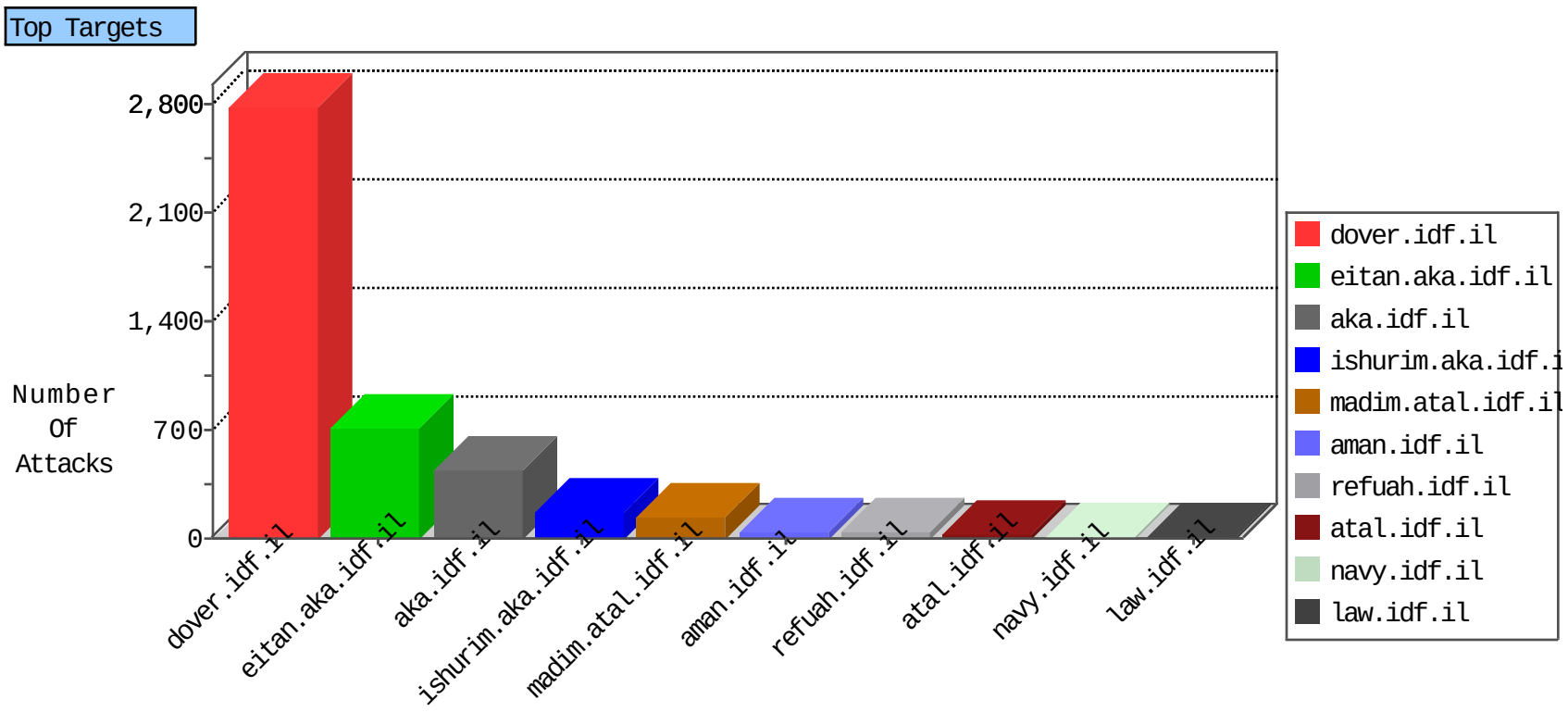
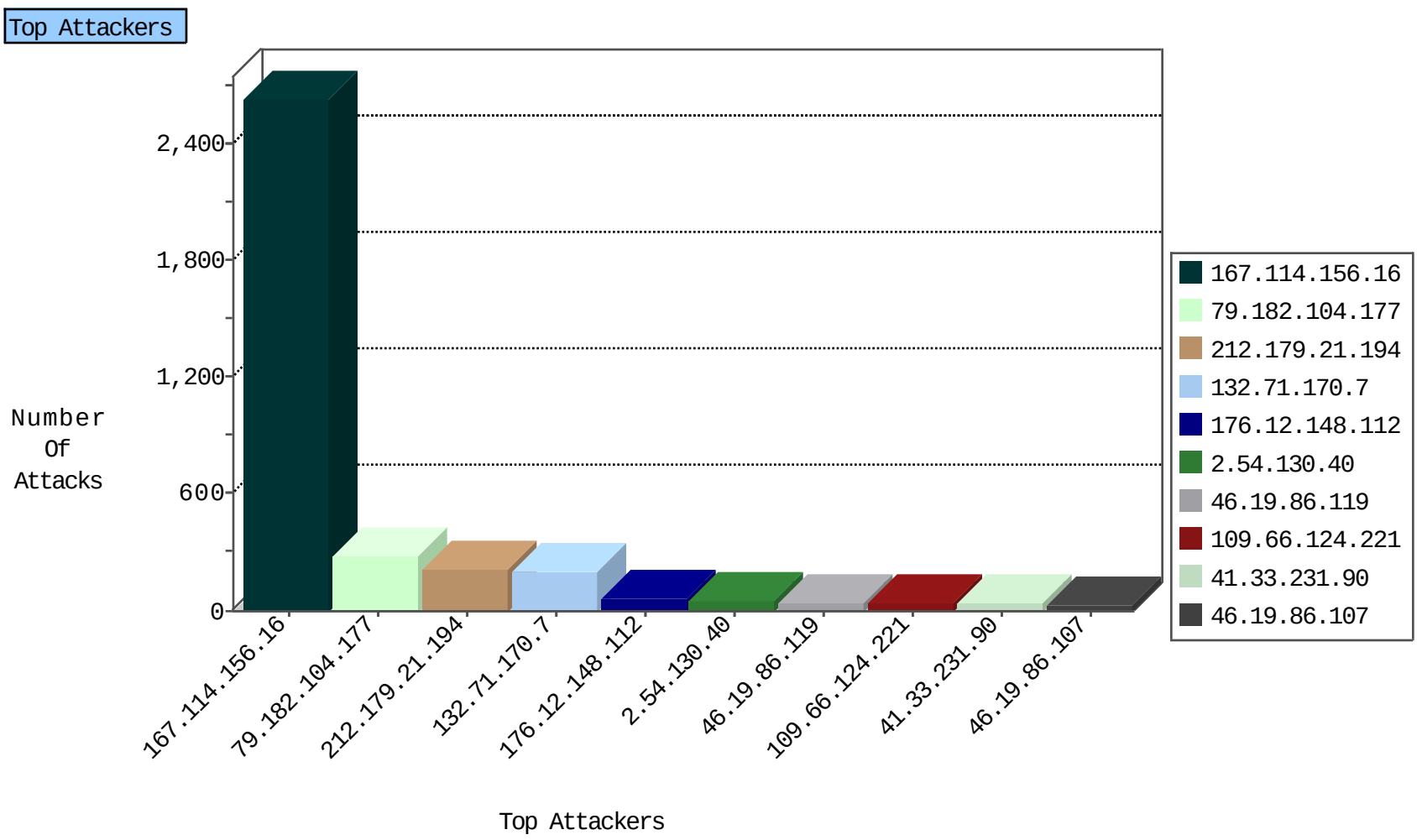
12-02-2015-11:04:07 to 12-02-2015-12:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-02-2015-11:04:07 to 12-02-2015-12:04:07

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	3530
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	64
192.3.170.124	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
192.3.170.124	United States	147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	1

12-02-2015-11:04:07 to 12-02-2015-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
180.255.8.241	Singapore	147.237.77.216	dover.idf.i	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

12-02-2015-11:04:07 to 12-02-2015-12:04:07

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	2
176.12.140.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.8.59.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.153	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
193.171.152.102	147.237.77.216	Austria	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.199.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.225.85.97	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1
79.177.11.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
186.225.85.97	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
186.225.85.97	147.237.76.39	Brazil	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
46.19.85.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.225.85.97	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
94.230.86.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.213.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.225.85.97	147.237.77.227	Brazil	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
80.82.65.82	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Poison Null Byte	1
186.225.85.97	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.120	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
186.225.85.97	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
46.121.208.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
186.225.85.97	147.237.76.30	Brazil	himush.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.46	147.237.0.200		m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-02-2015-11:04:07 to 12-02-2015-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.104.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	240
132.71.170.7	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
46.19.86.119	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
109.66.124.221	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
212.199.121.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.86.174	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
212.150.84.153	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	11
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.147.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.94.195.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.88.26.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
185.32.179.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.52	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.184.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.153.121	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.58	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.244.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.174.169	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.152.28	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
94.230.86.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.244.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.9.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.175.20	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.42.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
199.203.123.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.62.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.50	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
81.218.131.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.38	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
81.218.46.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.183.35.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.223	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
100.100.36.69		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.21	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.46.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.61.212	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

12-02-2015-11:04:07 to 12-02-2015-12:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.71.170.7	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	158
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	155
176.12.148.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.54.130.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
79.182.104.177	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
5.29.46.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	7
212.117.136.6	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	5
212.117.136.8	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
176.13.10.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.150.161.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
176.13.10.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.48.7.139	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
95.86.90.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
2.54.168.43	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	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	2
84.111.61.254	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
217.194.206.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
8.37.235.55	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/jquer×²Ö³Ö´	Block	2
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
197.48.7.139	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
82.166.140.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.108.161.194	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
192.116.108.17	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method POST for www.chinuch.aka.idf.il/900-he/chinuch.aspx	None	1
41.220.193.1	Mozambique	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
80.246.136.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.174.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.160	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
212.117.136.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
62.219.112.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.108.161.194	Romania	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
176.13.19.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/kapatz/resources/images/mainpage/up-banner.gif	None	1
2.54.3.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.160.25	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.66.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
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	1
84.108.52.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.108.161.194	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
192.116.172.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	1
150.70.173.5	Japan	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
212.143.172.93	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.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/0/size100x0/3250.jpg	Block	1
197.134.216.101	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1

12-02-2015-11:04:07 to 12-02-2015-12:04:07