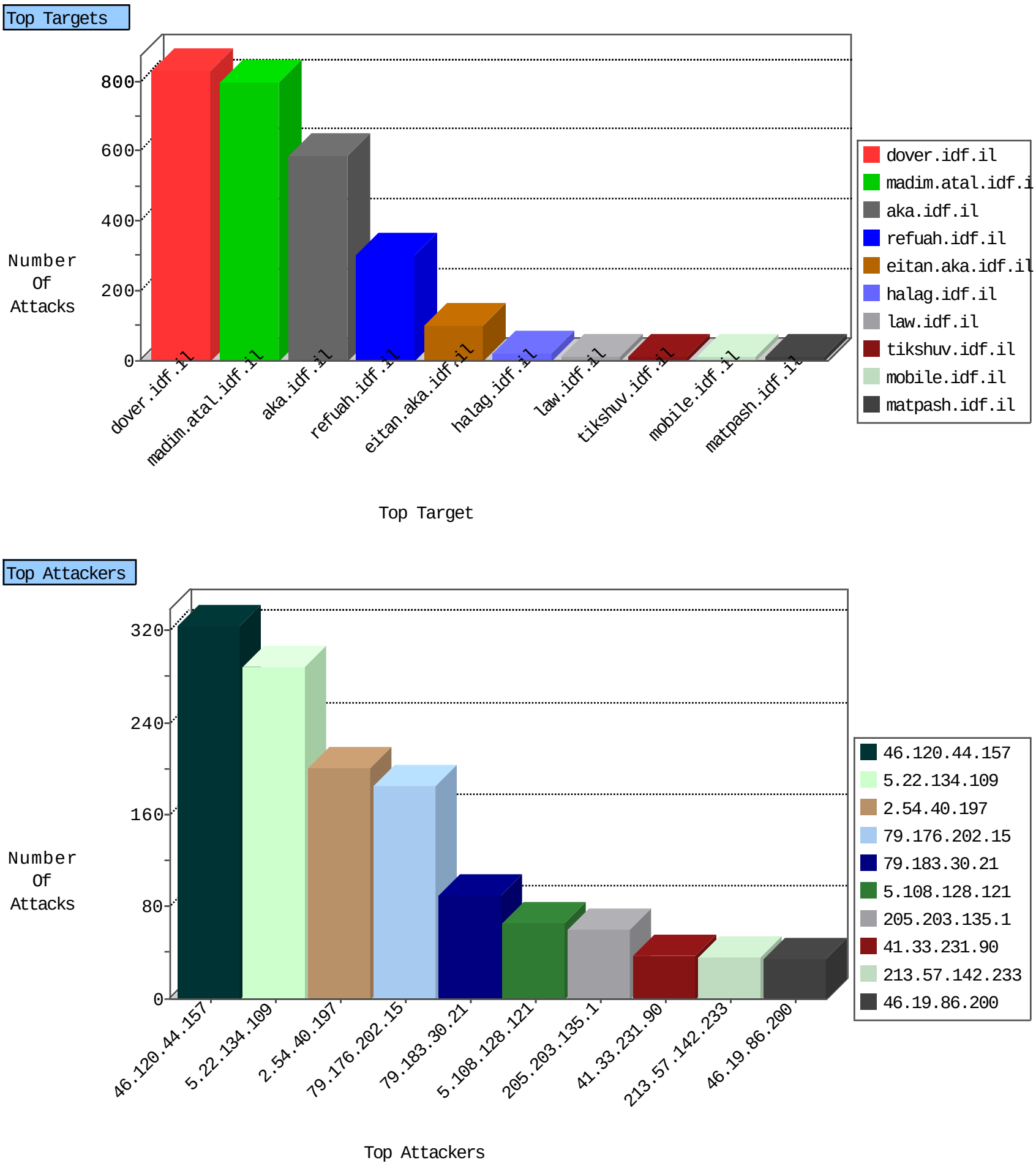
11-21-2015-20:04:03 to 11-21-2015-21:04:03

IDF Under Attack
Daily Report



11-21-2015-20:04:03 to 11-21-2015-21:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	55
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
5.102.254.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
2.52.189.249	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
80.246.139.59	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
5.22.131.124	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.183.184.8	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	3
2.54.145.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
5.22.134.109	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.182.11.68	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
84.228.165.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.73.219.155	Russian Federation	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
85.250.222.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.138.140	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.82.64.198	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
5.28.141.41	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

11-21-2015-20:04:03 to 11-21-2015-21:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.176.19	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-21-2015-20:04:03 to 11-21-2015-21:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.125.118.204	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
27.97.129.199	147.237.77.176	India	matpash.idf.il	GPL SCAN nmap TCP	4
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
5.108.128.121	147.237.77.216	Saudi Arabia	dover.idf.il	ET SCAN NMAP -sA (2)	2
85.64.126.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.117.209.135	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
60.30.73.78	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
178.62.126.13	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
60.30.73.78	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
125.211.158.135	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
43.229.53.89	147.237.0.200	Japan	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.65.8.23	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
43.229.53.89	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
103.63.212.167	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
86.108.103.180	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
210.50.197.154	147.237.77.212	Australia	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
60.30.73.78	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.0.34	Italy	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
60.30.73.78	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
123.191.137.19	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
43.229.53.89	147.237.0.35	Japan	akaws.idf.il	ET SCAN Potential SSH Scan	1
103.63.212.167	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
31.168.67.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.63.212.167	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1

11-21-2015-20:04:03 to 11-21-2015-21:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.22.134.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	282
79.183.30.21	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
5.108.128.121	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
100.100.29.120		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
77.126.92.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
183.79.219.188	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.75.106		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
93.207.77.59	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
213.57.142.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
37.26.147.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
37.26.147.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
177.32.216.146	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
89.139.38.199	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
100.100.87.120		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
213.57.130.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
100.100.111.88		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.183.22.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
213.57.142.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
100.100.120.23		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.66.122.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
95.86.117.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.179.119.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
213.57.183.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.52.16.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.180.191.173	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
220.255.97.4	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.125.118.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer. Urgent data indication was stripped. Please refer to sk36869.	alert	9
185.120.126.78		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.180.180.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.108.128.121	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
173.252.89.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.57.142.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
100.100.107.242		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.125.130.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
67.186.32.148	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.22.131.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.67.188.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.76.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.11.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.139.176.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.61.223	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
46.120.44.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	173
79.176.202.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
2.54.40.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
46.120.44.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.54.40.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
79.176.202.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
46.120.44.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	45
46.19.86.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
41.248.119.41	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.248.119.41	Block	30
2.54.40.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	20
46.19.86.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.28.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.12.148.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.180.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
109.67.206.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.32.179.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.14.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
2.54.43.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.85.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.21		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.23.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.63.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.126.92.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	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
24.150.138.227	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
89.138.76.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19075-he/dover.aspx	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3176.pdf	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
124.73.1.18	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11435-he/cogat.aspx/trackback/	Block	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
176.228.207.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
84.108.71.49	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.179.192.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding XS:}T1.g2BHrvh]jMI:7	None	1
46.121.213.187	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
168.235.206.229	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clien	Block	1
109.160.193.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	1
77.127.14.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
213.57.43.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.44.138.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.38.199	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1