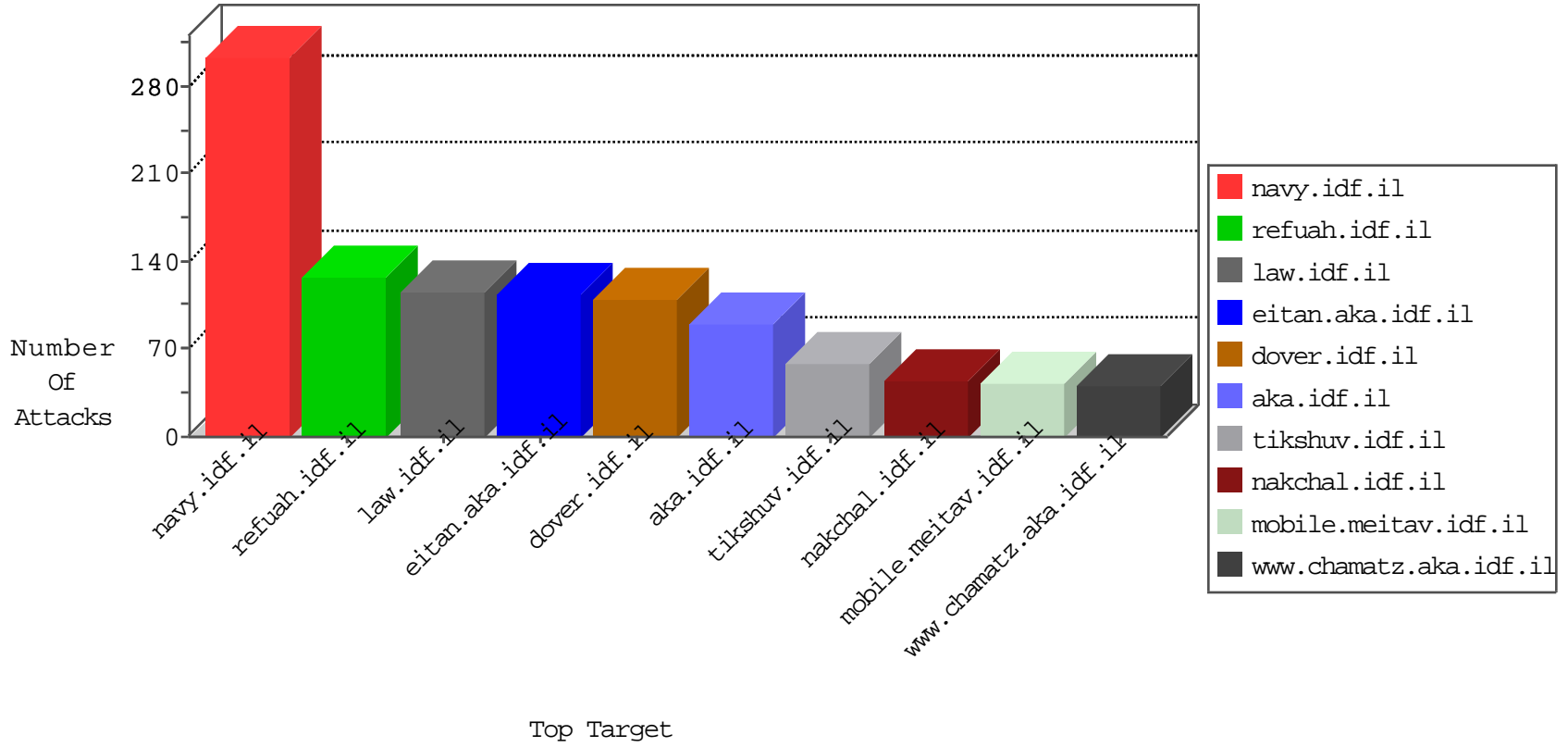


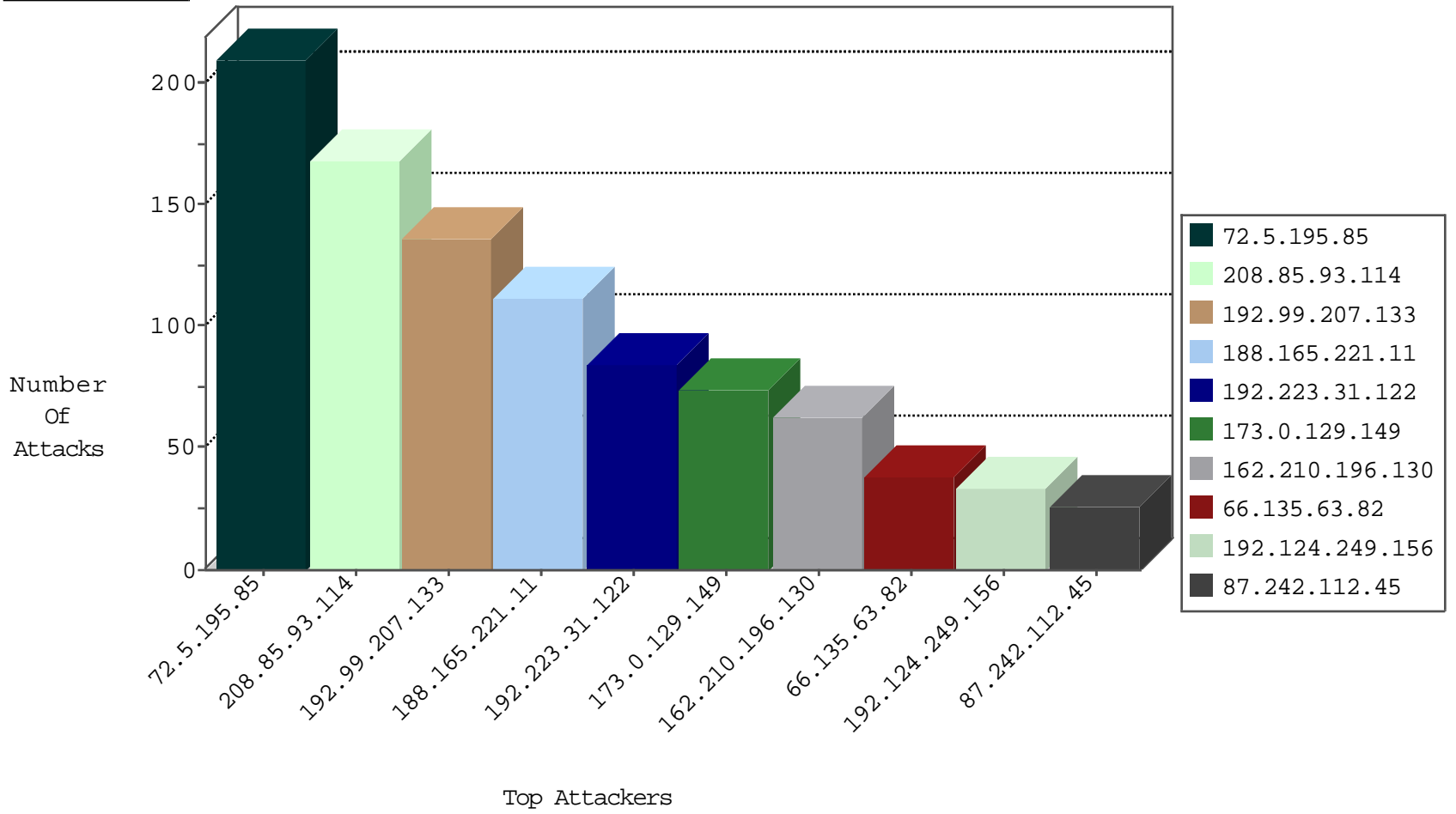
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
114.79.4.2	Indonesia	147.237.76.39	mobile.meitav.idf.il	Black List	drop	3
59.174.44.226	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
111.76.233.94	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
123.116.157.239	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
66.249.76.108	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
209.126.136.2	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
27.10.136.14	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.130	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	30
173.0.129.149	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
173.0.129.149	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
66.135.63.82	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
87.242.112.45	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
173.0.129.149	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
66.135.63.82	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.203.204.143	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.75	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.9	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.34.186.9	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
180.169.20.5	China	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
162.210.196.130	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
184.168.27.116	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
113.240.194.166	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
195.74.38.14	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
180.109.231.31	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
173.0.129.149	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	38
66.135.63.82	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	20
180.169.20.5	147.237.77.74	China	law.idf.il	SQL Injection - Select From	18
87.242.112.45	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	14
213.203.204.143	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	8
72.167.131.75	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
64.34.186.9	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	8
50.63.197.9	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
36.80.184.188	147.237.77.216	Indonesia	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	4
195.74.38.14	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	3
36.80.184.188	147.237.77.176	Indonesia	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	3
184.168.27.116	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	3
93.158.203.195	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
50.116.123.135	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.149.151	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.71.122	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
163.172.149.151	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
119.70.107.166	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.48.93.217	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
93.158.203.196	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
202.65.138.2	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.65.51	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
163.172.149.151	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.37.81	147.237.76.196	Vietnam	e.sviva.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
72.5.195.85	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	167
208.85.93.114	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
208.85.93.114	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
208.85.93.114	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
208.85.93.114	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
208.85.93.114	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
208.85.93.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
208.85.93.114	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
208.85.93.114	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
184.168.27.116	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
207.241.226.200	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
93.104.215.125	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
72.5.195.85	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
72.5.195.85	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
72.5.195.85	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
109.253.158.107	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
139.162.172.71	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
195.74.38.14	Sweden	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.223.31.122	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.223.31.122	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
83.168.250.50	Sweden	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
83.168.250.50	Sweden	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
188.165.221.11	France	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
188.165.221.11	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
73.21.180.91	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
188.165.221.11	France	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
72.5.195.85	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
188.165.221.11	France	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
188.165.221.11	France	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
188.165.221.11	France	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.223.31.122	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.165.221.11	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.165.221.11	France	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.165.221.11	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.184	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
216.189.154.118	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.165.221.11	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.223.31.122	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.165.221.11	France	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.184	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.223.31.122	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.88.144	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
218.101.81.89	New Zealand	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
91.224.49.183	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/responsible-disclosure	Block	1
45.79.71.122	United States	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
66.249.79.134	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
198.20.87.98	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.69.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
66.249.79.138	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
198.20.87.98	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/robots.txt	Block	1
66.249.69.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
66.249.88.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.79.71.122	United States	147.237.77.170	maarachot.idf.il	Malformed HTTP Header Line 3	Block	1
207.46.13.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/news/<a href=	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
45.79.71.122	United States	147.237.77.170	maarachot.idf.il	Malformed URL	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1