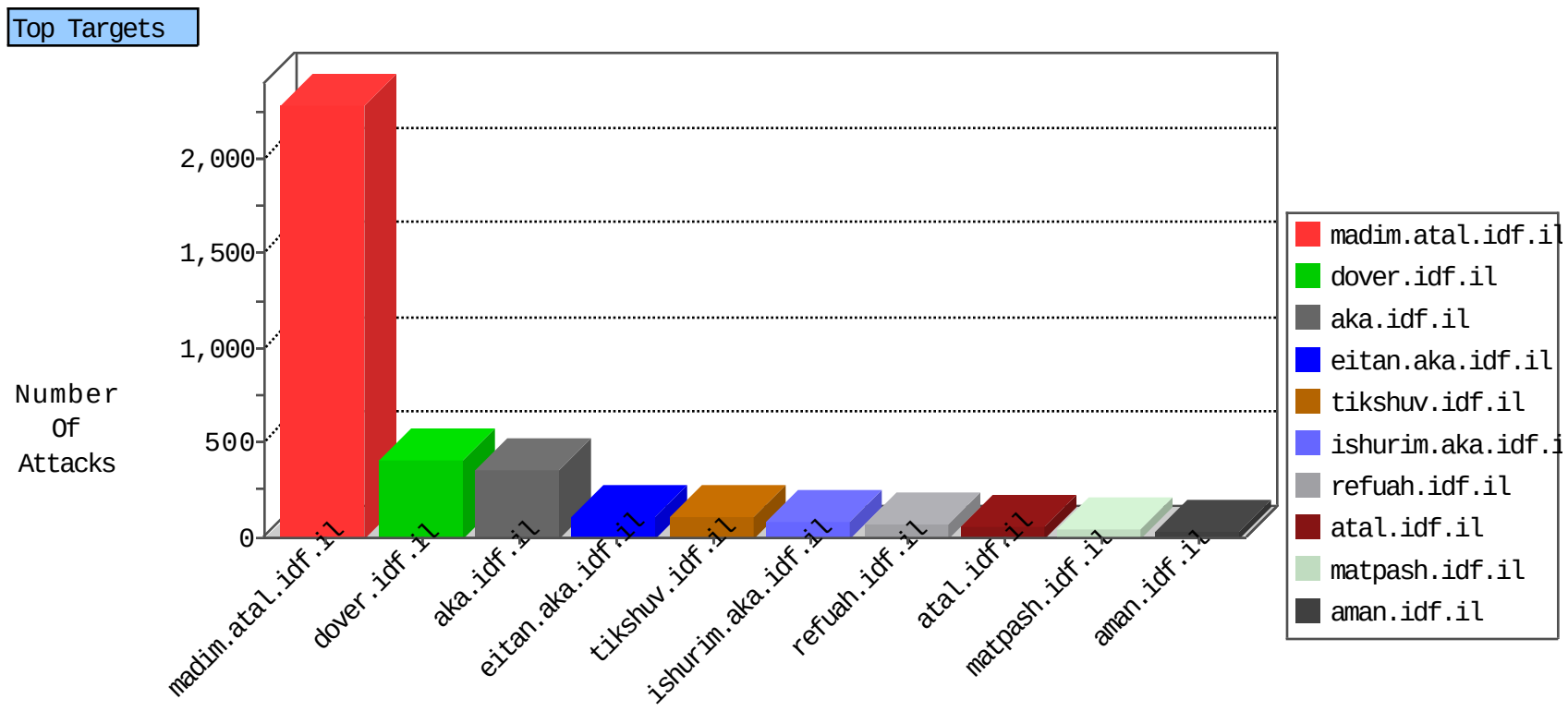
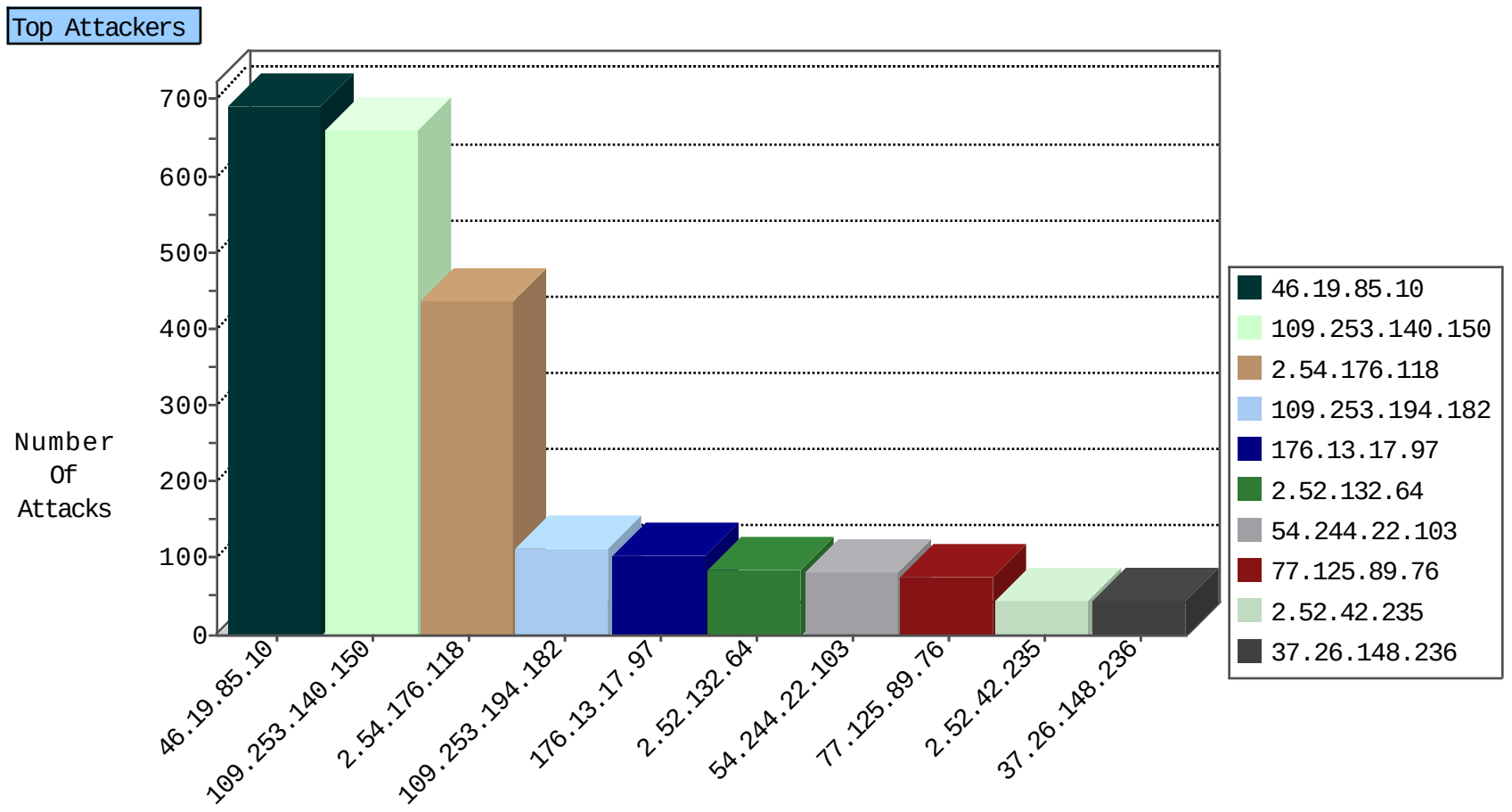
02-22-2016-10:04:01 to 02-22-2016-11:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-22-2016-10:04:01 to 02-22-2016-11:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	47
10.0.0.1		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
31.154.27.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
107.150.33.61	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
122.34.13.148	Korea, Republic of	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

02-22-2016-10:04:01 to 02-22-2016-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.22.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.246.130.98	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
212.235.81.242	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
77.248.12.153	Netherlands	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.123	Italy	147.237.77.226	www.chamatz.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-22-2016-10:04:01 to 02-22-2016-11:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.57.141.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.144	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.91.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.170.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.100.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.25.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.91.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.158.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.151.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.157.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.144	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.76.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.209.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.59.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.77.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.4.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.0.33	Sweden	idf.il	ET SCAN NMAP -sS window 1024	1
2.52.37.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.43.141.234	147.237.77.121	Switzerland	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.44.133.108	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
217.194.199.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

02-22-2016-10:04:01 to 02-22-2016-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.89.76	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	72
2.52.42.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
188.247.77.187	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	28
2.54.22.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
85.65.225.187	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
80.246.133.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
2.54.180.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
109.66.103.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
148.251.21.227	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
2.52.42.235	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.85.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.10.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.220.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.220.172	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.253.205.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.220.172	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.62.189	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.253.220.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
176.13.18.165	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
194.252.5.66	Finland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
80.246.139.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.0.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.190.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.190.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.57.158.224	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.52.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.52.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.54.52.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.52.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
185.32.179.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.52.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.253.210.231	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
93.172.233.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-22-2016-10:04:01 to 02-22-2016-11:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	514
109.253.140.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	462
2.54.176.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	225
2.54.176.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	212
109.253.140.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	199
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
176.13.17.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.194.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
2.52.132.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
37.26.148.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
109.253.194.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
2.52.132.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
40.143.1.4	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.143.1.4	Block	27
2.54.148.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.52.38.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
77.125.2.59	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.2.59	Block	19
109.253.201.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
2.54.51.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.17.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Illegal Response Code	None	15
80.246.136.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
40.143.1.4	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	13
37.26.148.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.52.132.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.54.156.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.17.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
77.75.88.110	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	6
104.131.175.126	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 104.131.175.126	Block	4
2.54.148.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
46.19.85.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.157.187	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
109.253.158.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.89.216.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.181.168.32	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.253.223.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
180.109.228.124	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
31.44.141.84	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/3/2933.pdf&sa=u&ved=0ahukewir9sgd_orlahxcshqkhwnxb1uqfggimak&usg=afqjcnebgrh_jd4xn0yfflyaznvwlddhtq	Block	2
173.252.114.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.177.155.82	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	2
217.165.23.198	United Arab Emirates	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
82.80.196.44	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.89.216.229		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.228.240.81	Israel	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	2
184.168.193.151	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	2
46.19.85.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
81.169.144.135	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	2

02-22-2016-10:04:01 to 02-22-2016-11:04:01