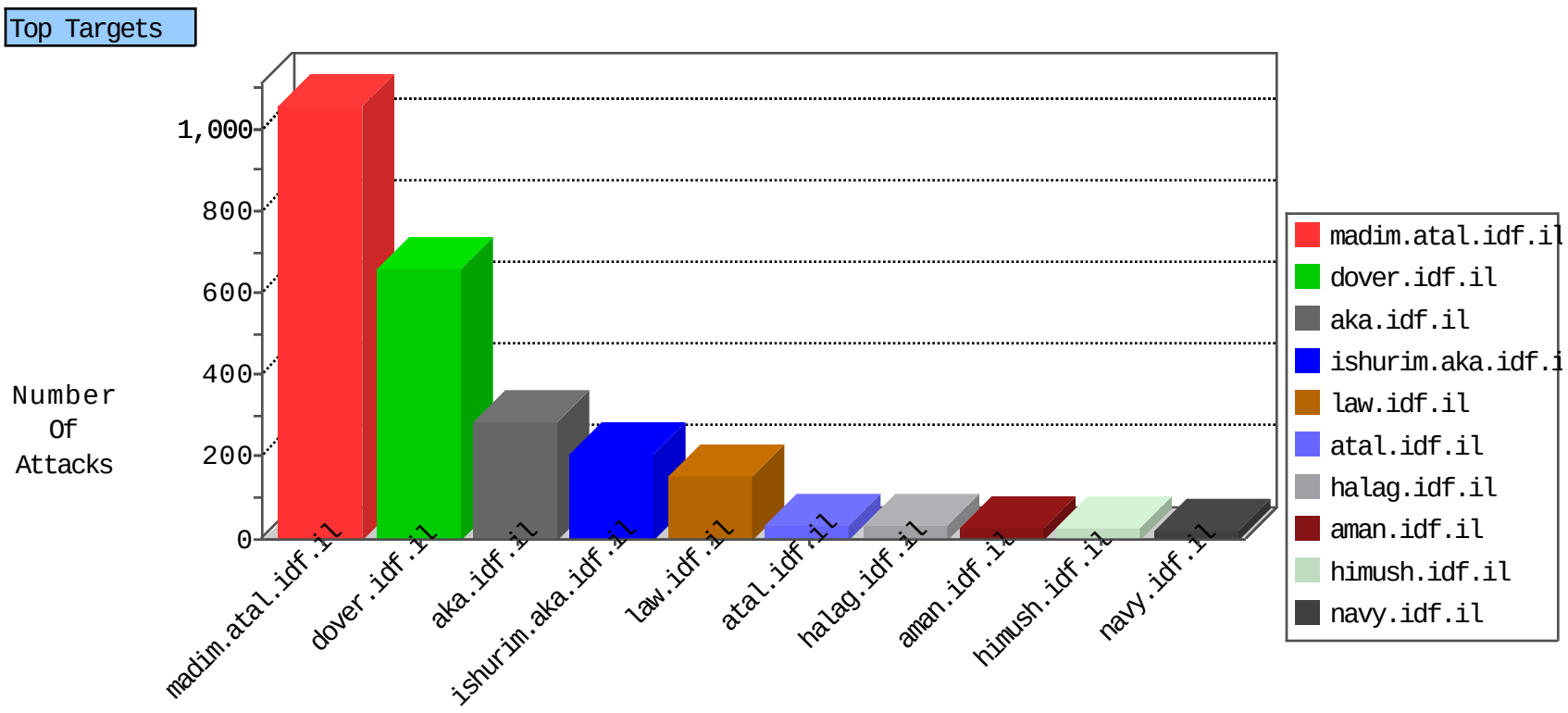
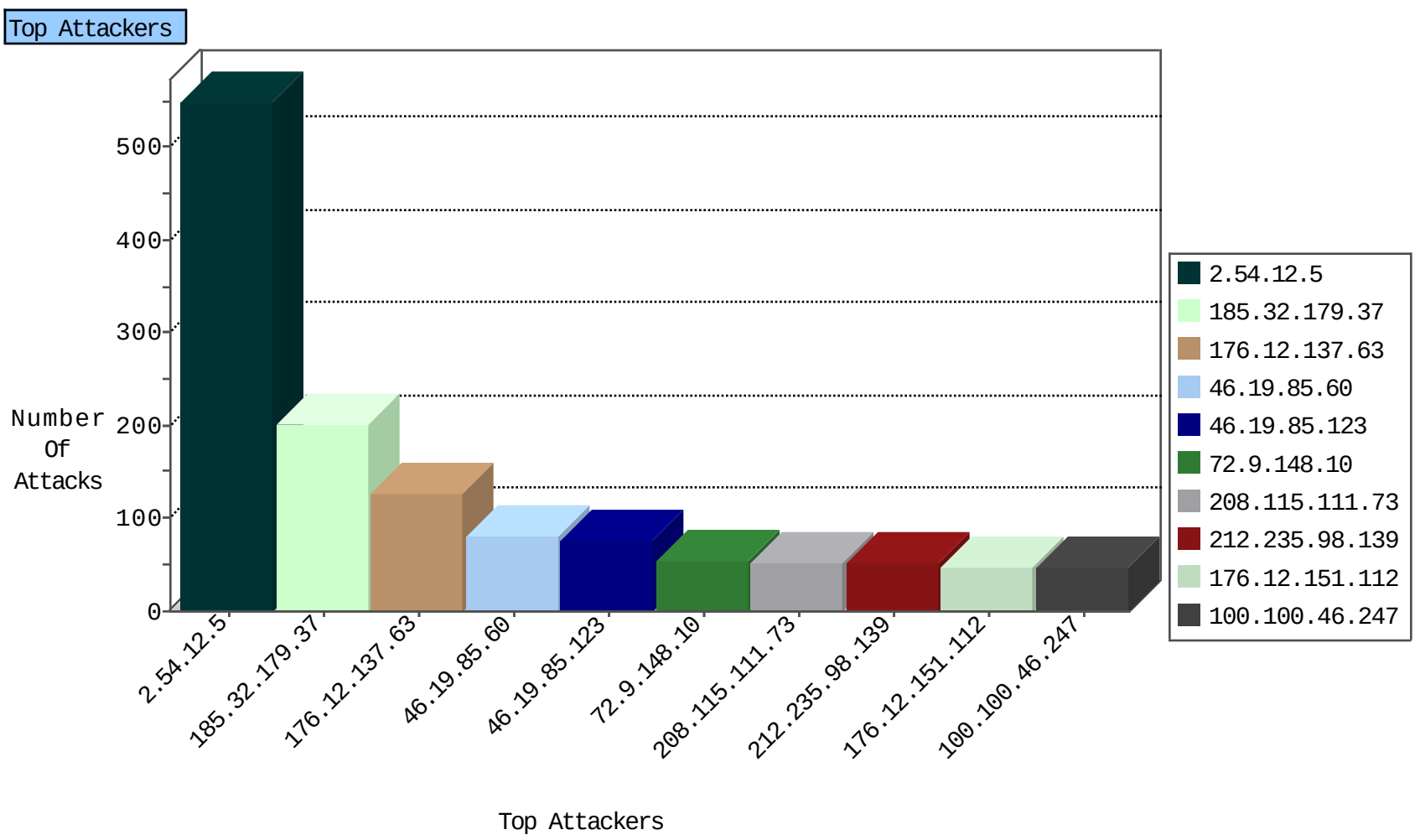
11-22-2015-08:04:05 to 11-22-2015-09:04:05

IDF Under Attack Daily Report





11-22-2015-08:04:05 to 11-22-2015-09:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.83.224	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
176.12.138.213	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
79.182.221.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
89.139.186.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
2.54.62.62	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
85.17.189.18	Netherlands	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
132.68.141.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
147.236.38.135	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.134.157	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.56.236.17	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
2.54.138.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
168.235.69.168	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
37.26.147.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
168.235.69.168	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
37.26.149.144	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.64.209.150	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-22-2015-08:04:05 to 11-22-2015-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-22-2015-08:04:05 to 11-22-2015-09:04:05

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
98.119.105.221	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.93.0.15	147.237.76.31	Germany	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.198.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.146.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.227.196.29	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
221.214.237.245	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.42.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.62.126.13	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.111.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.72.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.93.0.15	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.42	Germany	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.160.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.88.183.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.158.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1

11-22-2015-08:04:05 to 11-22-2015-09:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.60	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	81
46.19.85.123	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	76
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	52
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	42
178.140.239.49	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	42
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.64.29.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.46.247		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.86.181	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.86.251	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
23.27.220.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
109.65.214.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
183.79.222.77	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.34	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
2.52.133.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.46.247		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
176.13.18.175	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.46.247		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.63.123		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.179.223.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.18.175	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.166.186.209	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.30	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
173.252.88.244	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
107.170.62.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
194.90.66.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
220.255.97.158	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
217.132.55.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
173.252.88.249	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.35.193.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.22.187	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.179.220.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.188.132.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.184.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.167.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.11.240	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.56.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

11-22-2015-08:04:05 to 11-22-2015-09:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.12.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	300
2.54.12.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
176.12.137.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
185.32.179.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
2.54.12.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	97
185.32.179.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
176.12.151.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
176.13.20.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
176.12.137.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
37.26.147.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
37.26.147.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.12.141.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.12.151.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
46.19.85.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.12.144.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.13.12.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.202	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
176.13.16.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.152.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.147.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.173.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.147.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	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
79.176.187.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1796.jpg	Block	2
176.13.18.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.36.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.138.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
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	2
84.94.186.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.120.156.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
80.246.133.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 113 cookies	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
31.154.92.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.36.231.143	United States	147.237.76.30	himush.idf.il	URL is Above Root Directory chimush.atal.idf.il/../shared/usercontrols/headerupper/	Block	1
176.228.38.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.117.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.63	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18503-en/dover.aspxÖ²Â ×'×ŸÂ¿Â½Â¦	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19478-he/idfgdover.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

11-22-2015-08:04:05 to 11-22-2015-09:04:05