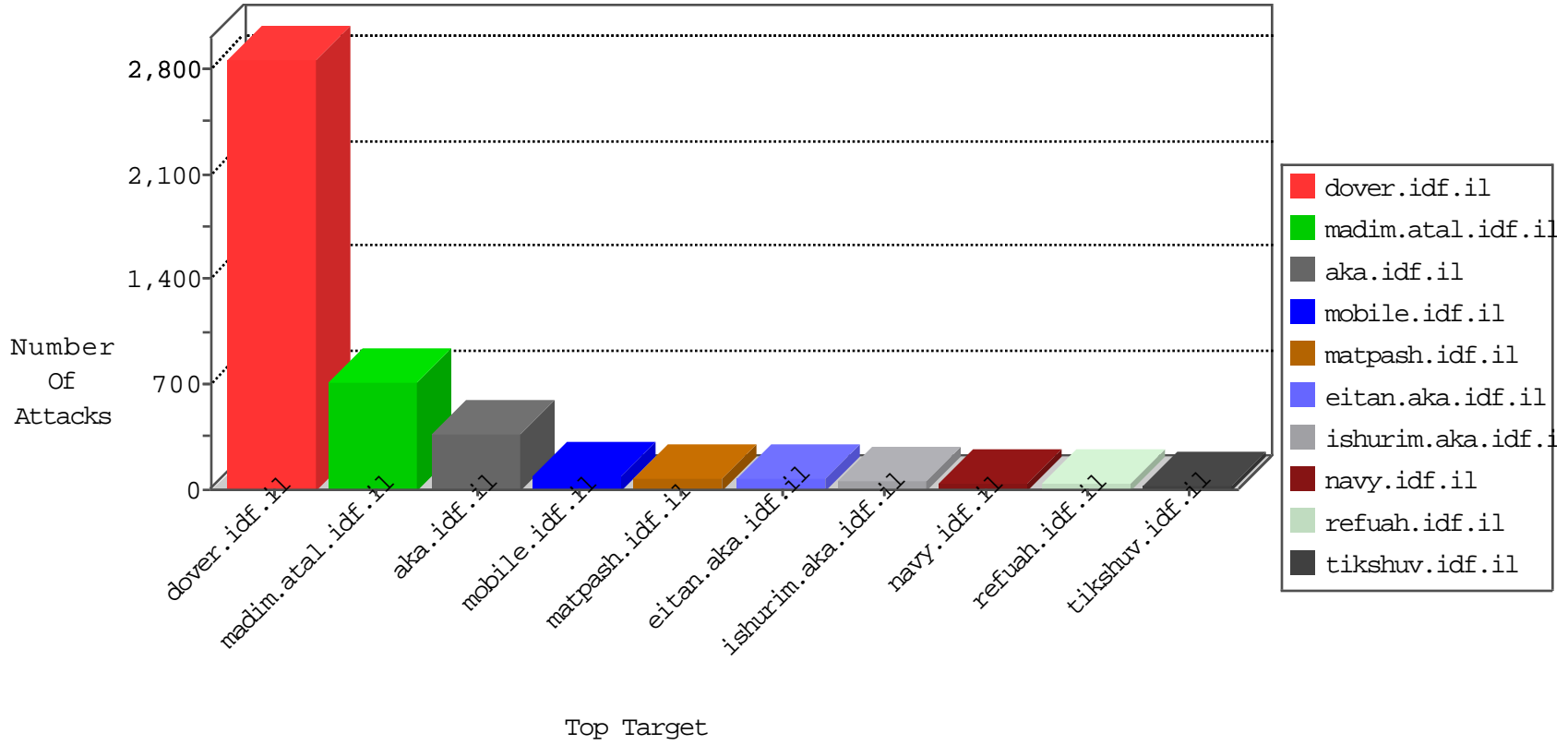


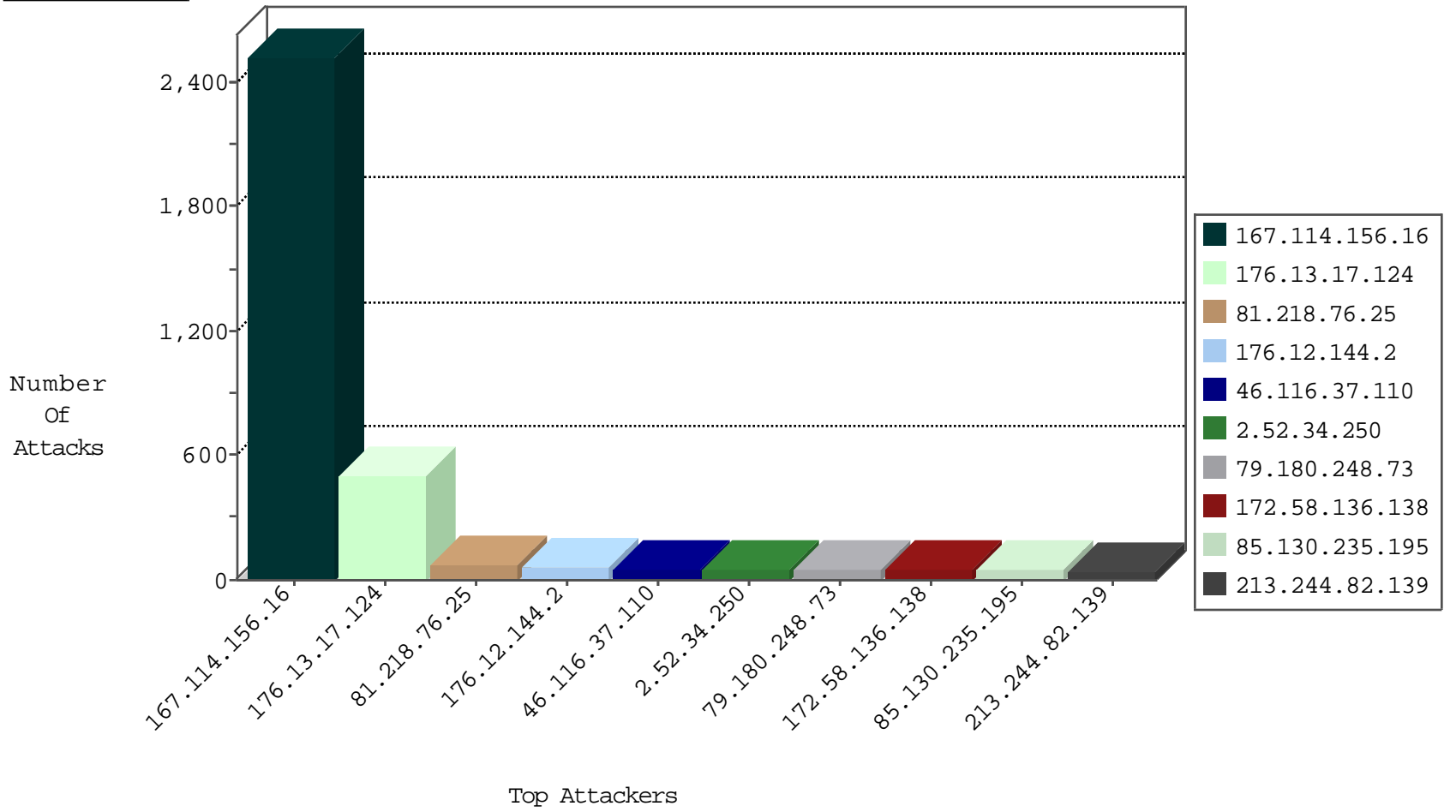
# IDF Under Attack Daily Report



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	3300
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	281
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
45.32.246.5		147.237.77.19	law-forum.idf.il	Invalid TCP Flags	drop	5
130.75.174.234	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

12-09-2015-13:04:04 to 12-09-2015-14:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.166.137.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.120.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.169.170.130	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential SSH Scan	1
78.128.92.192	147.237.76.30	Bulgaria	himush.idf.il	ET SCAN NMAP -sS window 1024	1
49.238.49.185	147.237.77.216	India	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.128.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.226.206.204	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
92.43.70.181	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -f -sS	1
92.43.70.181	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
85.65.51.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -f -sS	1
82.80.230.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
78.128.92.192	147.237.76.30	Bulgaria	himush.idf.il	ET SCAN NMAP -sS window 3072	1
77.125.15.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.185.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.42.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.79.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.22.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
92.43.70.181	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
85.250.207.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 2048	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.76.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
79.180.248.73	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
172.58.136.138	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
85.130.235.195	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
213.244.82.139	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	40
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
37.26.148.194	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	29
109.66.48.111	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	18
5.28.158.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
46.116.37.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
5.28.158.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
5.28.158.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
2.52.34.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.116.37.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
5.28.158.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.34.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
17.78.164.103	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.52.34.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.52.34.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.34.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
109.66.48.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.137.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.154	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.116.37.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.182.57.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.116.37.110	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.48.111	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.245.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.95.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.163	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.163	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.28.158.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
79.182.175.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.245.77.65	Czech Republic	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.58.139.74	Denmark	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.116.37.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.138.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.128	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.228.89.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.9.81	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	292
176.13.17.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
176.13.17.124	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.17.124	Block	90
176.12.144.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.85.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
176.13.3.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.52.128.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.144.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
207.46.13.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
176.13.17.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.10.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.194.203.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
62.114.126.197	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	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
84.111.111.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.114.126.197	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.12.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.9	Block	2
69.171.231.226	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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
61.243.42.111	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
46.19.85.57	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.229.131.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.94.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.121.114	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.97.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
212.150.255.134	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	1
109.67.103.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.139.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.98.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/71568.pdf&sa=u&ved=0ahukewjcu-p10s7jahwdcrcqkhdzuaa4qfggkmae&usg=afqjcnqiknoqt1lrznnrdar0syeusq81vmq	Block	1
84.108.72.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.35.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
137.226.113.7	Germany	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
77.125.76.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
85.250.37.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.7.242	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9709-he/refuah.aspx	Block	1
213.8.204.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
128.232.110.29	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
95.86.104.3	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1