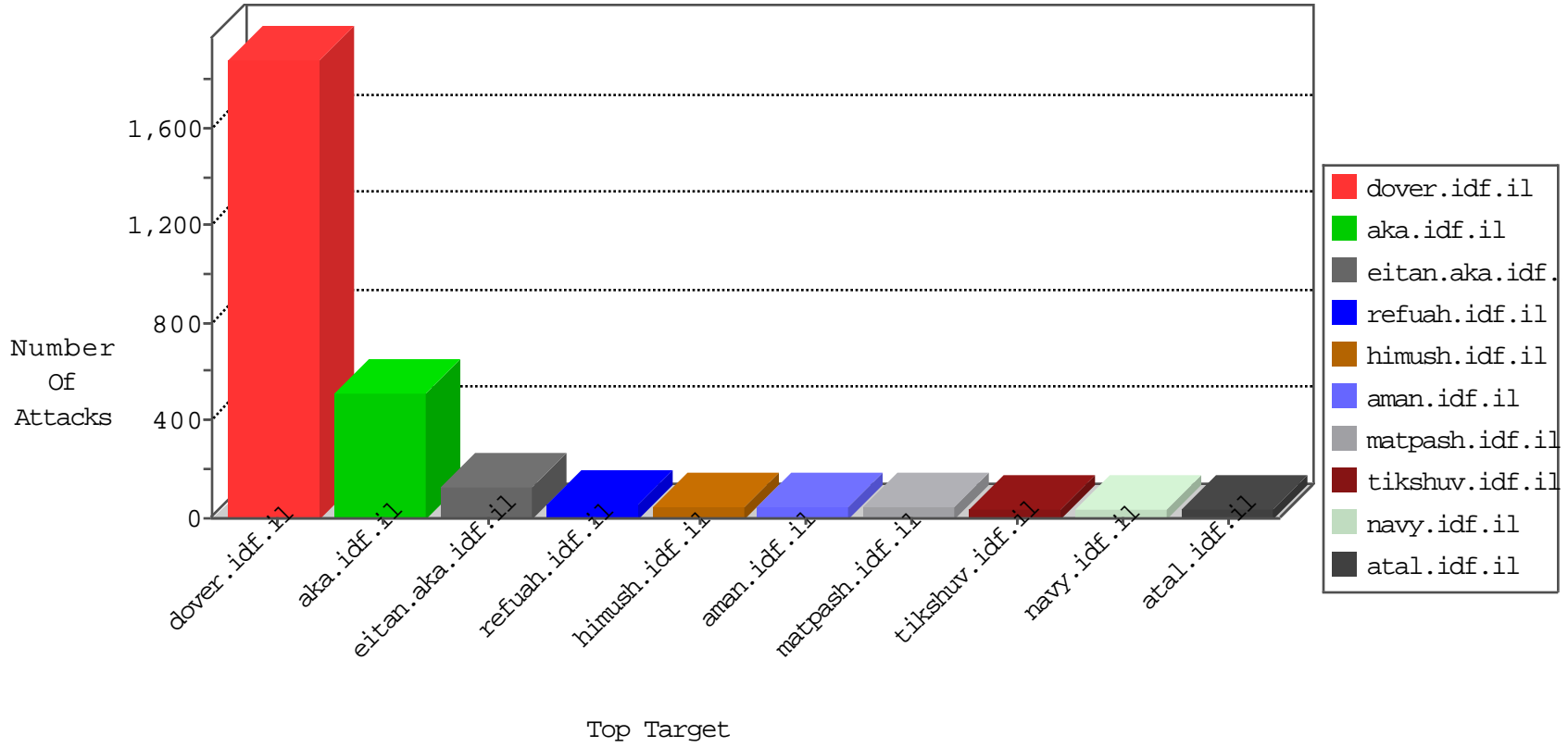


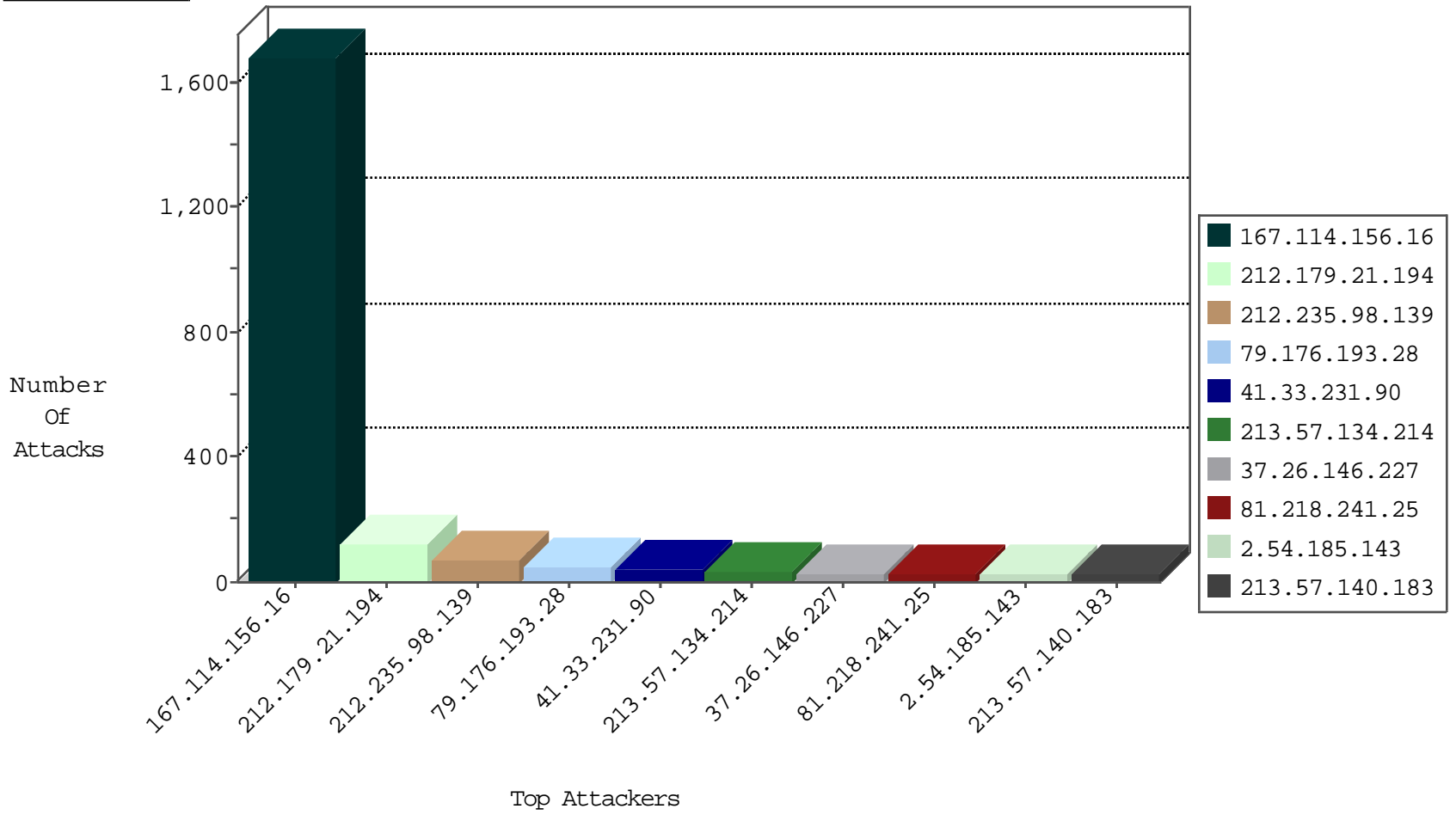
# IDF Under Attack Daily Report



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	3218
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
79.178.205.9	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.111.65.41	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3

12-15-2015-14:04:03 to 12-15-2015-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.247.9	Israel	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.176.193.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.177.49.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.24.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.247.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.116.98.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.18.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.100.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.244.49.137	147.237.0.16	Hong Kong	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.49.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.4.210.53	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.32.179.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.139.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	68
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.134.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
79.176.193.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
37.26.146.227	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	24
95.35.37.225	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	15
62.90.212.207	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.140.183	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
213.57.140.183	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.176.193.28	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
2.52.189.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
195.200.205.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.23	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.185.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
95.35.37.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.57.182.163	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.8.204.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.187.218	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.233.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.7.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.201.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.21.194	Israel	147.237.76.177	ncore.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.209.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.17.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.145.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.179.124.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.187.218	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.140.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.29	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.139.11	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.6.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.135.102.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.177.56.240	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
106.187.49.117	Japan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.150.189.2	Israel	147.237.77.170	marachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.29	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.117.148.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.17.212	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	112
89.138.55.209	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 89.138.55.209	Block	16
66.249.66.81	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	11
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	10
46.19.85.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
149.78.10.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.10.57	Block	8
147.236.238.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	6
2.52.176.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.12.141.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
68.180.228.49	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
82.81.23.72	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
149.78.139.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
157.55.39.88	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.65.187.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/default.aspx <https://www.aka.idf.il/main/sachar/default.aspx	Block	2
93.173.224.149	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
176.12.142.170	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	2
157.55.39.3	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
147.236.238.22	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 147.236.238.22	Block	2
37.26.148.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.10.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
82.80.198.164	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.70	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/×Ž×?×™× ×@×-×ž×•×ÿ.aspx	Block	1
147.236.238.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
82.38.119.79	United Kingdom	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
208.115.111.74	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
180.76.15.14	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.201.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.235	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.247.9	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19916-he/idfgdover.aspx	Block	1
80.179.202.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.177.16.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
46.117.154.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.218.82	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.113.124	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1217-he/refuah.aspx&sa=u&ved=0ahukewj21sut793jah ub5rokhd4ddo8qfggimaa&usg=afqjcnfizkndff3fqlewsd0woh6p4ybbg	Block	1
77.125.134.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.7.43	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
31.210.181.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.55.209	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1	Block	1