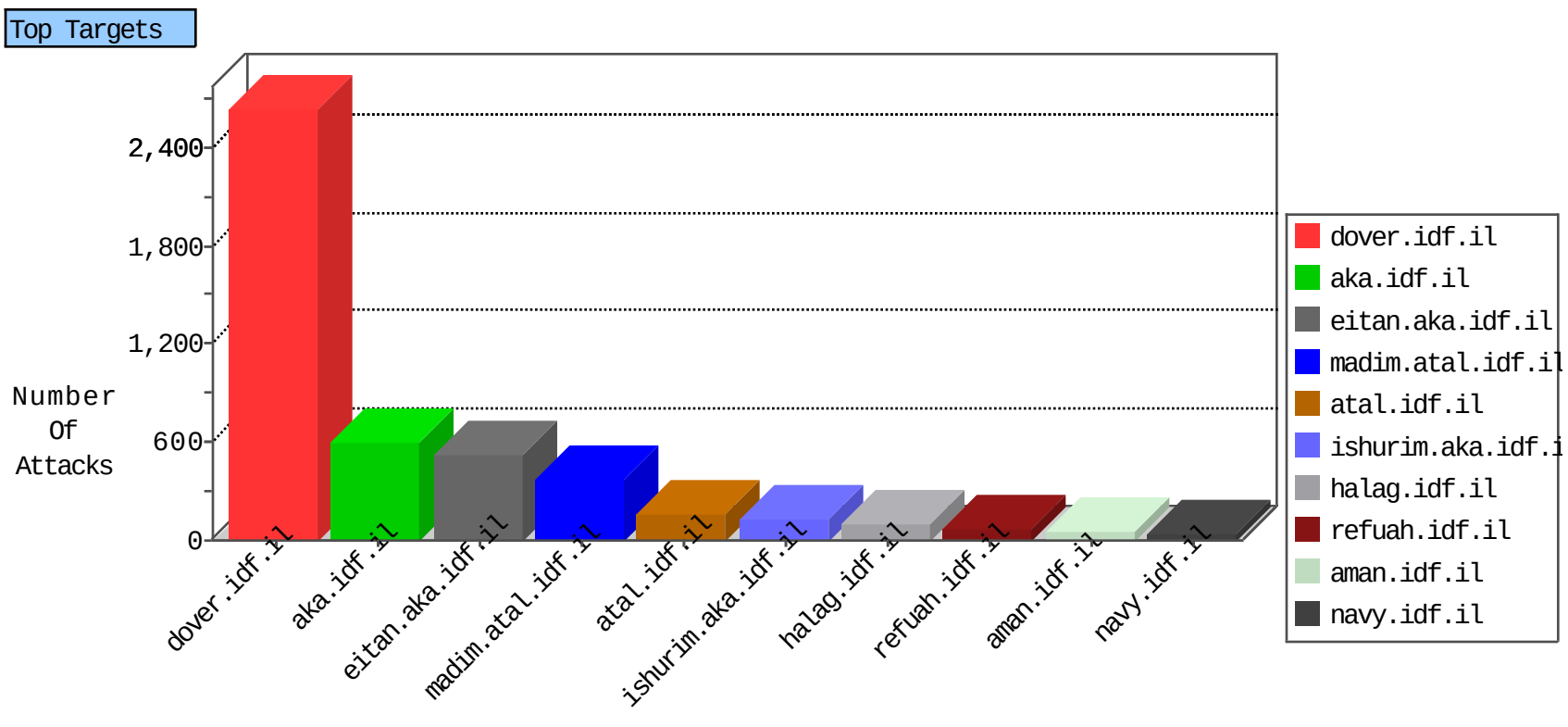
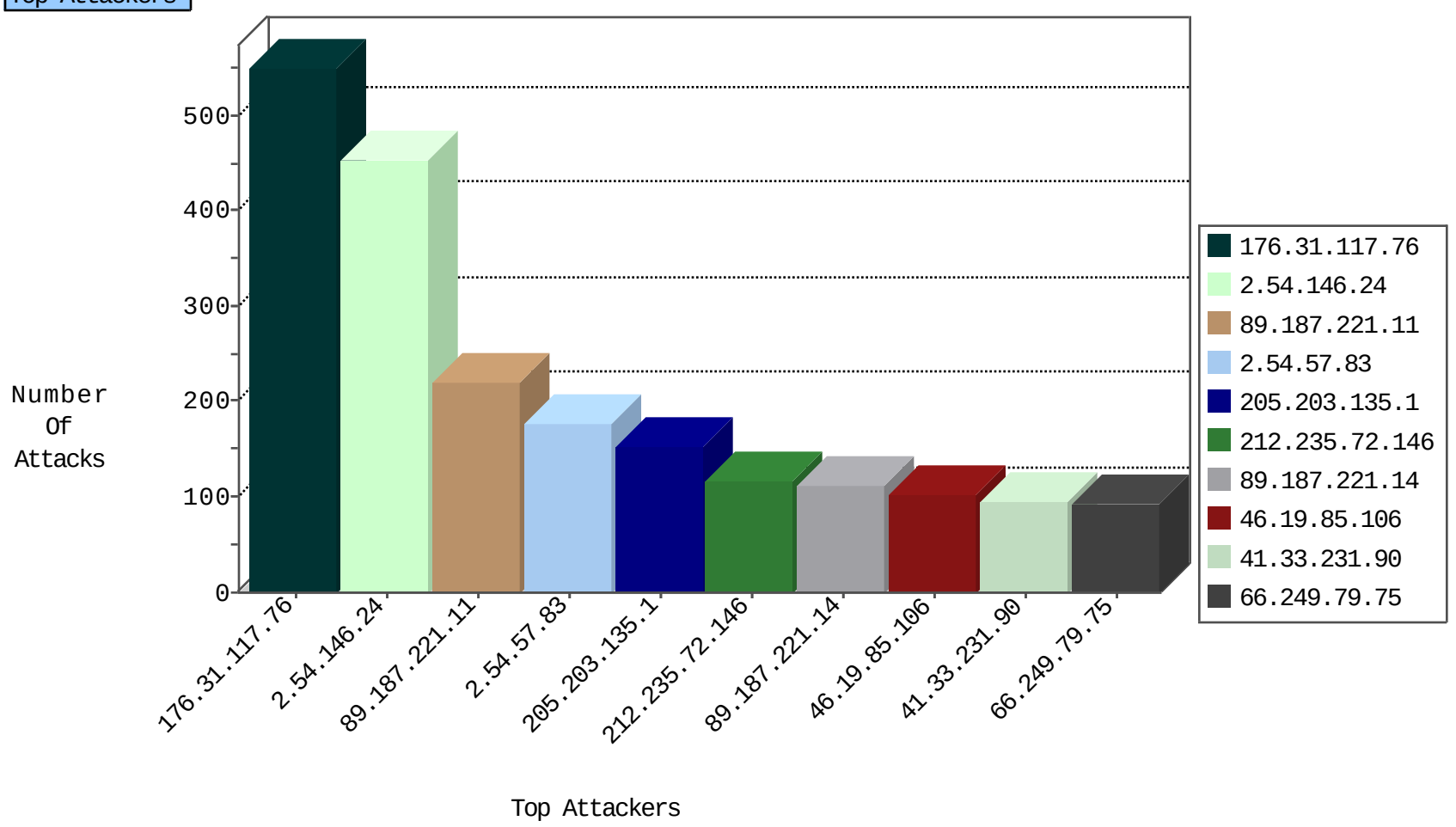
11-24-2015-13:04:01 to 11-24-2015-14:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-24-2015-13:04:01 to 11-24-2015-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.113.250	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
123.151.42.61	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
119.81.40.146	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
123.151.42.61	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

11-24-2015-13:04:01 to 11-24-2015-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.168.193.34	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
89.187.221.11	Lebanon	147.237.77.216	dover.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
93.172.144.215	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
89.187.221.12	Lebanon	147.237.77.216	dover.idf.il	2023: HTTP: Cross Site Scripting in GET Request	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	1

11-24-2015-13:04:01 to 11-24-2015-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.168.193.34	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	GPL WEB_SERVER /etc/passwd	5
80.179.223.31	147.237.77.176	Israel	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	4
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attem	4
80.179.223.31	147.237.77.216	Israel	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
65.255.43.24	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
109.66.16.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.210	147.237.77.19	Netherlands	law-forum.idf.il	ET WEB_SERVER Poison Null Byte	1
46.19.86.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	1
5.29.145.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
82.80.25.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.68.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.58.102.125	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
65.255.43.24	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
65.255.43.24	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
94.102.49.210	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Poison Null Byte	1
46.19.86.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	SQL Injection - Paranoid	1
46.19.85.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.165.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.85.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.114.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-24-2015-13:04:01 to 11-24-2015-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.31.117.76	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	551
2.54.146.24	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	423
89.187.221.11	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	211
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
89.187.221.14	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
46.19.85.106	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	102
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	85
37.26.146.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	74
89.187.221.12	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
96.238.188.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
66.87.147.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
212.235.72.146	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	58
80.246.133.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
212.235.72.146	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
151.80.40.88	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
77.42.193.101	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
64.134.70.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
213.57.130.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
109.66.61.4	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.20	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	23
213.57.128.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
100.100.81.83		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.66.61.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.10.33		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.146.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	16
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
200.97.134.94	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.79.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
155.250.255.144	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.133.38	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
176.13.1.91	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
217.194.202.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
100.100.81.83		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.57.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
2.54.57.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.187.221.13	Block	36
176.13.5.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
2.54.146.24	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.146.24	Block	32
176.13.23.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
176.13.9.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
176.13.13.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
176.12.138.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
89.187.221.11	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.187.221.11	Block	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	7
80.246.136.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
212.143.90.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.143.90.173	Block	5
2.54.57.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	5
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.12.150.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.188.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.9.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.52.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.5.96	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
89.187.221.14	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.187.221.14	Block	2
37.26.146.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.11.28	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
37.26.146.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.135.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.1.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.94.96.198	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
192.115.97.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	2
85.250.8.139	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 85.250.8.139	Block	2
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.12.145.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.17.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.198	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover	Block	1
109.65.184.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.241.160	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
95.35.186.223	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.86.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1