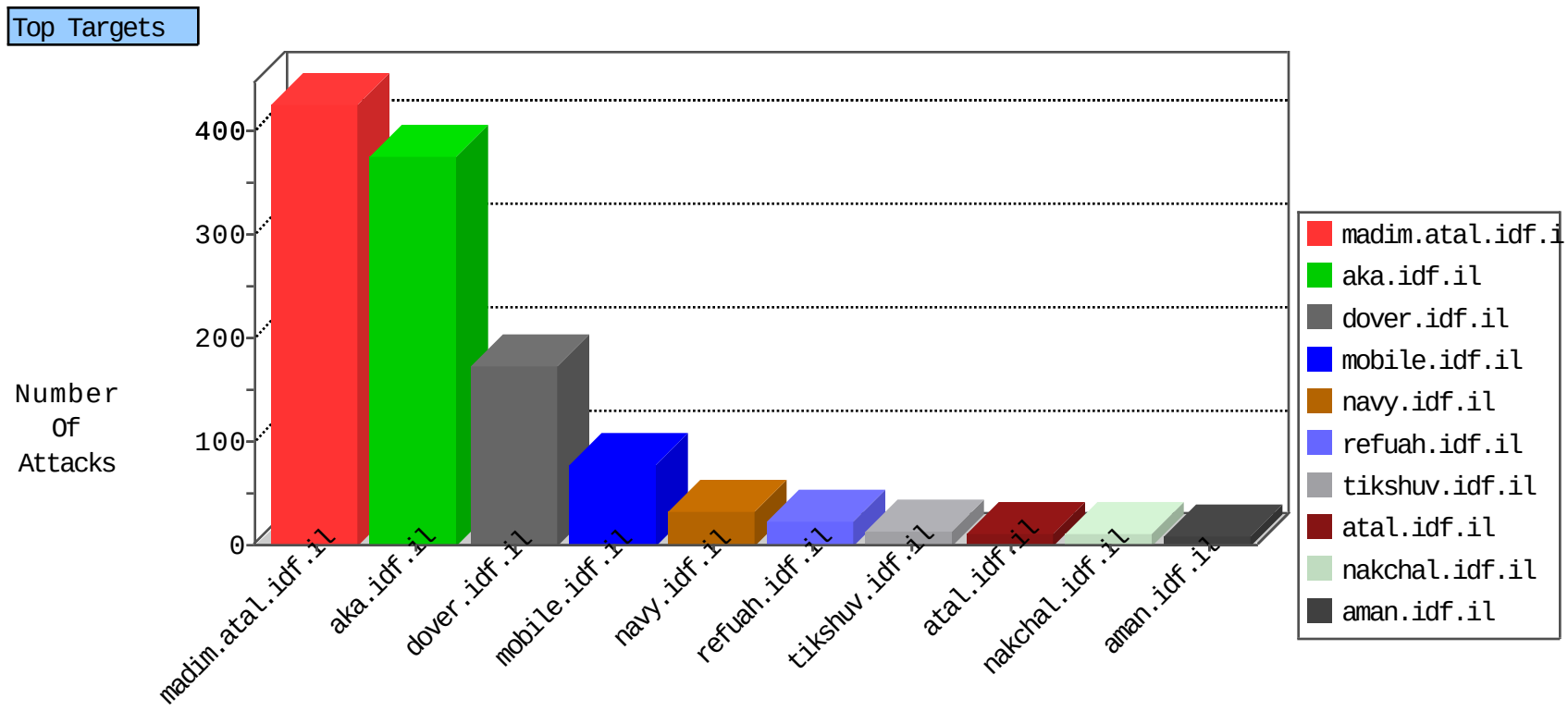
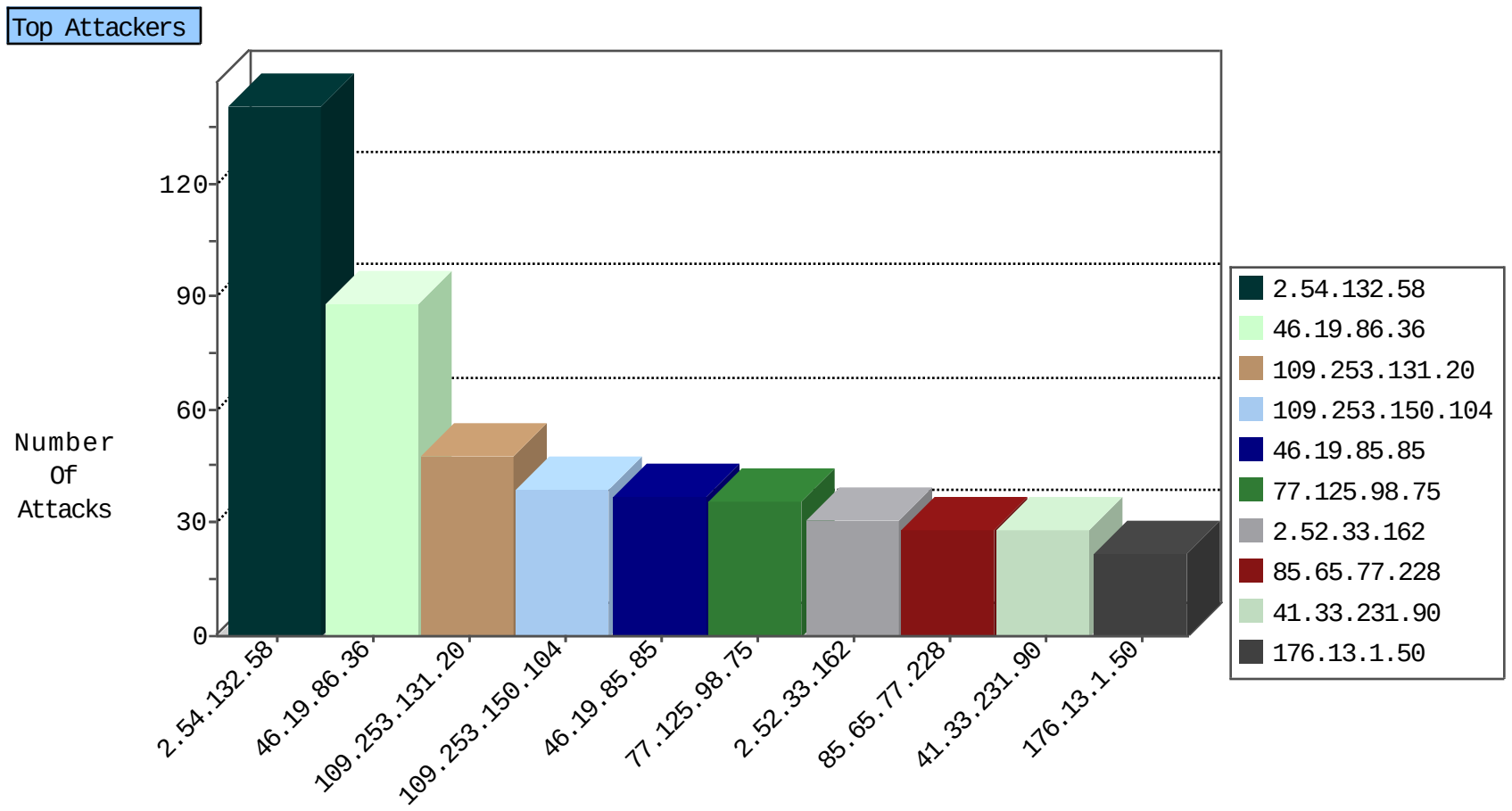
02-28-2016-09:04:01 to 02-28-2016-10:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-28-2016-09:04:01 to 02-28-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	8
123.203.139.71	Hong Kong	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-28-2016-09:04:01 to 02-28-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.131	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
195.162.67.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
40.77.167.75	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.41.169	Italy	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
31.168.101.163	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

02-28-2016-09:04:01 to 02-28-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.208.153.47	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.168.14.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.76.15.158	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.75.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.10.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.129.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.199.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.57.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.245.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.103.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.50.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.146.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.180.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.101.222.43	147.237.72.166	Ecuador	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.228.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.132.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.21.248.87	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
2.52.41.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.145.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.121.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.178.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.151.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-28-2016-09:04:01 to 02-28-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.98.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
82.81.66.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.178.137.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.54.33.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.52.160.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.106.46.74	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.33.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.253.136.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.188	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.33.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.6.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.33.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.54.23.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
149.78.98.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
212.179.226.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.33.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.130.132.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
149.78.98.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.33.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.188	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.130.132.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
149.78.98.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.117.13.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
194.30.134.180	Cyprus	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.55.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
121.28.150.154	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
83.130.99.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.42.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.16.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.2.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.13.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.2.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.129.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.157.149	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.22.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.172.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.35.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.102.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.43.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.135.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.135	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

02-28-2016-09:04:01 to 02-28-2016-10:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.132.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
109.253.131.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.150.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
85.65.77.228	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	28
176.13.1.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.54.161.181	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	12
109.253.146.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	10
213.57.226.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.106.175.208	Block	9
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	5
74.208.153.47	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 74.208.153.47	Block	4
132.76.50.5	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 132.76.50.5	Block	4
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	4
176.13.2.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.196.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.135.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.101.163	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
85.65.151.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.139.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.3.146.207	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.182	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.140.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.120.148.137	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
94.230.93.179	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.105.139.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
139.162.40.248	Netherlands	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/bin/hostname	Block	1
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
189.218.109.235	Mexico	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1341-en/cogat.aspx'	Block	1
87.69.160.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.239	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.75	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/registrationwizard/register.aspx	Block	1
217.33.23.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
85.65.116.235	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	1
31.168.101.163	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.168.101.163	Block	1
139.162.40.248	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/bin/hostname	Block	1
74.208.153.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/abc123/	Block	1
189.219.226.149	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17570-en/dover.aspx'	Block	1
88.198.44.2	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
109.253.215.38	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.194.206.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1