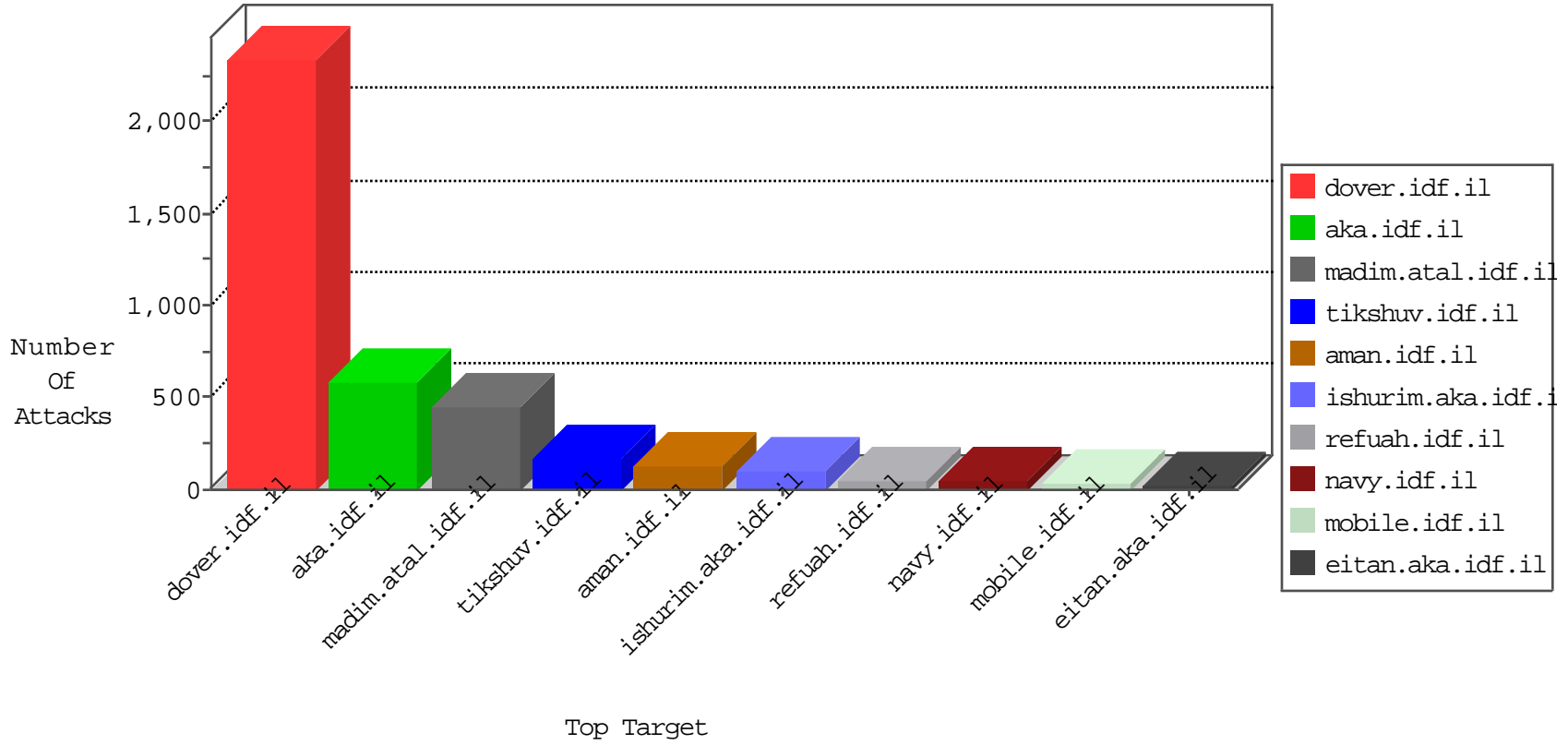


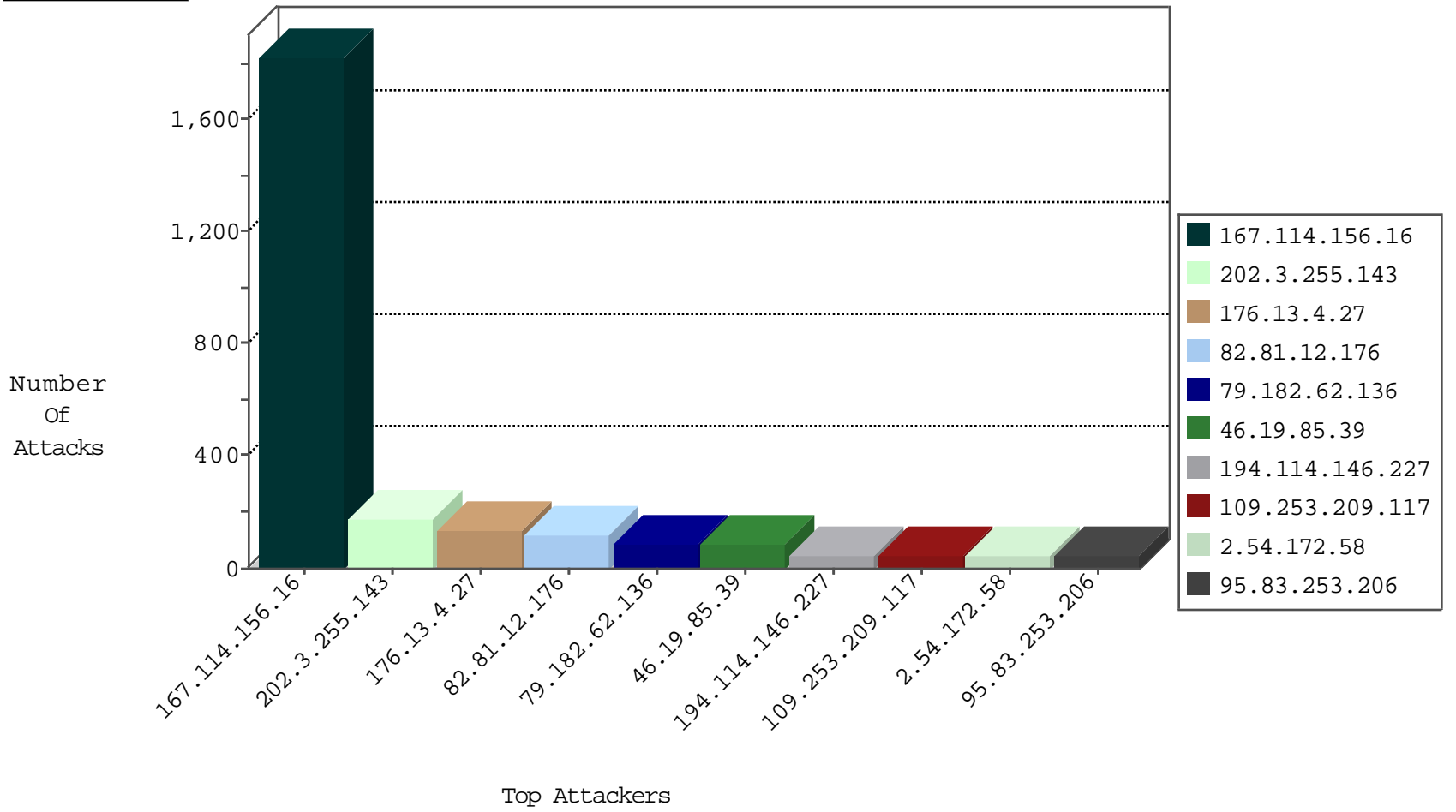
IDF Under Attack Daily Report



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	3160
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	115
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
204.42.253.130	United States	147.237.76.177	noore.idf.il	Block_Udp_All_Nets	drop	2
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
80.82.64.68	Netherlands	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
80.82.64.68	Netherlands	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
80.82.64.68	Netherlands	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
176.13.4.27	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
80.82.64.68	Netherlands	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	24
89.138.94.248	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.127	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
85.64.144.228	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	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	141
46.19.85.194	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
5.102.101.40	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.195	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.193.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.100.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
133.232.152.43	147.237.77.178	Japan	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
121.201.27.61	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
82.81.34.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.68	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.127.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
176.106.44.151	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
133.232.152.43	147.237.77.178	Japan	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
120.24.175.112	147.237.72.166	China	aka.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
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
80.246.133.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
62.128.48.10	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	21
95.83.253.206	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
2.54.25.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.176.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
58.110.110.176	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.85.65	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
95.83.253.206	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
176.13.17.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.168.209.12	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
85.130.216.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.228.22.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
157.55.39.67	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.2.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.25.67.206	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.168.209.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
95.83.253.206	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
2.54.172.185	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.28	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.106.44.151	Palestinian Territory Occupied	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.172.185	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.199.57.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.172.185	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.190.244	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.210.232.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.143.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.246.136.25	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.89	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.140.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.38.249.134	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.172.185	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.187.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.4.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
79.182.62.136	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.62.136	Block	83
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
109.253.209.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
2.54.172.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
176.13.4.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.4.27	Block	24
176.13.8.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
217.132.119.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.5.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
85.250.111.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
82.81.11.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.81.11.62	Block	4
46.19.86.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.195.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.81.11.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/8/	Block	3
109.253.220.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
2.54.163.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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
112.78.4.229	Vietnam	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
109.253.133.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.145.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.187.25.49	France	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
176.13.13.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
176.13.8.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.218.26.108	Kazakistan	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
46.19.86.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
89.218.26.108	Kazakistan	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
192.115.177.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
145.100.36.85	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 145.100.36.85	Block	1
5.196.98.204	Spain	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
88.198.4.37	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
187.45.195.13	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
176.13.23.75	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
46.120.69.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.140.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.92.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.133.114	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
46.19.85.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.149.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.214.201.107	Moldova, Republic of	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1