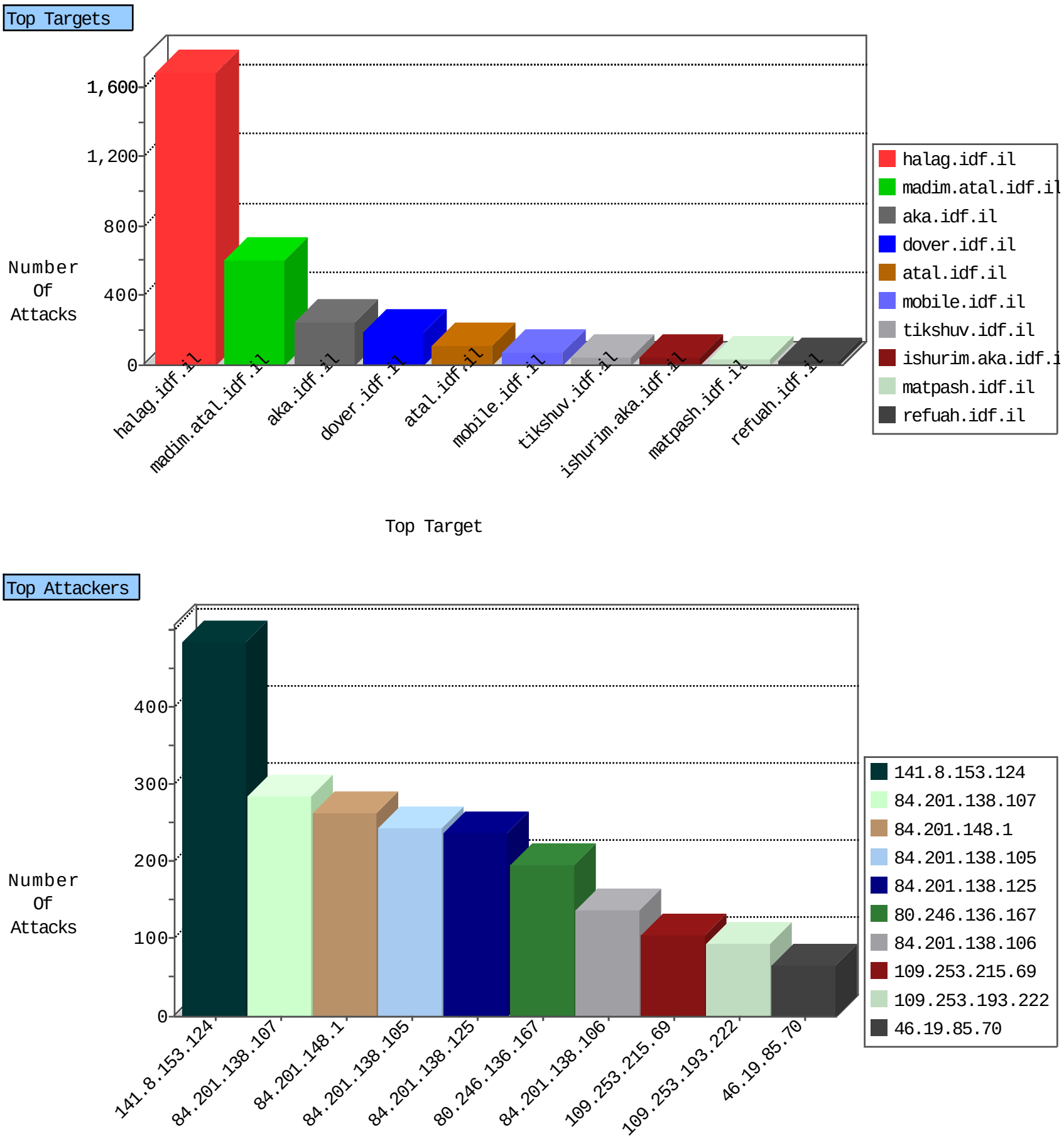
02-11-2016-11:04:04 to 02-11-2016-12:04:04

IDF Under Attack
Daily Report



02-11-2016-11:04:04 to 02-11-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
10.10.10.47		147.237.76.42	refuah.idf.il	Invalid L4 Header Length	drop	6
10.10.10.47		147.237.77.216	dover.idf.il	Invalid L4 Header Length	drop	6
79.181.115.120	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
23.27.250.56	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.253.93.83	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	1
80.178.157.53	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
50.147.46.86	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
88.150.177.186	United Kingdom	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
79.181.115.120	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
88.150.177.186	United Kingdom	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

02-11-2016-11:04:04 to 02-11-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.76.86	navy.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

02-11-2016-11:04:04 to 02-11-2016-12:04:04

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
2.52.15.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.183.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.172.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.20.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.69.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.17.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.166.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.165.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.125.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.2.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.188.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.112.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.222.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.101.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.12.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.76.182	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.81.171	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
199.203.215.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.27.250.56	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
164.39.11.198	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 1024	1

02-11-2016-11:04:04 to 02-11-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.8.153.124	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	486
84.201.138.107	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	285
84.201.148.1	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	263
84.201.138.105	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	245
84.201.138.125	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	237
84.201.138.106	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	139
66.249.81.167	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	36
2.52.48.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
66.249.81.171	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	24
66.249.81.163	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
46.19.86.71	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
176.13.13.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.201.148.7	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	15
82.205.17.110	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
77.125.114.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.8.153.117	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	12
2.52.142.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
82.205.17.110	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
65.55.213.255	United States	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
176.13.22.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
31.168.154.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
209.88.196.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
156.109.18.122	Europe	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	8
175.106.22.23	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.9.125	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
80.179.40.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.201.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.175.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.198	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.253.219.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
176.13.22.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.22.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
199.30.24.179	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
86.163.191.80	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.106.47.109	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.78.184	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.239	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.106.47.109	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
81.218.57.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.177.168.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.163.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.216.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.190.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-11-2016-11:04:04 to 02-11-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
80.246.136.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	88
109.253.193.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
109.253.215.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 216.72.40.185	Block	37
109.253.215.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
176.13.0.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
80.246.138.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.52.48.65	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	9
109.253.193.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
112.17.247.6	China	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	7
112.17.247.6	China	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	7
46.19.85.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.17.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.66.164.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.132.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.206.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
128.194.131.235	United States	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	2
192.114.91.230	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
80.246.136.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.161.133	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
2.54.26.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
156.109.18.122	Europe	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 156.109.18.122	Block	2
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	2
156.109.18.122	Europe	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
165.91.12.68	United States	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	2
79.180.24.251	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
5.29.182.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.177	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
84.108.204.229	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
36.229.150.24	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
156.109.18.122	Europe	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
77.127.217.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
109.253.219.168	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
62.219.232.131	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
197.116.246.138	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
109.175.111.226	Bosnia and Herzegovina	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
40.77.167.103	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1506-en/dover.aspx+idf units	Block	1

02-11-2016-11:04:04 to 02-11-2016-12:04:04