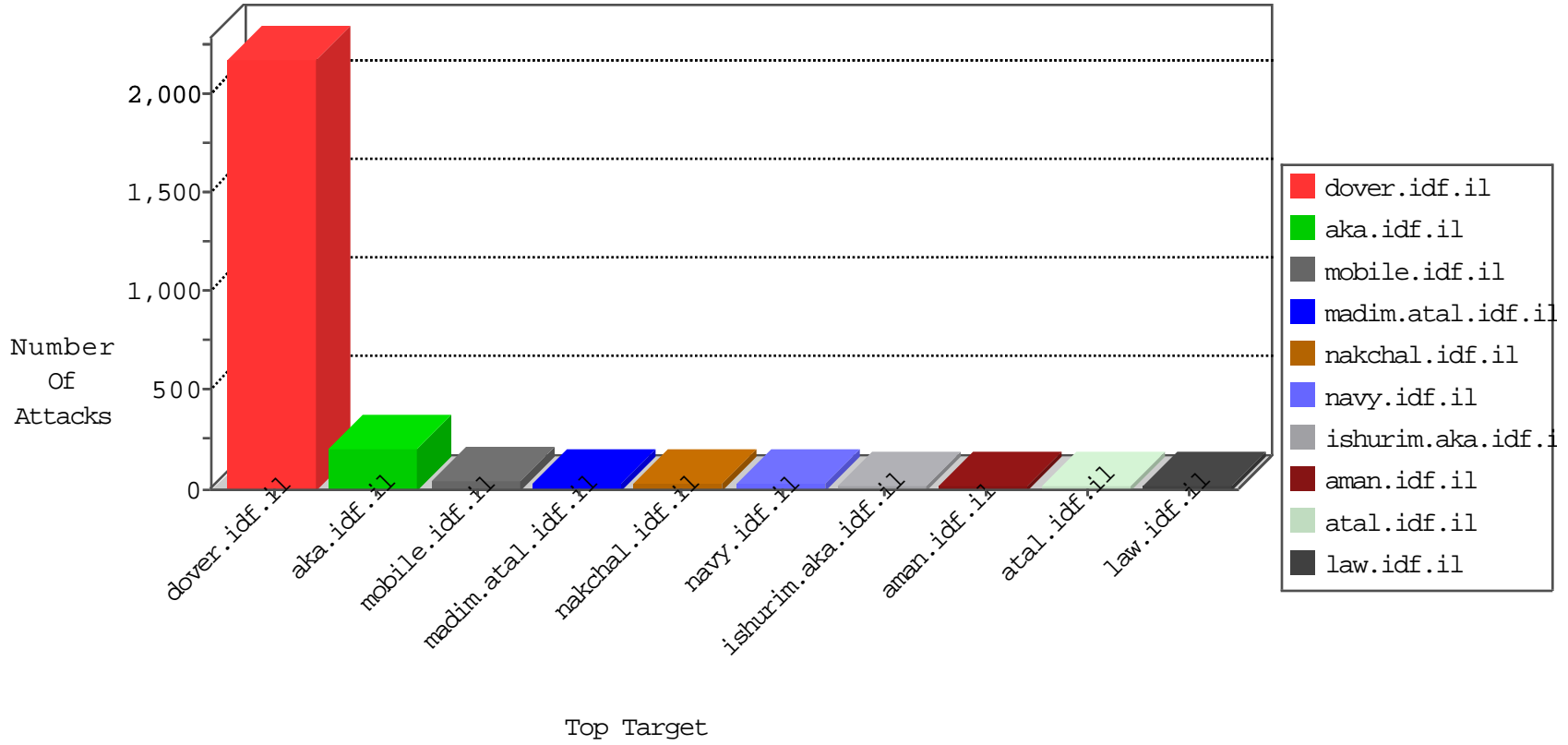


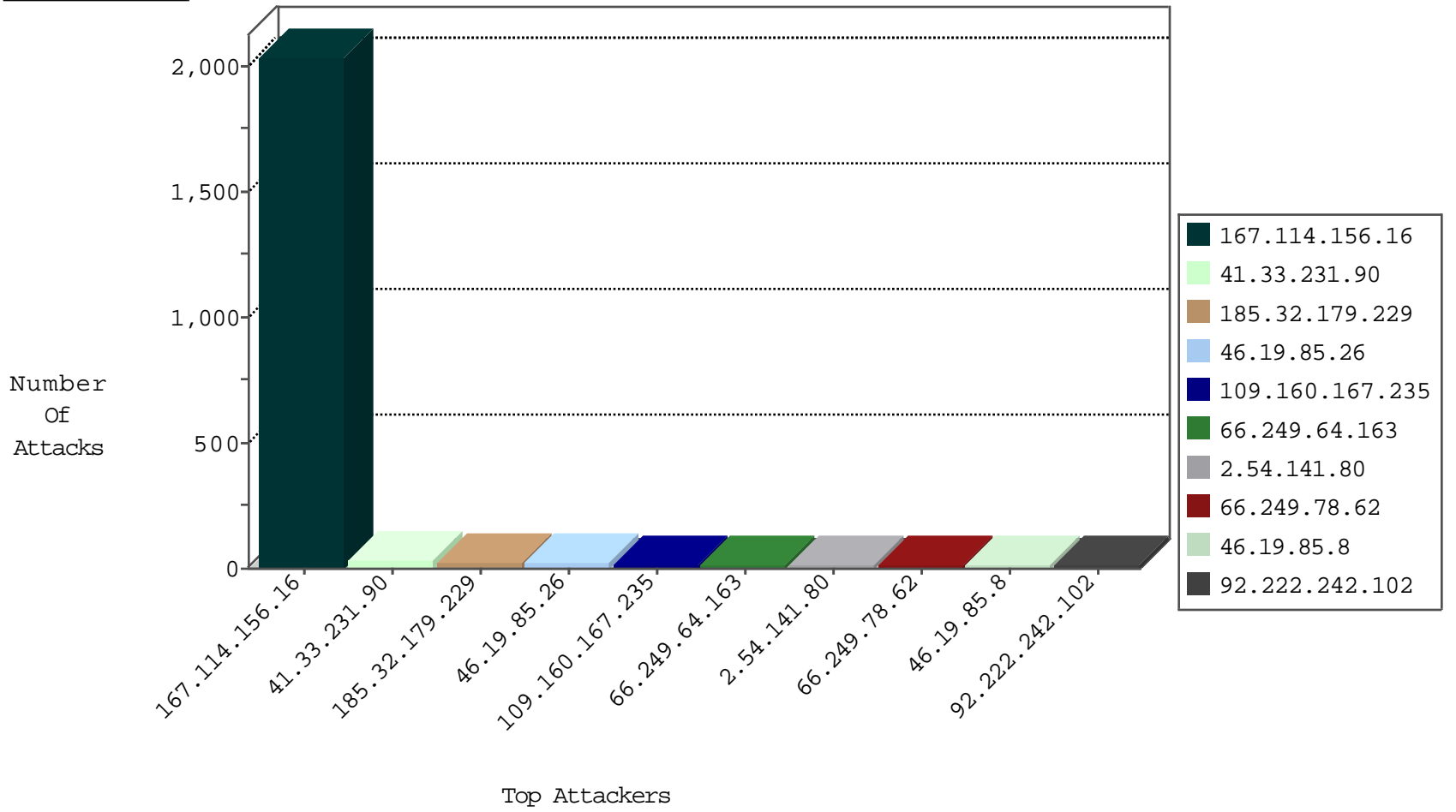
# IDF Under Attack Daily Report



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	3279
66.249.64.191	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3213

12-25-2015-13:04:03 to 12-25-2015-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

## 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	2
176.12.147.154	147.237.77.74	Israel	law.idf.il	INDICATOR-SCAN myscan	2
176.12.147.154	147.237.77.74	Israel	law.idf.il	GPL SCAN myscan	2
37.48.65.39	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
187.160.83.218	147.237.72.156	Mexico	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
87.197.159.157	147.237.76.42	Slovakia	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.161.221	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
1.190.114.142	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
187.160.83.218	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
151.80.43.57	147.237.77.226	Italy	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.120	147.237.77.212	Russian Federation	e.dover.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.26	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
2.54.141.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.62	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.90.255.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.135.80	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.133.57	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.160.167.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
188.120.148.229	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.160.167.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.49	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.0.117.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.146.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.170.92	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.174.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.139.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.138.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.174.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
85.250.161.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.12.146.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.126.8.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.19.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.146.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.22.134.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.247.36.84	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.64.5.155	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.159.146.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.136.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
79.180.97.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.47		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.15.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.189	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.180.123.200	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.120.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.142.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-25-2015-13:04:03 to 12-25-2015-14:04:03

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.148.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.181.59.157	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
185.32.179.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
107.170.42.128	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	4
157.55.39.178	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.178	Block	4
176.13.1.122	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
149.88.48.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	3
157.55.39.54	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	3
185.32.179.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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
2.54.149.92	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
46.19.86.35	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
176.13.18.106	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/1133-22638-he/dover.aspx.	Block	2
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/x-x"	Block	1
46.19.86.47	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtContent in mobile.meitav.idf.il/1494-he/meitav.aspx	Block	1
5.29.68.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
80.246.137.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.120.148.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.19.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.29	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	1
109.67.198.133	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.148.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.128.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.45.15.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
85.250.161.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.85.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
5.29.145.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.8.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
81.218.163.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
190.2.57.241	Argentina	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.22.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.32	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.219.45	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
37.46.44.119	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.149.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
206.214.219.90	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
98.143.148.135	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method [[#1]]I20100	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
46.166.188.246	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.168.178.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.241.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.102.244.254	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
192.0.113.50	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.228.128.6	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
46.19.86.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
119.47.121.67	New Zealand	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1