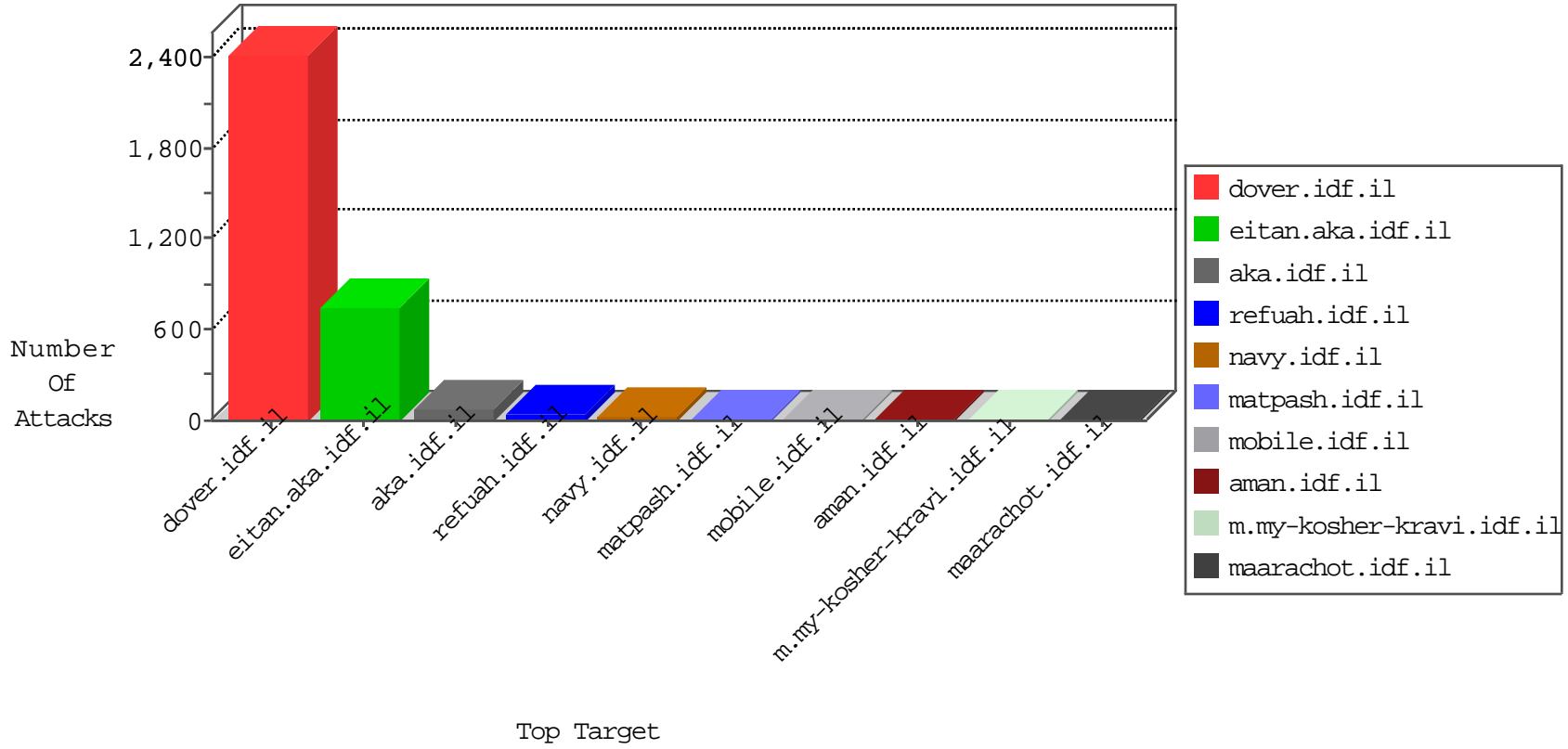


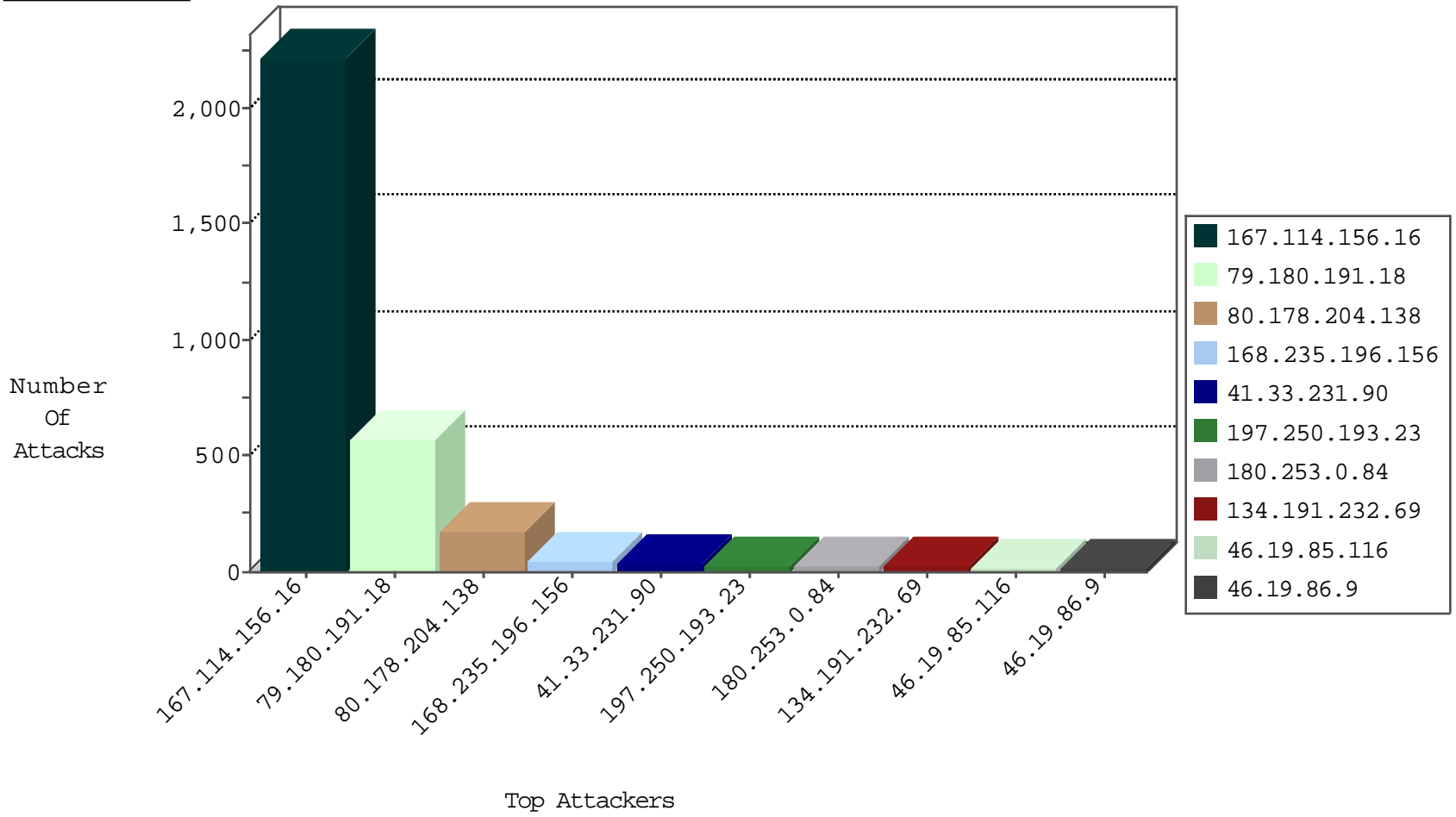
# IDF Under Attack Daily Report



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	3281
134.191.232.69	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	82
134.191.232.69	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	32
168.235.196.156	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
168.235.196.156	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Https	drop	2
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
71.6.216.56	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.210	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1

12-08-2015-07:04:06 to 12-08-2015-08:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	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
180.97.106.161	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
159.122.238.133	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.114	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
78.111.185.92	147.237.77.216	Ukraine	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.34.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
199.168.136.165	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.76.199	China	e.nakchal.idf.i	ET SCAN Potential SSH Scan	1
159.122.238.133	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.77.227	Ukraine	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
5.135.139.53	147.237.77.216	France	dover.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
212.25.102.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.191.18	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	504
80.178.204.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	171
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
168.235.196.156	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
180.253.0.84	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
197.250.193.23	Tanzania, United Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
62.219.136.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.9	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.186.169	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
197.250.193.23	Tanzania, United Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
121.54.54.175	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
197.250.193.23	Tanzania, United Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
121.54.54.251	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.178.186.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
131.253.25.197	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
134.191.232.69	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
121.54.54.250	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.114.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.143.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
37.26.149.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.124.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.9	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.143.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.50.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.109.38.24	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
197.250.193.23	Tanzania, United Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.49.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.246.169	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
84.109.38.24	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.24.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.250.153.207	Israel	147.237.77.226	www.chamatz.aka.idf .il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
121.54.54.174	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
166.170.5.62	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
121.54.54.175	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
197.250.193.23	Tanzania, United Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
40.77.167.8	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
183.79.223.125	Japan	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.190.233	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.237	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.171	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.191.18	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.191.18	Block	63
176.12.151.28	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
2.54.181.38	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
2.54.16.196	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	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
208.184.112.75	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
212.76.100.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
159.203.78.213	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 159.203.78.213	Block	2
84.228.175.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
178.254.62.71	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
109.65.142.194	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.127.224.202	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
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	1
62.219.136.219	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1672	Block	1
159.203.78.213	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
88.208.252.224	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
183.79.219.184	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.65.142.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.36.54	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
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	1
65.99.237.207	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
171.25.193.132	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/minhalnews/pages/knesiyothaghamolad.aspx	Block	1
184.168.200.108	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
37.26.149.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.160.219.252	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
79.180.191.18	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1196-he/refuah.aspx	Block	1
66.249.78.93	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1316-he/x?x'xE x"x x>x x.xæx.x'x™x" x.x"æx.x'x™x;x~x™x\$".aspx	Block	1
188.40.0.147	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
37.142.126.229	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
157.55.39.72	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/110539.pdf,	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.65.115	Block	1
176.13.11.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.49.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
67.205.209.225	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
192.42.116.16	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2427.jpg	Block	1