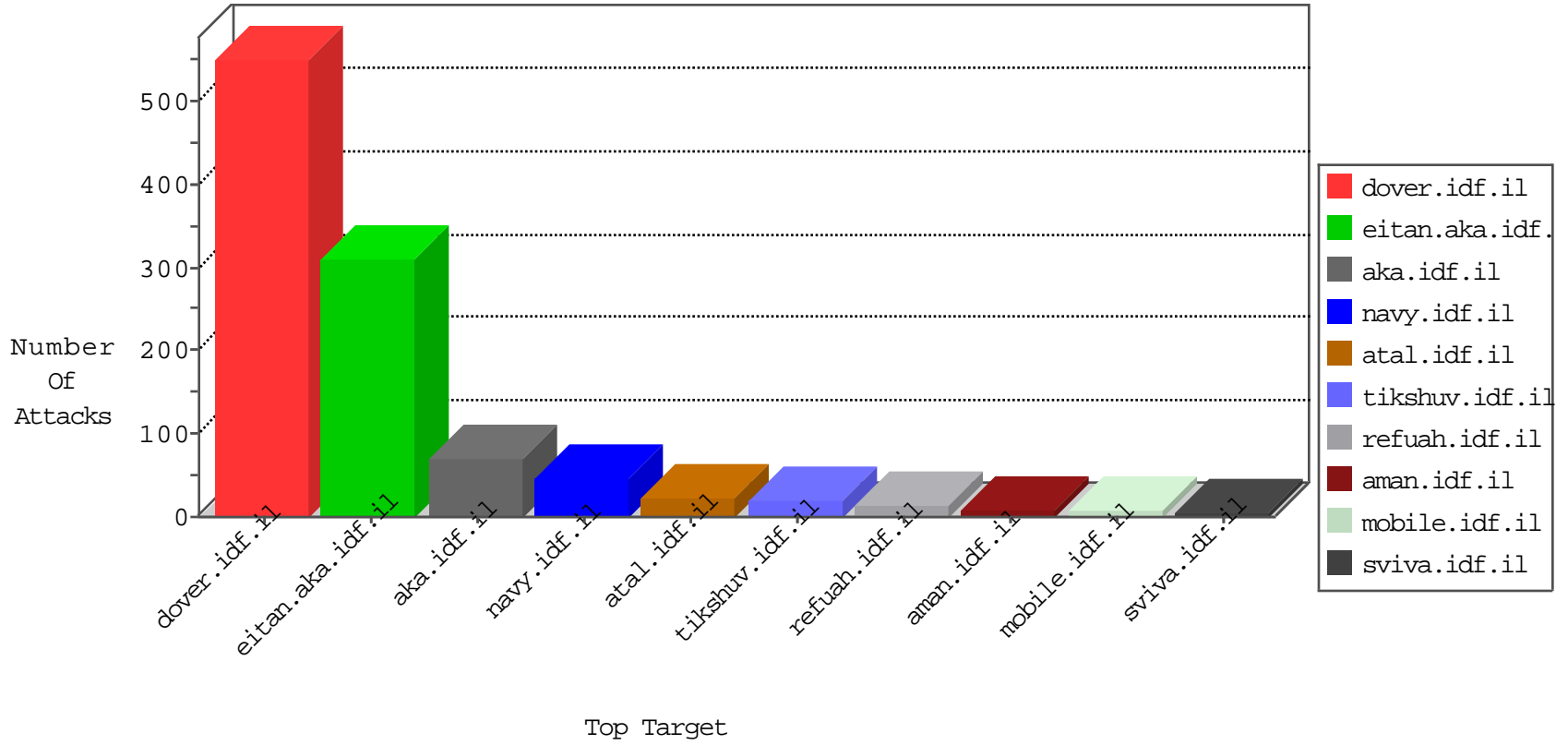


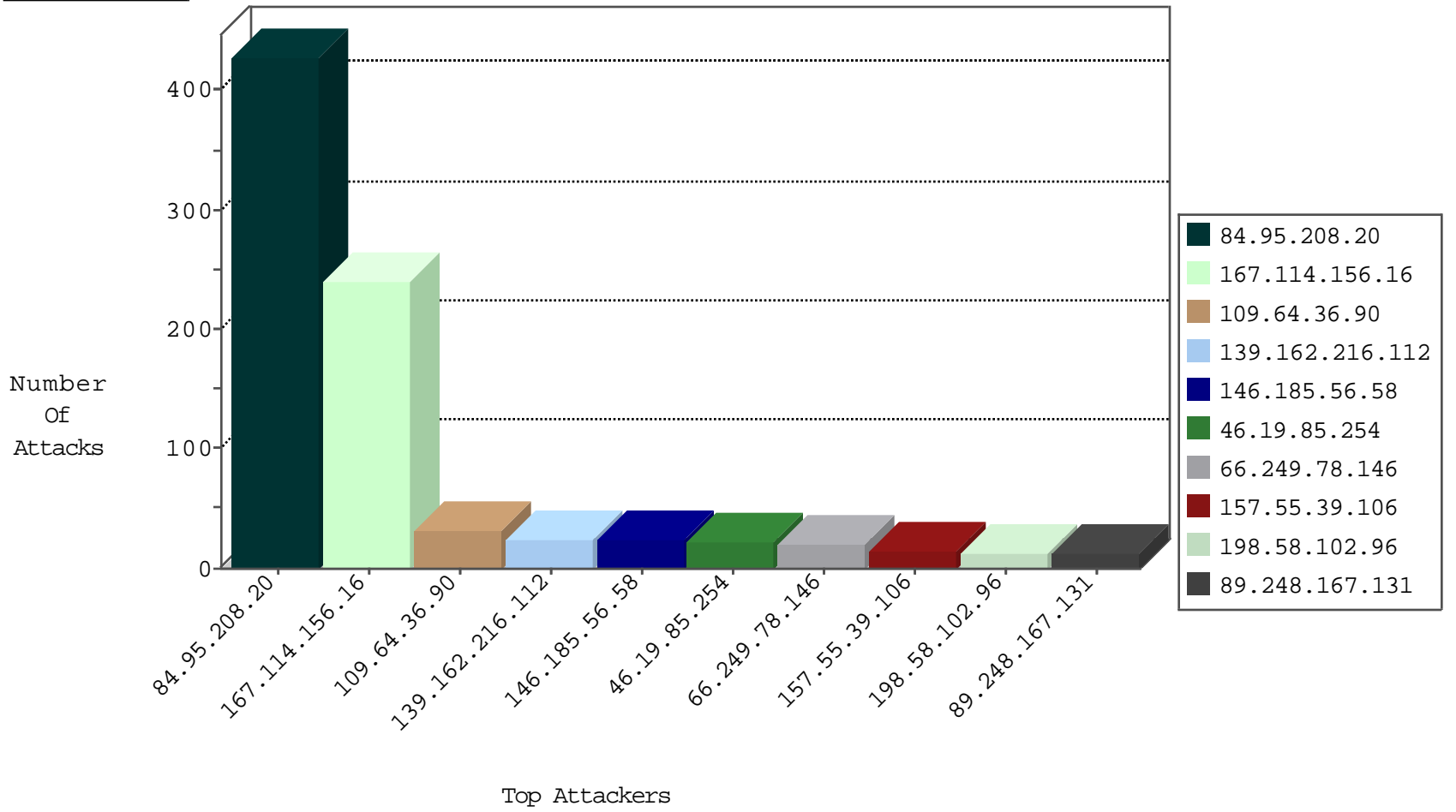
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	9932
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	267
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
94.102.49.116	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
104.131.108.100	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
104.131.108.100	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.78.250.41	Russian Federation	147.237.72.166	aka.idf.il	4654: HTTP: PHP Code Injection	Block	1
211.220.63.148	Korea, Republic of	147.237.0.34	tikshuv.idf.	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.185.56.58	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
146.185.56.58	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	2
91.201.236.155	147.237.76.148	Ukraine	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.167.131	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.131	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.74	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
189.220.46.43	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.167.131	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.79.104	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.148	Ukraine	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
52.29.223.39	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.76.148	Ukraine	ggcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
211.220.63.148	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
89.248.167.131	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
178.162.208.154	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
89.248.167.131	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.61	Netherlands	e.cogat.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
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
109.64.36.90	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	9
77.126.196.240	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.72.208.176	Canada	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.133.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
97.74.24.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.254	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.254	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.63.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.85.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.65.185.173	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
105.106.79.188	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
174.118.63.6	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
88.191.204.49	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.30.24.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
149.78.124.218	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
149.78.124.218	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.159	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.236	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.135	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.145	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.106	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	103
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
146.185.56.58	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 146.185.56.58	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.153.233.130	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	2
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
203.127.96.237	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.153.233.130	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
66.249.69.5	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
88.198.44.46	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
157.55.39.135	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/skira/default.asp	None	1
17.142.155.123	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/apple-app-site-association	Block	1
66.249.82.88	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal/izkor/view_img.asp	Block	1
203.127.96.231	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.36.90	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.82.47.4	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
220.255.148.8	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22721	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluum/hovot/templates/main.asp	Block	1
17.142.159.155	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/apple-app-site-association	Block	1
66.249.82.91	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8924-he/refuah.aspx	Block	1
2.53.131.71	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/general/mobile	Block	1
80.246.133.95	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
164.132.161.24	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15554-he/dover.aspx-title=	Block	1
146.185.56.58	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/69312.pdf	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.58.234	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1