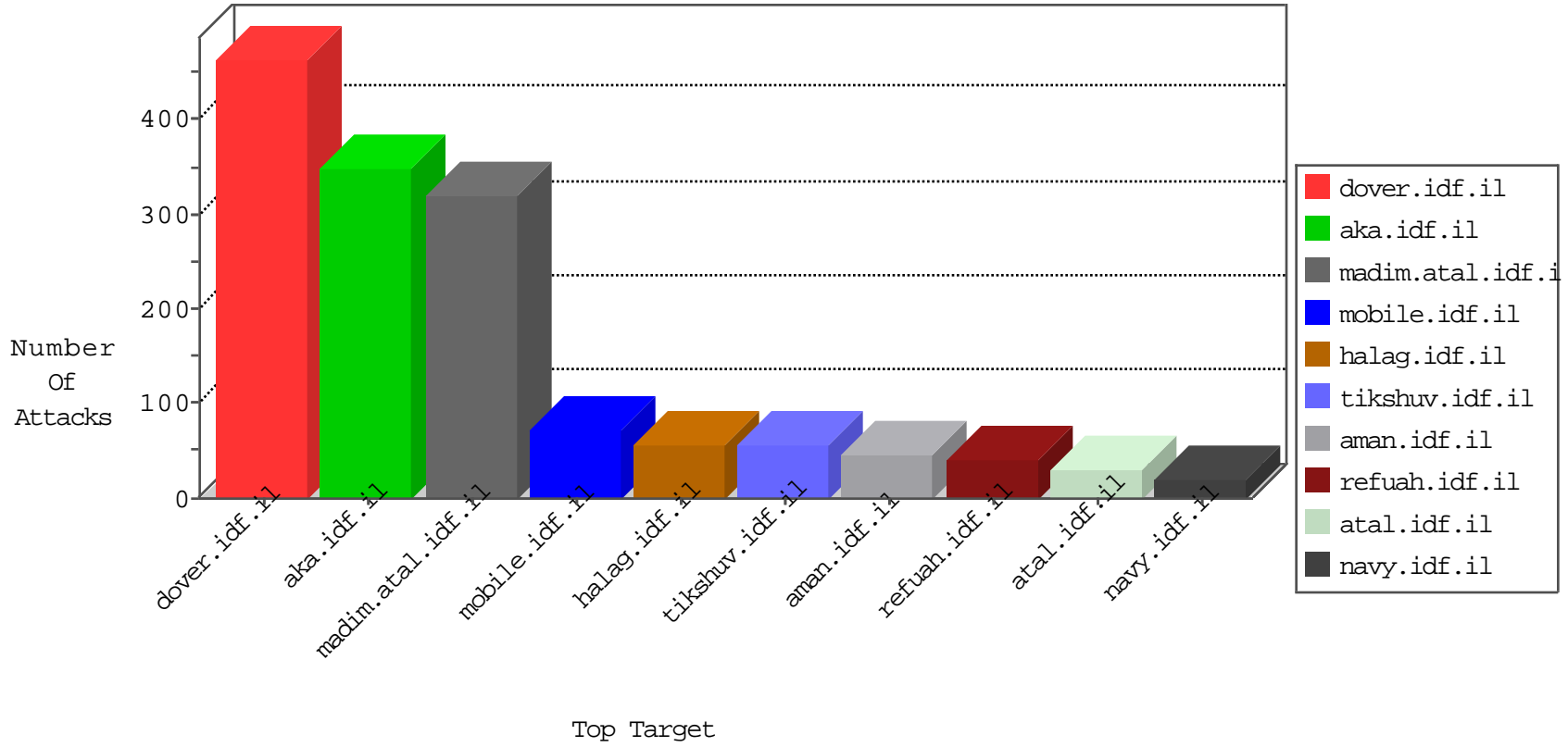


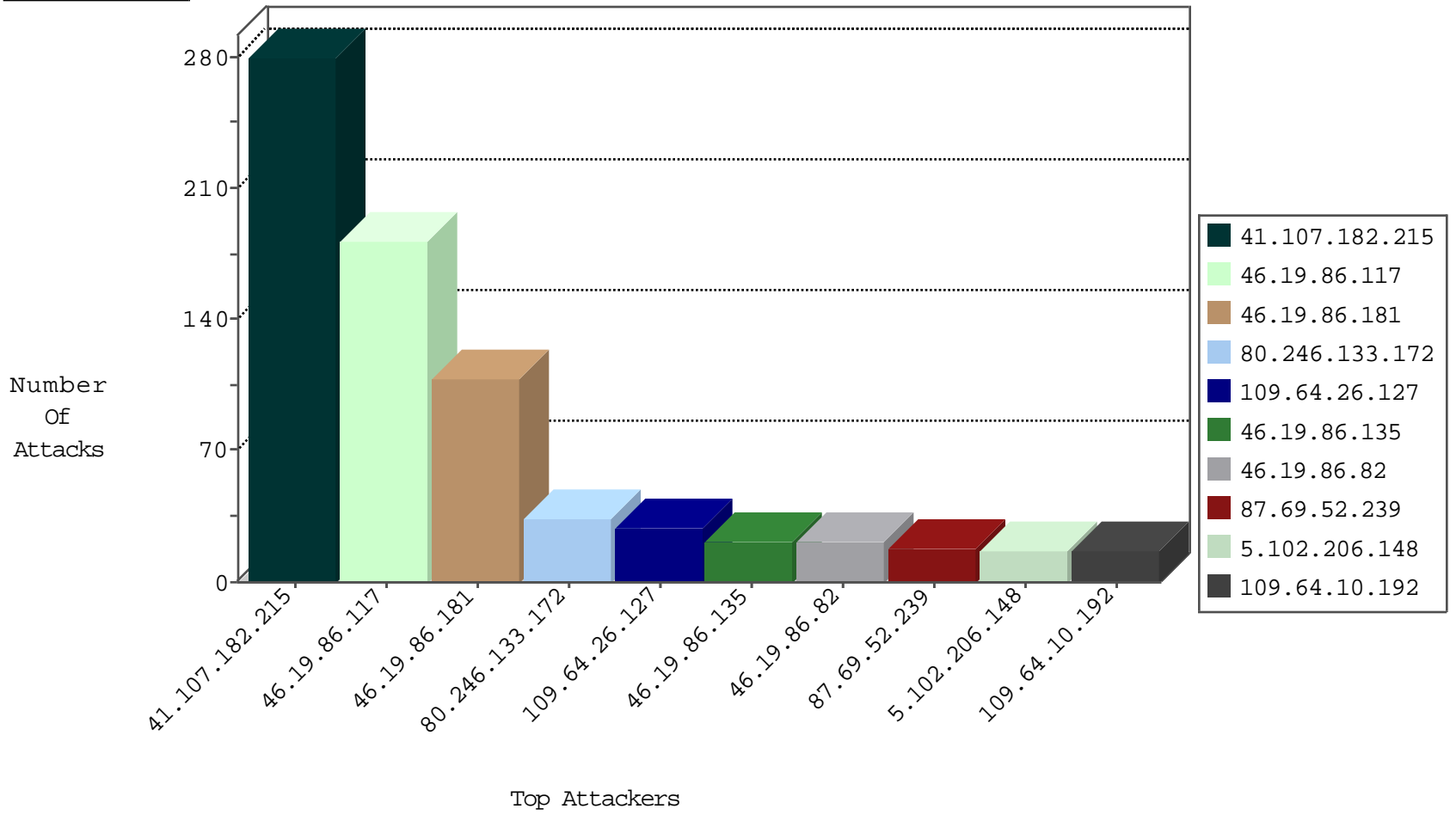
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.107.182.215	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4591
41.107.182.215	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	34
62.219.224.99	Israel	147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.80.217.70	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
108.186.168.25	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
41.107.182.215	Algeria	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.206.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
212.179.159.253	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.57.141.156	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.26.147.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.26.147.155	Israel	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
149.78.79.197	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.142.152.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.116.55.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.17.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.93.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.231.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.143.185.217	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
152.62.109.202	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
69.248.129.181	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
118.112.185.236	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
109.253.129.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.107.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.84.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.39.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.234.177.176	147.237.77.216	Sweden	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.180.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.51.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.242.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.71.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
118.112.185.236	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
46.116.5.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.168.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.177.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.77.74	Canada	law.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.26.127	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
80.246.133.172	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
109.64.10.192	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
213.8.204.78	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	15
46.19.86.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.17.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.40	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.8.204.25	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.22.129.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.175	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.140.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.174.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.7	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.253.222.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.123.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.78	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.41.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.52.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
93.173.181.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.8.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.46.39.201	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.8.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.226.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.36.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.210.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.67.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.178.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.33.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.52.239	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.8.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.178.14.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.165.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-06-2016-17:04:04 to 03-06-2016-18:04:04

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.139.50.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.163.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.183.95	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
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	182
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.86.135	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	22
2.54.151.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.95.211.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
109.65.9.8	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	6
87.68.66.27	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.68.66.27	Block	5
109.65.9.8	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	5
46.19.86.82	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.157.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.199.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.184	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.3.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.151.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
104.130.141.191	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.130.141.191	Block	3
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.93.47	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.64.118.164	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.80.50.10	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	2
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.215.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.86.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
37.26.148.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	2
141.212.122.129	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /x	Block	1
37.26.148.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.252.91	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
69.112.37.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
178.121.13.39	Belarus	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.86.150	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1
37.187.157.108	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
80.178.157.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/print.css	Block	1
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.241.229.215	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
37.26.146.144	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.26.127	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
91.240.235.225	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
80.246.140.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.7	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
145.253.125.210	Germany	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.26.148.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.9.8	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 109.65.9.8	Block	1
77.125.147.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1