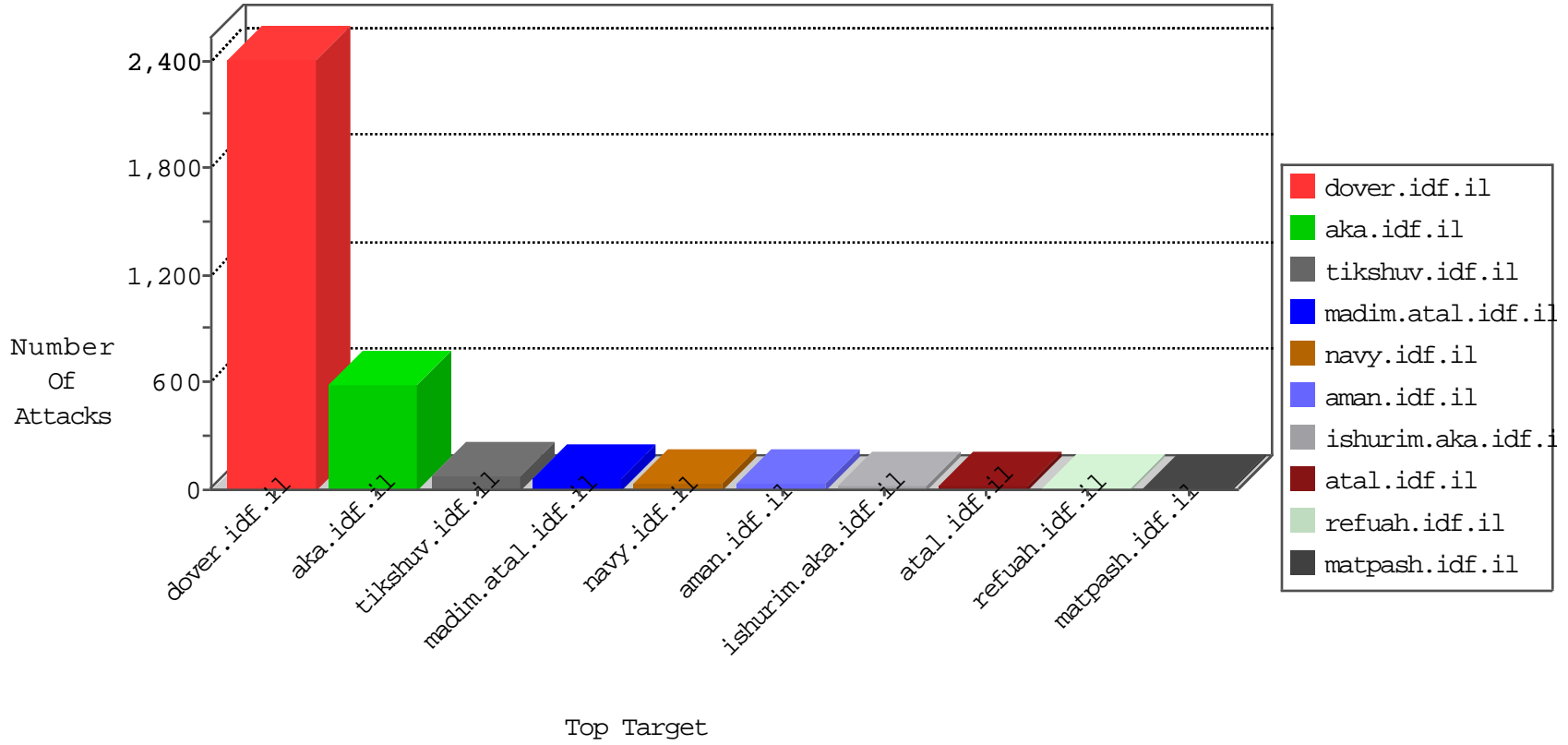


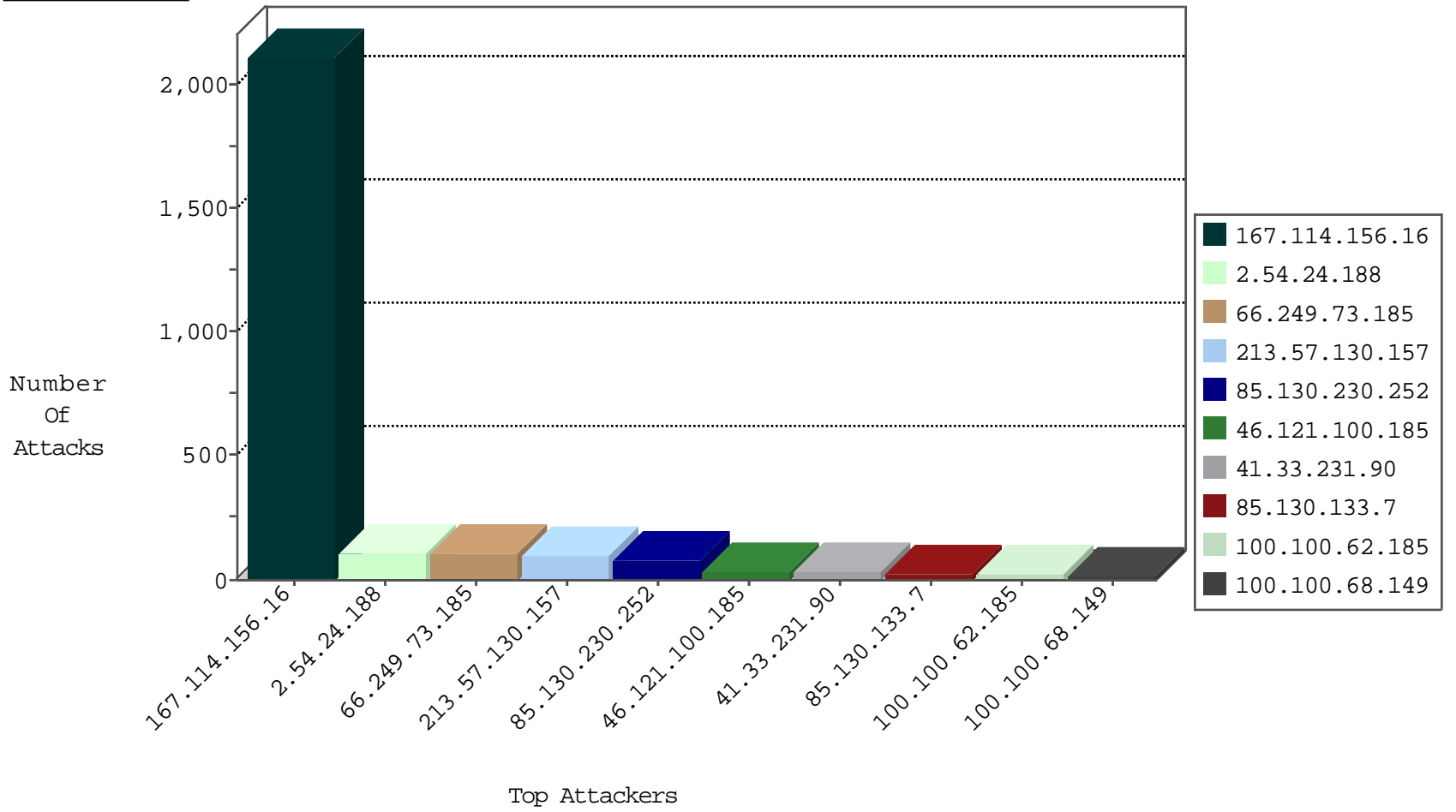
IDF Under Attack Daily Report



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	3256
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	41
82.145.209.86	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
180.97.106.37	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.45.192.62	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
141.212.121.199	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
51.254.212.184	United Kingdom	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

11-26-2015-23:04:07 to 11-27-2015-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.120	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
180.210.201.106	147.237.76.39	Singapore	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
180.210.201.106	147.237.0.200	Singapore	m4u.idf.il	ET SCAN Potential SSH Scan	1
113.233.97.130	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.113	147.237.76.86	Ukraine	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
87.236.214.178	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential SSH Scan	1
186.167.18.178	147.237.8.28	Venezuela	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
87.236.214.178	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential SSH Scan	1
186.167.18.178	147.237.8.24	Venezuela	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
185.56.80.31	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.210.201.106	147.237.76.86	Singapore	navy.idf.il	ET SCAN Potential SSH Scan	1
180.210.201.106	147.237.72.156	Singapore	aman.idf.il	ET SCAN Potential SSH Scan	1
2.52.161.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.210.201.106	147.237.0.15	Singapore	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
198.23.176.210	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
87.236.214.178	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential SSH Scan	1
186.167.18.178	147.237.8.46	Venezuela	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
87.236.214.178	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
186.167.18.178	147.237.8.27	Venezuela	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
87.236.214.178	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
186.167.18.178	147.237.8.14	Venezuela	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.56.80.31	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.117.220.63	147.237.77.227	Spain	e.hamaz.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
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
213.57.130.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	97
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
100.100.62.185		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
85.130.230.252	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
85.130.230.252	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
100.100.19.209		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
100.100.68.149		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
85.130.230.252	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
100.100.77.33		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.84.162		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.29.63		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
77.127.245.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.116.187		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
89.139.39.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
85.64.157.231	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
100.100.4.146		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.228	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.130.230.252	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
85.130.230.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.248	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.133.7	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.130.230.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.65.120.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.178.164.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.43.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.133.7	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
100.100.124.9		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.46.39.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.133.7	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.180.200.122	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
100.100.92.98		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.67.164.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
46.116.87.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
87.68.72.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.2	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
84.109.108.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.0.103.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.68.153.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
85.130.230.252	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.108.188.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.183.35.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.48		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.173.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.53.86	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
2.54.24.188	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 2.54.24.188	Block	107
46.121.100.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.85.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
207.241.226.41	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	7
85.65.153.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
107.150.56.90	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 107.150.56.90	Block	4
79.176.110.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	3
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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
84.228.246.244	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/	Block	2
149.78.155.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.116.86.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
31.210.186.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.120.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.116.99.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
2.52.129.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.29.62.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.240.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.145.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
176.12.137.58	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
40.77.167.35	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.180.128.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.55.179.201	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
31.210.189.252	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
87.68.72.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.163.194.40	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/4636.jpg	Block	1
31.154.92.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
2.54.8.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.216.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.200.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
31.210.187.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
85.65.185.40	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.73.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
46.120.194.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
176.13.9.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.246.130	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
84.108.102.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
40.77.167.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19116-en/dover.aspxhaz	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.180.162.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1