Threat Alert

#OPISRAEL

Benishti Eyal, Balmas Yaniv, Matan Atad
Emergency Response Team

November 18, 2012

EXECUTIVE SUMMARY

The recent Israel Defense Forces ‘Operation Pillar of Cloud’ in the Gaza Strip, which was officially launched on 14 November, 2012, has raised strong protests from the Anonymous cyber group, which have in response launched #OpIsrael, a cyber-attack campaign whose main objectives are:

1. Ensure communication channels availability in the Gaza Strip, and provide alternative communication methods in case of an Israeli communication blackout as part of the military operation.
2. Take down Israeli and Israeli related Web sites.
3. Deface Israeli sites and promote anti-Israeli agendas.
4. Stop the violence.

Since #OpIsrael started, several Israeli government sites were reported down, and additionally many other small privately held sites were defaced.

The following message was published as a kickoff to this operation: http://pastebin.com/9M0HLC3d, followed by a request to target more substantial infrastructures like banks and airlines.

At this point more information started to flow over the IRC channels explaining to new attackers how to download the attack tools of choice, and how to stay anonymous using TOR and free VPN services.

As time goes by, more and more attackers are taking part in these attacks and more attack vectors are being discussed over the channels. SQLi and more sophisticated HTTP attack vectors are discussed heavily.

Needless to say, the attackers are mostly looking to deface the target sites in order to plant their pro-Palestinian/anti Israeli messages.

The following is a partial list of some of the reported attacks and their impacts:

Attacked Site	Impact
www.pmo.gov.il	Reoccurring short-term outages
www.isa.gov.il	Taken offline
www.philippine-embassy.org.il	Defacement
http://deplus.co.il	Defacement
http://www.falcon-s.co.il/	Defacement
president.gov.il	Taken offline
idfblog.com	Taken offline
libi.org.il	Taken offline
police.gov.il	Taken offline

For a full list of defacements, refer to **http://pastebin.com/Ms4nJSZx**

ATTACK CAMPAIGN DETAILED INFORMATION

The attack campaign is being coordinated through Twitter and a dedicated IRC Channel: http://webchat.voxanon.org/ (Channel #OpIsrael).

Currently the attackers have published a care package for Palestinian citizens and have made several public announcements, including in Hebrew.

ATTACK CAMPIGN SPECIFIC TARGETS

Currently the main attack target is www.idf.il. At the time of the writing this document, no outages have yet been reported to this site.

Several other targets have also been reported, such as idfblog.com. This site runs WordPress, and brute force attacks have been reported to have taken place which have caused an outage to the site.

It seems that in the initial stage of the attacks, the attackers were looking for 'low hanging fruit' and did not put much effort or sophistication in their attacks.

The same is true for the DDoS campaign delivered by this Anonymous group, using well known, easy to get and operate attack tools.

PUBLISHED ATTACK TOOLS VS. DEFENSEPRO MITIGATION

The following attack tools have been announced by the attack coordinators and other active participants:

Attack Tool	Attack Vectors	DefensePro Mitigation
ByteDos version 3.2	ICMP Flood SYN Flood	BDoS SYN Protection
Mobile LOIC	HTTP Floods	Signatures
LOIC for android devices	HTTP Floods UDP Flood TCP Flood	Web Cookies BDoS Signatures
Tor's Hammer	HTTP Post Flood Using TOR Network	Web Cookies
SlowLoris	Slow HTTP Attack	Signatures
PyLoris	Slow HTTP POST Attack	Signatures
THC SSL DOS	SSL Renegotiation Flood	Signatures

RECOMMENDED DEFENSEPRO CONFIGURATION

ERT recommends that customers apply the following configuration to the relevant security policies in order to ensure that #OpIsrael attacks are properly mitigated:

1. Apply BDoS and SYN Protection profiles
2. Apply Web Cookies 'JavaScript' with aggressive Activation Threshold
3. Update the DefensePro signature file to the latest (0009.0172.00)
4. Apply 'DoS-All' Signature Profile
5. Perform the following signature tuning-
    a. **Mobile LOIC-** Apply 'Suspend Source' action on RWID 15416
    b. **Slowloris-** Move RWID 10526 to 'Drop' and apply suspend action
    c. **Slowloris-** Move RWID 12912 to 'Drop' action
    d. **Pyloris-** Move RWID 14816 to 'Drop' and apply suspend action
    e. **THC-SSL-DOS-** Move both RWID 11018 and RWID 11024 to 'Drop' action
    f. **Android LOIC-** Apply custom signatures; console commands are shown below:

Console Commands to Apply a Custom Signature for Android LOIC

Enter the following commands at the console to apply a custom signature against 'Android LOIC' (line-by-line):

```
dp signatures-protection filter basic-filters user create Android-LOIC-TCP-
whe -p tcp -c “When\20harpoons,\20air” -ct Text -ce "Case Sensitive" -dp http

dp signatures-protection attacks user create 0 -n Android-LOIC-TCP-whe -f
Android-LOIC-TCP-whe

dp signatures-protection filter basic-filters user create Android-LOIC-UDP-
whe -p udp -c “When\20harpoons,\20air” -ct Text -ce "Case Sensitive" -dp http

dp signatures-protection attacks user create 0 -n Android-LOIC-UDP-whe -f
Android-LOIC-UDP-whe

dp update-policies set 1
```