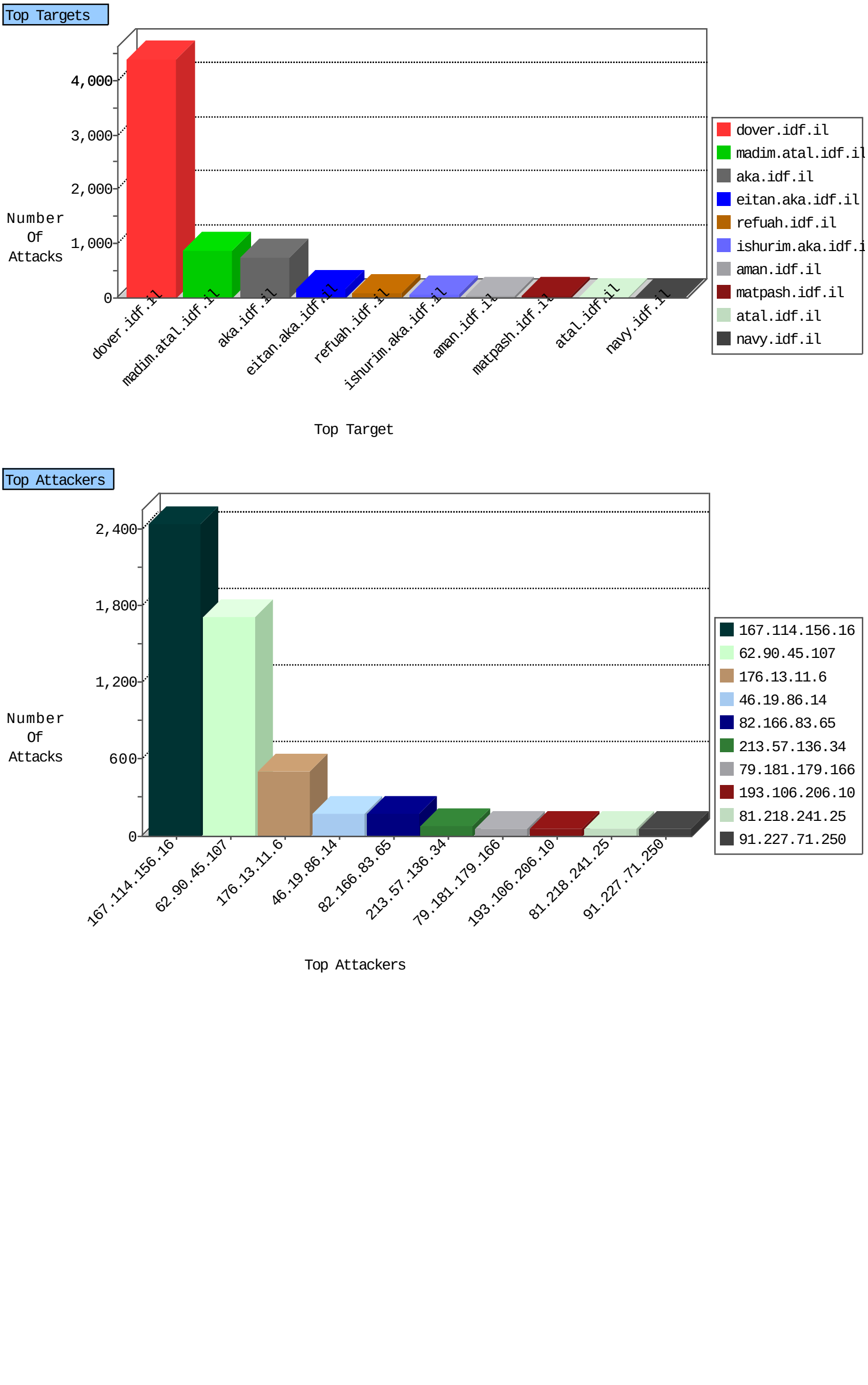
12-02-2015-13:04:02 to 12-02-2015-14:04:02

IDF Under Attack Daily Report



12-02-2015-13:04:02 to 12-02-2015-14:04:02

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	DOS-Tool-SwitchbladG	dest-reset	3478
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
37.26.148.174	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	102
109.65.215.149	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
203.87.112.185	Australia	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
141.212.122.64	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.65	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
1.36.240.250	Hong Kong	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.25.51.226	Lithuania	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
83.169.10.185	Germany	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	1
141.212.122.75	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.76	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

12-02-2015-13:04:02 to 12-02-2015-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.77.227	e.hamaz.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

12-02-2015-13:04:02 to 12-02-2015-14:04:02

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
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
77.127.240.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.197.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.12.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.120.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.103.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.226.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.147.121.138	147.237.76.197	Korea, Republic of	e.himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.116.81.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.20.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.36.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

12-02-2015-13:04:02 to 12-02-2015-14:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.166.83.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
213.57.136.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	83
79.181.179.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
100.100.78.10		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	32
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
100.100.17.237		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
24.187.162.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
92.253.124.62	Jordan	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.3	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
62.90.45.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
149.78.251.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.179.205.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
79.179.205.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.116.99.141	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
100.100.3.24		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.194	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
141.0.15.147	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.246.140.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.149.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
82.145.218.200	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
93.172.167.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
147.235.8.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.148.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.235.8.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
193.106.206.10	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.91.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.235.8.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.27.105.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.99.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.197.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.182.165.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.220	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.197.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
100.100.105.146		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.2.195	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.132.130	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.228.162.193	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.194.206.43	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.144.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.162	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.227.71.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.109.10.136	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
92.253.124.62	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.208	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.90.45.107	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.90.45.107	Block	1695
176.13.11.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	307
176.13.11.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
176.13.11.6	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.11.6	Block	97
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.14	Block	81
193.106.206.10	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
91.227.71.250	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
2.54.178.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
176.12.147.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
37.26.146.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
82.166.83.65	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	45
80.74.97.54	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.74.97.54	Block	14
2.52.152.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	5
87.68.155.156	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.68.155.156	Block	4
2.54.38.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.155.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
87.68.155.156	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	3
176.13.4.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.152.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.5.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
192.117.170.194	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
176.12.145.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
103.30.90.134	Indonesia	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
79.178.114.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.14.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
176.12.148.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.217.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.220.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.138.61	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/	Block	1
54.183.227.107	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
147.235.8.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.74.97.54	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	1
185.32.179.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.176.11.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
176.13.9.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.131.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.99.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.140.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.168.165	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1