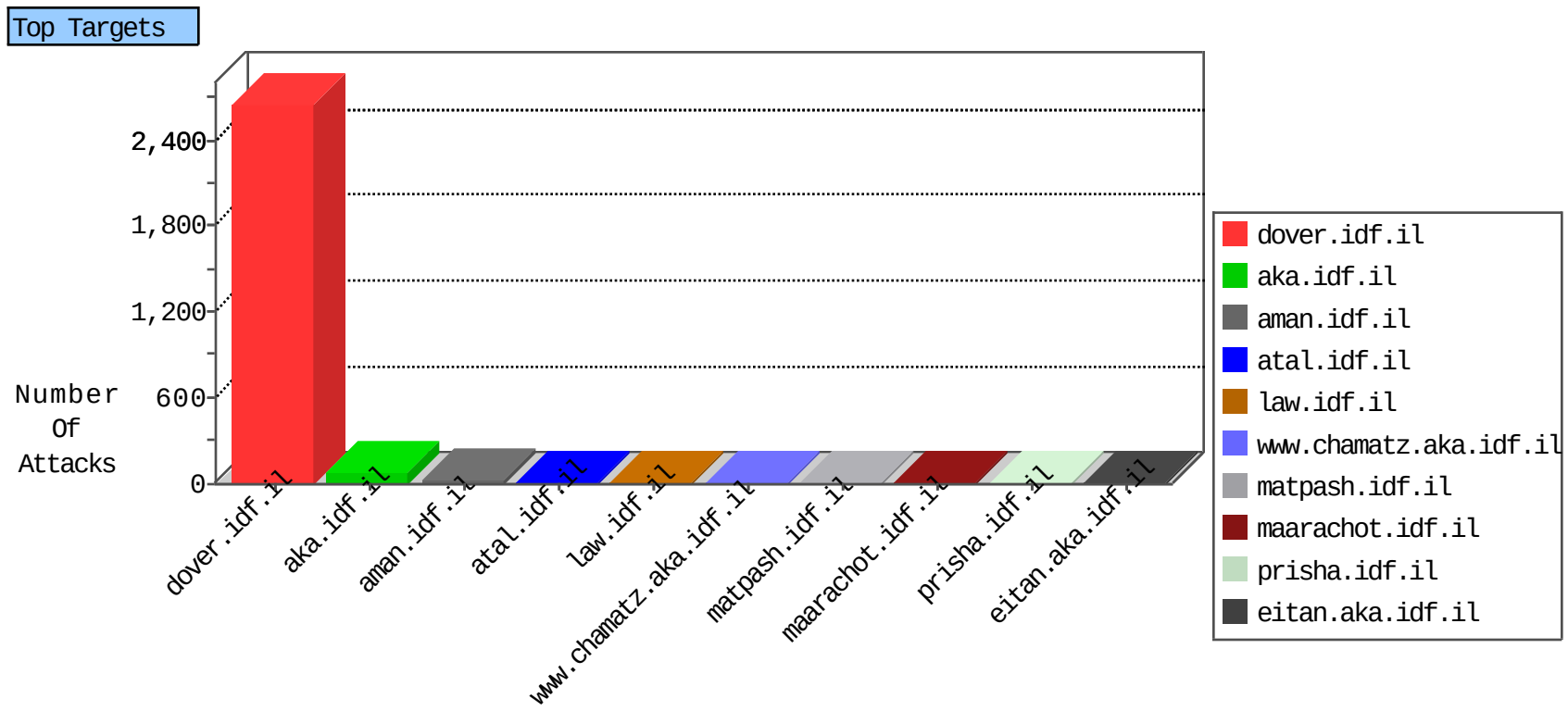
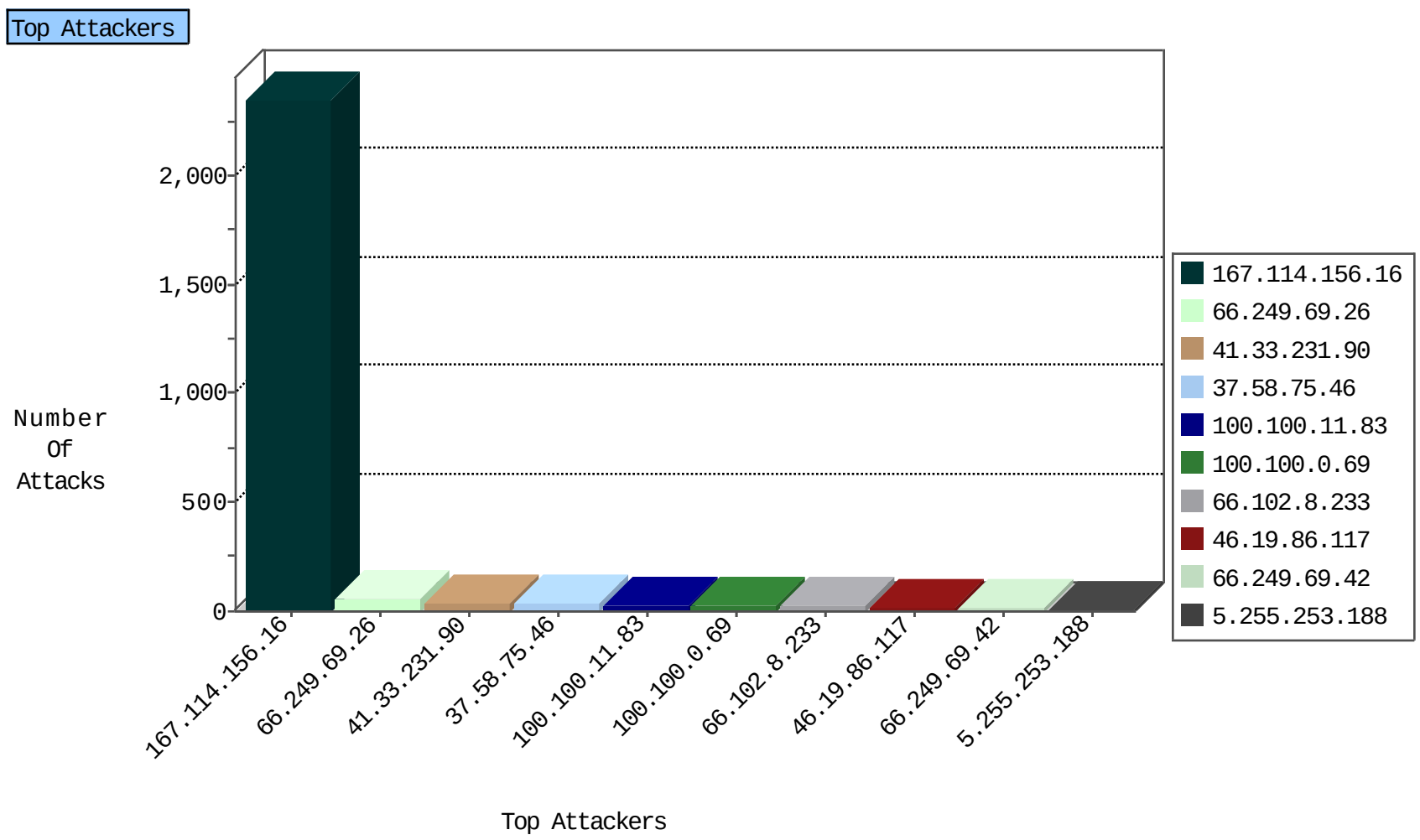
11-30-2015-04:04:05 to 11-30-2015-05:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-30-2015-04:04:05 to 11-30-2015-05:04:05

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	3532
1.69.68.240	China	147.237.77.178	e.matpash.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
195.154.233.163	France	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
159.148.186.196	Latvia	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
85.25.134.4	Germany	147.237.0.16	my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
93.174.93.151	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

11-30-2015-04:04:05 to 11-30-2015-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.211.20	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.211.212	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.217.123	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-30-2015-04:04:05 to 11-30-2015-05:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.201.236.113	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.70.230	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
206.15.106.34	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
206.15.106.34	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
173.165.25.100	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.235	Ukraine	sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.82.70.230	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
206.15.106.34	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
206.15.106.34	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

11-30-2015-04:04:05 to 11-30-2015-05:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
100.100.11.83		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
66.102.8.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
46.19.86.117	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
40.77.167.12	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.58.75.46	Netherlands	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	6
37.58.75.46	Netherlands	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
37.58.75.46	Netherlands	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	6
199.30.24.3	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.58.75.46	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
37.58.75.46	Netherlands	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
37.58.75.46	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	6
185.3.146.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.126.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.22.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.3.125	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.108.126.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
108.29.132.127	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.67.155	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.64	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.5	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
184.105.139.72	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.211	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.56.80.192	Netherlands	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
37.142.242.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.76	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.10	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.111	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
84.111.120.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
71.184.207.162	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.215	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
158.69.2.151	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
216.218.206.76	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.18	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.200	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.111.120.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.19	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.245	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.148.167	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
83.166.235.60	Russian Federation	147.237.76.34	yohalan.idf.il	drop		drop	1
218.22.211.69	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.112.133	Canada	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
112.109.80.41	New Zealand	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
166.63.124.152	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
67.222.12.77	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
198.46.81.15	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
162.144.117.76	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
194.150.113.81	Denmark	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
192.163.209.98	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
186.202.127.136	Brazil	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
54.152.34.170	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
50.22.252.18	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
182.160.163.30	Australia	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
173.44.38.200	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
208.43.14.213	United States	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
119.47.121.65	New Zealand	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	3
162.144.117.76	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
194.150.113.81	Denmark	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
173.44.38.200	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
84.108.126.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.43.14.213	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
192.163.209.98	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
119.47.121.65	New Zealand	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
167.114.112.133	Canada	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
112.109.80.41	New Zealand	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
54.152.34.170	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
186.202.127.136	Brazil	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
198.46.81.15	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
166.63.124.152	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
67.222.12.77	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
50.22.252.18	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
182.160.163.30	Australia	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
162.144.117.76	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
194.150.113.81	Denmark	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
178.18.126.54	United Kingdom	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
192.163.209.98	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
208.43.14.213	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
173.44.38.200	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
54.152.34.170	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
186.202.127.136	Brazil	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
119.47.121.65	New Zealand	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
178.18.126.54	United Kingdom	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	2
167.114.112.133	Canada	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
112.109.80.41	New Zealand	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
50.22.252.18	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
182.160.163.30	Australia	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
166.63.124.152	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
67.222.12.77	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
198.46.81.15	United States	147.237.77.216	dover.idf.i	Distributed Admin Blocking	Block	2
41.109.12.68	Algeria	147.237.77.216	dover.idf.i	Distributed PHP Attempt	Block	1

11-30-2015-04:04:05 to 11-30-2015-05:04:05