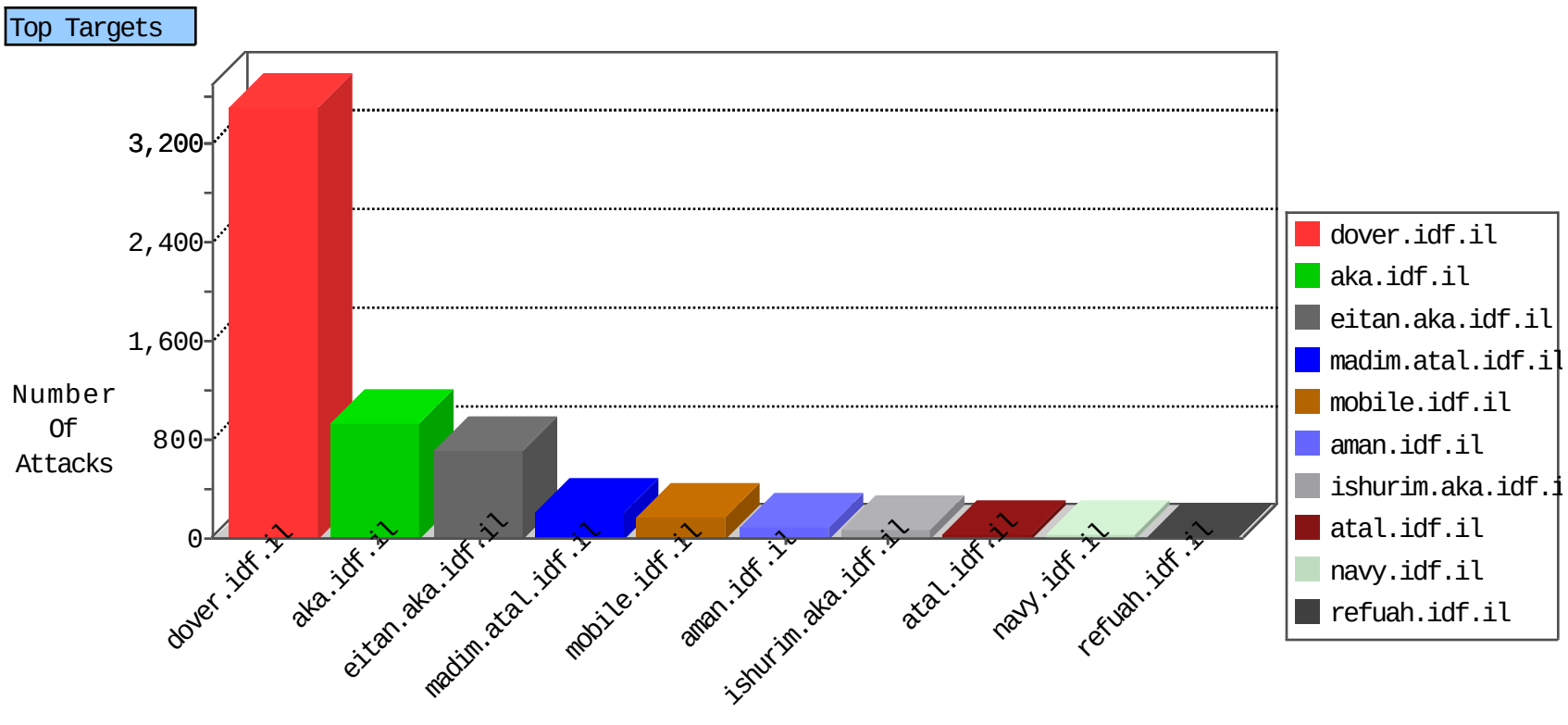
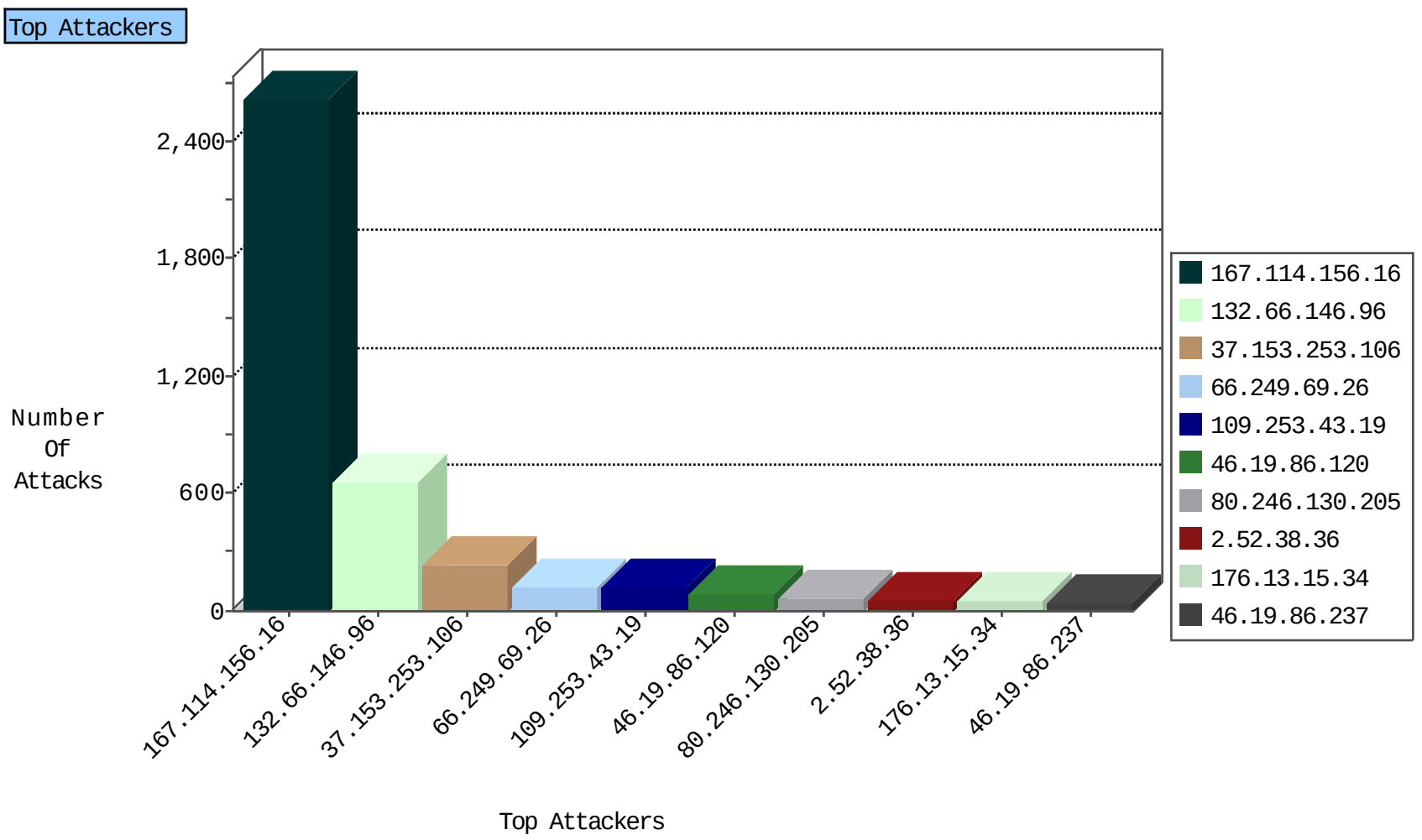
11-30-2015-14:04:08 to 11-30-2015-15:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-30-2015-14:04:08 to 11-30-2015-15:04:08

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	3581
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
80.246.136.44	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
81.218.56.125	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
216.119.7.56	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-30-2015-14:04:08 to 11-30-2015-15:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.118.245	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
192.118.12.102	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
195.154.194.47	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
85.89.73.242	Sweden	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-30-2015-14:04:08 to 11-30-2015-15:04:08

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	2
149.202.186.50	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
77.127.23.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.163.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.0.35	Poland	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
149.202.186.50	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.202.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.137.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.77.226	Poland	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

11-30-2015-14:04:08 to 11-30-2015-15:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
132.66.146.96	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
37.153.253.106	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
176.13.15.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
109.253.43.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
130.245.145.19	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
100.100.65.116		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.51	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
100.100.92.229		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
213.57.134.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
46.19.86.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
82.80.42.181	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
95.35.208.73	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
2.52.38.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
37.46.39.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
2.54.131.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
46.19.85.133	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
185.3.146.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.94.18.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
84.94.18.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.213	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.76.186		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.26.210		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.90.234		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.12.147.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.76.150		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
87.68.62.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.52.14		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.52.36.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
37.142.227.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.66	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
192.116.134.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
132.64.184.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
66.249.81.206	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.54.4.82	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.38.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.69.28.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.38.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
212.199.244.112	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
79.179.39.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.38.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
82.80.42.183	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
220.255.181.141	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.226.44.156	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.131.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8

11-30-2015-14:04:08 to 11-30-2015-15:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.66.146.96	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
109.253.43.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
80.246.130.205	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
46.19.85.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
176.13.15.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
109.253.43.19	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
82.166.219.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	8
109.160.151.152	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
176.13.15.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
149.78.134.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
87.68.18.90	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
149.78.35.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
79.176.9.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
5.102.215.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
46.19.86.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.66.80.23	Denmark	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.54.21.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
74.208.246.249	United States	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
87.68.62.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
95.86.89.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/&sa=u&ved=0ahukewimsllmlljjahukwbqkhfzrcmmqfgghmaa&sig2=y1ef3bb7myzf5z4kho4vaq&usg=afqjcneeywysowwcocycbntx0qxav9lbkw	Block	3
198.154.225.251	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
82.166.190.11	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.166.190.11	Block	3
213.190.100.236	Iceland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
198.1.87.23	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
37.26.147.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.90.176.233	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	3
208.67.183.198	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
54.252.99.49	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
188.191.153.20	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
79.178.18.220	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.18.220	Block	3
37.26.147.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.137.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
50.87.119.203	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
188.165.212.14	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
108.179.251.85	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
213.190.100.236	Iceland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
198.1.87.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
79.178.18.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	2
74.208.246.249	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 Admin Blocking	Block	2
79.179.155.205	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
208.67.183.198	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
2.54.148.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
198.154.225.251	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2

11-30-2015-14:04:08 to 11-30-2015-15:04:08