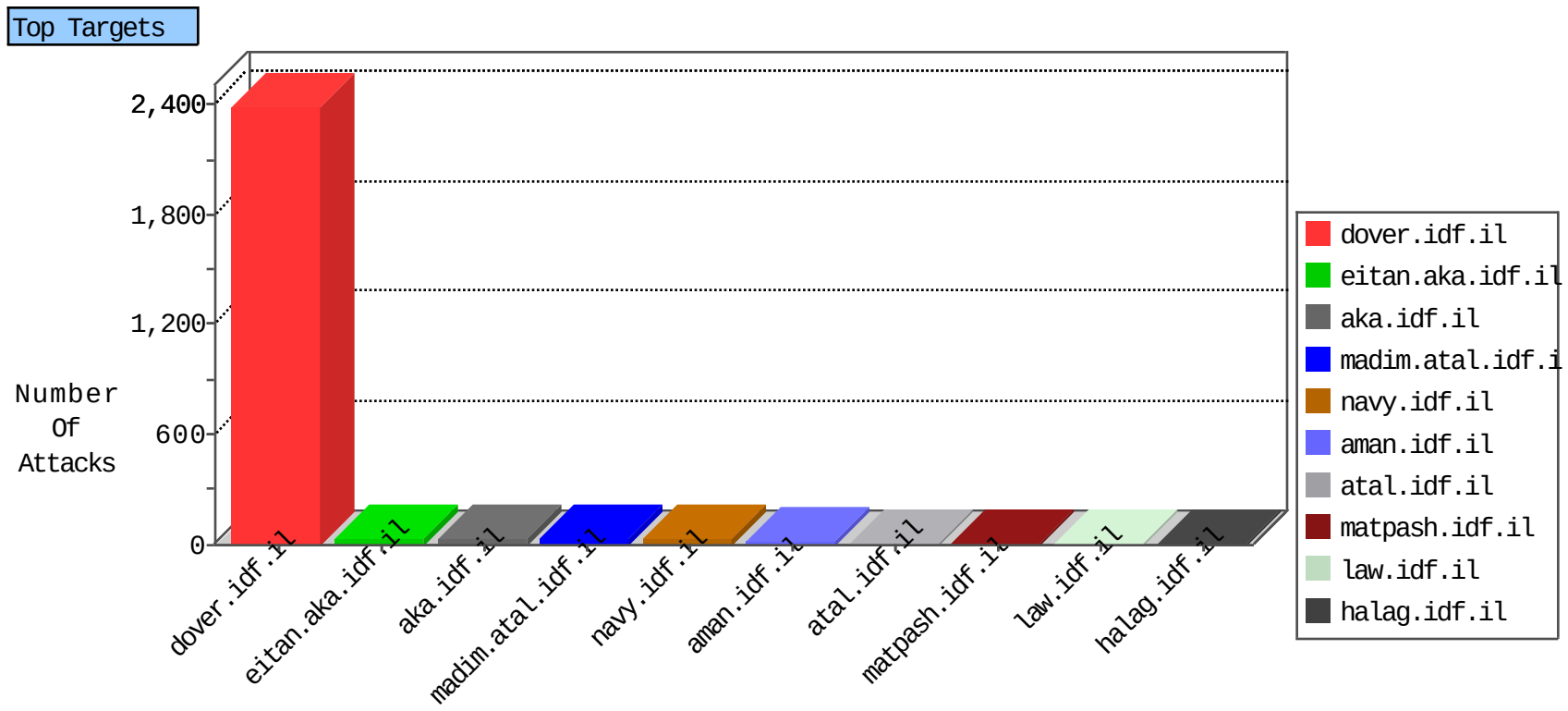
11-30-2015-02:04:00 to 11-30-2015-03:04:00

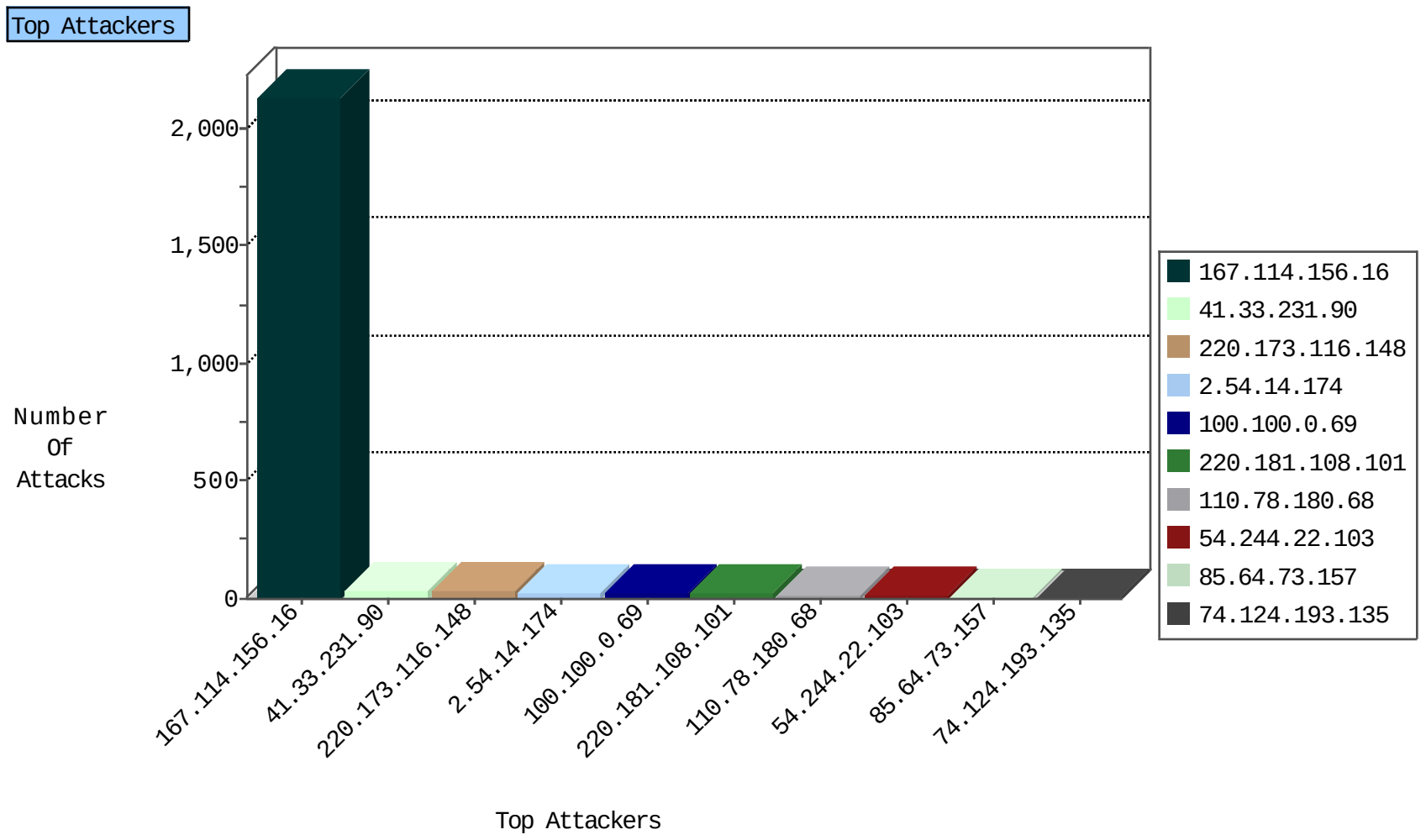
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-30-2015-02:04:00 to 11-30-2015-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.108.101	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	53690
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3337
61.18.77.23	Hong Kong	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
93.174.93.151	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
203.106.68.83	Malaysia	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.51.30	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
159.148.186.196	Latvia	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

11-30-2015-02:04:00 to 11-30-2015-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-30-2015-02:04:00 to 11-30-2015-03:04:00

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	6
31.6.71.154	147.237.77.74	Poland	law.idf.il	ET SCAN NMAP -sS window 1024	1
198.23.176.210	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
195.175.45.198	147.237.76.201	Turkey	e.atal.idf.il	ET SCAN Potential SSH Scan	1
195.175.45.198	147.237.76.199	Turkey	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
195.175.45.198	147.237.0.200	Turkey	m4u.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1
169.54.91.220	147.237.72.167	Netherlands	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
113.240.250.155	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
220.231.195.122	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
31.6.71.154	147.237.76.198	Poland	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
195.175.45.198	147.237.76.202	Turkey	e.halag.idf.il	ET SCAN Potential SSH Scan	1
195.175.45.198	147.237.76.200	Turkey	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
195.175.45.198	147.237.76.30	Turkey	himush.idf.il	ET SCAN Potential SSH Scan	1
183.80.162.188	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
151.80.88.30	147.237.77.74	Italy	law.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
94.102.48.195	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1

11-30-2015-02:04:00 to 11-30-2015-03:04:00

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	drop	SAM rule	drop	34
220.173.116.148	China	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
110.78.180.68	Thailand	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
109.66.146.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.73.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
203.127.58.233	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
119.81.160.220	Hong Kong	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
31.186.228.59	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.175.0.137	Germany	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.186.228.94	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
111.118.222.150	Australia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
113.240.250.155	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.64.73.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
190.31.135.167	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
93.173.24.126	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
24.145.95.208	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.108.191.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
220.173.116.148	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.68	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.56.80.192	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
80.246.133.123	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.121.253.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.76.15.26	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.70	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.138.17.205	France	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.6.16.77	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
123.57.250.139	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.225	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
213.139.53.54	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.11	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.6.16.77	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
123.57.250.139	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.65.17.32	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
64.125.239.226	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

11-30-2015-02:04:00 to 11-30-2015-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.14.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
209.41.178.51	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
74.124.193.135	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
200.98.224.39	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
91.201.63.116	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
199.59.158.146	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
192.184.83.150	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
103.241.148.4	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
50.87.12.21	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
119.9.40.13	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
173.205.127.98	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
173.199.163.32	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
89.138.47.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
221.121.154.42	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
192.184.83.150	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
103.241.148.4	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
221.121.154.42	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
50.87.12.21	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
176.12.143.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
119.9.40.13	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
74.124.193.135	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
209.41.178.51	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
173.205.127.98	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
200.98.224.39	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
91.201.63.116	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
173.199.163.32	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
199.59.158.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
192.184.83.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
103.241.148.4	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
50.87.12.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
221.121.154.42	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
119.9.40.13	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
173.205.127.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
173.199.163.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
74.124.193.135	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
209.41.178.51	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
200.98.224.39	Brazil	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
192.200.199.199	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
91.201.63.116	Sweden	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	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
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Suspicious Response Code_Custom_Temporary	Block	2
199.59.158.146	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
31.193.51.78	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
173.199.163.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-admin/admin-ajax.php	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17225-he/dover.asp	Block	1
131.162.130.180	Canada	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.200.199.199	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.200.199.199	Block	1
220.173.116.148	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	1

11-30-2015-02:04:00 to 11-30-2015-03:04:00