

**DoS Attack Campaign against a country - January 2012**  
**Bypassing CDN**

**Table of Content**

**Preamble .....3**

    About Radware’s DefensePro..... 3

    About Radware’s Emergency Response Team ..... 3

**Summary .....4**

    Executive Summary ..... 4

**Attack Details .....6**

    Attack Vector I - HTTP Dynamic Flood..... 6

    Attack Vector II: UDP Flood ..... 8

    Attack Vector III: HTTP Static Flood..... 9

    Attack Vector IV: SYN Flood or Scan Attempt ..... 11

    Attack Vector V: Fragmented UDP Flood ..... 12

## Preamble

This case summary describes one of the real life attacks which was experienced by Radware's customer and successfully mitigated thanks to Radware's DefensePro product and Radware's Emergency Response Team (ERT) expertise. The customer's name is undisclosed for privacy purposes and is referred to by "customer" in this report.

### About Radware's DefensePro

Radware's award-winning DefensePro is a real-time network attack prevention device that protects the application infrastructure against network & application downtime, application vulnerability exploitation, malware spread, network anomalies, information theft and other emerging network attacks. It combines a set of security modules which altogether provide a complete attack mitigation solution: Intrusion Prevention System (IPS), Network Behavioral Analysis (NBA), Denial-of-Service (DoS) Protection and Reputation Engine. The vast majority of the attacks are successfully mitigated and stopped by DefensePro alone.

### About Radware's Emergency Response Team

Radware's Emergency Response Team (ERT) is a service, complementary to Radware's DefensePro, designed to provide 24x7 security services for customers facing a denial-of-service (DoS) attack or a malware outbreak. Often, these attacks require immediate assistance. The ERT provides instantaneous, expert security assistance in order to restore network and service operational status. IT is staffed by experts that have vast knowledge and experience with network threats, their detection and mitigation, and in-depth experience of the DefensePro family of products. In addition, the ERT takes information from each customer engagement and simulates the same scenario internally for further analysis and proactive implementation of defense techniques for other customers that may be facing a similar security threat.

## Summary

### Executive Summary

#### Background

This attack report describes an attack campaign against a country (Israel) and how several sites in this country were attacked simultaneously over a full week. A Pro Palestinian hackers group, the “Nightmare group” and Oxomar, a Saudi hacker member of the Saudi Arabian Anonymous collective, have disclosed credit card information of thousands of Israeli citizens, later leading to retaliation action by Israeli hackers. Prior to the attack, the media reported that few Israeli websites, both in public and private sectors, were about to be attacked.

#### The Attack Campaign

On Day 1, a cyber attack campaign started against various Israeli websites lasting for several days. The first victims were as announced in the media while another target was attacked as well. The attack was a dynamic HTTP flood (Attack Vector I), in which the URL is changed at each HTTP request packet to bypass any proxy or CDN on the way. It caused serious outage that lasted for several hours. Nevertheless and as explained below, the sites were eventually able to overcome the attack.

On Day 2, more Israeli websites were attacked – one of them was attacked with a UDP flood on port 443 (Attack Vector II) where the attacker sent very large packets.

On Day 3, another massive HTTP flood was launched against an additional Israeli website. This static HTTP flood (Attack Vector III) was different from the first one. On one hand it was simpler as it used the same URL again and again, but about 800 attackers came from a local host proxy which may be a new technique to bypass challenge-based mitigation technologies. The attack peak reached 50K concurrent connection which is 10 times more the sites normal activity.

On Day 4, the victim’s website attacked on Day III was hit again with the same attack vector. Later, it was attacked with a UDP flood on port 80 (Attack Vector V).

#### Mitigation

Four out of the five attacked organizations are now fully protected by Radware DefensePro (DP). They are either protected in their own premises, or by their ISP or both. The outage time each organization suffered was mostly determined by the protection they had in place or not, and how much time it took to arrange it. The first day it took the organizations more time to deploy the solution. This time was used by the ERT to conceive the proper protection by analyzing the capture files containing the attack, and therefore causing mitigation to start shortly after the deployment.

One of the victims had an old protection device model and its policies were disabled. Once they enabled them and installed the ERT’s protection; the site came alive and they are now fully protected.

By not responding to Radware’s offer to assist, one of the other victims is the only organization that is not protected by any anti-DoS device. They were able to partly mitigate the attack as one

of their ISPs placed their traffic under their DefensePro device protection (which was already configured with suitable protections), but this was just one internet pipe out of two. It is not clear if they were able to mitigate the attack on their own or just waited for it to stop. In another case, the victim, which was not primarily protected by Radware's device, attempted to mitigate the attack on their own, but eventually protected themselves (only pipe saturation) using their ISP's DefensePro unit, and later on installed an additional device on site to get full security coverage. Finally, two more victim websites both hosted and protected by a government agency hosting service were able to successfully mitigate the attack without any ERT intervention, as this government agency installed DefensePro devices over six months ago.

### **Aftermath**

Following this attack campaign, Israeli hackers had formed their own group called the "IDF-Team". They said that if the attacks didn't stop on Israeli sites, they will hit back hard. This same month, the IDF-Team launched retaliation attacks taking down Saudi Arabia and the UAE's stock exchange websites. One member of the Israeli hacking team stated: we will "disable stock market, government, economic and security sites".

## Attack Details

### Attack Vector I - HTTP Dynamic Flood

#### Summary

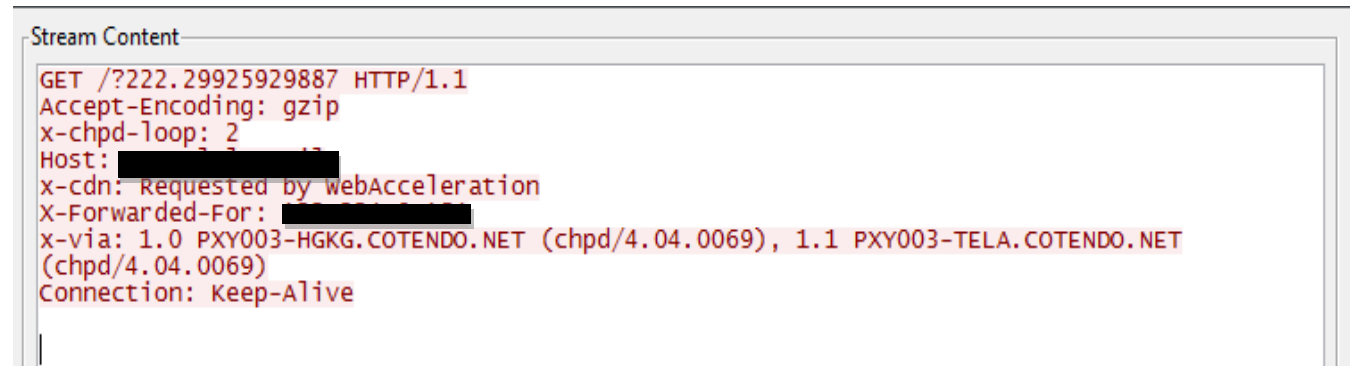
This attack vector occurred on the first day of the attack and caused outages at three high profile Israeli websites. The outage lasted for several hours, and was reported on both domestic and international media.

The attackers constantly changed the URL to ensure that each and every attacking packet reached its final destination and was not cached by a CDN or proxy.

The attack was overcome by three technologies: a signature that searched for the unique pattern used by attackers, and web challenges. Web Challenge are usually preferred over manual signatures, however, the first target site ERT involved was using CDN services for which Web Challenge are not applicable. Finally SYN Protection was used, not for a Syn Flood per se, but to offload TCP negotiation from server to the DefensePro protection device.

#### Attack Description

Here is a snapshot of the attacking packet.



The “GET /?222.29925929887 HTTP/1.1” constantly changed and was very dynamic.

#### Motivation for using the dynamic URLs

One of the problems of HTTP flood attacks (from attacker’s perspective) is that HTTP request may be answered by the local ISP proxy or by CDN, and not reach the actual targeted web server. The attacker used a technique to ensure each and every HTTP Request reaches its final target.

By making each URL random and dynamic, the proxies and CDN had to pass the requests to the end web server.

#### Mitigation

##### Signature Based

Since the attacker used a unique and predictable pattern, it was possible to create a signature for it, that checks for "?", then one or more digits and finally consecutive "." (dot). The actual Regular Expression used was: "\?[0-9]+\."

### **SYN Protection**

SYN protection was also used, not to protect a SYN flood per se, but to offload the TCP handshake from the attacked server to the DefensePro.

Indeed, when SYN Protection is triggered the DefensePro conducts the TCP handshake then receives the first data packet, and only then the DefensePro device sends the first SYN packet to the web server. Now, since the malicious data packet was dropped, the handshake with the web server did not take place, and the web server TCP/IP stack resources were protected.

### **Web Challenge**

For sites that do not use CDN, Web Challenges were additionally implemented and blocked the attack in an efficient way.

This protection couldn't always be used for sites which are behind CDNs as the true IP of the attacker is not always known.

## Attack Vector II: UDP Flood

### Summary

On day 2, a massive UDP flood was launched against an additional Israeli site. The flood was comprised of very large UDP packets targeting port 443 (SSL).

### Attack Description

A UDP flood generally tries to saturate. This is normally done by sending a rapid succession of UDP datagram's with spoofed IP's to a server within the network to various different ports, forcing the server to respond with ICMP traffic. The saturation of bandwidth happens both ways (inline (UDD)/upstream (ICMP)).

The traffic looks similar to the below Capture.

63387	1.997252			ICMP	590 Destination unreachable	63387	43381
63387	2.003662			UDP	1066 Source port: 63387	63387	62319
63387	2.004041			ICMP	590 Destination unreachable	63387	62319
63387	2.010884			UDP	1066 Source port: 63387	63387	6654
63387	2.011354			ICMP	590 Destination unreachable	63387	6654
63387	2.017982			UDP	1066 Source port: 63387	63387	56248
63387	2.018292			ICMP	590 Destination unreachable	63387	56248
63387	2.024237			UDP	1066 Source port: 63387	63387	64868
63387	2.024544			ICMP	590 Destination unreachable	63387	64868
63387	2.028850			UDP	1066 Source port: 63387	63387	24782
63387	2.029052			ICMP	590 Destination unreachable	63387	24782

However, since UDP protocol doesn't have any congestion control built in, its datagram size is limited more by MTU (maximum transmission unit) than the protocol itself. If the receiving application hasn't been programmed to handle high rate traffic, coupled with large packet sizes the service could become unstable or unusable.



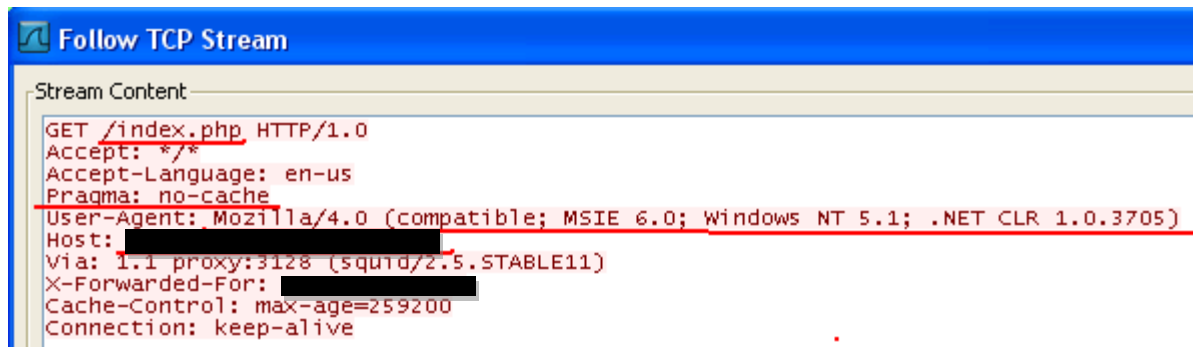
## Attack Vector III: HTTP Static Flood

### Summary

On Day 3 of the attack campaign, another high profile Israeli site was attacked by an HTTP flood. Unlike [Attack Vector I - HTTP Dynamic Flood](#), this attack was to a static URL.

### Attack Description

The HTTP flood targeted a static URL (“index.php”) and contained a specific not popular “User-Agent” attribute which used the Pragma HTTP header with no cache value, to bypass proxies.



```
Follow TCP Stream
Stream Content
GET /index.php HTTP/1.0
Accept: */*
Accept-Language: en-us
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)
Host: [redacted]
Via: 1.1 proxy:3128 (squid/2.5.STABLE11)
X-Forwarded-For: [redacted]
Cache-Control: max-age=259200
Connection: keep-alive
```

### Attack Measurement

#### Number of attackers:

Capture file analysis indicates 600~800 attackers. Real number is much higher since capture file was taken when heavy protection was already on.

#### Request per second

Each attacker conducted the request every 4 seconds on average.

#### Concurrent connections

50,000 - at first strike

2400 - with Web Challenge only

1100 - with signature (in addition to Web Challenge)

500 – with inserting attacking IPs to blacklist (Suspend Action) and ISP line cut off.

Note: the measurements were taken at different times in which the attack volume may have been different.

### Attack Distribution

The following map shows distribution of the attackers. This however is based on a partial list of attackers of about 700 IPs.



### Usage of Local Proxy

Multiple numbers of attackers (at least 800) appeared to be coming behind a proxy set to 127.0.0.1 (localhost).

```

Follow TCP Stream
Stream Content
GET /index.php HTTP/1.1
Accept: */*
Accept-Language: en-us
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
Host: [REDACTED]
Via: 1.0 wienerwald-proxy (squid/3.1.14)
X-Forwarded-For: 127.0.0.1
Cache-Control: max-age=259200
Connection: keep-alive

```

We suspect that the attacker installed a local proxy so it would pass web challenges for the script.

### Attack Mitigation

#### Web Cookies (For HTTP flood and possible SYN flood)

Web Challenge (JavaScript) effectively blocked the attackers (enabled on the SYN protection).


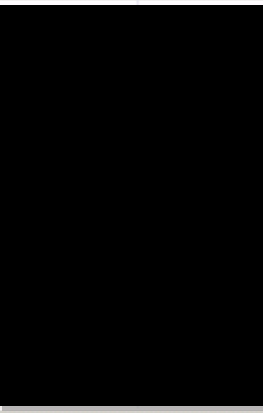














#### IPS Signature (For HTTP Flood)

Signature was created based on the attackers known pattern. The signature effectiveness was to block those that passed the Web Challenge.

## Attack Vector IV: SYN Flood or Scan Attempt

### Attack Description

Another minor attack was a certain SYN Flood or Scan attempt:

Table							
Start Time	Category	Status	Risk	Attack Name	Source Address	Destination Address	Destination L4 Port
5:17 PM	Intrusions	Occurred		SIP-Scanner-SIPficious			5060
5:17 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			48601
5:16 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			36954
5:16 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			9008
5:16 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			80
5:16 PM	Anomalies	Terminated		Unsupported L4 Protocol			0
5:15 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			21674
5:15 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			47096
5:15 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			35845
5:15 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			46937
5:12 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			47506
5:12 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			57298
5:11 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			36336
5:11 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			45002
5:10 PM	Anomalies	Terminated		L4 Source or Dest Port Zero			49270

### Attack Mitigation

The scanner source SRC Port was 0, it targeted multiple IPs and multiple ports within the ISP range. It was protected by the "Packet Anomaly" protection for sending Zero SRC Ports.

## Attack Vector V: Fragmented UDP Flood

### Summary

On the fourth day of the attack, one of the victims was targeted again by a UDP flood to Port 80 with over 5Mbits of traffic.

### Attack description

The attackers sent large (1500 bytes) UDP packets to port 80 on the target's web site. The IP's sources were spoofed.

### Motivation for using a Fragmented UDP flood

This was an attempt to saturate bandwidth upstream as well as possibly tie up web servers processing resources for replying with ICMP Destination unreachable packets.

### Mitigation

As you can see in the screenshot below, DefensePro BDOS protection successfully created a footprint for this attack in under a minute time and the attack was successfully blocked. A blacklist for UDP port 80 was also created since there is generally no reason for this port to be open.

