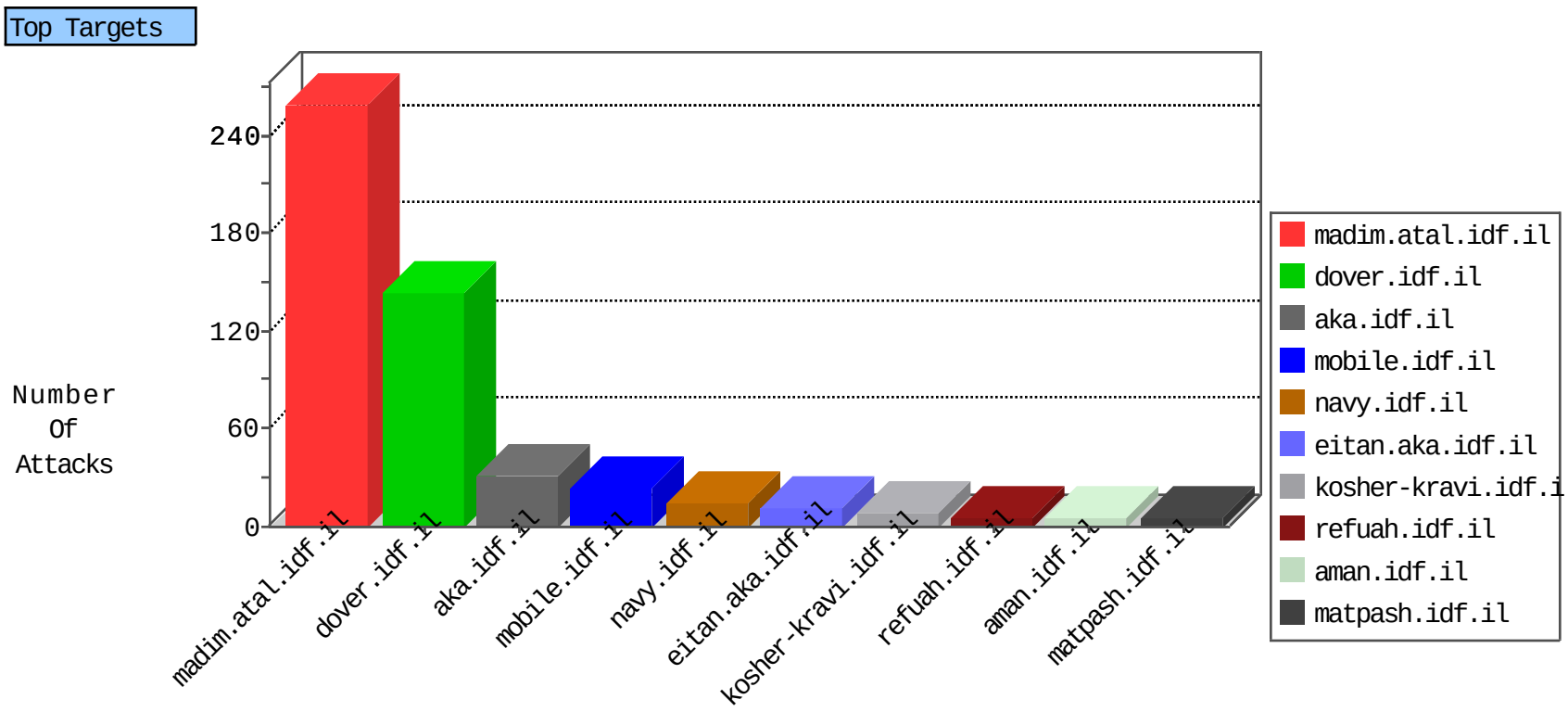
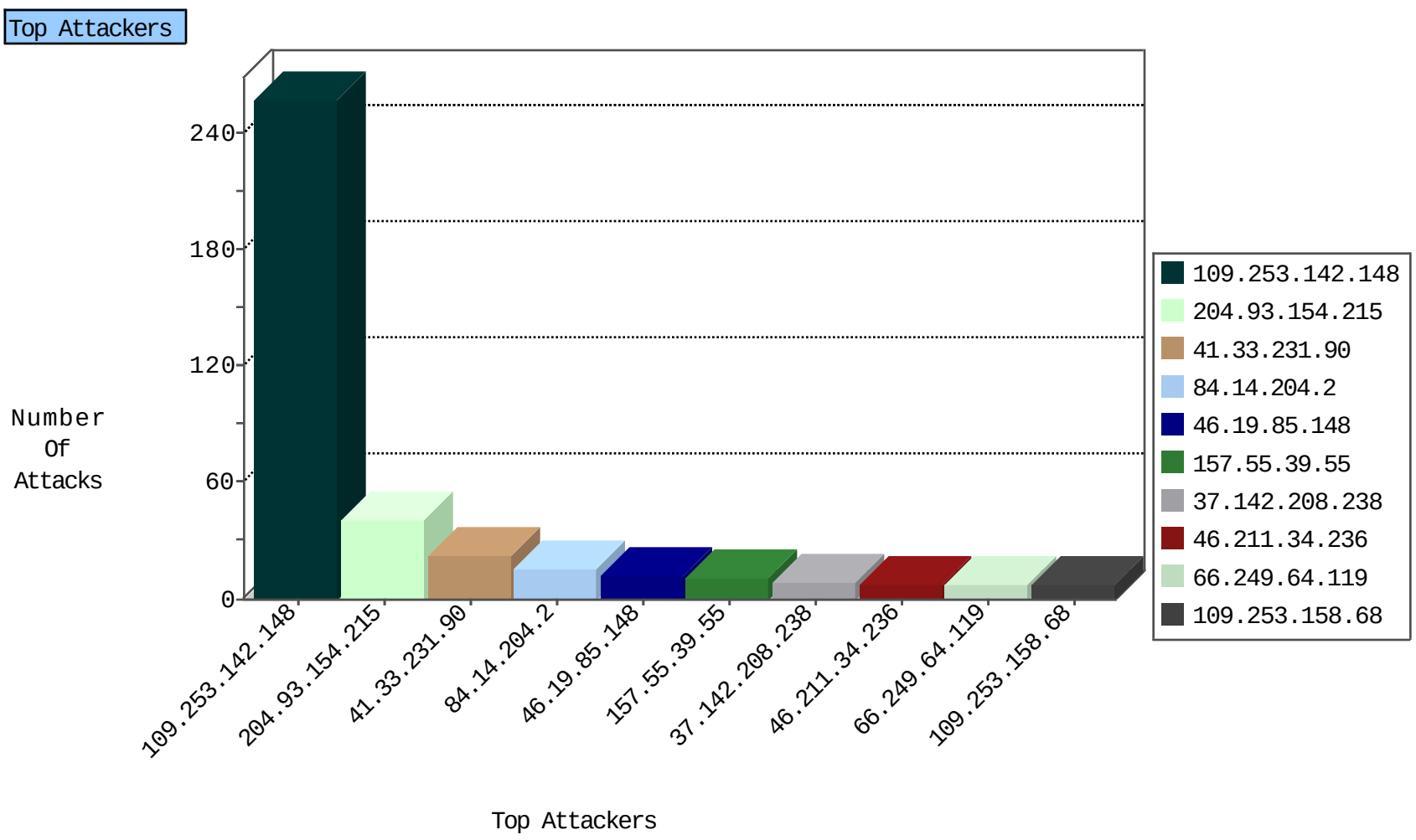
12-29-2015-02:04:08 to 12-29-2015-03:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-29-2015-02:04:08 to 12-29-2015-03:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.215	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	186
192.114.150.50	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
151.217.178.35		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
39.114.248.163	Korea, Republic of	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
183.59.116.36	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
46.163.153.70	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
183.59.116.36	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
80.82.64.177	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
183.59.116.36	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

12-29-2015-02:04:08 to 12-29-2015-03:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-29-2015-02:04:08 to 12-29-2015-03:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.155.203.54	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.76.196		e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.155.203.54	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.76.44		e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.211.34.236	147.237.0.15	Ukraine	kosher-kravi.idf.il	SERVER-WEBAPP admin.php access	1
151.217.178.88	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
12.139.41.189	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.14.42	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.155.203.54	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
61.155.203.54	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.155.203.54	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.76.177		ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.155.203.54	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.72.156		aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.14.42	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
131.109.15.15	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
61.155.203.54	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1

12-29-2015-02:04:08 to 12-29-2015-03:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
84.14.204.2	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
157.55.39.55	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.64.119	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
113.185.1.13	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.142.208.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.158.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.14.204.2	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
42.112.79.238	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.201	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.111.0.23	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
70.210.4.20	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.187.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.237.146.28	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
149.88.139.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
50.163.248.234	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.142.208.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
141.212.122.112	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
82.196.201.186	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
31.168.80.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
66.249.64.3	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
31.210.187.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.122.195	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
38.229.1.15	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.118	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.39.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.3.146.197	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.199	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.147.129	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.116.71.170	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.159.63.249	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
79.116.25.197	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
151.217.178.55		147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
40.77.167.105	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
141.212.122.121	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.39.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
101.198.159.31	China	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.120.126.10		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
70.210.4.20	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop		drop	1

12-29-2015-02:04:08 to 12-29-2015-03:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.142.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	187
109.253.142.148	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.142.148	Block	40
109.253.142.148	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	30
2.54.146.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 46.211.34.236	Block	2
109.253.158.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.12.142.128	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.i	PHP Attempt	Block	2
79.178.195.239	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.66.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.63.94.144	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.253.142.148	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
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	1
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/wp-login.php	Block	1
150.70.173.6	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.180.9.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.49	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.i	Admin Blocking	Block	1
180.76.15.10	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
204.17.56.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
62.90.143.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.208.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.55	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	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
66.249.66.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
180.76.15.29	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.i	Multiple Admin Blocking from 46.211.34.236	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.118	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/apparel/img/profile/image	Block	1
66.249.66.27	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1745	Block	1
37.142.242.174	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 37.142.242.174 (sigalgs DoS Attack)	None	1
157.55.39.55	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
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	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
207.46.13.178	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/exportemojitagjs.blog	Block	1
66.249.66.31	Israel	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
37.142.242.174	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	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
150.70.173.6	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

12-29-2015-02:04:08 to 12-29-2015-03:04:08