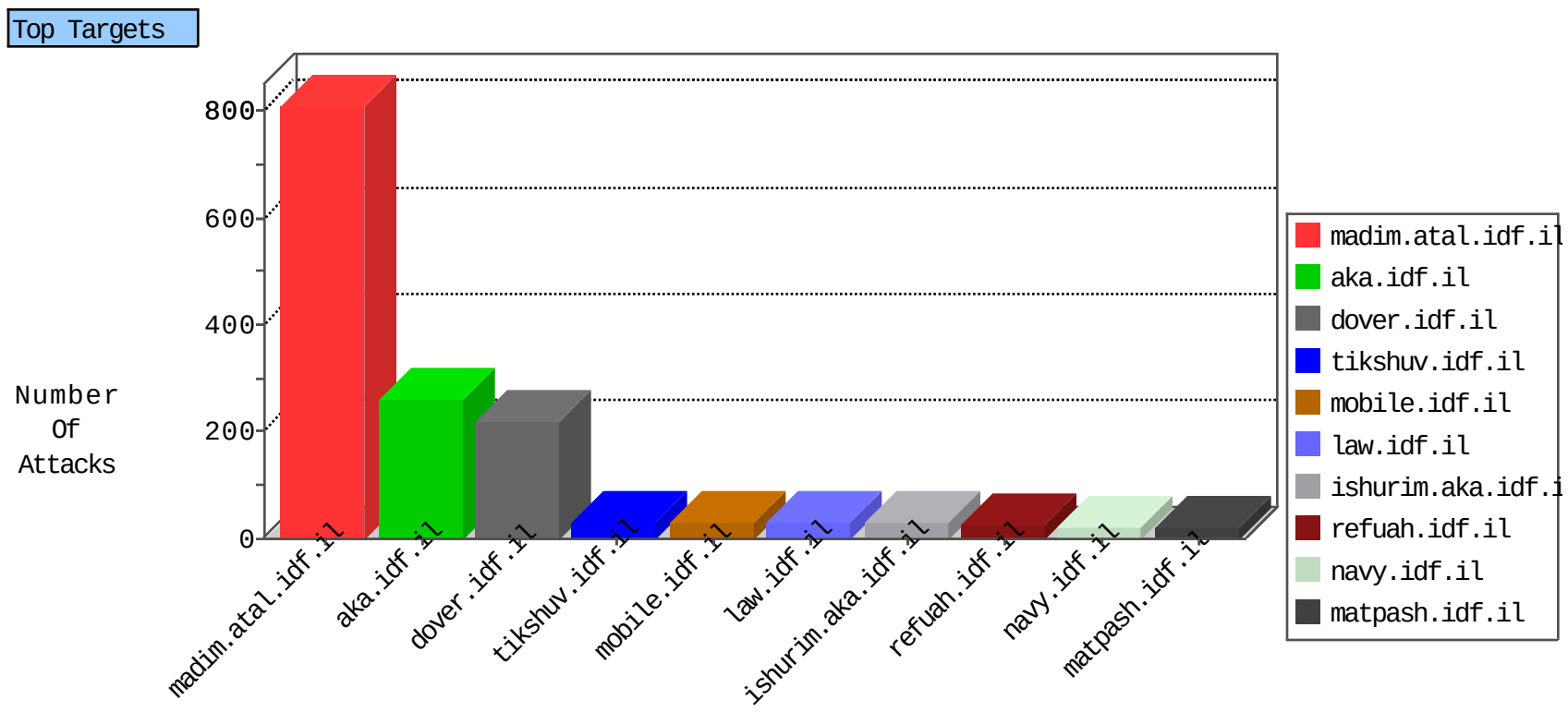
03-08-2016-14:04:06 to 03-08-2016-15:04:06

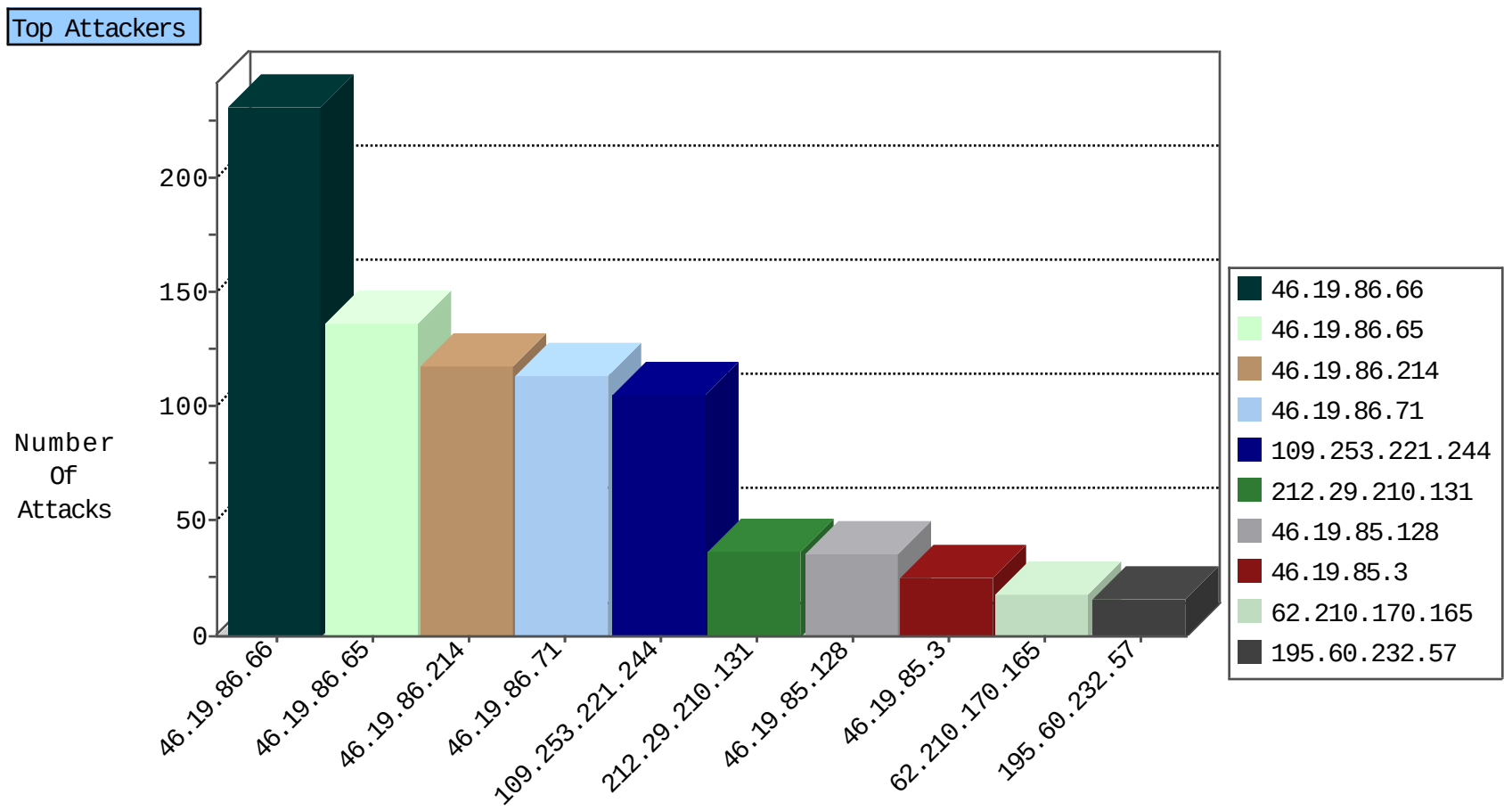
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-08-2016-14:04:06 to 03-08-2016-15:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.99.175.82	Japan	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	244
31.154.41.13	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
2.52.34.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
82.145.218.26	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
176.13.4.193	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.54.176.22	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.109.216.123	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.253.198.244	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
199.203.84.160	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
74.82.47.29	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
2.54.39.137	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

03-08-2016-14:04:06 to 03-08-2016-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.170.165	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	10
5.29.142.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
2.54.140.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
62.210.170.165	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
62.210.170.165	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
82.81.55.155	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.15	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.102.9.117	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.68	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.112	Italy	147.237.77.176	matpash.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.102.9.127	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.69.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
37.187.94.202	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
77.127.22.242	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
37.187.95.7	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-08-2016-14:04:06 to 03-08-2016-15:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.51.129	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	Tehila - Perl LWP with fake user agent	1
2.54.1.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.235.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.61	Spain	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.198.210	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
217.132.23.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.171.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.52.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.233	United States	atal.idf.il	ET DROP Dshield Block Listed Source	1
2.54.39.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.97.55.52	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.103.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.32.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.184.198.210	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
217.132.27.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.43.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.161.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

03-08-2016-14:04:06 to 03-08-2016-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.29.210.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
212.29.210.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
85.130.191.143	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.145.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.3.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
176.13.15.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.140.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.140.214	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
195.60.232.57	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.173.51	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
76.16.254.9	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.169.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.24	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.220	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.151.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
195.60.232.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.46.39.47	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.150.203.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.222	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.70.29.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.110		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.32.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.2.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.241	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
87.68.249.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.62.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.0.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.184.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.174	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	3
79.178.5.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.156.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.140.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.183.217.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.56.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.155.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-08-2016-14:04:06 to 03-08-2016-15:04:06

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

03-08-2016-14:04:06 to 03-08-2016-15:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	231
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
46.19.86.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
46.19.86.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
109.253.221.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
176.13.13.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.22.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
2.54.53.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.15.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
62.219.153.212	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.219.153.212	Block	4
62.219.153.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size338x0/2371.jpg	Block	4
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	3
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.7.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
89.138.206.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
178.36.225.22	Poland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.89.217.235		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.166.192	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
84.228.177.111	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
2.54.186.243	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
194.90.15.61	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
76.16.254.9	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
203.193.1.23	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected ********** ********** **********, Observed ********** ********** ********** ****	None	1
85.64.168.222	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.64.168.222 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
79.181.107.239	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/8/size338x0/1668.jpg	Block	1
37.110.117.31	Russian Federation	147.237.77.74	law.idf.il	PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
87.70.48.31	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
194.90.15.61	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
185.89.217.231		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.73	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.13.48	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
77.91.34.230	Poland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/default.aspx 	Block	1
94.230.86.241	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
85.64.168.222	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.182.118.172	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.110.117.31	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
184.106.10.128	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
75.119.221.245	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1

03-08-2016-14:04:06 to 03-08-2016-15:04:06