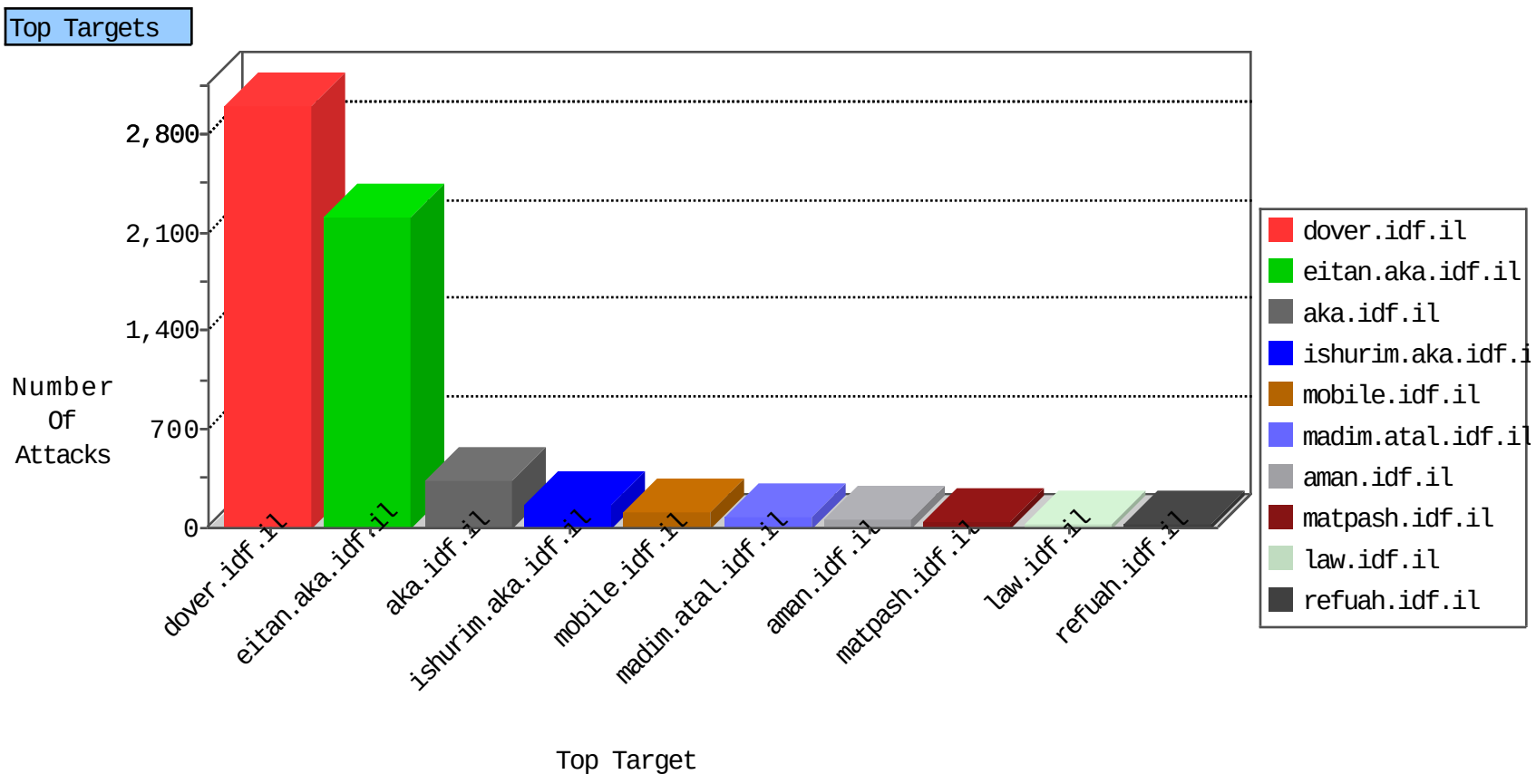
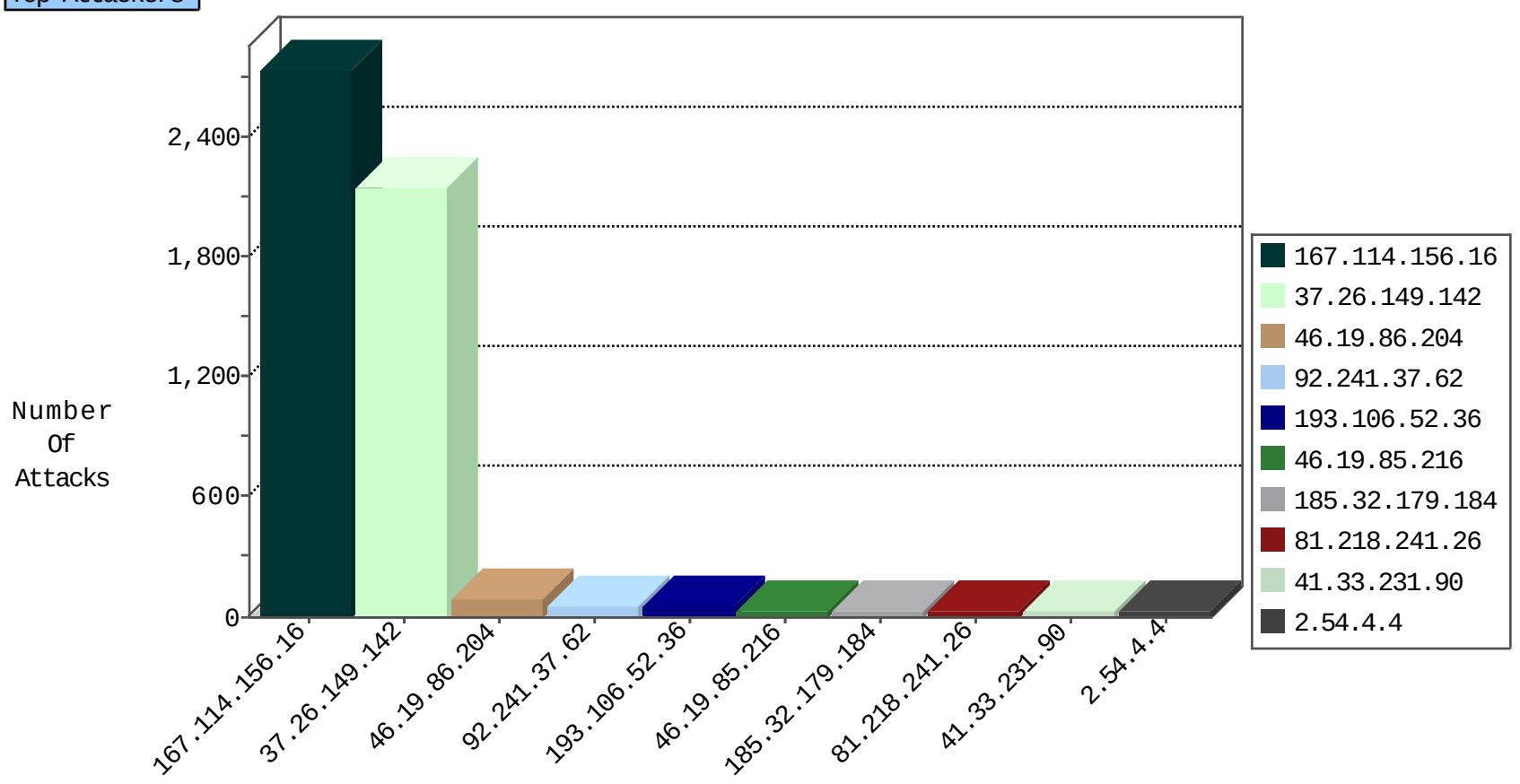
12-09-2015-18:04:02 to 12-09-2015-19:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-09-2015-18:04:02 to 12-09-2015-19:04:02

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	3399
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
45.32.246.5		147.237.72.14	dover.idf.il(old)	Invalid TCP Flags	drop	3
79.183.126.42	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
45.32.246.5		147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	2
89.248.160.229	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
173.195.0.24	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.248.160.229	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

12-09-2015-18:04:02 to 12-09-2015-19:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.98	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-09-2015-18:04:02 to 12-09-2015-19:04:02

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
150.107.119.154	147.237.76.31	India	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.169.48.140	147.237.76.176	United Kingdom	test.ncore.idf.i	ET SCAN Potential SSH Scan	1
85.64.202.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.56.3.111	147.237.77.227	Spain	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
79.181.0.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.217.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.72.14		dover.idf.il(old	ET SCAN NMAP -sS window 2048	1
39.89.6.234	147.237.0.19	China	madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
184.2.159.186	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.169.48.140	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN Potential SSH Scan	1
83.56.3.111	147.237.77.227	Spain	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
81.218.50.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.245.240.26	147.237.77.74	Australia	law.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.246.5	147.237.72.14		dover.idf.il(old	ET SCAN NMAP -sS window 3072	1
213.8.204.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.72.14		dover.idf.il(old	ET SCAN NMAP -f -sS	1
193.105.134.220	147.237.77.235	Sweden	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
184.2.159.186	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1

12-09-2015-18:04:02 to 12-09-2015-19:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.142	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1692
46.19.86.204	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	95
92.241.37.62	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.32.179.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.54.4.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.57.134.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
92.241.37.62	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.125	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
94.159.152.34	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
94.159.152.34	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.66.137.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.21.122.174	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
79.183.172.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
5.28.155.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.34	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
183.79.222.67	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
5.28.155.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
87.68.243.22	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.105	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
5.102.254.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
207.241.226.39	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	7
46.19.85.186	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.254.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.16.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.94.208.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.170.107	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.55.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.144.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.136.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.81.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.58.80.11	Netherlands	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.54	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.106.94.2		147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
77.127.133.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.54.172	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.125.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.159.206.107	Italy	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.21.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.26.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.32.179.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

12-09-2015-18:04:02 to 12-09-2015-19:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.142	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	458
193.106.52.36	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	30
85.65.200.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
84.228.236.165	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	7
46.19.85.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
93.175.34.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.175.34.106	Block	4
2.54.4.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.120.18.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.136.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.31.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.137.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.59	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.109.73.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.175.34.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	2
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.63.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.29.157.203	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
128.232.110.29	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.74.9	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/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/1133-22461-he/dover.aspx.	Block	1
37.26.148.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.65.112.247	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
188.138.17.205	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/modiin/default.aspx	Block	1
80.246.136.178	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.12.145.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	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
2.54.182.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.90.142.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20353-he/kkkkkkk=c98d1d98kkkkkkk_c98d1d98	Block	1
84.108.81.186	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 84.108.81.186	Block	1
77.125.108.229	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.19.85.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.129	United States	147.237.76.31	nakchal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.75.30	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
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
2.52.134.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
176.13.9.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.140.38	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1

12-09-2015-18:04:02 to 12-09-2015-19:04:02