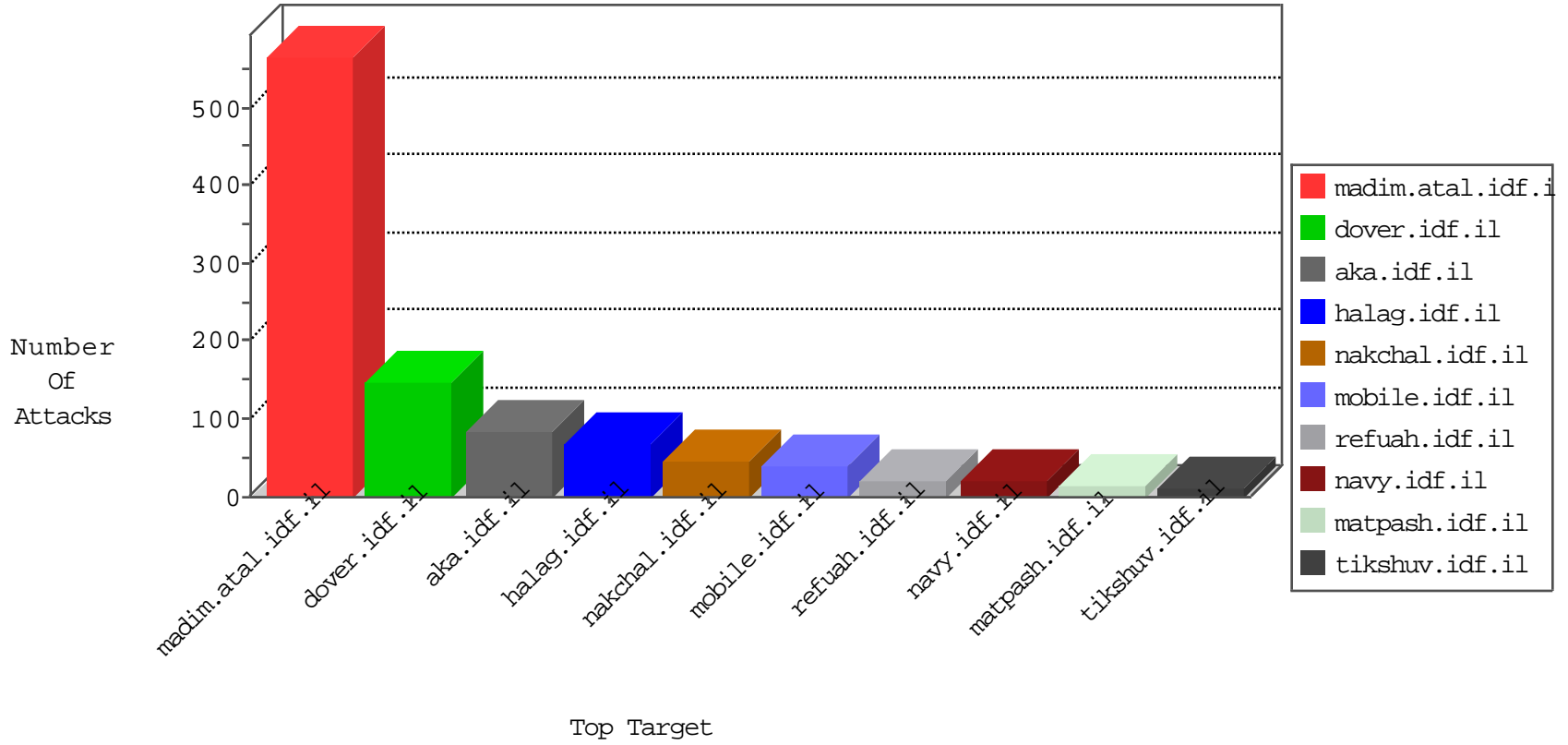


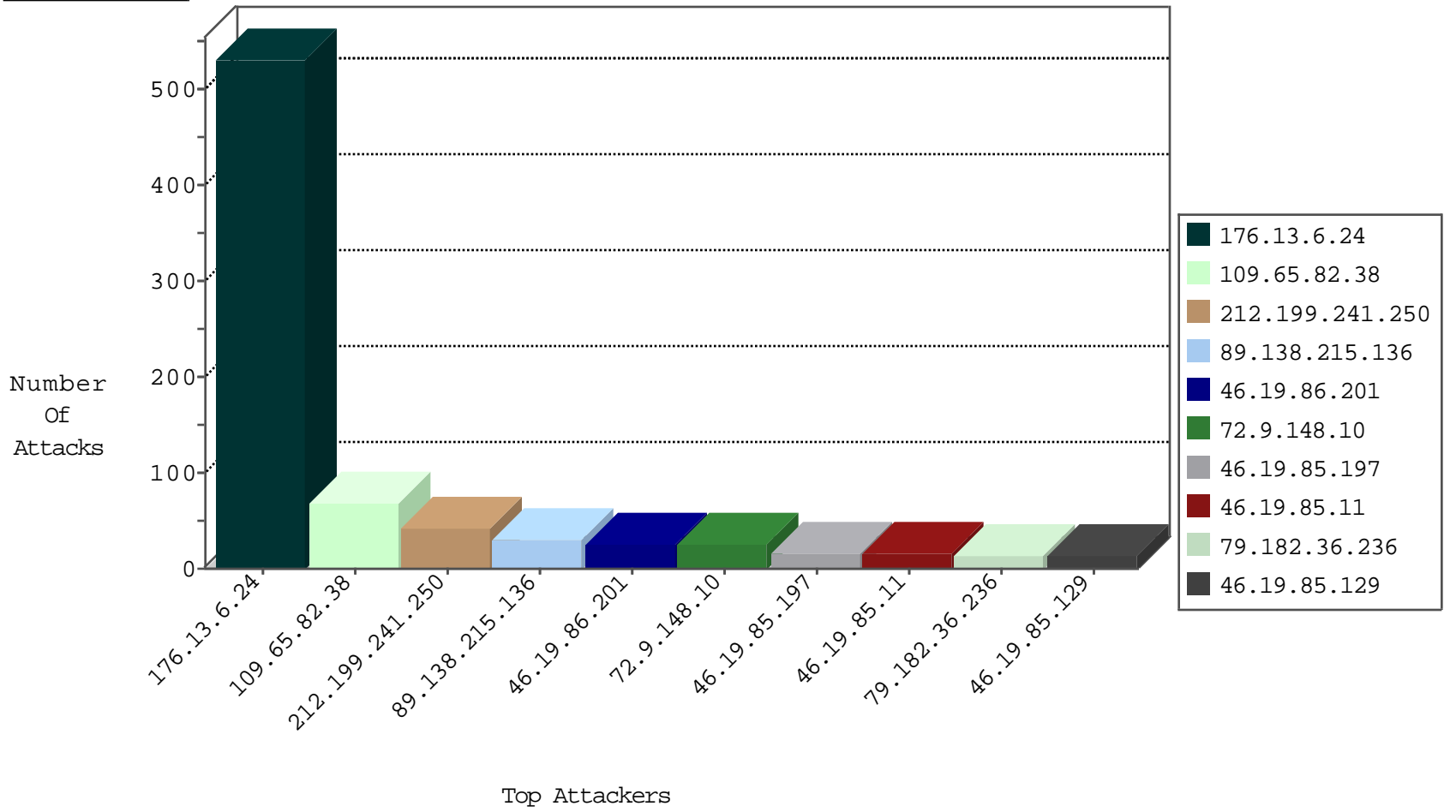
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.241.250	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	42
79.176.197.214	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
71.6.216.50	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
66.240.236.119	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.37	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.41	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
185.72.177.106		147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.202.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
86.132.215.31	United Kingdom	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
212.179.42.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.6.24	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
31.168.14.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.98	147.237.76.197	United States	e.himush.idf.il	ET DROP Dshield Block Listed Source	1
112.213.95.142	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
112.213.95.142	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.193	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.244.49.137	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
198.180.198.185	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
114.33.114.158	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.213.95.142	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
82.117.208.243	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.82.38	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
89.138.215.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
79.182.36.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.149.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.30.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.39.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.57.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.120.125.48		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.193.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
196.217.169.106	Morocco	147.237.77.176	matpash.idf.il	drop		drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
79.181.179.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.120.125.48		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.127.32.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.124.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.44.186.255	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.28.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.8.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.49		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.30.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.203	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
204.126.132.241	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.12.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.216.152	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.47.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.190.49	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.187.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.190.49	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.176.221.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.226.203	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	522
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
109.253.199.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born2.htm	Block	1
37.26.147.153	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzyy	Block	1
81.218.2.118	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
52.33.240.114	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
198.58.103.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
149.78.44.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.73.190	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/4/444.doc	Block	1
197.48.72.82	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	1
107.182.230.72	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.53	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
204.126.132.241	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.114.132.61	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
197.48.72.82	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
107.182.230.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.58	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/110386.pdf	Block	1
207.46.13.187	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
79.114.132.61	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
51.254.44.137	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
197.48.72.82	Egypt	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
109.65.82.38	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
216.113.160.71	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.112.248.32		147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
79.179.6.225	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
52.33.240.114	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
197.48.72.82	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1