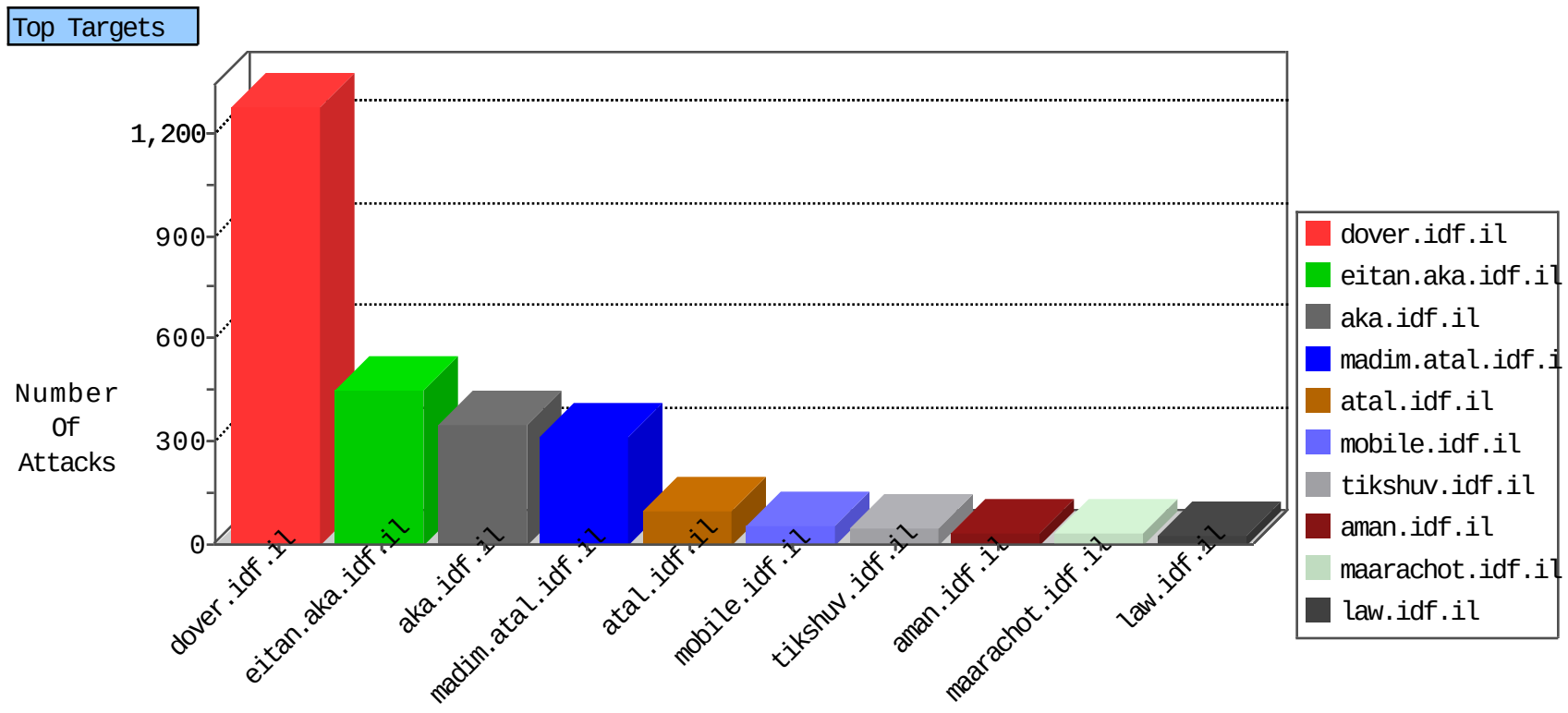
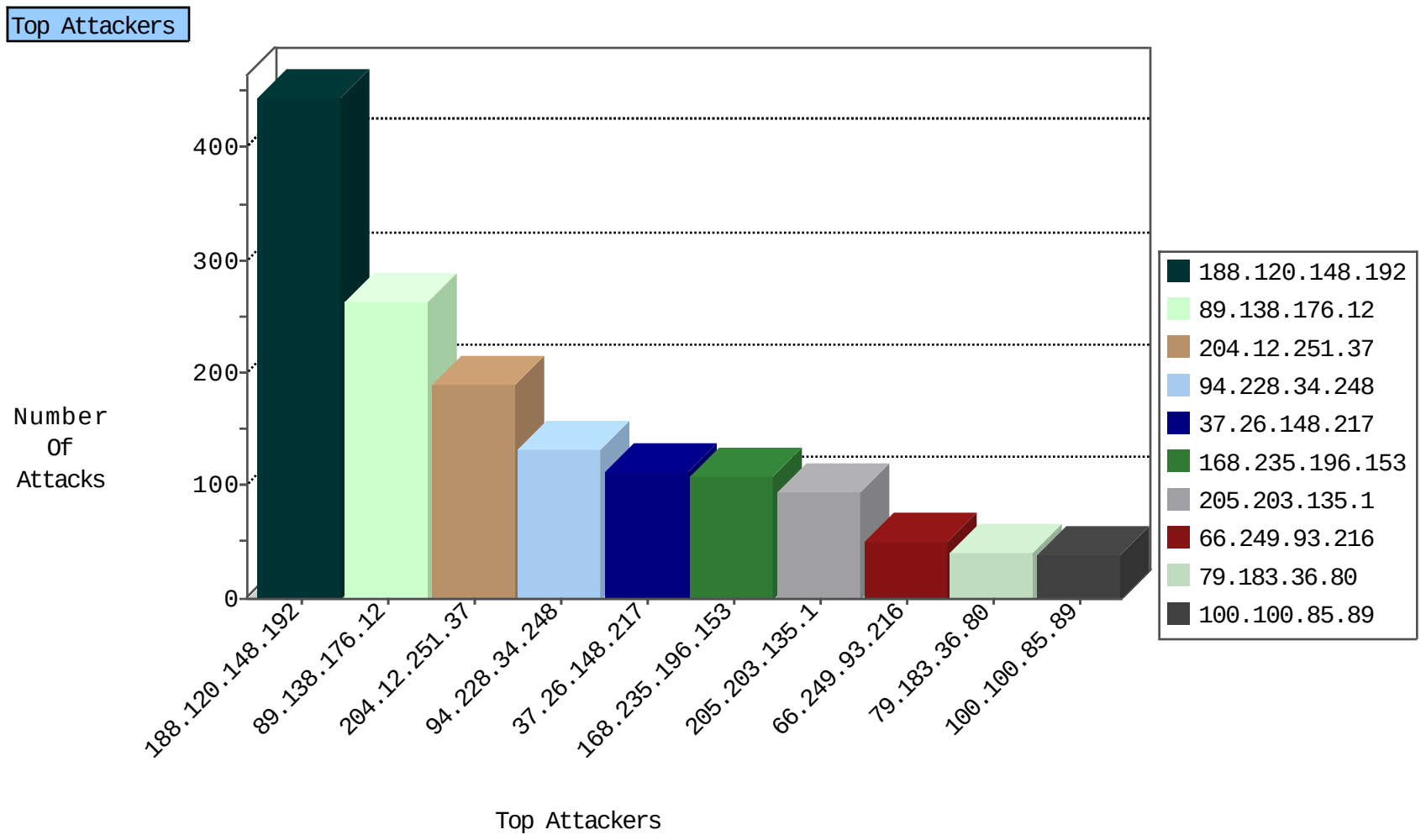
11-22-2015-22:04:08 to 11-22-2015-23:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



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

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	TCP handshake violation, first packet not syn	drop	4078
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	15
168.235.196.153	United States	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	3
79.180.153.184	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
168.235.196.153	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

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

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
60.249.182.34	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.228.207.18	147.237.8.24	Germany	e.lifestyle.idf.	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
183.10.184.125	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
110.244.180.138	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.87.201.199	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.136	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
58.133.188.200	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
169.54.233.119	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.87.201.199	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.206.227	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.120.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	302
204.12.251.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	190
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
37.26.148.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
168.235.196.153	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
66.249.93.216	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	50
168.235.196.153	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	50
100.100.85.89		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	39
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.180.15.47	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
37.201.170.47	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
77.37.223.42	Russian Federation	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	24
85.130.224.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.77.33		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
181.40.106.6	Paraguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
85.250.87.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
149.254.235.34	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
89.101.21.73	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.34.171.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
65.49.14.58	Anonymous Proxy	147.237.72.166	aka.idf.il	drop		drop	12
100.100.41.121		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
124.121.62.133	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.183.36.80	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
100.100.77.33		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	11
89.139.15.190	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.183.36.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.172.109	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
88.147.17.114	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
77.12.183.237	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
141.0.15.160	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.183.36.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.211.72.193	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
105.104.176.121	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.46.39.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.91.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.26		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.16.66	Israel	147.237.72.166	aka.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
188.120.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 188.120.148.192	Block	138
89.138.176.12	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.138.176.12	Block	137
89.138.176.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
84.108.145.219	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.108.145.219	Block	13
199.19.105.111	United States	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 199.19.105.111	Block	9
190.7.138.130	Colombia	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	9
199.19.105.111	United States	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 199.19.105.111	Block	9
79.177.29.73	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	8
5.22.131.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
176.13.9.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.177.110.26	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	5
85.250.87.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.141.26	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	3
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
37.142.151.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.68.40.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.130.224.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.184	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
79.179.179.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.21.151	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.21.151	Block	2
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	2
85.65.174.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	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
2.54.48.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.67.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
85.250.94.108	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
84.228.43.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.120.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
124.73.1.18	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he/matpash.aspx/trackback/	Block	1
80.179.14.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.176.12	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
85.65.221.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
109.160.177.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.152.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
95.86.105.184	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
84.228.185.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
46.166.190.160	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
149.78.23.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.120.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.96.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.79.180.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
176.13.10.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1