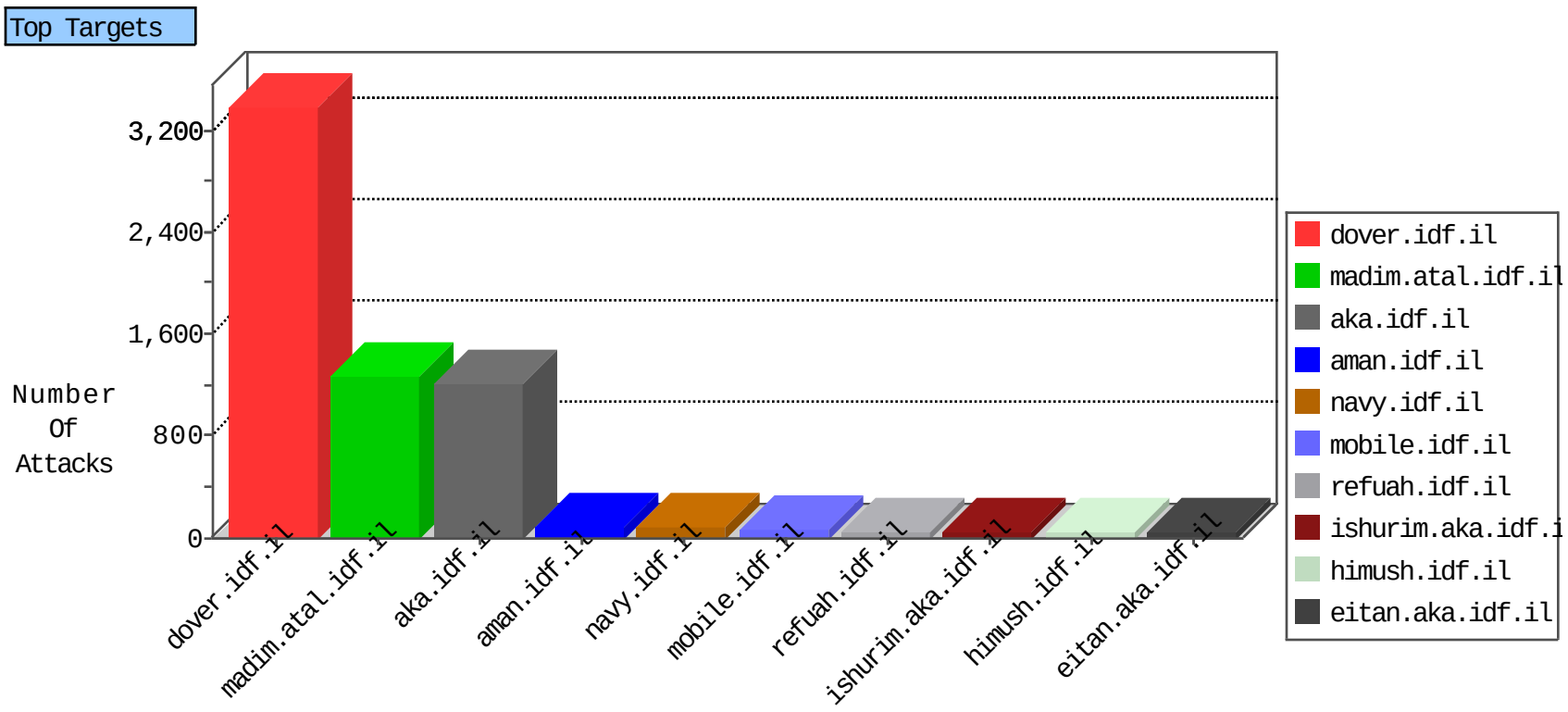
11-30-2015-13:04:04 to 11-30-2015-14:04:04

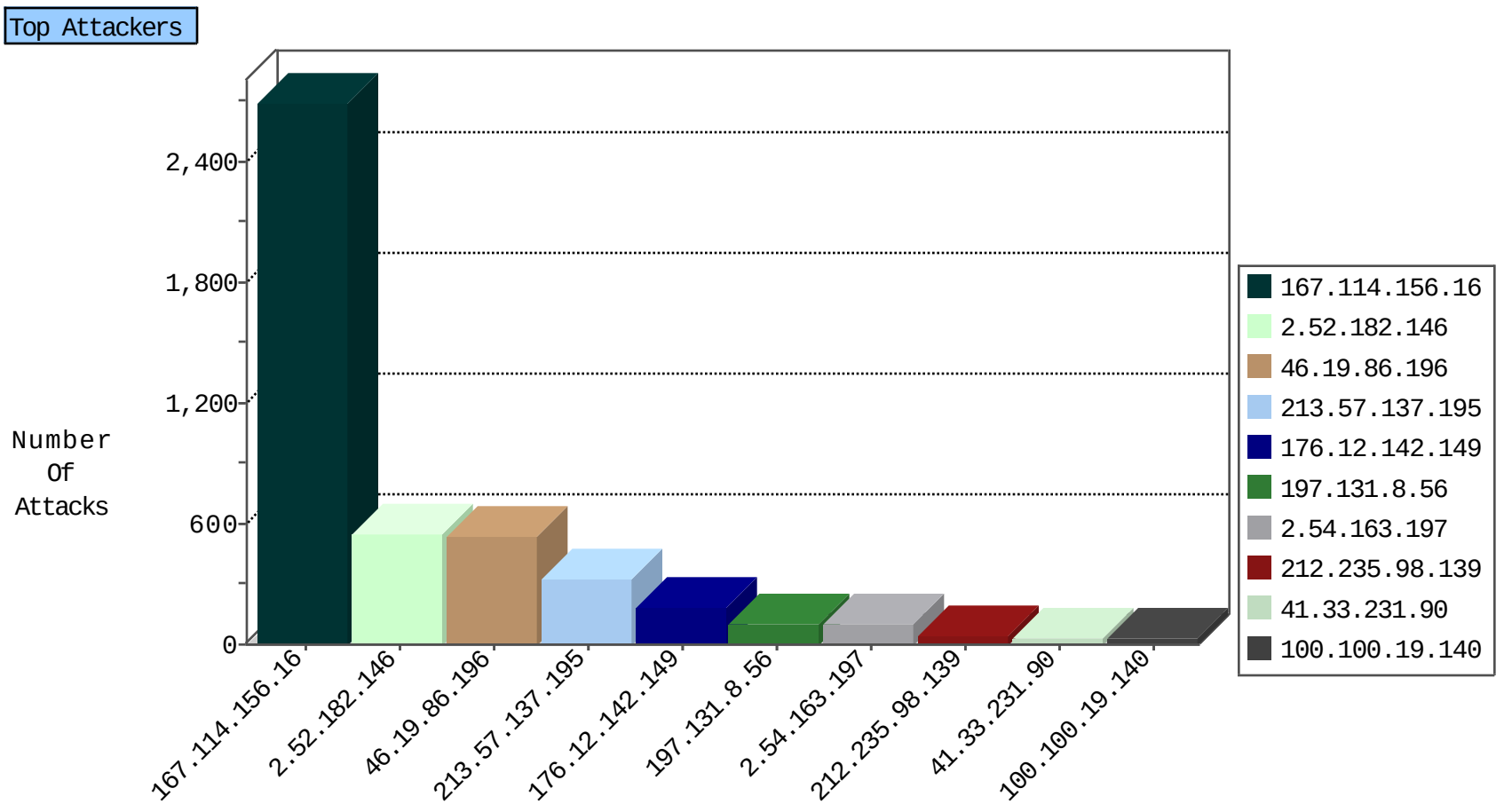
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-30-2015-13:04:04 to 11-30-2015-14:04:04

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	3711
79.180.203.10	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
2.54.53.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
93.174.93.151	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.157	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
54.183.27.199	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

11-30-2015-13:04:04 to 11-30-2015-14:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.239.84	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.120.170.50	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
151.80.31.128	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.180.22	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-30-2015-13:04:04 to 11-30-2015-14:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
14.142.33.102	147.237.0.16	India	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
80.74.105.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.142.33.102	147.237.77.233	India	atal.idf.il	ET SCAN Potential SSH Scan	1
14.142.33.102	147.237.77.205	India	prisha.idf.il	ET SCAN Potential SSH Scan	1
2.52.40.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.170.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
37.26.146.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
14.142.33.102	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
149.78.63.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.176.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-30-2015-13:04:04 to 11-30-2015-14:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	168
213.57.137.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	118
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	42
2.54.163.197	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	37
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.67.152.93	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
192.116.172.254	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
100.100.90.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.163.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
2.54.163.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	22
5.28.154.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.19.140		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	17
100.100.19.140		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
62.219.112.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
192.114.3.241	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	16
2.52.166.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
37.26.148.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.54.163.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.86.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.180.203.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
80.179.125.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
192.114.3.241	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
100.100.39.184		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
100.100.82.99		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	12
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.32.179.3	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.96.125		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
100.100.86.253		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
49.149.178.11	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
130.245.145.19	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.53.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.163.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.249.73.221	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
213.57.130.162	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
217.194.207.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
176.13.14.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.52.163.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
173.252.88.244	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.182.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	301
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	284
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	141
2.52.182.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	137
176.12.142.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
2.52.182.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
197.131.8.56	Morocco	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	101
176.12.142.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	62
199.30.25.20	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
213.8.104.66	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.8.104.66	Block	9
2.54.159.217	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	9
85.130.247.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	4
59.188.5.122	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.116.239.84	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/matash/	Block	3
37.18.176.23	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
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
85.114.142.187	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
174.136.96.189	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.54.52.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
173.255.139.12	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
104.219.52.250		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
173.254.51.74	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.13.14.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
116.12.55.118	Singapore	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
205.186.162.88	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/$$$&?&?$$$	Block	3
50.87.52.131	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
85.114.142.187	Germany	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
176.13.8.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
2.52.165.243	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
173.254.51.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ufi/reaction/	Block	2
85.64.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
109.67.133.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
174.136.96.189	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
116.12.55.118	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
205.186.162.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
173.255.139.12	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
104.219.52.250		147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
176.13.19.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
50.87.52.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
173.254.51.74	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
59.188.5.122	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
212.199.57.202	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.24.92	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
116.12.55.118	Singapore	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
205.186.162.88	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
37.18.176.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2

11-30-2015-13:04:04 to 11-30-2015-14:04:04