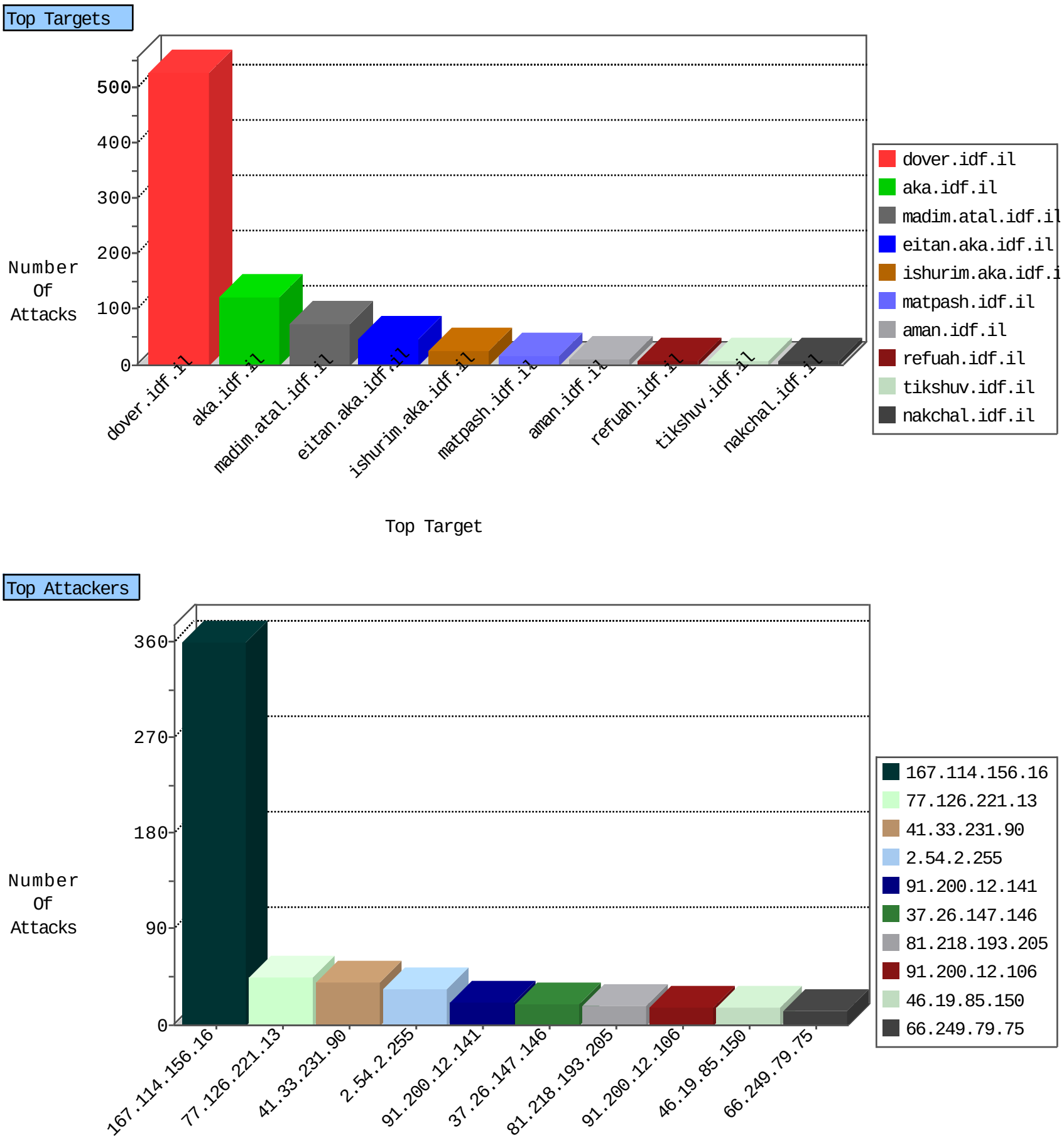
12-23-2015-07:04:07 to 12-23-2015-08:04:07

IDF Under Attack Daily Report



12-23-2015-07:04:07 to 12-23-2015-08:04:07

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	3017
66.249.79.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
37.26.146.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
207.46.13.1	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
173.252.90.239	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.61.185.64	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
109.61.185.64	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
109.61.185.64	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.61.185.64	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

12-23-2015-07:04:07 to 12-23-2015-08:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-23-2015-07:04:07 to 12-23-2015-08:04:07

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	4
61.132.161.130	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
61.132.161.130	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.132.161.130	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
2.54.169.136	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
98.116.89.160	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
61.132.161.130	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.132.161.130	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
23.96.213.135	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1

12-23-2015-07:04:07 to 12-23-2015-08:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.221.13	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.150	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
81.218.193.205	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
2.54.46.91	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.37.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
81.218.193.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.106	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
46.19.85.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.106	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.179.28.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.204.101.26	Lebanon	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
146.185.234.48	Russian Federation	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
91.200.12.139	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
46.19.85.99	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.204.101.26	Lebanon	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.47.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.226	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	3
46.19.85.130	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
117.228.60.118	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
94.230.86.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
40.77.167.21	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.90.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.36.79	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.99	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.228.182.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.3.95.165	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.99.12.99	Canada	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.48.103	Israel	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
40.77.167.20	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.254.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.127.107.81	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

12-23-2015-07:04:07 to 12-23-2015-08:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.2.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
37.26.147.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
2.54.56.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
91.200.12.141	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.141	Block	11
91.200.12.141	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	11
146.185.234.48	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	4
5.255.253.62	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.148.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.13.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.87.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	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
89.138.87.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
157.55.39.54	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17765.jpg	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20027-he/dover.aspx	Block	1
40.77.167.20	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.136	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
109.201.152.235	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
82.221.105.6	Iceland	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/robots.txt	Block	1
207.46.13.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
185.120.126.29		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.69.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	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
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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/strike_heb2.asf	Block	1
46.19.85.176	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
157.55.39.174	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
37.26.146.197	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
109.201.154.175	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.46.13.184	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
192.116.142.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	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
149.88.69.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
157.55.39.224	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
109.201.154.229	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
207.46.13.184	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/plugins/editors/jckeditor/typography/typography2.php	Block	1
195.154.191.97	France	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
150.70.173.51	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
40.77.167.5	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
2.54.25.235	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	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
207.46.13.65	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
61.135.190.197	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1

12-23-2015-07:04:07 to 12-23-2015-08:04:07