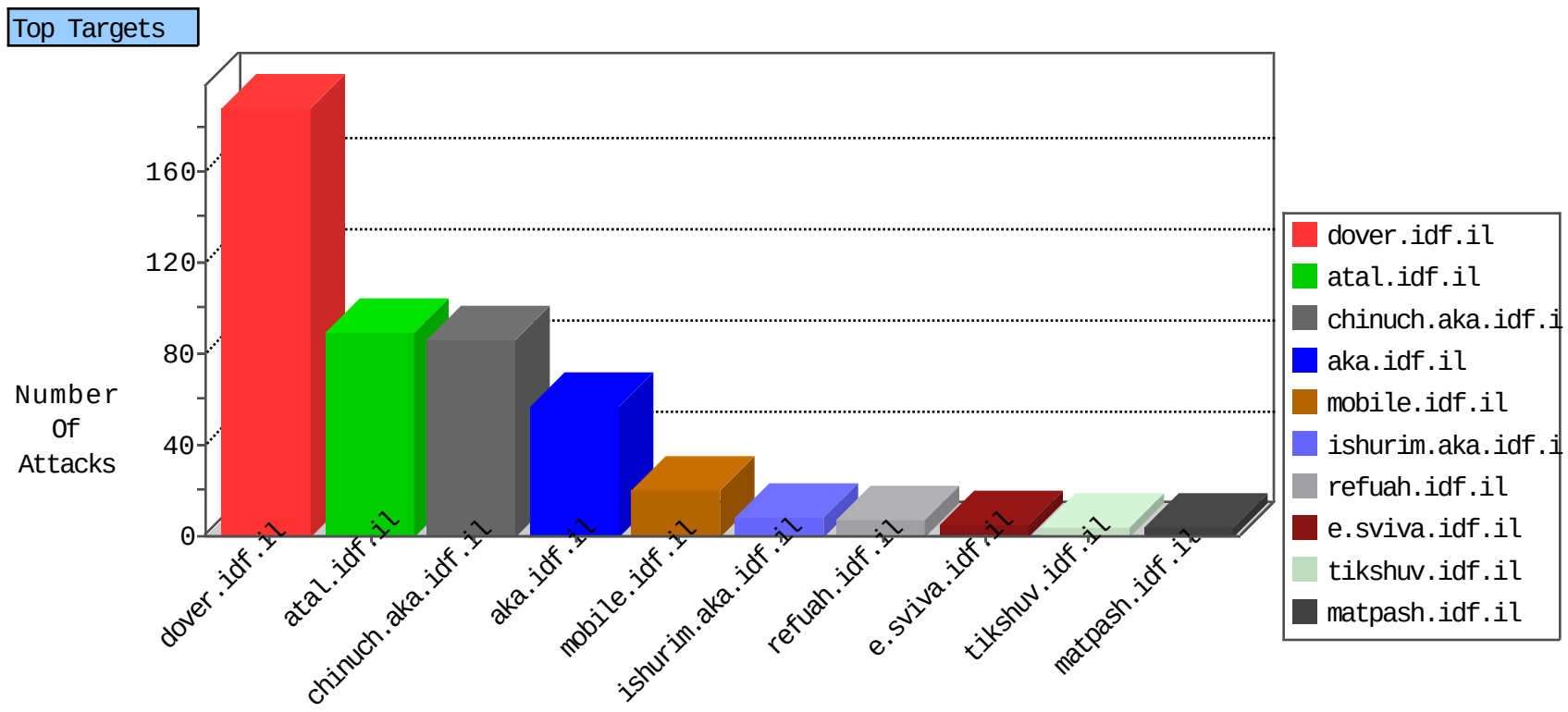
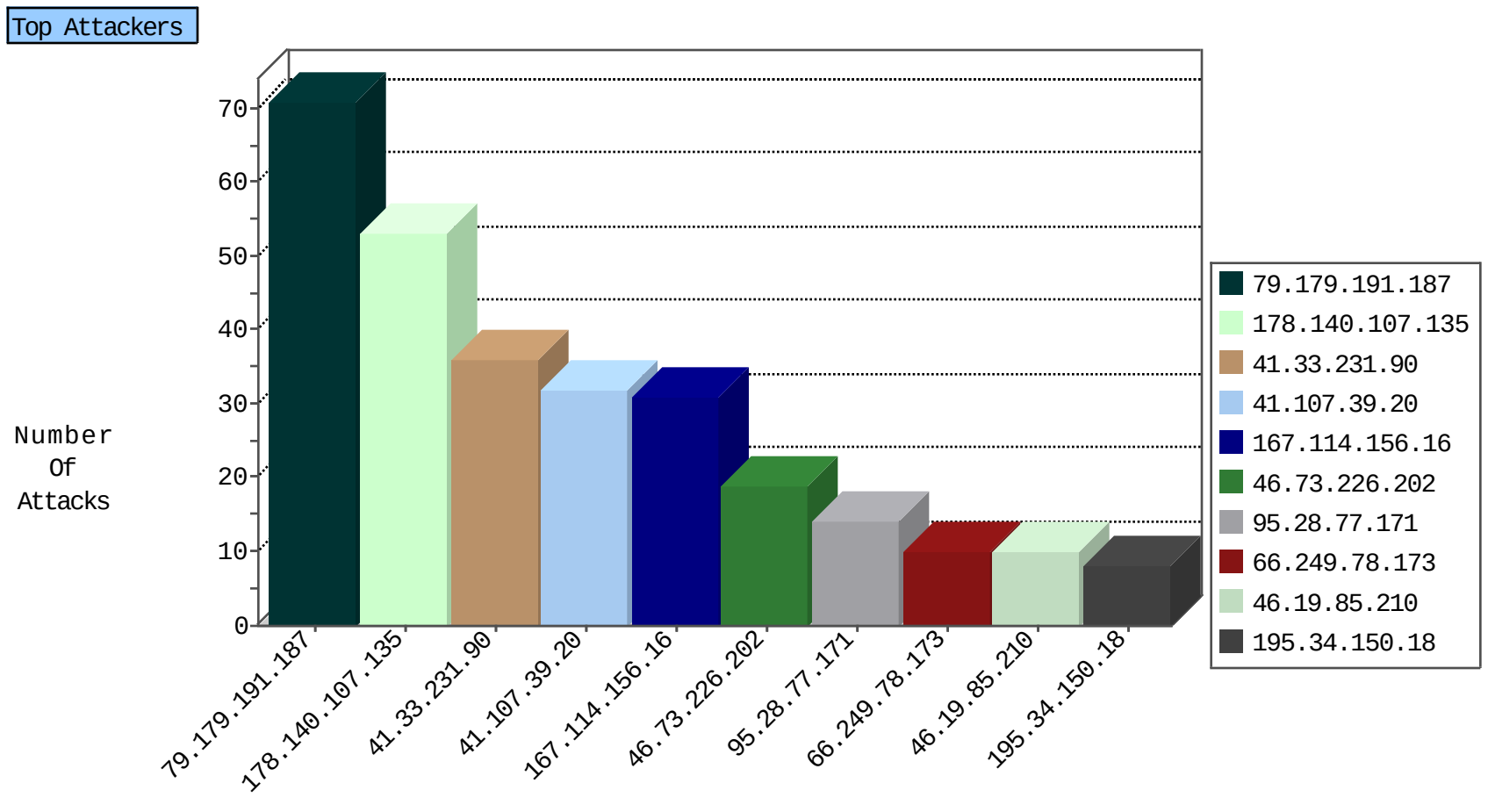
12-30-2015-02:04:01 to 12-30-2015-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-30-2015-02:04:01 to 12-30-2015-03:04:01

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	803
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
41.107.39.20	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1
173.252.73.106	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
151.217.178.80		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
192.185.4.15	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-30-2015-02:04:01 to 12-30-2015-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.8.27	e.madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

12-30-2015-02:04:01 to 12-30-2015-03:04:01

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
151.217.178.86	147.237.77.19		law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
151.217.178.86	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.76.196		e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.219.238.10	147.237.77.235		sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
64.38.133.137	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
190.249.184.162	147.237.76.196	Colombia	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.86	147.237.76.201		e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.76.197		e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.62.153	147.237.77.170		maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.131.21.39	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
190.249.184.162	147.237.76.196	Colombia	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
151.217.178.86	147.237.77.74		law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.86	147.237.76.202		e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-30-2015-02:04:01 to 12-30-2015-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
178.140.107.135	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
41.107.39.20	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
46.73.226.202	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.54	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.145.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.147.228.210	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.91.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.28.77.171	Russian Federation	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.180.224.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.28.77.171	Russian Federation	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
118.173.129.101	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
95.28.77.171	Russian Federation	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.177.226.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.28.77.171	Russian Federation	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
82.81.5.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.28.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.185.4.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.93.18	United States	147.237.76.42	refuah.idf.il	Directory Traversal	directory traversal overflow	monitor	2
95.28.77.171	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
185.3.144.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.228.62.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
173.252.90.229	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.93.21	Israel	147.237.76.42	refuah.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.229.3.91	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
50.63.197.105	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
173.252.73.106	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.221	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.73.226.202	Russian Federation	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.109	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.1.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
173.252.90.229	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
2.52.21.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
67.52.118.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

12-30-2015-02:04:01 to 12-30-2015-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.191.187	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	71
140.180.248.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	4
95.90.251.149	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
212.143.91.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.61	Israel	147.237.76.147	chinuch.aka.idf.i	Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.178	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.194.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
197.242.94.250	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.229.31	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.55	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.15.22	China	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.107.39.20	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
114.97.48.57	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1956-he/cogat.aspx/trackback/	Block	1
91.185.112.149		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
213.57.29.4	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
186.202.127.238	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
150.70.173.52	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
50.87.221.60	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
31.44.136.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter usg in www.aka.idf.il/main/haredim/faq.aspx	None	1
109.65.150.141	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.65.150.141	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.61	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.15.34	China	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.90.251.149	Germany	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
186.202.127.238	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1759	Block	1
157.55.39.44	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/×œ×›×ª×‘×” ×”×žx×œ	Block	1
50.87.221.60	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
31.44.136.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/haredim/general.aspx	None	1
109.201.152.27	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
207.46.13.62	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
79.180.140.5	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.168.200.187	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.66.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.46.230.203	Ukraine	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
109.201.154.219	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
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	1
85.93.91.84	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
184.168.200.187	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
50.87.60.110	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
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	1
197.242.94.250	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

12-30-2015-02:04:01 to 12-30-2015-03:04:01