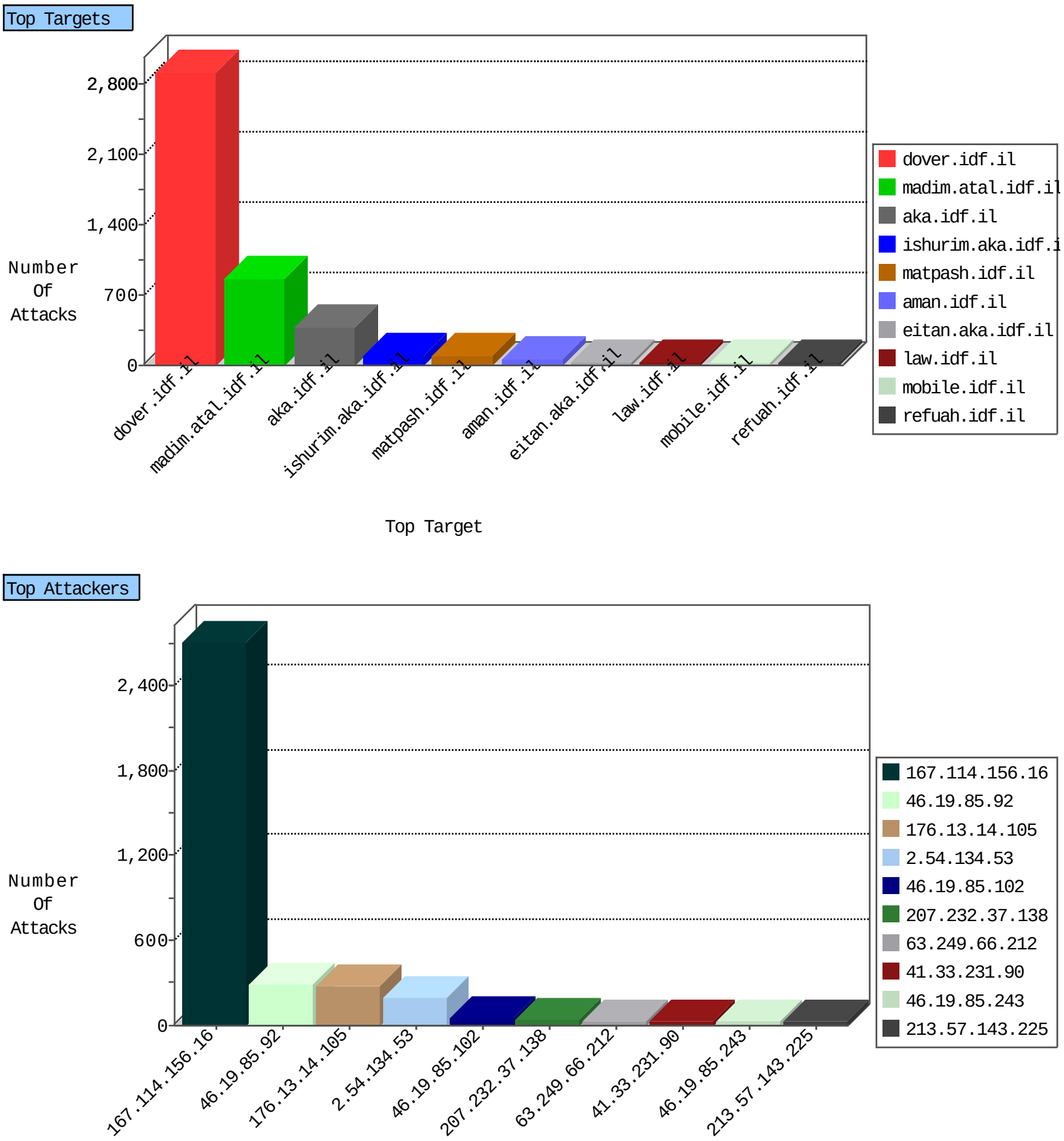
12-09-2015-16:04:06 to 12-09-2015-17:04:06

IDF Under Attack Daily Report



12-09-2015-16:04:06 to 12-09-2015-17:04:06

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	3440
115.239.228.8	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
89.248.160.229	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
118.232.237.176	Taiwan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.229	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
71.6.158.166	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.229	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
118.232.237.176	Taiwan	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

12-09-2015-16:04:06 to 12-09-2015-17:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
111.94.200.3	Indonesia	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1

12-09-2015-16:04:06 to 12-09-2015-17:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
188.120.148.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.64.208.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.2.43.66	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.144	147.237.77.216	China	dover.idf.il	portscan: TCP Distributed Portscan	1
221.2.43.66	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
84.228.111.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.2.43.66	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
84.108.147.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.2.43.66	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
80.246.139.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.249.175.225	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
46.120.30.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.101.186.178	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
5.39.222.253	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.77.179	Italy	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
221.2.43.66	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
85.64.133.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.2.43.66	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
84.109.13.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.2.43.66	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
82.80.216.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.2.43.66	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.206	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.149.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.139.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.157.244.243	147.237.0.19	Somalia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

12-09-2015-16:04:06 to 12-09-2015-17:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.232.37.138	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	46
63.249.66.212	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.243	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
80.246.136.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
176.12.139.232	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.145	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
5.29.159.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.134.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.8.204.19	Israel	147.237.8.45	e.eitan.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
213.57.143.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.151.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.57.143.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
213.57.135.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
138.134.192.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
213.57.135.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
5.28.147.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
173.252.114.118	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
213.57.143.225	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
5.28.147.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.180.176.99	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.137.41	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.3.144.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.57.135.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
173.162.34.45	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.114.91.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.25.94.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.158.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
173.252.114.117	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.54.32.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.80	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
199.203.47.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.132.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
173.252.114.119	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.106.94.2		147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	6
173.252.114.115	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.180.176.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.151.41.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.64.146.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
173.252.114.116	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
213.8.173.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
173.252.114.112	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
80.74.124.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

12-09-2015-16:04:06 to 12-09-2015-17:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	187
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	147
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	93
176.13.14.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	88
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.92	Block	41
46.121.247.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
2.54.158.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
193.106.52.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	3
176.13.4.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
2.52.158.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.179.119.87	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/540-he/patzar.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
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.3.144.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.23.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
110.77.235.118	Thailand	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.75.30	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/dynamic_map/dynamic_map.aspx	Block	1
212.199.53.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.135.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
178.59.42.135	Greece	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
80.246.137.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
150.129.121.86	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.106	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
207.46.13.155	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/	Block	1
109.235.189.141	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-en/cogat.aspx	Block	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
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
185.32.179.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.101.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
35.0.127.52	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
2.52.163.126	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
66.249.75.30	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
54.153.33.145	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176/	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
109.67.214.172	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
178.59.42.135	Greece	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.94.80.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.240.183.227	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
5.174.121.210	Poland	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
150.129.121.86	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	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
109.235.189.141	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1

12-09-2015-16:04:06 to 12-09-2015-17:04:06