support of the Palestinians.

NetVision

NetVision released a statement on Oct. 26, 2000 saying that it was having difficulty maintaining its services due to the attacks against government sites it was hosting. NetVision General Manager Gilad Rabinovich said, *"We are taking measures, which for obvious reasons, we would rather not reveal, to prevent similar attacks. We have not come across to date any case in which*

access to the Internet through us was shut down for even a moment." Under further questioning by a journalist, Rabinovich said, *"NetVision is exposed to serious violence which is part of the struggle between Israel and Palestinian groups. This violence, which consisted of hacker attacks to try to crash official Web sites of the State of Israel, caused blockages to Internet infrastructures and damaged services the company offers it customers."*

Pf1 Systems Ltd. (www.pf1.co.il)

On Nov. 3, 2000, the site of Pf1 Systems Ltd. was defaced by GForce Pakistan in support of the Palestinians.

Shemayisrael.co.il

On Nov. 3, 2000, shemayisrael.co.il was defaced by GForce Pakistan in support of the Palestinians.

Shenkar College (www.shenkar.ac.il)

On Nov. 2, 2000, m0r0n and nightman defaced the site of Shenkar College at www.shenkar.ac.il in support of the Palestinians.

Tel Aviv Stock Exchange Site

The site has been under attack by a number of sites deploying FloodNet type tools since at least Oct. 25, 2000 and possibly earlier. It is likely that the site has been under additional types of attack as well.

UNITY issued a statement on Oct. 28, 2000 that said, *"Zionist Stock Exchange were disabled last night for 5 hours."*

Visiting Israel Students Association (www.visa.org.il)

On Nov. 3, 2000, GForce Pakistan defaced the site of the Visiting Israel Students Association in support of the Palestinians.

Yizrael Valley College (Mihlelet Emek Yizrael) (www.yvc.ac.il)

On Nov. 3, 2000 m0r0n and nightman defaced the site of Yizrael Valley College (Mihlelet Emek Yizrael) at www.yvc.ac.il in support of the Palestinians.

VIII. Pro-Israeli Sites Hosting Live Attack Tools

Sites listed in alphabetical order.

1. a.israforce.net

2. Hizballa - No More - home.online.no/~oelpeleg/hiz.htm

3. http://members.nana.co.il/planet/yair_n/index.htm

4. Members.nana.co.il/planet/carmelb

5. Mock Hezbollah Site - www.hizballa.org

6. SmallMistake - smallmistake.welcome.to

7. www.crashme.com (iDEFENSE recommends against visiting this site since it attacks visitors' browsers)

8. www.wizel.com

IX. Pro-Palestinian Sites Hosting Live Attack Tools

Sites listed in alphabetical order.

1.   angelfire.com/oh4/irsa2000
2.   defend the Resistance - members.tripod.com/irsa2001
3.   defend.unity-news.com/
4.   hizbollah.unity-news.com/
5.   irsa2000.jumpfun.com
6.   killisrael.arjika.com/arabic.htm
7.   resistance-defend.freeservers.com
8.   unity.vdirect.com
9.   www.bahraingate.8k.com
10.   www.fightisrael.com
11.   www.freespeech.org/unity-nes/defend
12.   www.ummah.net/unity/defend

X. Pro-Palestinian Sites Supporting the Campaign

Sites listed in alphabetical order.

1. http://pub23.ezboard.com/fbaderonlinefrm13
2. http://quds.gq.nu/killisrael.htm
3. http://unity-news.org
4. http://www.almuhajiroun.com
5. http://www.fightisrael.com

XI. Pro-Israeli Targets

Sites listed in alphabetical order.

1. 195.138.224.2
2. 207.222.197.194
3. Al-Bawaba Portal site at http://www.albawaba.com
4. al-Manar at http://www.almanar.com.lb
5. al-Manar at http://www.manartv.com
6. Hafeez Center Global Internet Café at http://www.hafeezcentre.com.pk
7. Hamas at Hamas.org
8. Hezbollah at Hezbollah.org
9. Hezbollah at Moqawama.org
10. Hezbollah at Nasrallah.net
11. Hezbollah site at http://www.hizbollah.org
12. Iranian Foreign Ministry site at http://mfa.gov.ir
13. Iranian Ministry of Agriculture at http://www.moa.or.ir
14. Islam Web at http://www.islamweb.net
15. Islamic Republic News Agency at http://www.irna.com
16. Islamic Society of North America at http://www.isna.net
17. Islamic University, Gaza site at http://www.iugaza.edu
18. Khaleej.com at http://www.khaleej.com
19. Ministry of Awqaf and Islamic Affairs, Qatar site at http://www.islam.gov.qa
20. Palestine National Databank State Information Service at http://www.sis.gov.ps
21. Palestine-Info at Palestine-info.net
22. Palestinian National Authority at http://www.pna.gov.ps
23. Palestinian National Authority at PNA.org
24. Sakhr Software Co. site at http://www.ajeeb.com
25. Talk Islam, Library of Islamic Web Sites at http://www.talkislam.com
26. Ummah.net at 212.240.0.12
27. Ummah.net at http://kano.virtual-pc.com
28. Ummah.net at Ummah.com
29. Ummah.net at Ummah.net

30. Ummah.net at Ummah.org

31. United Arab Emirates Dept. of Civil Aviation site at http://www.dcaauh.gov.ae

32. webhosting.ajeeb.com

33. www.primebank.com.pk

Pro-Israeli Tradecraft

Sites listed in alphabetical order.

1. .To (Free Web Referrals)

2. Dreambook (Guestbook Service)

3. Geocities.com (Free Web Hosting)

4. Namezero.com (Free Web Hosting)

5. Nana.co.il (Free Web Hosting)

6. Surfree.net.il

7. Yahoo! (Free Email)

XII. Pro-Palestinian Targets

Sites listed in alphabetical order.

1. ABIS site at http://www.asbis.sk
2. Achva Academic College's E-learning at http://online.achva.ac.il
3. albert.ph.biu.ac.il
4. Al-Libaas Accessories site at http://www.al-libaas.com
5. All-Kosher Index at http://www.kosher.co.il
6. American Israel Public Affairs Committee at http://www.aipac.org)
7. AMTEL Slovensko Ltd. Site at http://www.amtel.sk
8. Anti-Defamation League (ADL) at http://www.adl.org
9. Ardom Telecomputing of Israel at http://www.ardom.co.il
10. ARON site at http://www.aron.be
11. AT&T Corp. at http://www.att.com
12. Bank of Israel at http://www.bankisrael.gov.il (161.58.232.244)
13. Bayan Systems at http://www.bayan.co.il
14. Borha Torah at http://www.borhatorah.org
15. BSNL Nagpur (Depart of Telecom) site at http://nagpur.dotindia.com
16. Cairo University at http://www.cairo.eun.eg
17. Caspit Ltd. at http://www.caspit.co.il
18. Central Florida Bankruptcy Law Association site at http://www.cfbla.org
19. Christian Sharing Center site at http://www.christiansharing.org
20. Cognifit Ltd. at http://www.cognifit.co.il
21. Compact Studio site at http://www.dvdbest.sk
22. Comsec Group Ltd. at http://www.comsec.co.il (194.90.202.39)
23. Comune di Scandiano at http://www.comune.scandiano.re.it
24. Corporacion Peruana de Aeropuertos y Aviacion Comercial S.A. site at http://www.corpac.gob.pe
25. Cowboys Orlando Night Club site at http://www.cowboysorlando.com
26. Cursos de Bolsa site at http://www.cursobolsa.com
27. CVD Data Services at http://lab.cvdds.com
28. delhinms.mtnl.net.in

29. Deutsche Forschungsanstalt fuer Luft – und Raumfahrt e.V. (DLR) site at http://www.weblab.dlr.de

30. Dilim Site at http://www.dilim.co.il

31. Dizasta Productions site at http://www.dizasta.net

32. dns0.whuci.edu.cn

33. Ebrick Inc. at http://lotus.ebrick.com

34. Efrat DSP Group at http://www.efratdsp.co.il

35. EgyNile ISP at http://egynile.com

36. Elgev Electronics at http://www.elgev.co.il

37. Forma, Ltd. Site at http://www.deiure.sk

38. Frostbit.com at http://www.frostbit.com

39. Gega Net ISP at http://dev.gega.net

40. Gilo High School at http://www.gilo.jlm.k12.il

41. Golden Lines at http://www.goldenlines.co.il (212.117.129.81)

42. Gvanim Financim, Kibutz Shefayim Israel at http://www.gvanim.co.il

43. Health Infosystems Association, Israel at http://www.healthinfonet.co.il

44. Hebrew University of Jerusalem, Israel site at http://daat.ls.huji.ac.il

45. Hebrew University of Jerusalem, Israel site at http://www.music.md.huji.ac.il

46. Hed-Arzi at http://www.hed-arzi.co.il

47. Indian Institute of Science Dept. of Mechanical Engineering site at http://mecheng.iisc.ernet.in

48. Indian Institute of Science Dept. of Metallurgy at http://www.metalrg.iisc.ernet.in

49. Indian Institute of Science Materials Research Center site at http://arun.mrc.iisc.ernet.in

50. Indian Institute of Science Solid State and Structural Chemistry Unit at http://zeolite.sscu.iisc.ernet.in

51. Israel.com at http://www.israel.com (63.194.226.226)

52. Israeli Academic at http://www.yvc.ac.il

53. Israeli Academic Sub-Domain at http://www.netanya.ac.il

54. Israeli Air Force at http://www.iaf.org.il

55. Israeli Defense Forces (IDF) at http://www.idf.il (192.117.1.1 and 212.14.3.30.101)

56. Israeli Foreign Ministry at http://www.mof.gov.il

57. Israeli Government at http://www.israel.org (194.90.246.13 and 212.143.236.4)

58. Israeli Government Site (147.237.72.20)

59. Israeli Knesset

60. Israeli Ministry of Defense at http://www.mod.gov.il

61. Israeli Ministry of Interior at http://www.moin.gov.il

62. Israeli Ministry of National Infrastructures at http://www.mni.gov.il

63. Israeli National Police at http://www.police.gov.il

64. Israeli Prime Minister's Office at http://www.pmo.gov.il (147.237.72.93)

65. Jen Communications at http://www.jen.co.il

66. Jerusalem Books at http://www.jerusalembooks.com

67. Jerusalem Post at http://www.jpost.com

68. Jewish Bible Association at http://www.jewishbible.org

69. JMJ Internet Services at http://www.jmjservices.com

70. KAIZ site at http://www.kaiz.com

71. Karnataka Telecom Circle site at http://www.karnataka.dotindia.com

72. KIS Technologies at http://www.kisnet.co.il

73. Kolhapur Telecom District site at http://www.kolhapur.dotindia.com

74. Kuala Lumpur Department of Urban Transportation site at http://www.jpbdbkl.gov.my

75. La Cruz Azul de Puerto Rico Inc. site at http://www.cruzazul.com.mx

76. Lal Bahadur Shastri National Academy of Administration, Mussoorie at http://www.lbsnaa.ernet.in

77. Lantronics Computer Networking Ltd. at http://www.lantronics.co.il

78. Los Alamos Neutron Science Center site at http://www.lansce.lanl.gov

79. Lucent Technologies at http://www.lucent.com (192.11.229.2)

80. Lymphedema Awareness Foundation site at http://www.lymphaware.org

81. mail.topnet.co.il

82. Malaysian Rubber Board site at http://www.lgm.gov.my

83. MBA International School of Business Administration Management at http://www.eiba.biu.ac.il

84. MBA International School of Business Administration Management at http://www.mba.biu.ac.il

85. Merical (IN) at http://email.merical.ac.in

86. modiin.haifa.ac.il

87. National Centre for Radio Astrophysics site at http://sakthi.ncra.tifr.res.in

88. NB a.s. site at http://www.nbas.cz

89. Netanya Academic College at http://mars.netanya.ac.il

90. NetVision

91. Open University-Jerusalem at http://www.jccopenu.ac.il

92. Order in a Click at http://www.order-click.co.il

93. Ornetix at http://ntserver.ornetix.co.il

94. Partners in Torah at http://www.partnersintorah.org

95. PC Center at http://www.pc-center.co.il

96. Pelenews site at http://www.pelenews.co.il

97. Pf1 Systems Ltd. at http://www.pf1.co.il

98. Phillips Community College-University of Arkansas site at http://www.pccua.cc.ar.us

99. Pirchei Shoshanim at http://www.pirchei.co.il

100. Qatar Ministry of Awqaf and Islamic Affairs at http://www.islam.gov.qa

101. Rabia Gupta Design site at http://www.styletantra.com

102. Radwiz at http://www.radwiz.co.il

103. Retirement Living Management site at http://www.retliv.com

104. Rooster at http://mail.rooster.co.il

105. Rotter.net at http://www.rotter.net (194.90.202.20)

106. Scicom site at http://www.scicom.com.my

107. Server Computers site at http://www.netserver.co.il

108. sgl1.lanres.com

109. Shavatz High School at http://www.savatz.givataim.k12.il

110. Shema Yisrael Torah Network at http://shemayisrael.co.il

111. Shenkar College at http://www.shenkar.ac.il

112. Shop.chemolak.sk

113. Sira1.sira.it

114. Sivan-North Computer at http://www.sivan-north.co.il

115. SofTech Tecnologia em Informatica LTDA at http://www.stn.com.br

116. Solski Center PTUJ site at http://www.s-scptuj.mb.edus.si

117. SOMA Galleries at http://www.somagalleries.com

118. Tahal Group at http://www.tahal.co.il

119. Tel Aviv Chamber of Commerce at http://www.chamber.org.il

120. Tel Aviv Stock Exchange at http://www.tase.co.il (192.116.46.129)

121. Temple Mount in Jerusalem at http//www.templemount.org (216.10.100.29)

122. Terminal-Computers & Multimedia at http://www.terminal.co.il

123. The American University in Cairo at http://www.aucegypt.edu/hi.html

124. The Temple Institute at http://www.templeinstitute.org (161.58.226.14)

125. The Ultimate Shabbat Site at http://www.shabat.co.il

126. topcom.topnet.co.il

127. Torah Educator at http://www.toraheducator.org

128. United Studios Corp. at http://www.usidentity.com

129. University of Oklahoma Administration site at http://admin-scb.ouhsc.edu

130. University Medical Center Nijmegen Dept. of Urology, Netherlands site at http://uroworld.azn.nl

131. University of Chicago Computer Science Dept. site at http://hamachi.cs.uchicago.edu/

132. Visiting Israel Students Association at http://www.visa.org.il

133. VOLasia limited site at http://www.volasia.com

134. Watersports World at http://www.watersportsworld.com

135. Web of India site at http://dmss.webindia.com

136. Web of India site at http://servlet.webindia.com

137. Web of India site at http://servlet2.keralatourism.org

138. Web of India site at http://tanishq.webindia.com

139. Web of India site at http://webmail.webindia.com

140. WebStyle Internet Solutions at http://www.webstyle2000.com (207.159.139.113)

141. Western-Galilee College at http://wgalil.ac.il

142. Wisconsin K12 Schools site at http://www.sharon.k12.wi.us

143. Wizel.com at http://www.wizel.com (64.33.48.76)

144. World Peace Center at http://www.worldpeacecenter.org

145. www.ann-arbor.med.va.gov

146. www.arttalk.com

147. www.aztek.co.il

148. www.cardcentrum.sk

149. www.carroll.k12.ga.us

150. www.cog.co.jp

151. www.dol.wa.gov

152. www.files4u.co.il (same as www.karate.org.il)

153. www.hmcnet.com

154. www.infinity.com.eg

155. www.microconnectors.com

156. www.pryor.k12.ok.us

157. www.robotec.co.il

158. www.scjh.kh.edu.tw

159. www.stadtklima.de

160. www.syscom.co.il

161. www.topnet.co.il

162. www.whuci.edu.cn

163. www.xmlprobe.com

164. www3.co.oakland.mi.us

165. Yizrael Valley College (Mihlelet Emek Yizrael) at http://www.yvc.ac.il

166. Zefat Regional College at http://www.zrc.ac.il

Pro-Palestinian Tradecraft

Sites listed in alphabetical order.

1. Angelfire (Free Web Hosting)

2. eGroups (Free List Hosting)

3. GeoCities (Free Web Hosting)

4. Homestead.com (Free Web Hosting)

5. Hotmail.com (Free Email)

6. Hushmail.com (Free Secure Email)

7. Jumpfun.com (Free Web Hosting)

8. ListBot (Free List Hosting)

9. Tripod.com (Free Web Hosting)

10. Ummah.net (Web Hosting)

11. Xdrive.com (Free File Sharing)

12.   Yahoo! (Free email)

Israeli-Palestinian Cyber Conflict (IPCC) Report v2.0PR – Jan. 3, 2000 – 15:41 GMT
CONTACT INFO: analysis@idefense.com, voice (703) 383.5280, fax (703) 359-5323

XIII. Other Targeted Sites

Sites listed in alphabetical order.

1. Hebrew University of Jerusalem, Israel at http://shemesh.fiz.huji.ac.il
2. Jarvis Entertainment Group at http://www.gamingrevolution.com
3. Sheffield Hallam University site at jeff.sci.shu.ac.uk
4. US Geological Survey's Mineral Resources Online Spatial Data at http://mrdata.usgs.gov
5. www.as.huji.ac.il

XIV. Tools

Current activity by the pro-Palestinian and pro-Israeli attackers includes FloodNet-type attacks, system penetrations and other more sophisticated tactics. Detailed below are some of the tools in use:

ahlizevil aka evilping

Attack tool being distributed by pro-Palestinian attackers. It is believed to be the same as evilping. *See evilping entry below.*

Attack 2.41 and Attack 2.51

Attack versions 2.41 and 2.51 are used by the Palestinians to conduct three different types of assault: ping attacks, HTTP GET requests and web attacks. All three can be used at the same time. The difference between 2.41 and 2.51 seems to be minor bug fixes.

Bounce Spam Mail v1.4

Email attack tool being distributed by pro-Palestinian attackers.

defend

A FloodNet-type tool known as "defend" is being used by a number of pro-Palestinian groups to attack at least seven different targets. At least three different versions of the tool are known to be in existence, each successive version that added additional sites to defend's target list. The tool is simple in nature but requires several attackers to be effective. It uses a new method of defeating

caching problems experienced by cyber activists in the past. During an attack, defend requests non-existent pages on targeted sites by calling for URLs based on the current date and time. The pro-Palestinians have mirrored the attack tool on Angelfire.com, Tripod.com, Ummah.net and Jumpfun.com hosting sites.

evilping (07/98 release & 11/99 release) aka ahlizevil
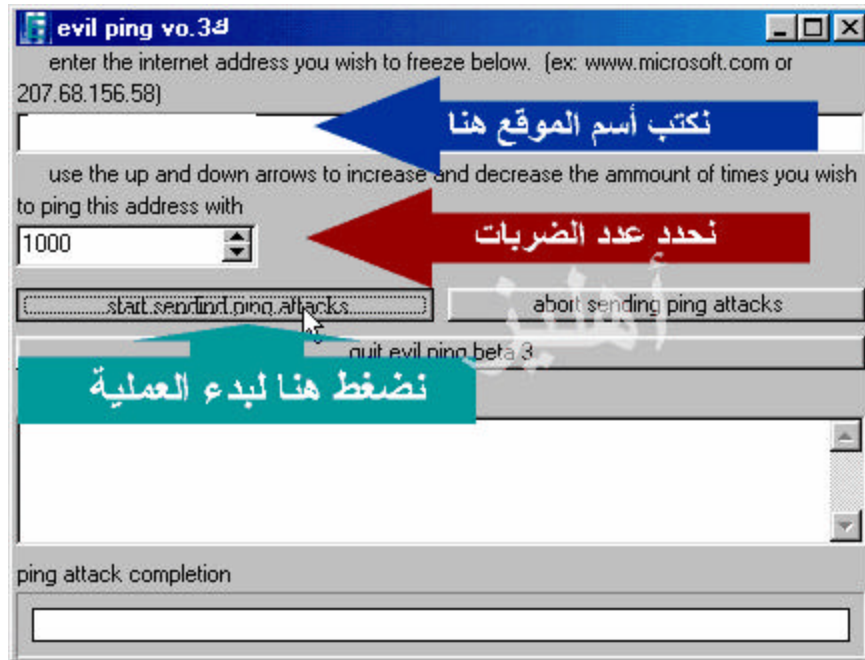
Attack tool being distributed by pro-Palestinian attackers.

FakeMail
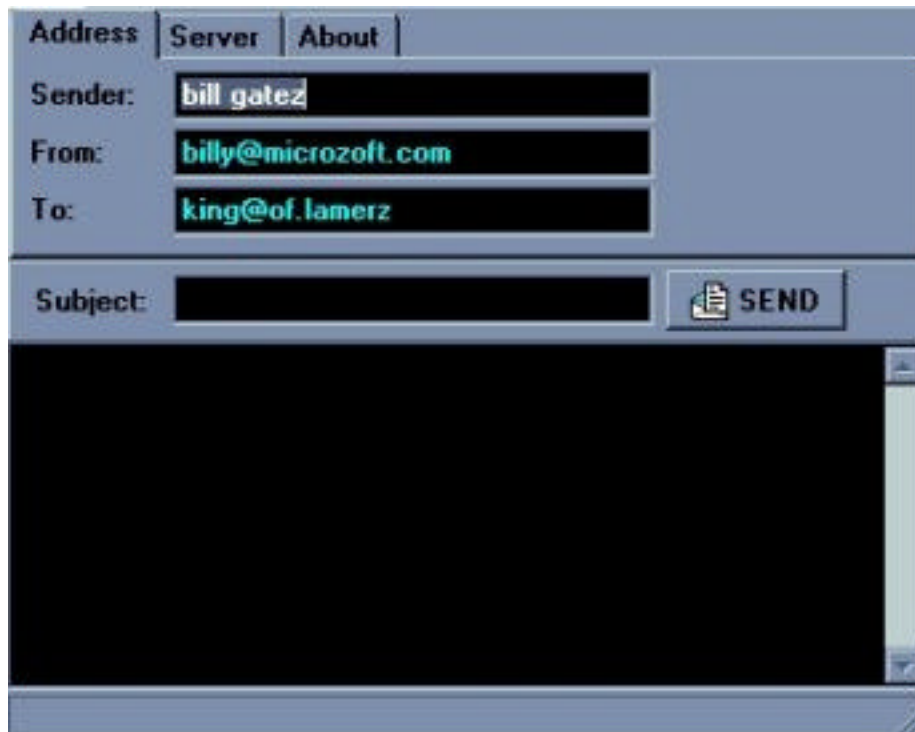
Email attack tool being distributed by the pro-Palestinians.

HTTP Bomber 1.0
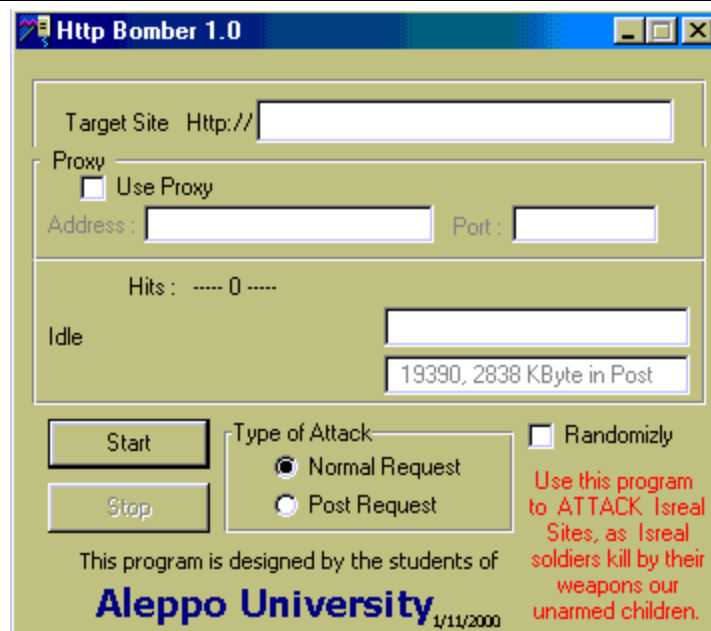
Pro-Palestinians are using a tool called HTTP Bomber. The tool was distributed on the www.kuds.8k.com site, which was taken offline in early Nov. With its very simple user interface, Bomber appears to allow a user to target specific web sites either by its URL or IP address. The attack tool claims to generates numerous HTTP GET and POST requests. In addition, the attacker has the option of letting the tool randomly implement either of the two attacks.

HTTP Bomber 1.001b

Distributed on the www.kuds.8m.com site. It is believed to have gone into circulation on Nov. 7, 2000. The graphical user interface (GUI) appears to be identical to HTTP Bomber 1.0.

juno

A SYN flood tool.

Ping Attack

US university students are being asked to attack pro-Palestinian web sites. iDEFENSE can confirm that posts on listservs belonging to at least one prominent American university have given students directions for launching ping floods against prominent Palestinian targets. These emails are also circulating (with unknown prevalence) to members of the public. Among targeted web sites are those belonging to Hezbollah; Hezbollah Secretary General Sayyed Hassan Nasrallah; Hezbollah's al-Manar Television; Hamas; the Hamas-supported Palestinian Information Center; Hezbollah's Islamic Resistance Support Association; and the Palestinian National Authority.

Ping of Death

The Ping of Death uses a utility to create an IP packet that exceeds the maximum size allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot when they receive such a maliciously crafted packet. This attack is not new. Operating systems and some Layer 3 communications hardware can be configured to filter out oversize packets, thus preventing a ping of death.

QuickFire

Email attack tool being distributed by pro-Palestinian attackers, capable of generating more than 32,000 messages to a targeted address with a single click.

Shell Script by dodi

iDEFENSE examined a portion of shell code that was posted on the COGNIFIT defacement. Preliminary analysis of the code indicates that if placed onto a Linux or Unix system, it would delete essentially all files on the computer with the exception of the OS at a specified time. It would then execute an attack tool, if it is located in the local directory and begin to attack a targeted site. The code examined by iDEFENSE executes the "juno" SYN flooder and begins an attack against the www.idf.il site on port 80. This could easily be modified, however, to utilize a different tool and target any site the attacker wished. It is reasonable to suspect that dodi and other attackers may have installed such code on previously defaced or compromised sites or will begin to do so in future attacks. Organizations whose sites have been targeted or are victims of attacks connected to the current Israeli/Palestinian cyber conflict are advised to immediately begin searching for a file called "isat". Companies are also advised to examine all "cron" and "at" jobs to see if anything unusual is scheduled to run.

slice

A SYN flood tool.

Smurf attacks (suspected)

Smurf attacks are an early variation of a ping attack. The Smurf attack exploits networks misconfigured to reply to a ping sent to a network broadcast address. By sending one packet, an attacker can trigger hundreds of packets to bounce back in reply. The use of these attacks, however, raised awareness of this misconfiguration. Most administrators have since fixed the problem. With the number of viable Smurfing targets reduced, many hackers turned to denial of service attacks that involved compromising a number of hosts and manually sending floods against a target. This required hackers to log into each of these machines individually -- a time-consuming process. In response, hackers and security experts began to develop new DDoS tools. These tools were designed to speed up DDoS attacks by automating the process. The tools still require an intruder to penetrate each host and load the slave server. However, with the tools, this need only be done once. Thereafter, a machine designated as the "master" of the network can be used to communicate with all of the slaves, and command them to launch the packet flood at the appropriate moment.

WinSmurf

Attack tool being distributed by pro-Israeli group Hackers of Israel Unite. The tool is also now being distributed by pro-Palestinian attackers. Hackers of Israel Unite claimed to have successfully downed an Arab site using this tool over a 56K dial-up connection and one ADSL line.

XV. Palestinian/Israeli Conflict Timeline

Sept. 27, 2000

- Palestinian leaders warn of possible danger if Sharon visits holy sites.

Sept. 28, 2000

- Sharon enters old city.

Oct. 6, 2000

- Wizel.com attack tools go online at http://www.wizel.com.

Oct. 7, 2000

- The site at http://www.hizbollah.org hit.

Oct. 12, 2000

- Yemen attack on USS Cole.
- Two Israeli soldiers killed in Ramallah.

Oct. 16, 2000

- Peace summit held in Egypt.
- US State Department issues warnings.

Oct. 18, 2000

- Unconfirmed reports suggest that some Israeli systems were hit by cyber attack.

Oct. 20, 2000

- Hezbollah webmaster Ali Ayoub verifies that its site has been hit.
- JMJ Internet Services at http://www.jmjservices.com defaced by dodi.

Oct. 21, 2000

- Ebrick Inc. at http://lotus.ebrick.com defaced by dodi.
- Arab League opens summit in Cairo.

Oct. 23, 2000

- Israeli government systems continue to be plagued by cyber attacks.

Oct. 24, 2000

- Clinton invites Arafat to Washington.

Oct. 25, 2000

- Wizel.com at http://www.wizel.com listed as possible target by anti-Israeli web site.

- Israeli Government site at http://www.israel.org, Israeli Defense Forces (IDF) at http://www.idf.il and Wizel.com at http://www.wizel.com targeted by the pro-Palestinian attack site Ummah.net at http://www.ummah.net/unity/defend, which is hosting the "defend" tool.

- ReALiST, a pro-Palestinian attacker, claims credit for the defacement of EgyNile Internet service provider site at http://www.egynile.com ReALiST+ProjectGamma claim credit for the defacement of Cairo University's site at http://www.cairo.eun.eg.

- ReALiST using the name Anti-Israel posts a message saying, "I'm thinking of something like DDoS, on major Israel networks and sites, and sending emails helping all Arab ISP's and sites for more security, we will just tell them what we know... I'm thinking of installing TFN3K servers and doing the cnn.com and Yahoo.com thing again any one in, mail me quick."

Oct. 26, 2000

- Bank of Israel at http://www.bankisrael.gov.il targeted by pro-Palestinian attack site.

- Israeli Foreign Ministry site at http://www.mof.gov.il forced down by attackers.

- Tel Aviv Stock Exchange site at http://www.tase.co.il targeted by pro-Palestinian attack site.

- Israeli Knesset site attacked by pro-Palestinian attacker; a Lebanese attacker known as Walid claims responsibility.

- Islamic extremist group al-Muhajiroun urges individuals to participate in cyber attacks against Israeli web sites, listing the following attack sites: http://members.tripod.com/irsa2001, http://www.angelfire.com/oh4/irsa2000 and http://irsa2000.jumpfun.com.

Oct. 27, 2000

- Another Hezbollah site at http://www.hizballah.org reported down due to an overwhelming number of hits.

- Pro-Israeli attackers create several decoy sites targeting Hezbollah site visitors; the two decoy sites are located at http://www.hizballa.org and http://www.hizballa.com; both sites contain pro-Israeli messages.

- Israeli Army contracts with AT&T Corp. to help deal with cyber attacks.

- Messages begin circulating among students at universities in the US, asking students to contribute to online actions against pro-Palestinian web sites.

Oct. 29, 2000

- al-Manar, a Hezbollah news site at http://www.manartv.com, defaced by Nir M.

Oct. 30, 2000

- Israeli Knesset site restored.

- UNITY issues a call for Muslims and Arabs in the US to boycott AT&T Corp.

- ReALiSt+ProjectGamma claim credit for defacing the site belonging to The American University in Cairo at http://www.aucegypt.edu/hi.html.

- UNITY's attack site at http://www.ummah.net/unity/defend/ is moved to http://defend.unity-new.com/ and http://hizbollah.unity-news.com/ after the ISP hosting Ummah.net threatens to take its sites offline if the attack site is not removed.

- SmallMistake web site at http://smallmistake.welcome.to hosts pro-Israeli Attack Tool.

- Kala defaces the Netanya Academic College site at http://mars.netanya.ac.il in support of the Palestinians.

Oct. 31, 2000

- UNITY launches Phase 3 against ISP infrastructure in Israel, announces intentions to launch a Phase 4 targeting "Zionist" E-Commerce sites, and distributes new tool among its members.

- m0r0n and nightman deface the MBA International School of Business Administration Management site at http://www.eiba.biu.ac.il in support of the Palestinians.

- m0r0n and nightman deface the MBA International School of Business Administration Management site at http://www.mba.biu.ac.il in support of the Palestinians.

Nov. 1, 2000

- Doctor Nuker breaks into the American Israel Public Affairs Committee site at http://www.aipac.org and posts pro-Palestinian messages in addition to the credit card numbers and contact information of those who purchased items through the site, member contact information, and thousands of email addresses of individuals who signed up to receive email alerts

- DeTH 'Sauron defaced Jarvis Entertainment Group's web site at http://www.gamingrevolution.com with a message deriding both sides in the conflict: *"Not many people realise the severity of the constant religious warfare and other CRAP that goes on in the middle east between Jews and arabs."*

Nov. 2, 2000

- m0r0n and nightman deface the site of Shenkar College at http://www.shenkar.ac.il in support of the Palestinians.

Nov. 3, 2000

- Cognifit Ltd. site at http://www.cognifit.co.il defaced by dodi. Defacement urges pro-Palestinian attackers to target two DNS servers at NetVision with SYN flood attacks. dodi also says he is not only interested in Israeli targets but US as well.

- Pakistan Hackerz Club (PHC) and GForce Pakistan join the pro-Palestinian side.

- GForce Pakistan defaces Jen Communications site at http://www.jen.co.il.

- GForce Pakistan defaces Health Infosystems Association, Israel site at http://www.healthinfonet.co.il. Greets were given to rsh, hackweiser, *m0r0n, nightman, doctornuker, phc, rootworm alldas,* and *attrition*.

- GForce Pakistan defaces the Visiting Israel Students Association site at http://www.visa.org.il.

- GForce Pakistan defaces the Pf1 Systems Ltd. site at http://www.pf1.co.il.

- m0r0n and nightman deface the site of the Yizrael Valley College (Mihlelet Emek Yizrael) at http://www.yvc.ac.il in support of Palestine.

- GForce Pakistan defaces the site of the Jewish Bible Association at http://www.jewishbible.org.

- GForce Pakistan defaces the Shema Yisrael Torah Network site at http://shemayisrael.co.il.

- m0r0n and nightman deface the Israeli Academic site http://www.yvc.ac.il.

Nov. 4, 2000

- m0r0n and nightman deface Bayan Systems site at http://www.bayan.co.il in support of the Palestinians.

- m0r0n and nightman deface Capit Ltd. site at http://www.caspit.co.il in support of the Palestinians.

- Lion&type_o ha k'eil deface the site of the Iranian Ministry of Agriculture at http://www.moa.or.ir in support of the Israelis. Lion&type_o ha k'eil threatens to take down .ir and .lb sites and then .pk sites if GForce keeps defacing .il sites.

Nov. 5, 2000

- GForce Pakistan defaces Jerusalem Books at http://www.jerusalembooks.com in support of the Palestinians.

- GForce Pakistan defaces Pirchei Shoshanim site at http://www.pirchei.co.il in support of the Palestinians.

- GForce Pakistan defaces the World Peace Center site at http://www.worldpeacecenter.org in support of the Palestinians.

- GForce Pakistan defaces the Ultimate Shabbat Site at http://www.shabat.co.il in support of the Palestinians.

- GForce Pakistan defaces Caspit Ltd. site at http://www.caspit.co.il in support of the Palestinians.

- GForce Pakistan defaces the All-Kosher Index at http://www.kosher.co.il in support of the Palestinians.

- GForce Pakistan or group claiming to be defaces Shenkar College site at http://www.shenkar.co.il in support of the Palestinians.

Nov. 6, 2000

- Hackers of Israel Unite calls for attacks against chats and ICQ, as well as Palestinian National Authority at http://www.pna.gov.ps, al-Manar at http://www.almanar.com.lb, Palestine National Databank State Information Service at http://www.sis.gov.ps, Islamic Republic News Agency at http://www.irna.com and www.albawaba.com.

- GForce Pakistan defaces the Borha Torah site at http://www.borhatorah.org in support of the Palestinians.

- GForce Pakistan defaces the Torah Educator site at http://www.toraheducator.org in support of the Palestinians.

- GForce Pakistan defaces the Partners in Torah site at http://www.partnersintorah.org in support of the Palestinians.

Nov. 7, 2000

- m0r0n and nightman deface the Elgev Electronics site at http://www.elgev.co.il in support of the Palestinians.

- m0r0n and nightman deface the Efrat DSP Group site at http://www.efratdsp.co.il in support of the Palestinians.

- HTTP Bomber 1.001b believed to go into circulation.

- AnIcLaToR defaces the SofTech Tecnologia em Informatica LTDA site at http://www.stn.com.br, advocating an end to the Israeli-Palestinian ground conflict.

Nov. 8, 2000

- "pakistan is gay" defaces URMIA site at http://mail.urmia.ac.ir in apparent retaliation for GForce Pakistan attacks against pro-Israeli sites.

- tR|cky, Boss and KUCAU deface Order in a Click site at http://www.order-click.co.il and Dilim Site at www.dilim.co.il in support of the Palestinians.

- m0r0n and nightman deface the Hed-Arzi site at http://www.hed-arzi.co.il in support of the Palestinians.

- GForce Pakistan defaces the Ornetix site at http://ntserver.ornetix.co.il in support of the Palestinians. Defacement announces the addition of a new member to the group: nicks xtremist.

- GForce Pakistan defaces the Radwiz site at http://www.radwiz.co.il. Defacement announces the addition of a new member to the group, nicks xtremist.

- Possible GForce Pakistan imposter defaces the KIS Technologies site at http://www.kisnet.co.il. The defacement style does not fit GForce Pakistan's traditional form.

- Possible GForce Pakistan imposter defaces the Tel Aviv Chamber of Commerce site at http://www.chamber.org.il in support of the Palestinians. The defacement style does not fit GForce Pakistan's traditional form.

- GForce Pakistan defaces the Terminal-Computers & Multimedia site at http://www.terminal.co.il. Threatens attacks against DNS servers and NetVision in the defacement.

- GForce Pakistan defaces the Rooster site at http://mail.rooster.co.il. Threatens attacks against DNS servers and NetVision in the defacement.

- m0r0n and nightman deface the Gvanim Financim, Kibutz Shefayim Israel site at http://www.gavnim.co.il in support of the Palestinians.

Nov. 9, 2000

- AnIcLaToR defaces the US Geological Survey site at http://mrdata.usgs.gov, advocating an end to the Israeli-Palestinian ground conflict.

Nov. 10, 2000

- ReALiSt+ProjectGamma deface the www.infinity.com.eg site in support of the Palestinians.

- tR|cky defaces the Western-Galilee College site at http://wgalil.ac.il in support of the Palestinians.

- Kuds launches coordinated HTTP Bomber 1.001b attack against Israel.com site at www.israel.com beginning at 08:30 GMT.

Nov. 11, 2000

- m0r0n and nightman deface the PC Center site at http://www.pc-center.co.il.

- tR|cky and Boss deface the Zefat Regional College site at http://www.zrc.ac.co.il in support of the Palestinians.

- tR|cky and Boss deface the Open University-Jerusalem site at http://www.jccopenu.ac.il in support of the Palestinians.

Nov. 12, 2000

- m0r0n and nightman deface the Lantronics Computer Networking Ltd. site at http://www.lantronics.co.il in support of the Palestinians.

- m0r0n and nightman deface the Sivan-North Computer site at http://www.sivan-north.co.il in support of the Palestinians.

- lion&type_o deface the www.primebank.com.pk site in support of the Israelis.

- lion&type_o deface the Hafeez Center Global Internet Café at http://www.hafeezcentre.com.pk site in support of the Israelis.

- tR|cky and Boss deface the Shavatz High School site at http://www.savatz.givataim.k12.il site in support of the Palestinians.

Nov. 13, 2000

- m0r0n and nightman deface the Tahal Group at http://www.tahal.co.il site in support of the Palestinians.

- m0r0n and nightman defaced the www.syscom.co.il site in support of the Palestinians.

- xZeroKiller defaces the Terminal-Computers & Multimedia site at http://www.terminal.co.il in a suspected pro-Palestinian attack.

Nov. 14, 2000

- m0r0n and nightman deface the www.robotec.co.il site in support of the Palestinians.

- UnsecurityBR defaces the Terminal-Computers & Multimedia site at http://www.terminal.co.il.

Nov. 15, 2000

- m0r0n and nightman deface the www.topnet.co.il site in support of the Palestinians.

- m0r0n and nightman deface topcom.topnet.co.il in support of the Palestinians.

- m0r0n and nightman deface mail.topnet.co.il in support of the Palestinians.

- Murtaza Baloch aka EdGe defaces the www.karate.org.il site in support of the Palestinians.

Nov. 18, 2000

▪ Kuds, a pro-Palestinian group, launches coordinated HTTP Bomber 1.001b against http://lgw.rotter.net.

▪ NETFORCE/PeRvErS deface the Iranian Ministry of Foreign Affairs site at http://www.mfa.gov.ir. It is not clear if the defacement is in any way related to the current conflict.

▪ tR|cky and petite_lourve deface the Open University-Jerusalem site at http://online.achva.ac.il in support of the Palestinians.

Nov. 19, 2000

▪ The Iranian Ministry of Foreign Affairs site at http://www.mfa.gov.ir defaced. It is not clear if the defacement is in any way related to the current conflict. The defacer(s) posted the following message, *"(HACKEADO POR USDL+{PH}+ BRASIL, greetz: L4ctus, SFx-1 e todos +{PH}+ ,securenet, hackernewsBRASIL... EU SOU BRASILEIRO COM MUITO ORGULHO APESAR DE TODA CORRUP€AO Q ENVOLVE ESTE PAIS. PLANET HACKER CLA ESTA COMIGO.)"*

▪ tR|cky and xoid deface the Open University-Jerusalem site at http://www.jccopenu.ac.il in support of the Palestinians.

Nov. 25, 2000

▪ Pro-Palestinian attackers launch a 3-hour coordinated assault against the Israel Ministry of Finance site at http://www.mof.gov.il and the email address webmaster@mof.gov.il.

Nov. 26, 2000

▪ m0sad defaces the Khaleej.com site at http://www.khaleej.com in support of the Israelis.

Nov. 28, 2000

▪ m0sad defaces Islam Web at http://www.islamweb.net in support of the Israelis.

Nov. 29, 2000

▪ m0sad defaces webhosting.ajeeb.com in support of the Israelis.

Nov. 30, 2000

▪ m0sad defaces the Sakhr Software Co. site at http://www.ajeeb.com in support of the Israelis.

Dec. 1, 2000

- m0r0n and nightman deface SOMA Galleries at http://www.somagalleries.com in support of the Palestinians. The defacement team also announces the duo have joined the World's fantabulous defacers (WFD).

- Israel Land Administration site forced to close down most of its site due to cyber attacks. Attacks began in the middle of the week but eventually overwhelmed the site on the Dec. 1.

Dec. 2, 2000

- [^CyBeRpUnK^] defaces the Hebrew University of Jerusalem, Israel site at http://shemesh.fiz.huji.ac.il with a pro-peace message.

- [^CyBeRpUnK^] defaces the www.as.huji.ac.il site with a pro-peace message.

- m0sad defaces www.talkislam.com in support of the Israelis.

Dec. 3, 2000

- m0r0n and nightman deface www.comune.scandiano.re.it in support of the Palestinians.

- m0sad defaces the Ministry of Awqaf and Islamic Affairs, Qatar site at http://www.islam.gov.qa in support of the Israelis.

Dec. 5, 2000

- m0r0n and nightman of WFD deface the Haifa University Campus Network site at http://modiin.haifa.ac.il in support of the Palestinians.

- B_Real and BrakeOFF deface the Los Alamos Neutron Science Center site at http://www.lansce.lanl.gov in support of the Palestinians.

Dec. 7, 2000

- m0r0n and nightman of WFD deface the Volasia Ltd. site at http://www.volasia.com in support of the Palestinians.

- [^CyBeRpUnK^] of WFD defaces admin-scb.ouhsc.edu in support of the Palestinians. Makes offer of cooperation to Doctor Nuker in defacement.

Dec. 8, 2000

- B_Real and BrakeOFF deface www.cruzazul.com.mx in support of the Palestinians.

Dec. 9, 2000

- SomeOneFromHeaven (SoFh) of WFD defaces www.cowboysorlando.com in support of the Palestinians.

- SomeOneFromHeaven (SoFh) of WFD defaces the Christian Sharing Center site at http://www.christiansharing.org in support of the Palestinians.

- SomeOneFromHeaven (SoFh) of WFD defaces the Central Florida Bankruptcy Law Association site at http://www.cfbla.org in support of the Palestinians.

- [^CyBeRpUnK^] and nightman of WFD deface albert.ph.biu.ac.il in support of the Palestinians.

- m0r0n and nightman of WFD deface the University Medical Center Nijmegen Dept. of Urology, Netherlands site at http://uroworld.azn.nl in support of the Palestinians.

Dec. 10, 2000

- m0r0n and nightman of WFD deface www.pccua.cc.ar.us in support of the Palestinians.

- m0sad defaces the United Arab Emirates Dept. of Civil Aviation site at http://www.dcaauh.gov.ae in support of the Israelis.

- BrakeOFF defaces www.corpac.gob.pe in support of the Palestinians.

- BrakeOFF defaces sgl1.lanres.com in support of the Palestinians.

- BrakeOFF defaces the ARON site at http://www.aron.be in support of the Palestinians.

Dec. 11, 2000

- h3ll rais3r and laughing3y3s of WFD deface www.asbis.sk in support of the Palestinians.

- SomeOneFromHeaven (SoFh) of WFD defaces www.al-libaas.com in support of the Palestinians.

Dec. 12, 2000

- m0r0n and nightman of WFD deface the Wisconsin K12 Schools site at http://www.sharon.k12.wi.us in support of the Palestinians.

- [^CyBeRpUnK^] and nightman of WFD deface the Hebrew University of Jerusalem, Israel site at http://www.music.md.huji.ac.il in support of the Palestinians.

- m0sad defaces the Iranian Foreign Ministry site at http://mfa.gov.ir in support of the Israelis.

Dec. 13, 2000

- SomeOneFromHeaven (SoFh) of WFD defaces Lymphedema Awareness Foundation site at http://www.lymphaware.org in support of the Palestinians.

- WFD defaces the Hebrew University of Jerusalem, Israel site at http://daat.ls.huji.ac.il in support of the Palestinians.

Dec. 14, 2000

- BrakeOFF defaces www3.co.oakland.mi.us in support of the Palestinians.

Dec. 15, 2000

- m0sad defaces the Talk Islam, Library of Islamic Web Sites at http://www.talkislam.com in support of the Israelis.

Dec. 16, 2000

- m0r0n and nightman of WFD deface www.ann-arbor.med.va.gov in support of the Palestinians.
- m0r0n and nightman of WFD deface www.dol.wa.gov in support of the Palestinians.
- h3ll rais3r and laughing3y3s of WFD deface the AMTEL Slovensko Ltd. site at http://www.amtel.sk in support of the Palestinians.
- Tå|{ê Ñø £Øgîç of WFD defaces the Malaysian Rubber Board site at http://www.lgm.gov.my in support of the Palestinians.

Dec. 17, 2000

- EdGe defaces the Server Computers site at http://www.netserver.co.il in support of the Palestinians.
- m0r0n and nightman of WFD deface the Karnataka Telecom Circle site at http://www.karnataka.dotindia.com in support of the Palestinians.
- GForce Pakistan defaces the Indian Institute of Science Materials Research Center site at http://arun.mrc.iisc.ernet.in in support of the Palestinians.
- GForce Pakistan defaces the Indian Institute of Science Dept. of Mechanical Engineering site at http://mecheng.iisc.ernet.in in support of the Palestinians.

Dec. 18, 2000

- m0r0n and nightman of WFD deface the BSNL Nagpur (Depart of Telecom) site at http://nagpur.dotindia.com in support of the Palestinians.
- Tå|{ê Ñø £Øgîç of WFD defaces the Kuala Lumpur Department of Urban Transportation site at http://www.jpbdbkl.gov.my in support of the Palestinians.
- GForce Pakistan defaces the Dizasta Productions site at http://www.dizasta.net in support of the Palestinians.

Dec. 19, 2000

- m0sad defaces the Islamic University, Gaza site at http://www.iugaza.edu in support of the Israelis.

- m0sad defaces the Islamic Society of North America site at http://www.isna.net in support of the Israelis.

- BrakeOff defaces the Qatar Ministry of Awqaf and Islamic Affairs at http://www.islam.gov.qa in support of the Palestinians.

- Laughing3y3s and h3ll rais3r from WFD deface shop.chemolak.sk in support of the Palestinians.

- Laughing3y3s and h3ll rais3r of WFD deface www.cardcentrum.sk in support of the Palestinians.

- SomeOneFromHeaven (SoFh) of WFD defaces United Studios Corp. at http://www.usidentity.com in support of the Palestinians.

- m0r0n and nightman of WFD deface the Kolhapur Telecom District site at http://www.kolhapur.dotindia.com in support of the Palestinians.

- Tå|{ê Ñø £Øgîç of WFD defaces the Scicom site at http://www.scicom.com.my in support of the Palestinians.

- GForce Pakistan defaces Web of India site at http://webmail.webindia.com in support of the Palestinians.

- GForce Pakistan defaces Web of India site at http://tanishq.webindia.com in support of the Palestinians.

- GForce Pakistan defaces Web of India site at http://servlet.webindia.com in support of the Palestinians.

- GForce Pakistan defaces Web of India site at http://servlet2.keralatourism.org in support of the Palestinians.

- GForce Pakistan defaces Web of India site at http://dmss.webindia.com in support of the Palestinians.

- [^CyBeRpUnK^] of WFD defaces the KAIZ site at http://www.kaiz.com in support of the Palestinians.

Dec. 20, 2000

- m0r0n and nightman deface the Ardom Telecomputing of Israel site at http://www.ardom.co.il in support of the Palestinians.

- GForce Pakistan defaces www.xmlprobe.com in support of the Palestinians.

- GForce Pakistan defaces the University of Chicago Computer Science Dept. site at http://hamachi.cs.uchicago.edu/ in support of the Palestinians.

- Kr4kr0k Industries defaces Arttalk.com at http://www.arttalk.com in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.hmcnet.com in support of the Palestinians.

Dec. 21, 2000

- m0r0n and nightman of WFD deface www.aztek.co.il in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.stadtklima.de in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.cog.co.jp in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface the University of North Texas site at http://www2.music.unt.edu in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.desisti.it in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.929rtl.at in support of the Palestinians.

Dec. 22, 2000

- EDGE & KARTOOS.AK.47 deface www.tamtravel.com in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.pryor.k12.ok.us in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.carroll.k12.ga.us in support of the Palestinians.
- GForce Pakistan defaces the Merical (IN) site at http://email.merical.ac.in in support of the Palestinians.
- ConClaveCrew defaces the Sheffield Hallam University site at http://jeff.sci.shu.ac.uk with a pro-peace message.

Dec. 23, 2000

- m0r0n and nightman of WFD deface the Centers for Disease Control and Prevention (CDC) site at http://phil.cdc.gov in support of the Palestinians.
- h3ll rais3r and laughing3y3s of WFD deface the Forma Ltd. site at http://www.deiure.sk in support of the Palestinians.
- GForce Pakistan defaces #2 National Centre for Radio Astrophysics site at http://sakthi.ncra.tifr.res.in in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface the Frostbit.com site at http://www.frostbit.com in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.nbas.cz in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface www.cursobolsa in support of the Palestinians.
- EDGE & KARTOOS.AK.47 deface the Deutsche Forschungsanstalt fuer Luft – und Raumfahrt e.V. (DLR) site at http://www.weblab.dlr.de in support of the Palestinians.

- EDGE & KARTOOS.AK.47 deface www.s-scptuj.mb.edus.si in support of the Palestinians.

- EDGE & KARTOOS.AK.47 deface the #3 Lal Bahadur Shastri National Academy of Administration, Mussoorie at http://www.lbsnaa.ernet.in in support of the Palestinians.

- EDGE & KARTOOS.AK.47 deface dns0.whuci.edu.cn in support of the Palestinians.

- EDGE & KARTOOS.AK.47 deface www.whuci.edu.cn in support of the Palestinians.

Dec. 24, 2000

- H3ll rais3r and laughing3y3s of WFD deface the Compact Studio site at http://www.dvdbest.sk in support of the Palestinians.

- GForce Pakistan defaces the Indian Institute of Science Dept. of Metallurgy at http://www.metalrg.iisc.ernet.in in support of the Palestinians.

- GForce Pakistan defaces delhinms.mtnl.net.in in support of the Palestinians.

- EDGE & KARTOOS.AK.47 deface www.scjh.kh.edu.tw in support of the Palestinians.

- EDGE & KARTOOS.AK.47 deface www.retliv.com in support of the Palestinians.

Dec. 25, 2000

- WFD defaces the Pelenews site at http://www.pelenews.co.il in support of the Palestinians.

- Kashmir Hackers Club (KHC) deface www.microconnectors.com in support of the Palestinians.

- GForce Pakistan defaces the Indian Institute of Science Solid State and Structural Chemistry Unit site at http://zeolite.sscu.iisc.ernet.in in support of the Palestinians.

Dec. 26, 2000

- Hezbollah site at http://www.hizbollah.org defaced by pro-Israeli attacker.

- m0r0n and nightman of WFD deface the Anti-Defamation League (ADL) site at http://www.adl.org in support of the Palestinians.

- m0r0n, nightman, and fighter4Isl@m of WFD deface www.dilim.co.il in support of the Palestinians. Announcement signaling the beginning of Phase 5 is made in the defacement.

Dec. 27, 2000

- m0r0n, nightman, and fighter4Isl@m of WFD deface www.order-click.co.il in support of the Palestinians. Announcement signaling the beginning of Phase 5 is made in the defacement.

- GForce Pakistan defaces the Rabia Gupta Design site at http://www.styletantra.com in support of the Palestinians.

Dec. 28, 2000

- EDGE & KARTOOS.AK.47 deface the sira1.sira.it in support of the Palestinians. The defacement announces the formation of THE SCYTHE by the two attackers.

XVII. Defacement Tables

Web site defacements only

	TOTAL	01/06/01	01/05/01	01/04/01	01/03/01	01/02/01	01/01/01	12/31/00	12/30/00	12/29/00	12/28/00	12/27/00	12/26/00	12/25/00	12/24/00	12/23/00	12/22/00	12/21/00	12/20/00	12/19/00	12/18/00	12/17/00	12/16/00	12/15/00	12/14/00	12/13/00	12/12/00	12/11/00	12/10/00	12/09/00	12/08/00	12/07/00	12/06/00	12/05/00	12/04/00	12/03/00	12/02/00	12/01/00	11/30/00	11/29/00	11/28/00	11/27/00	11/26/00
				WEEK 13							WEEK 12							WEEK 11							WEEK 10							WEEK 9							WEEK 8			
Pro-Israeli	**19**	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	2	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	1	1	0	1	1	1	1	0	1
lion&type_o	4																																										
pakistan is gay	1																																										
unknown	1																																										
Nir M	1																																										
m0sad	11																			2				1		1		1								1	1		1	1	1		1
Dhalsou	1												1																														
Pro-Palestinian	**163**	0	0	0	0	0	0	0	0	1	2	2	2	5	11	4	6	5	12	3	4	4	0	1	2	2	2	4	5	1	2	0	2	0	1	0	1	0	0	0	0	0	0
World's Fantabulous Defacers	45	0	0	0	0	0	0	0	0	0	1	2	1	1	2	0	1	1	7	2	1	4	0	1	2	2	2	4	5	1	2	0	2	0	1	0							
m0r0n and nightman	41											1			1		1	1	1	1	1	2			1		1	1	1		1		1		1	1						
m0r0n, nightman and fighter4isl@m	2										1	1																														
B_Real and BrakeOff	2																												1		1											
h3ll rais3r and laughing 3y3s	6												1	1			2		1			1																				
TakeNoLogic	3																1	1	1																							
[^CyBeRpUnK^]	3																1			1	1																					
[^CyBeRpUnK^] and nightman	1																				1																					
SoFh	6																1		1	1	3																					
unknown	2												1							1																						
BrakeOff	5																1	1	3																							
EdGe	1																		1																							
EdGe and KARTOOS.AK.47	20										1	2	8	3	5	1																										
Kr4kr0k Industries	1													1																												
tR|cky	8																																										
GForce Pakistan	41									1	1	2	1	1	2	5	1	2																								
Dr. Nuker	1																																										
dodi	7																																										
Kala	1																																										
ReAList+ProjectGamma	7																																										
poltergeists (smooth)	2																																										
xZeroKiller	1																																										
Murtaza Baloch aka EdGe	1																																										
afterstep and datalock	1																																										
Kashmir Hackers Club	0																																										
Neutral	**6**	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0
DeTH`Sauron	1																																										
AnCiLaToR	2																																										
[^CyBeRpUnK^]	2																																			2						
ConClaveCrew	1														1																											
TOTAL	**188**	0	0	0	0	0	0	0	0	1	2	3	2	5	11	5	6	5	14	3	4	4	1	1	2	3	2	5	5	1	2	0	2	0	2	3	1	1	1	1	0	1
WEEKLY TOTALS				0							13							48							18							12							8			

	WEEK 7							WEEK 6							WEEK 5							WEEK 4							WEEK 3							WEEK 2						
	11/25/00	11/24/00	11/23/00	11/22/00	11/21/00	11/20/00	11/19/00	11/18/00	11/17/00	11/16/00	11/15/00	11/14/00	11/13/00	11/12/00	11/11/00	11/10/00	11/09/00	11/08/00	11/07/00	11/06/00	11/05/00	11/04/00	11/03/00	11/02/00	11/01/00	10/31/00	10/30/00	10/29/00	10/28/00	10/27/00	10/26/00	10/25/00	10/24/00	10/23/00	10/22/00	10/21/00	10/20/00	10/19/00	10/18/00	10/17/00	10/16/00	10/15/00
Pro-Israeli	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	1	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
lion&type_o													2								1	1																				
pakistan is gay																		1																								
unknown																								1																		
Nir M																										1																
m0sad																																										
Dhalsou																																										
Pro-Palestinian	0	0	0	0	0	1	1	0	4	4	2	4	3	3	2	3	11	2	3	7	4	8	2	1	6	2	0	0	0	2	0	1	0	2	1	0	2	1	0	0	0	0
World's Fantabulous Defacers																																										
m0r0n and nightman										3	1	2	2		1		3	2		2		2	1	2		4																
m0r0n, nightman and fighter4isl@m																																										
B_Real and BrakeOff																																										
h3ll rais3r and laughing 3y3s																																										
TakeNoLogic																																										
[^CyBeRpUnK^]																																										
[^CyBeRpUnK^] and nightman																																										
SoFh																																										
unknown																																										
BrakeOff																																										
EdGe																																										
EdGe and KARTOOS.AK.47																																										
Kr4kr0k Industries																																										
tR|cky							1	1							1	2	1		2																							
GForce Pakistan																	7		3	7	2	6																				
Dr. Nuker																									1																	
dodi																						1		2									1			2	1					
Kala																									1																	
ReAList+ProjectGamma											3						1								1							2										
poltergeists (smooth)												1	1																													
xZeroKiller												1																														
Murtaza Baloch aka EdGe											1																															
afterstep and datalock											1																															
Kashmir Hackers Club																																										
Neutral	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DeTH`Sauron																										1																
AnCiLaToR																1		1																								
[^CyBeRpUnK^]																																										
ConClaveCrew																																										
	0	0	0	0	0	1	1	0	4	4	2	4	5	3	2	4	12	3	3	8	5	8	2	2	7	2	1	0	0	0	2	0	1	0	2	1	0	0	0	0	0	0
						1					20						35							27							3							3				

Defacement Activity By Day

Legend:
- Pro-Israeli
- Pro-Palestinian
- Neutral

Israeli-Palestinian Cyber Conflict (IPCC) Report v2.0PR – Jan. 3, 2000 – 15:41 GMT
CONTACT INFO: analysis@idefense.com, voice (703) 383.5280, fax (703) 359-5323
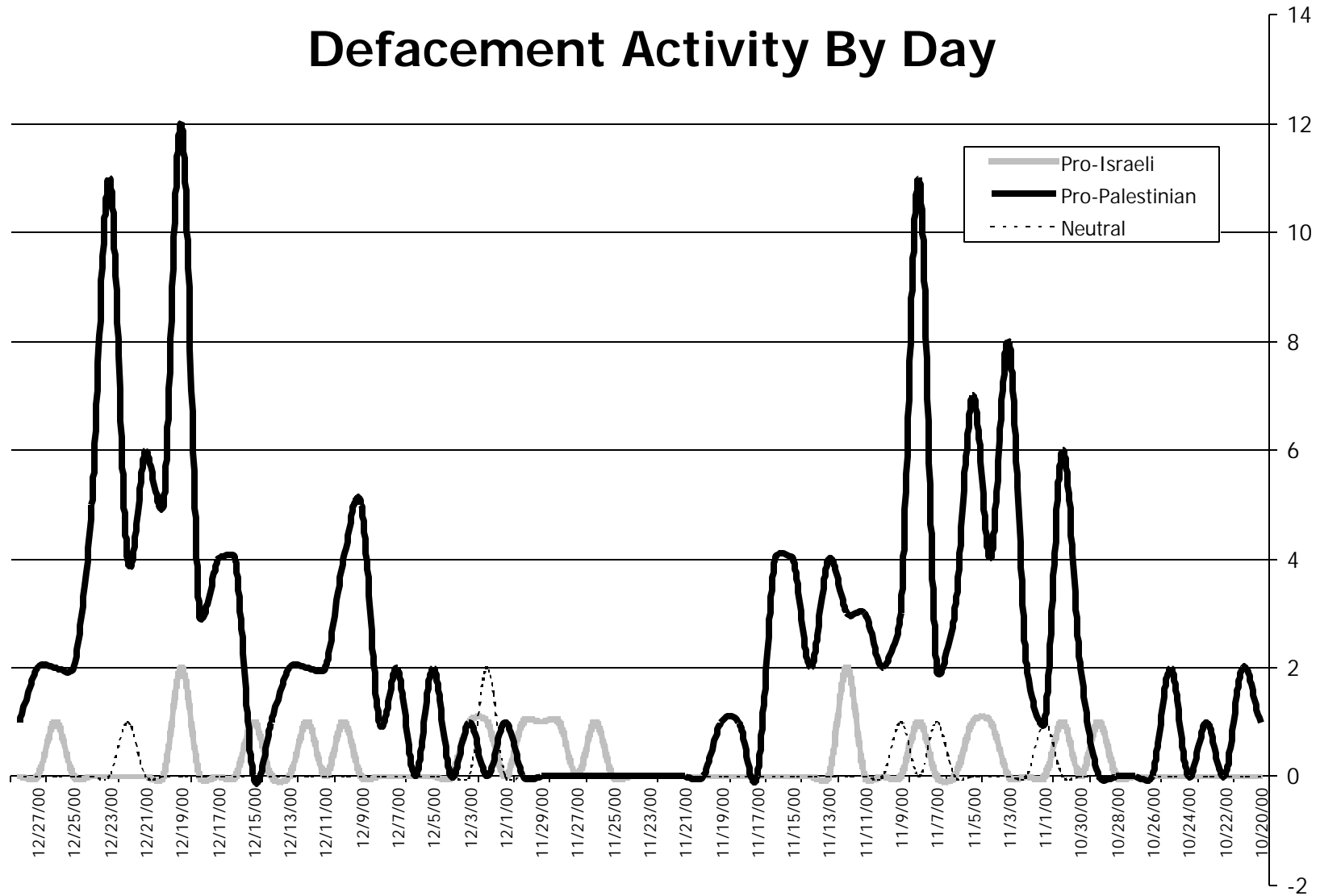
Total Defacements Over Time

Legend:
- Pro-Israeli
- Pro-Palestinian
- Neutral

Y-axis: 0, 20, 40, 60, 80, 100, 120, 140, 160, 180

X-axis: 10/21/00, 10/23/00, 10/25/00, 10/27/00, 10/29/00, 10/31/00, 11/02/00, 11/04/00, 11/06/00, 11/08/00, 11/10/00, 11/12/00, 11/14/00, 11/16/00, 11/18/00, 11/20/00, 11/22/00, 11/24/00, 11/26/00, 11/28/00, 11/30/00, 12/02/00, 12/04/00, 12/06/00, 12/08/00, 12/10/00, 12/12/00, 12/14/00, 12/16/00, 12/18/00, 12/20/00, 12/22/00, 12/24/00, 12/26/00, 12/28/00

Israeli-Palestinian Cyber Conflict (IPCC) Report v2.0PR – Jan. 3, 2000 – 15:41 GMT
CONTACT INFO: analysis@idefense.com, voice (703) 383.5280, fax (703) 359-5323

XVIII. Partial Open-Source List

iDEFENSE is an intelligence company that uses a global-collection network. This network, through automated and manual means, monitors national and foreign media sources, technical publications, an extensive array of vendor and security firm contacts, open channels of communication with various government agencies and a developing program, which cuts right through to groups and individuals actually involved in attacks.

Below is a partial listing of open sources used in the creation of this report:
- AFP
- Alldas.de
- Attrition
- CNN
- CNET
- ComputerUser.com
- Israel Radio
- *Jerusalem Post*
- *Jerusalem Report*
- *The Daily Star* (Lebanese)
- MSNBC
- Newsbytes
- Reuters
- *Washington Post*
- Wired.com
- Yahoo! News

XIV. Index