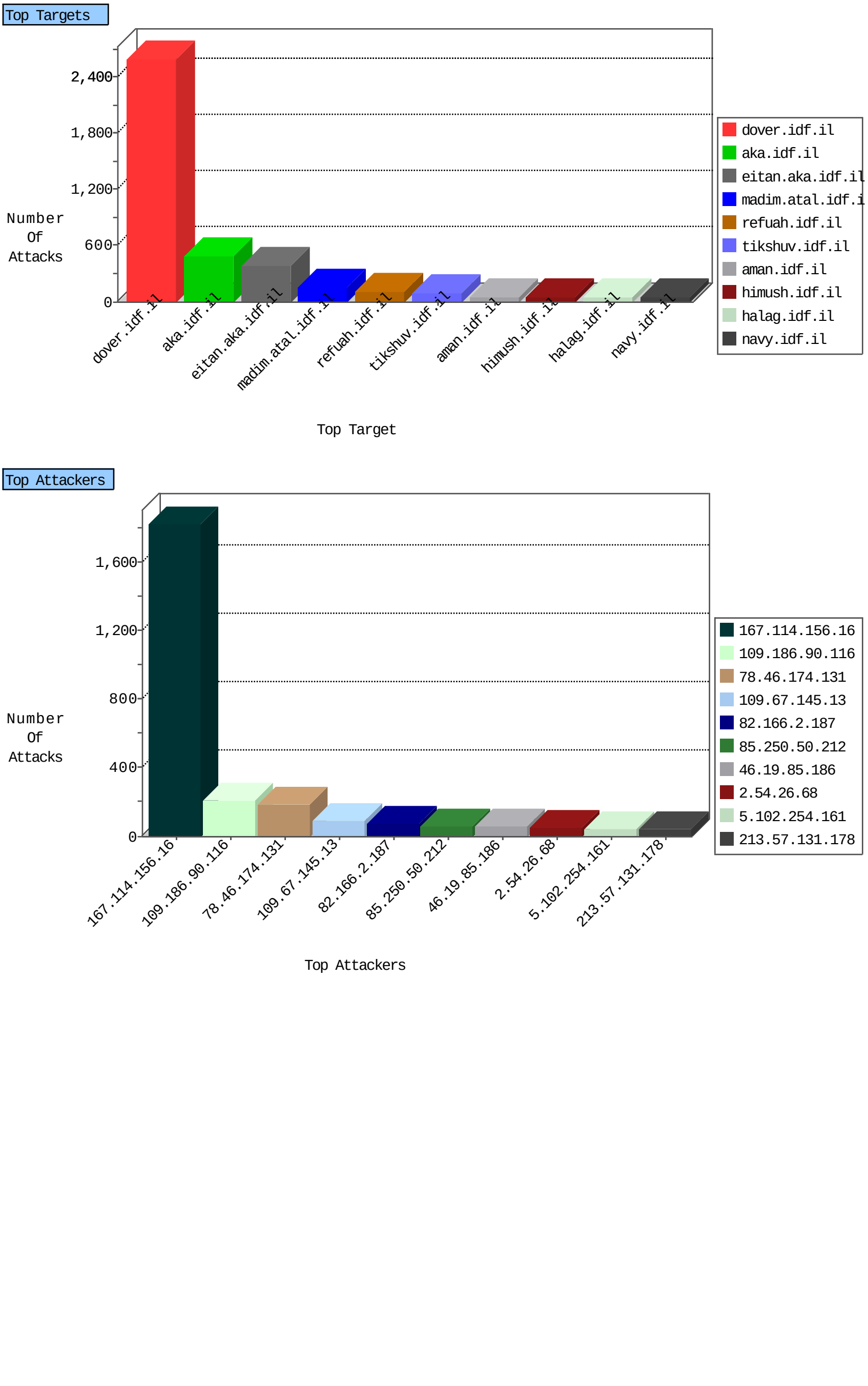
12-15-2015-20:04:06 to 12-15-2015-21:04:06

IDF Under Attack Daily Report



12-15-2015-20:04:06 to 12-15-2015-21:04:06

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	3471
37.26.149.236	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
70.39.186.45	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	17
84.228.162.39	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
176.13.10.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
80.246.133.98	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
79.177.235.134	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
87.68.63.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.177.235.134	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.86.96	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
124.141.17.192	Japan	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

12-15-2015-20:04:06 to 12-15-2015-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-15-2015-20:04:06 to 12-15-2015-21:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	4
213.57.109.144	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

12-15-2015-20:04:06 to 12-15-2015-21:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.145.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
82.166.2.187	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	74
5.102.254.161	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
85.250.50.212	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.52.33.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
70.39.186.45	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.54.26.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
213.57.131.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
46.121.206.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
37.26.147.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.250.50.212	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		monitor	13
213.57.131.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
213.57.131.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
66.102.9.15	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
213.57.128.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
86.111.148.242	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
37.26.148.197	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
84.109.184.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
2.52.159.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.186.90.116	Israel	147.237.76.34	yohalan.idf.il	drop		drop	9
213.57.137.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.54.30.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
110.171.37.147	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
178.162.216.32	Germany	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
51.36.128.142	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.26.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.111.181.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.54.26.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.26.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.26.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.52.6.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.249.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.80.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

12-15-2015-20:04:06 to 12-15-2015-21:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.186.90.116	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	194
78.46.174.131	Germany	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	182
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
31.168.28.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
37.26.149.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
93.172.160.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	8
213.57.224.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.57.224.198	Block	8
109.64.107.68	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.64.107.68	Block	6
84.228.180.118	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.180.118	Block	6
213.151.38.209	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
109.65.192.100	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
2.52.32.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.52.191.175	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.186	Block	3
84.228.180.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
149.78.42.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	3
37.26.149.201	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
87.69.208.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.181.34.20	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.90.148.93	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.90.148.93	Block	3
208.115.111.74	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.135.111.75	Ukraine	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
46.121.92.35	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.81	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
149.88.108.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.142	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
213.204.101.26	Lebanon	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
213.8.129.140	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.129.140	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
85.250.154.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.186.173.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.140.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.115.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/60045.pdf e 14-10-07, 11:25	Block	1
46.120.2.203	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
95.86.90.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucFaqControl$imgShowSubjectLinks.x in www.refua.atal.idf.il/1537-he/refuah.aspx	Block	1
87.68.80.88	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.68.80.88	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
176.13.15.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/71084.doc	Block	1
149.78.1.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.175.139	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.108.44.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-15-2015-20:04:06 to 12-15-2015-21:04:06