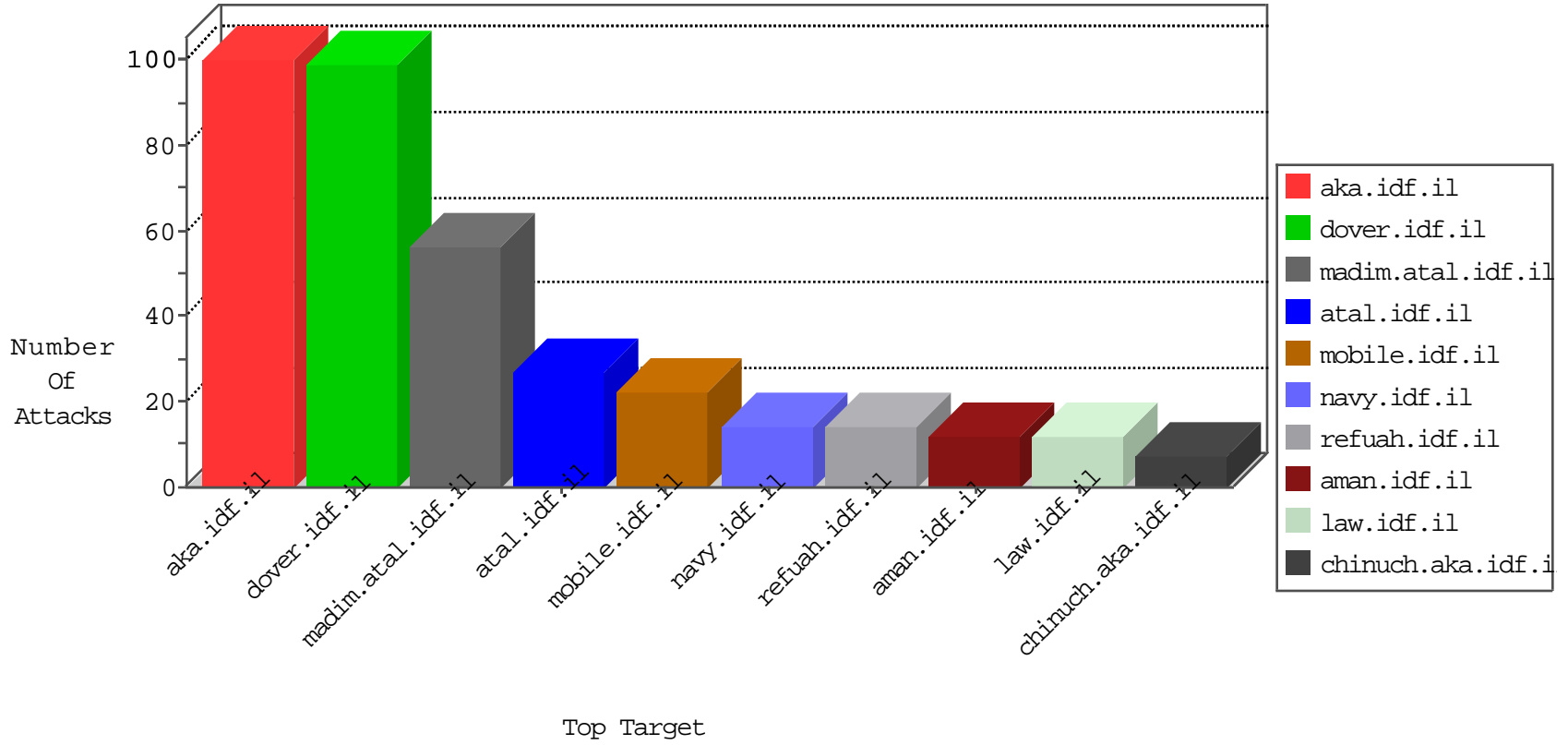


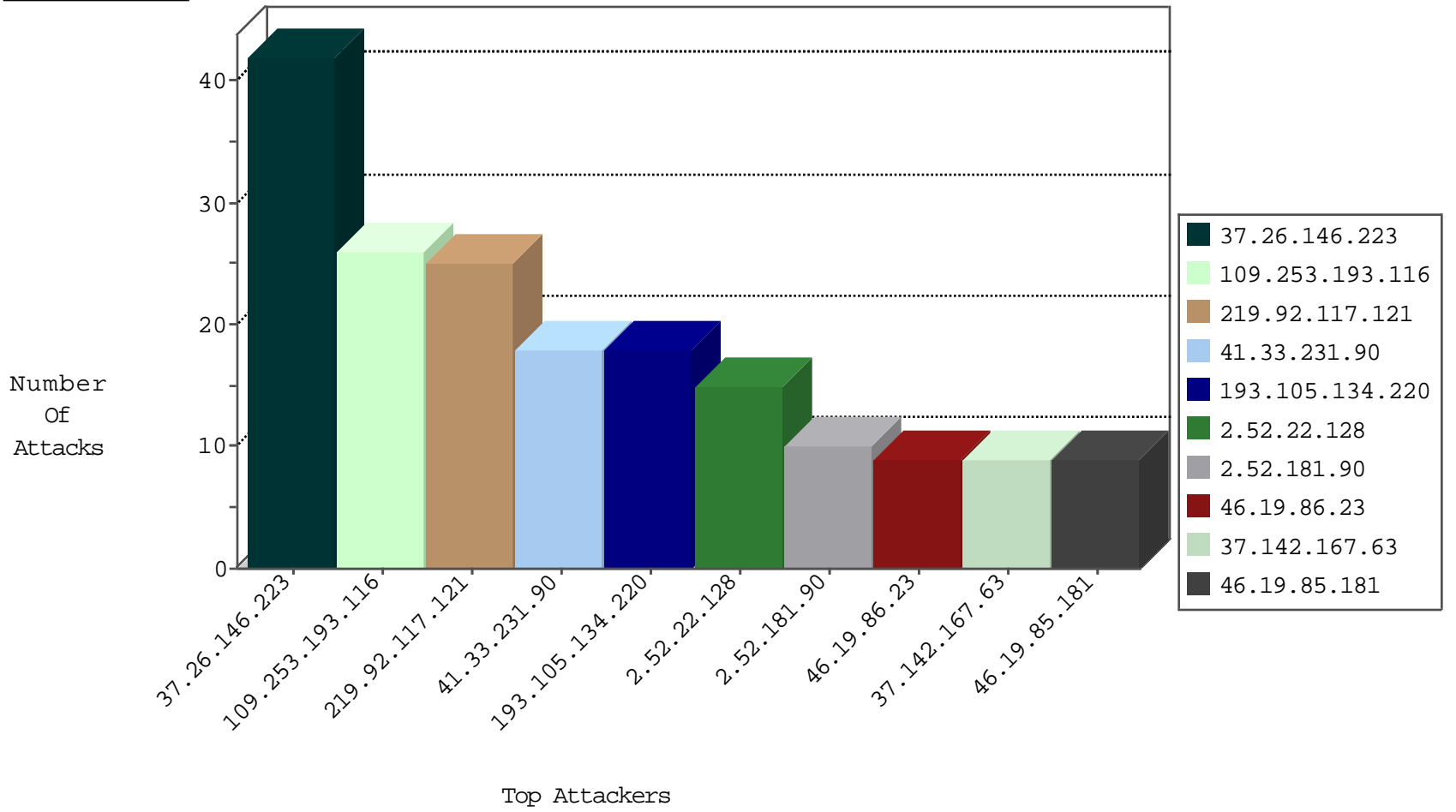
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.91.28.59	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
178.63.22.141	Germany	147.237.76.31	nakchal.idf.il	Invalid L4 Header Length	drop	1
85.31.186.131	Germany	147.237.8.28	e.mobile-ks.idf.il	Invalid L4 Header Length	drop	1
178.63.22.141	Germany	147.237.8.28	e.mobile-ks.idf.il	Invalid L4 Header Length	drop	1
178.63.22.141	Germany	147.237.8.28	e.mobile-ks.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.201.148.210	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
96.47.2.10	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
103.21.58.191	India	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
184.106.114.136	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
96.47.2.10	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
184.106.114.136	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
216.201.148.210	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
103.21.58.191	147.237.77.74	India	law.idf.il	SQL Injection - Select From	3
109.253.193.116	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
121.201.27.61	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.77.227	Turkey	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
201.187.74.95	147.237.8.28	Chile	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.173.72.139	147.237.76.176	Mexico	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.66	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.176	Sweden	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.174	147.237.76.148		ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
201.173.72.139	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.66	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.130.5.174	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.179	Indonesia	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.174	147.237.72.14		dover.idf.il(old)	ET SCAN Potential SSH Scan	1
128.199.61.237	147.237.77.74	Singapore	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	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	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
2.52.181.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
109.253.193.116	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.193.116	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.253.193.116	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.23	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
219.92.117.121	Malaysia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.59.192	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.142.167.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
219.92.117.121	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.46.39.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
219.92.117.121	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
219.92.117.121	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
219.92.117.121	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.210.186.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.203.136.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
185.3.147.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.22.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.211.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.22.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.23	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.41.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.97.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.22.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.186.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.29.130.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.52.22.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.22.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.210.188.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.44.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.209.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.155	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.111.161.246	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.194.131.136	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
128.194.131.136	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.42	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.201.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
82.102.169.113	Israel	147.237.72.166	aka.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
37.26.146.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	7
2.54.181.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/main.asp	Block	1
77.127.127.111	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
41.196.196.110	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	1
109.253.193.116	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.127.127.111	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
46.121.94.24	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
23.88.38.158	United States	147.237.77.216	dover.idf.il	E-mail collector robots l4	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
77.127.127.111	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2413.jpg	Block	1
41.196.196.110	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
109.253.209.148	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.127.127.111	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/xmlrpc.php	Block	1
51.255.127.25	United Kingdom	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
23.88.38.158	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 82.80.196.44	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
128.194.131.136	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
77.127.127.111	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
65.55.210.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/ylcebowm67a	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
91.226.212.39	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.78.198	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/894-he	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1523-en/dover.aspx+idf blog	Block	1
77.127.127.111	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
40.77.167.68	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
216.77.62.44	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9234-he/refuah.aspx	Block	1