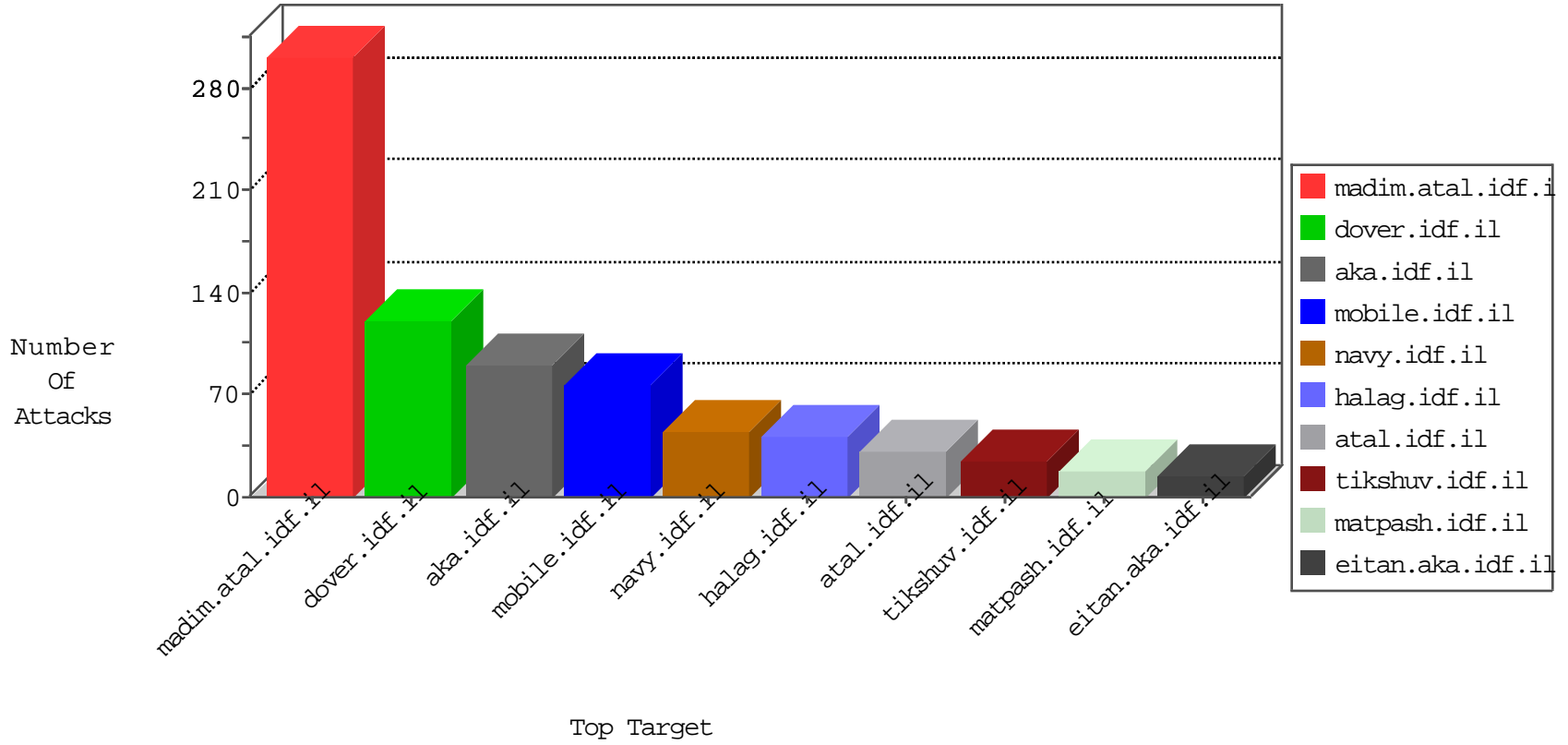


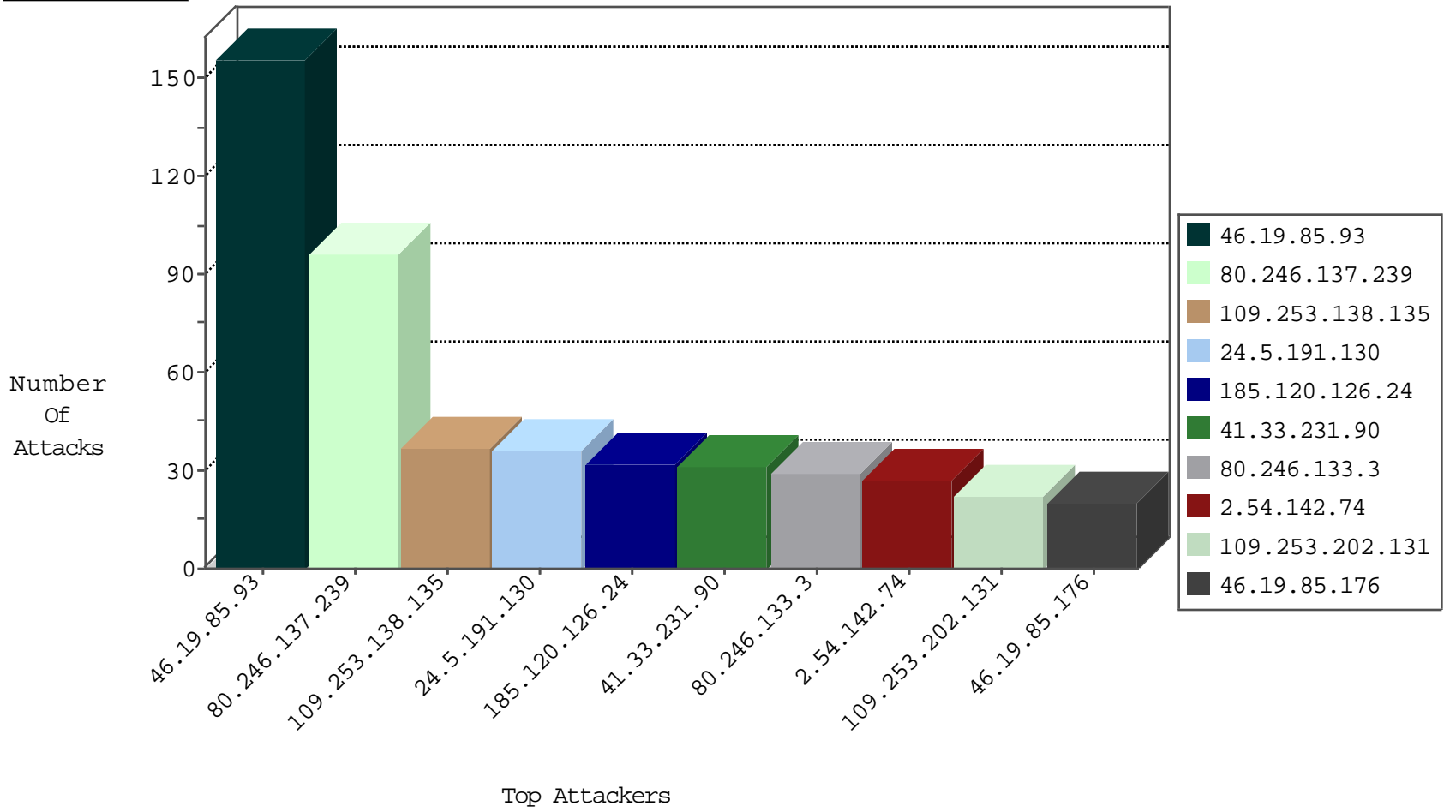
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.105.139.78	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
222.223.122.86	China	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
184.105.139.106	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
123.203.72.247	Hong Kong	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
198.23.165.141	United States	147.237.72.14	doover.idf.il(old)	Block_Ntp_All_Net	drop	1
123.203.72.247	Hong Kong	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.105	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.174.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.117.234.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	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
46.60.30.111	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
109.253.202.131	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
93.174.93.144	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.147	China	chimuch.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
5.17.146.226	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.180.198.185	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
104.215.89.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.144	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
198.180.198.185	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
104.215.89.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.93.144	147.237.77.235	Netherlands	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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
109.253.138.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.246.133.3	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
185.120.126.24		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	16
24.5.191.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
24.5.191.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
2.52.137.76	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
24.5.191.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.253.202.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.60.30.111	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
109.253.202.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.13.20.254	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.196	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.196	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.205.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.38.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.149.158	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.176.209.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
37.26.149.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.7.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.54.114	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.53.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.246	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.10.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.54.114	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.53.99	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.52.46.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.252.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.143.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.66.175	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.182.115.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.65.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
62.219.130.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.156.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.18.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.66.175	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.149.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.173.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.186.190.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.86.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
31.210.188.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.186.190.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.117.60.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.89.217.234		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	156
80.246.137.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
2.54.142.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
185.120.126.24		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
109.253.138.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.119.123.238	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	5
64.71.32.19	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.71.32.19	Block	3
128.177.161.186	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
2.54.145.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.168.21.77	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.168.21.80	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.20.254	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
103.14.60.219	Philippines	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.69.89	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
199.30.25.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
109.253.205.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.147.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.105.247.195	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
103.14.60.219	Philippines	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.69.97	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
213.151.49.238	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/&sa=u&ved=0ahukewjsrp-l-jtlahwiqjokhudcc_wqfggnm aa&usg=afqjcnh4ucr3bqpmkvh4yz9t7jscutsloq	Block	1
46.19.85.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.112.185.114	Austria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
64.71.32.19	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
37.26.149.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.89.217.224		147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/./images/shared/home.png	Block	1
109.65.141.167	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
69.197.169.202	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/main.htm/	Block	1
213.151.49.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-10625-he/dover.aspx&sa=u&ved=0ahukewjsrp-l-jtlahwiqjokhudcc_wqfggymai&usg=afqjcnf_b016rnmmdjafppqlxngfli8du6w	Block	1
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/	Block	1
85.64.68.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
185.89.217.230		147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/./images/shared/home.png	Block	1
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
46.117.30.165	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.164	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
66.249.69.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1321-he/atal.aspx	Block	1
40.77.167.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.202.131	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
80.246.133.3	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1