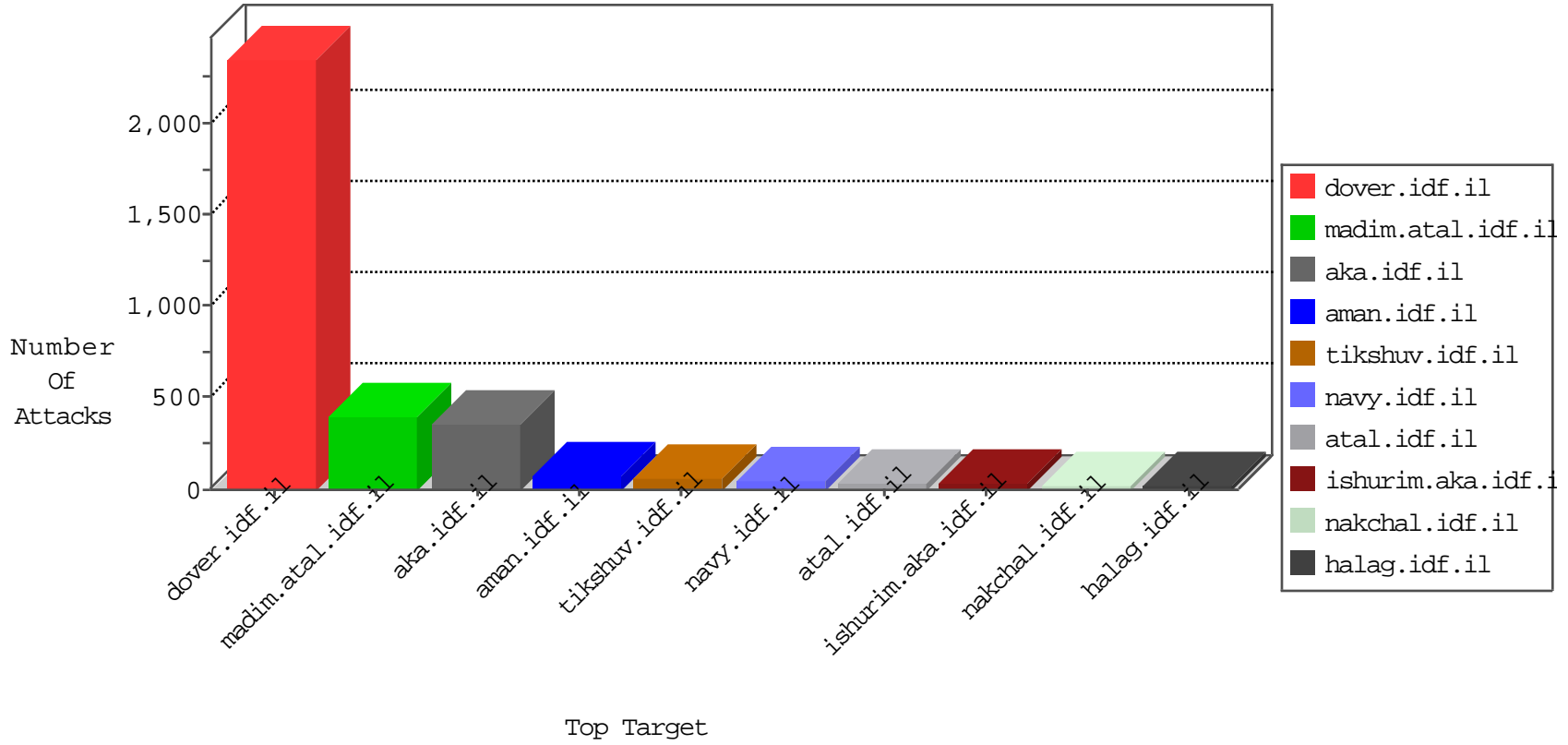


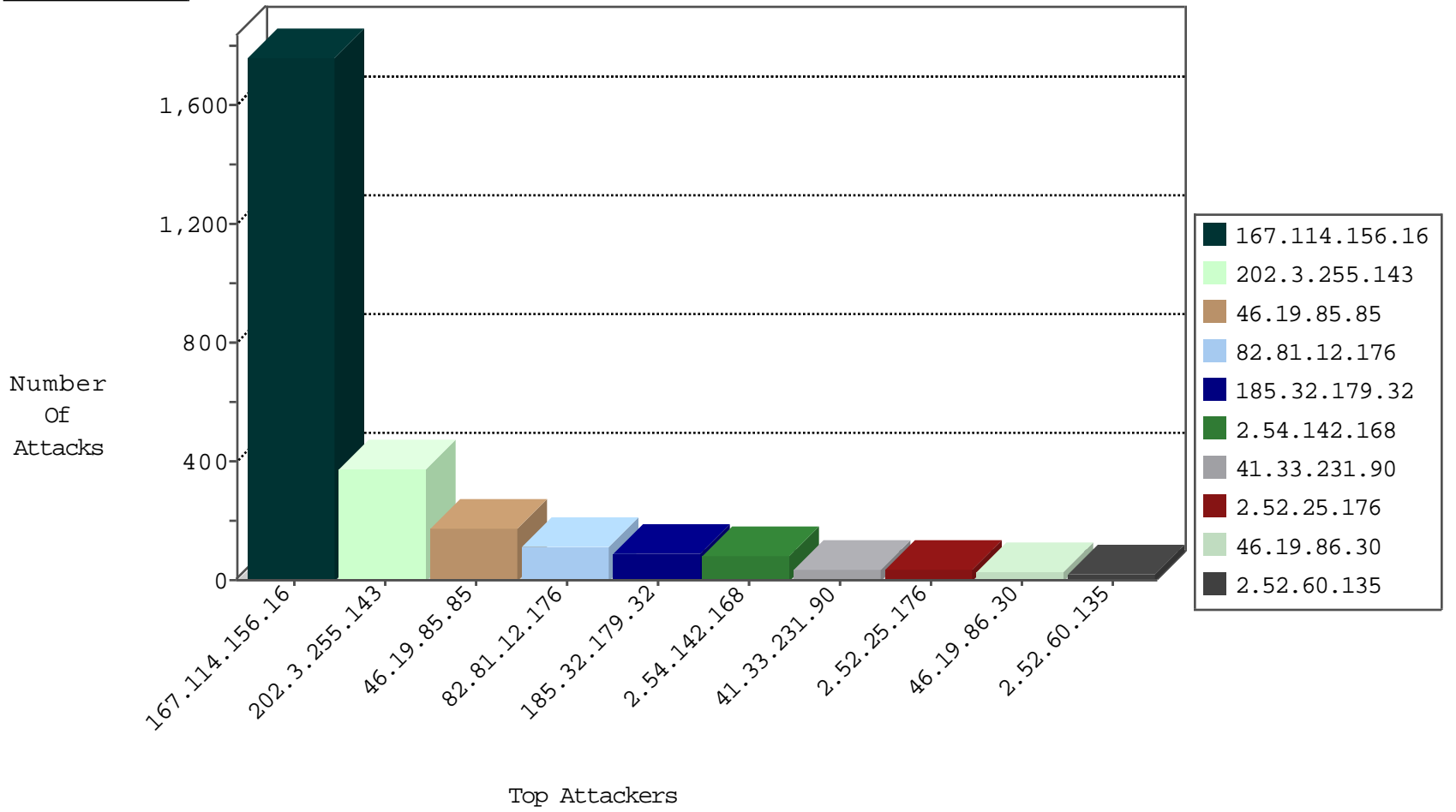
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3008
66.249.64.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	115
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
142.54.160.213	United States	147.237.77.234	halag.idf.il	block-sp-trafl	drop	1
142.54.169.166	United States	147.237.77.19	law-forum.idf.il	block-sp-trafl	drop	1
104.233.70.144		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.211	United States	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.117.9.26	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
79.176.126.211	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	7
10.0.0.3		147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
79.180.18.31	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
200.59.205.238	Argentina	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
184.106.114.136	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
184.168.193.34	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
23.91.70.51	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
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	340
200.59.205.238	147.237.77.74	Argentina	law.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
23.91.70.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
184.168.193.34	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	2
184.106.114.136	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
112.16.76.209	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
89.71.126.37	147.237.77.216	Poland	dover.idf.il	portscan: TCP Distributed Portscan	1
69.248.129.181	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
218.6.197.169	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
64.233.172.163	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
212.25.69.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.157.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.13.173	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
108.181.170.138	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.7.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.6.197.169	147.237.72.14	China	dover.idf.il(olc	ET SCAN NMAP -sS window 1024	1
68.81.158.224	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.70.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.67.1.11	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.30	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
5.22.135.140	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.52.60.135	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.106.44.151	Palestinian Territory Occupied	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
84.108.120.22	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
84.108.217.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.109.9.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
213.8.204.1	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
213.8.204.64	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
109.64.182.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.40.30.239	Egypt	147.237.77.19	law-forum.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.147.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.108.217.250	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
213.8.204.64	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.21	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.21	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.17.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.210.188.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.153.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.26.147.130	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.229.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.102.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
177.185.192.50	Brazil	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
37.46.39.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.127.10.40		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.180.97.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.220.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.13.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.1.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.148.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.125.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.191.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.115.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
185.32.179.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
2.54.142.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.52.25.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.142.168	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	27
185.32.179.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.66.20.33	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
46.19.85.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
87.69.195.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
86.109.107.245	Spain	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
157.55.39.136	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.136	Block	2
216.120.237.30	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
109.66.6.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.134	Block	2
216.120.237.30	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
2.52.133.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
202.20.18.5	Australia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.65.54.109	Israel	147.237.77.74	law.idf.il	Parameter Type Violation FreeText in www.law.idf.il/327-he/patzar.aspx	Block	2
80.246.137.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
86.109.107.245	Spain	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8900-he/refuah.aspx	Block	1
162.144.94.102	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
217.69.136.203	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
37.187.25.49	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
91.206.201.94	Ukraine	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
192.254.209.21	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.153.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.136.76.107	Germany	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
5.135.120.96	France	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
84.109.9.75	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
187.17.98.219	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
2.52.25.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.102.225	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
46.116.159.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
106.187.44.219	Japan	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
92.63.140.212	United Kingdom	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
197.40.30.239	Egypt	147.237.77.19	law-forum.idf.il	Distributed Unauthorized URL Access on 147.237.77.19/	Block	1
72.167.190.33	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
176.13.6.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.210.188.85	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
192.40.112.200	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
62.117.59.18	Egypt	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 62.117.59.18	Block	1