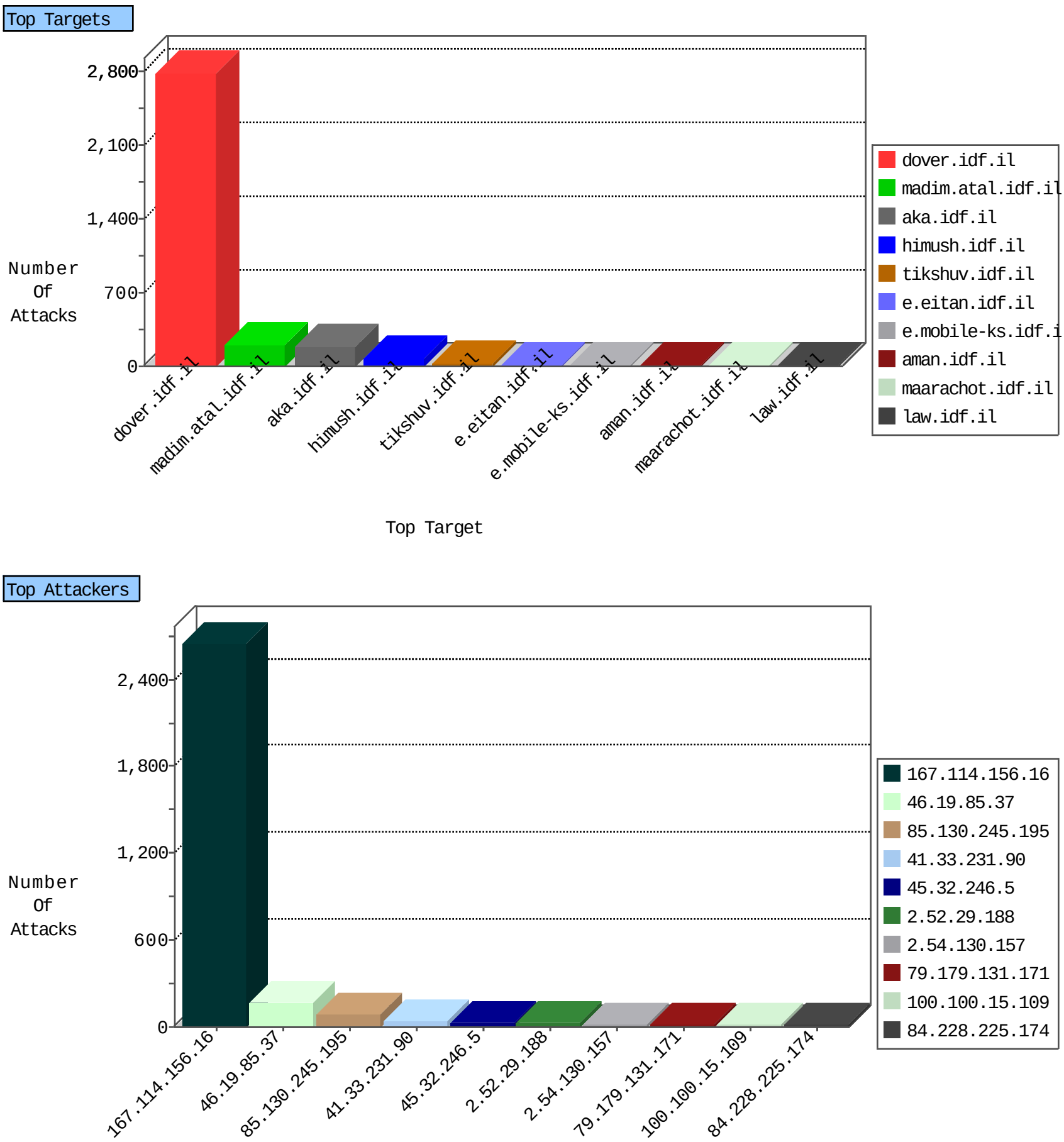
12-08-2015-23:04:05 to 12-09-2015-00:04:05

IDF Under Attack
Daily Report



12-08-2015-23:04:05 to 12-09-2015-00:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5003
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3454
45.32.246.5		147.237.8.45	e.eitan.idf.il	Invalid TCP Flags	drop	3
45.32.246.5		147.237.72.217	e.idf.il	Invalid TCP Flags	drop	2
77.69.168.154	Bahrain	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
220.163.110.126	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
45.32.246.5		147.237.8.28	e.mobile-ks.idf.il	Invalid TCP Flags	drop	1

12-08-2015-23:04:05 to 12-09-2015-00:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-08-2015-23:04:05 to 12-09-2015-00:04:05

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
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
166.63.125.149	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.246.5	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -f -sS	1
45.32.246.5	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
78.193.2.8	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
220.163.110.126	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
220.163.110.126	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
66.232.140.121	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
66.232.140.121	147.237.8.14	Korea, Republic of	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.129	147.237.76.177		ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.246.5	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
183.61.109.189	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.246.5	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
166.63.125.149	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.246.5	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -f -sS	1
117.25.155.164	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 2048	1
45.32.246.5	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
82.117.208.243	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
78.193.2.8	147.237.76.31	France	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
220.163.110.126	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
66.232.140.121	147.237.8.46	Korea, Republic of	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
220.163.110.126	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
66.232.140.121	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.129	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.8.45		e.eitan.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.129	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
183.61.109.189	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

12-08-2015-23:04:05 to 12-09-2015-00:04:05

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	36
85.130.245.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.15.109		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
84.228.225.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.245.195	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.179.131.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.176.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.131.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.245.195	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
85.130.245.195	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.245.195	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.182.199.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
45.32.246.5		147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	4
37.142.64.96	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
45.32.246.5		147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
45.32.246.5		147.237.72.217	e.idf.il	drop	SAM rule	drop	4
2.54.130.157	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
79.182.214.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.249.95	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	3
213.57.131.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.102.254.79	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.132.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.131.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.52.31.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.181.136.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.162.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.64.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.181.183.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.224.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.32.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.208.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.177.189.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
80.246.136.130	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
94.230.86.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.126.31.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.54.132.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.13.8.98	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.80.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.28.147.109	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2

12-08-2015-23:04:05 to 12-09-2015-00:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	119
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
2.52.29.188	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.52.29.188	Block	25
2.54.130.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.37	Block	15
176.12.149.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
89.138.207.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
95.86.87.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
2.52.29.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/67378.jp	Block	1
84.94.86.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/17672.jpg	Block	1
73.237.152.66	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.54.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.106.22.163	Germany	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
40.77.167.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jenin.stm)	Block	1
79.182.150.233	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/1133-22638-he/dover.aspx.	Block	1
173.252.88.191	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	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
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
2.52.54.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.67.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/6255.jpg	Block	1
77.126.97.230	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
49.205.171.69	India	147.237.77.74	law.idf.il	PHP Attempt	Block	1
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113055.pdf	Block	1
87.106.22.163	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/admin	Block	1
79.183.176.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sahar	Block	1
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	1
176.12.144.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=f7142f2a04e63355.1425928839.11.1449611917.1449611917.;	Block	1
84.108.184.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.116.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
49.205.171.69	India	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
157.55.39.20	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
80.246.136.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.199.104.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8763-he/refuah.aspx	Block	1
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 0.8afc=%5B%22%22%2C%22%22%2C1449611917%2C%22http%3A%2F%2Fm.facebook.com%2F%22%5D; in URL _pk_id.20.8afc=f7142f2a04e63355.1425928839.11.1449611917.1449611917.	Block	1
31.154.170.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.4.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.131.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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

12-08-2015-23:04:05 to 12-09-2015-00:04:05