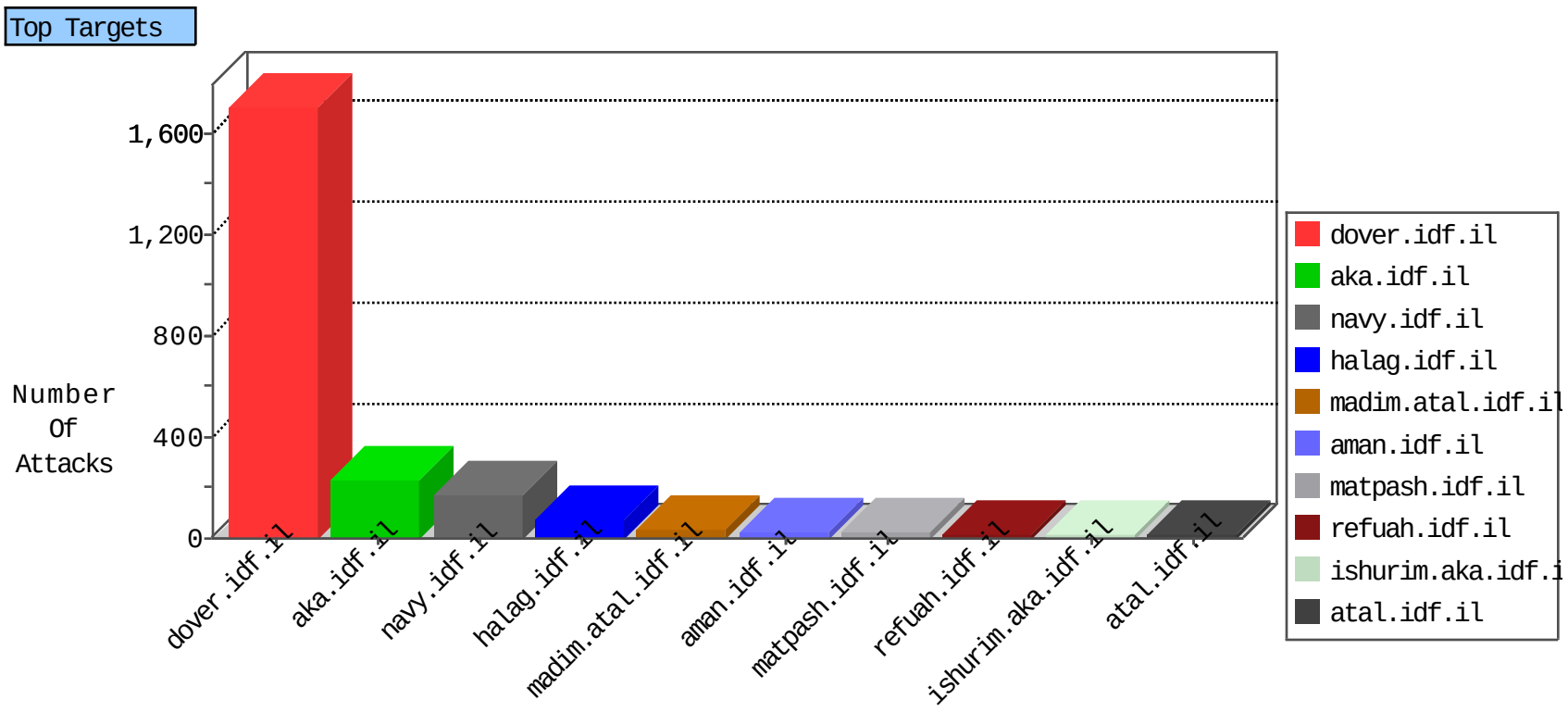
11-20-2015-22:04:08 to 11-20-2015-23:04:08

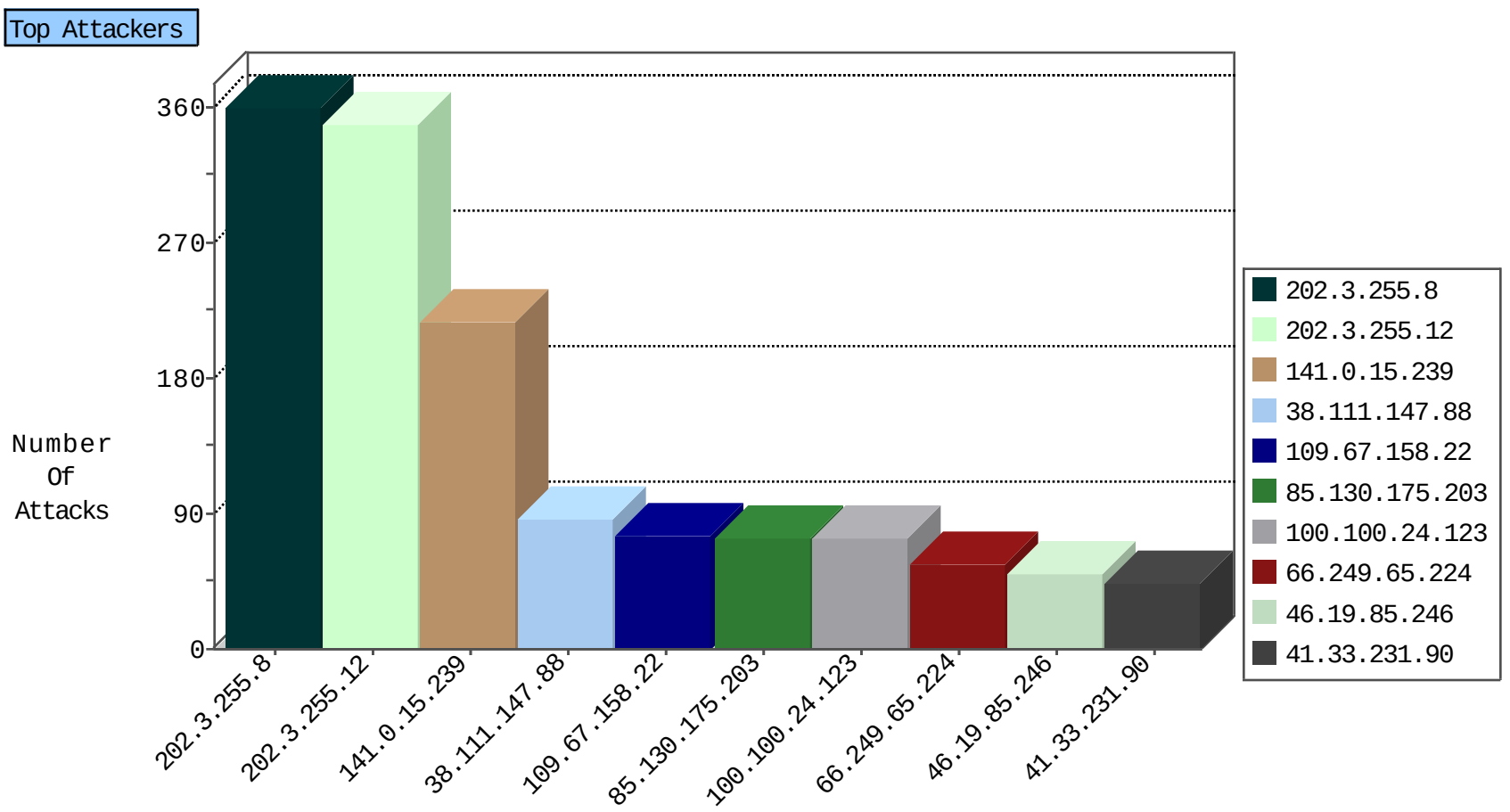
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-20-2015-22:04:08 to 11-20-2015-23:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
10.0.0.6		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	16
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	11
100.100.24.123		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.19.86.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
141.0.15.239	Norway	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
141.0.15.239	Norway	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
71.6.167.142	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
62.219.144.239	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.67.158.22	Israel	147.237.72.166	aka.idf.il	Invalid L4 Header Length	drop	1

11-20-2015-22:04:08 to 11-20-2015-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.69.198.82	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
201.7.49.69	Brazil	147.237.72.166	aka.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	1

11-20-2015-22:04:08 to 11-20-2015-23:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	336
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	324
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
98.119.105.221	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
23.99.54.247	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
220.245.240.26	147.237.76.198	Australia	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
183.138.153.82	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Poison Null Byte	1
98.119.105.221	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
77.109.38.223	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.55.35	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.76.199	Poland	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
220.245.240.26	147.237.76.198	Australia	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1

11-20-2015-22:04:08 to 11-20-2015-23:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
109.67.158.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	69
141.0.15.239	Norway	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	60
141.0.15.239	Norway	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	57
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
141.0.15.239	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	52
141.0.15.239	Norway	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
100.100.24.123		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
2.54.52.160	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
85.130.175.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
85.130.175.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.24.123		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
85.130.175.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
85.130.175.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
199.127.226.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
188.140.164.167	Oman	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
186.220.52.193	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
40.77.167.21	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
100.100.24.123		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	12
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.28.185		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
173.252.122.119	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	12
63.138.47.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
87.69.216.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
95.108.158.173	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
174.114.23.181	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.180.207.104	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
77.125.104.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
95.108.158.232	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.145.211.29	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
95.108.158.214	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.201.138.8	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
107.178.194.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.139.178.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.154.243.114	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.185	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.170.198.238	Netherlands	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
90.184.141.245	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.146.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.3.146.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
87.69.216.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
176.12.148.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.21.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.15.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.228.128.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.121.198.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.175.13.138	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 5.175.13.138	Block	2
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.141.2.160	Block	2
68.197.228.235	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.178.148.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.15.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.199.53.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.109.214.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.28.191.121	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
185.3.146.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.175.13.138	Germany	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 5.175.13.138	Block	2
89.139.178.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.93.154.198	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
84.94.37.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/nakhal/kkkkkkk=42db36a0kkkkkkk_42db36a0	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	1
111.161.127.182	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
84.228.188.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.105.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
2.54.166.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.127.226.150	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3167.pdf	Block	1
94.32.246.43	Italy	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
5.175.13.138	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	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
84.109.136.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
183.138.153.82	China	147.237.77.216	dover.idf.il	NULL Character in URL /english/organization/homefront/homefront2.stm[[#0]]	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
149.78.225.246	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
87.68.41.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.141.2.160	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ujdwjdxj	Block	1
5.22.131.91	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
201.220.244.136	Chile	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.175.13.138	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
77.125.93.22	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
149.78.225.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
87.69.185.203	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1