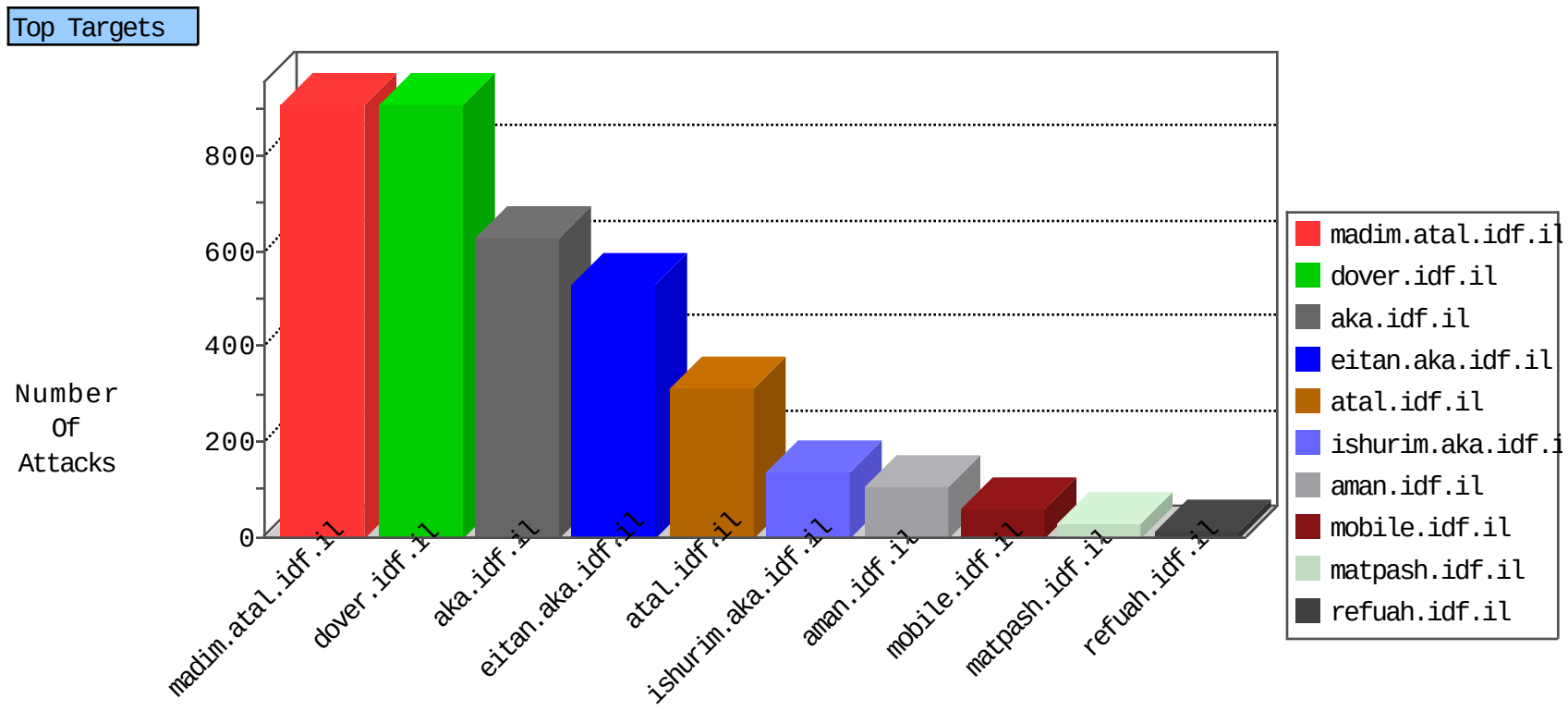
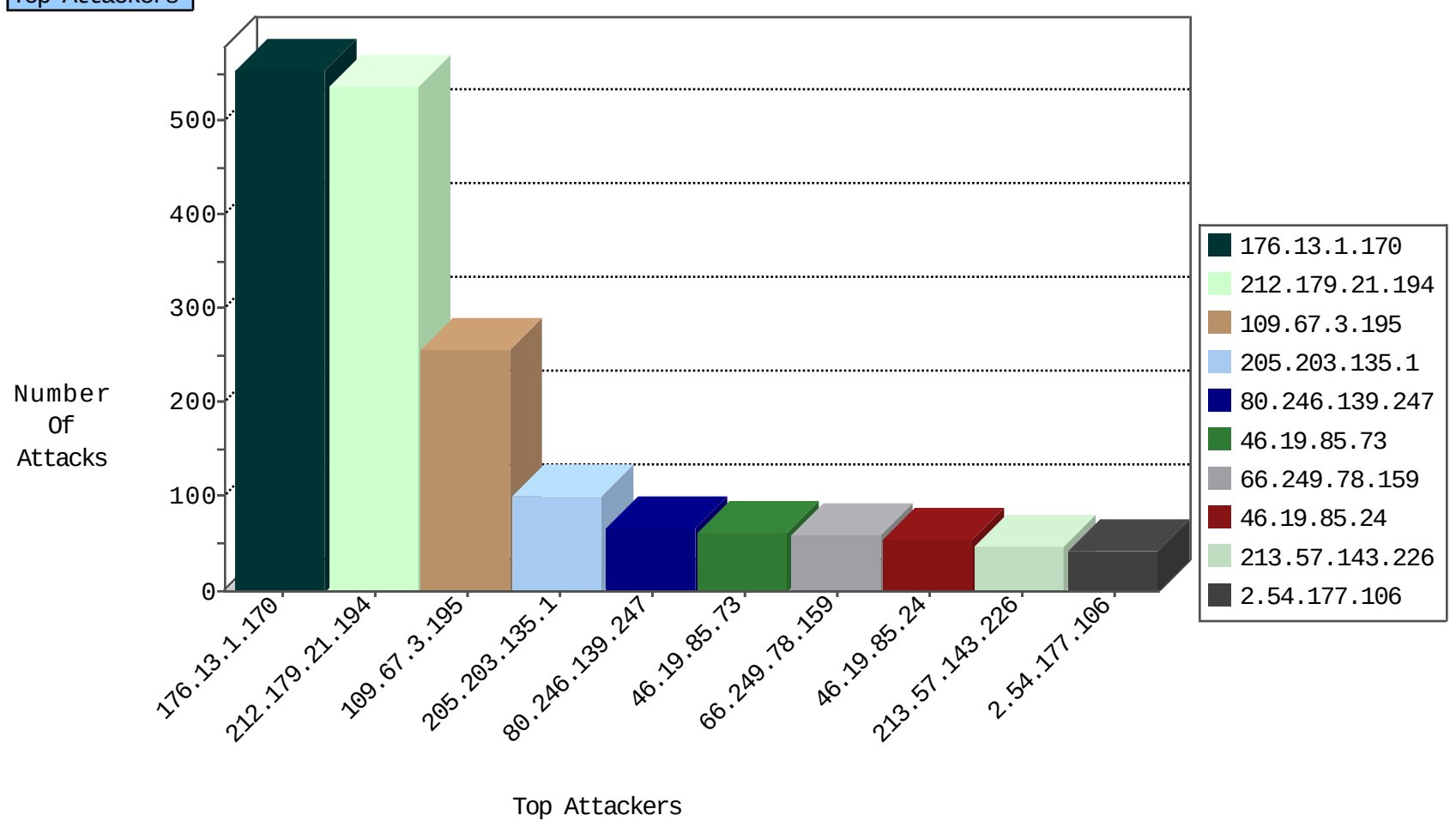
11-22-2015-14:04:04 to 11-22-2015-15:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-22-2015-14:04:04 to 11-22-2015-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
212.150.203.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
84.111.196.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.105.235	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
77.126.221.109	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.108.11.82	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
176.13.6.86	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
134.147.203.115	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
80.179.220.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.13.14.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.4.193.203	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.102.254.21	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-22-2015-14:04:04 to 11-22-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.57.242	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
149.78.76.170	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
195.160.240.11	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
5.29.126.78	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-22-2015-14:04:04 to 11-22-2015-15:04:04

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	3
82.102.169.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
185.27.105.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.93.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.108.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.165.88.20	147.237.77.216	Kenya	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.184.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.117.209.136	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.8.24	Cote D'Ivoire	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.18.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.192.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
1.235.195.234	147.237.77.170	Korea, Republic of	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
147.236.238.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.164.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.163.140.142	147.237.77.178	Germany	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.13	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.8.14	Cote D'Ivoire	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1

11-22-2015-14:04:04 to 11-22-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	372
109.67.3.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	244
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
213.57.143.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
107.167.117.8	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
79.180.15.47	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
46.19.85.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
176.12.140.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
100.100.92.151		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.25.69.114	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
37.26.146.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.19.116.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.46.151		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
80.246.139.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
80.246.139.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
80.246.139.247	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack		reject	16
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
80.246.139.247	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	15
79.179.12.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.30.169		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.182	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.102.140		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
212.25.69.114	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.46.151		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
213.57.128.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.179.222.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
100.100.120.7		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
132.76.50.6	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.65.130.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.95.183.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.143.133.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.29.182.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.137.94	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.47.28	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.148.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.14.227	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.95.251.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.22.134.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

11-22-2015-14:04:04 to 11-22-2015-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.1.170	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.1.170	Block	317
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	149
176.13.1.170	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.1.170	Block	132
176.13.1.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.85.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.54.177.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
176.12.138.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
176.13.1.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
176.12.148.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
176.13.11.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
176.13.13.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.12.143.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
176.12.140.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
109.66.141.26	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.141.26	Block	9
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	7
80.246.137.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
80.246.139.58	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	6
80.246.138.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.137.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
85.250.93.130	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
80.246.137.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
213.57.126.231	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ufi/reaction/	Block	3
79.177.185.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	3
80.246.137.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
72.43.136.243	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.138.229.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
212.235.34.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.235.34.65	Block	3
80.246.137.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.52.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.161.187	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.67.161.187	None	3
176.12.144.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.116.172.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.17.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.149.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	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
80.246.136.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.72.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
87.69.155.9	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	Distributed Suspicious Response Code	Block	1
110.170.18.186	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.95.246	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.114.105.254	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

11-22-2015-14:04:04 to 11-22-2015-15:04:04