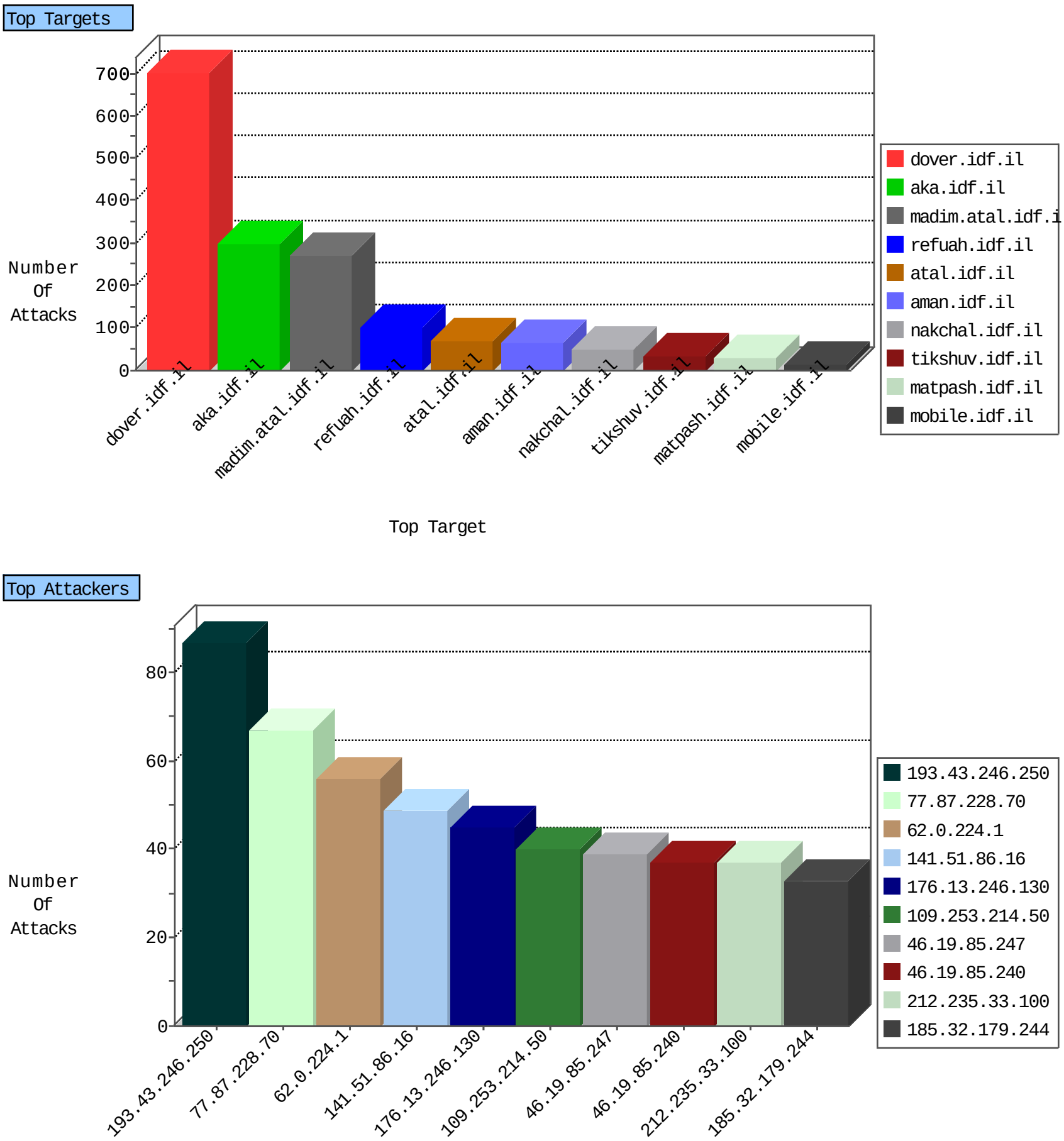
09-19-2016-12:04:08 to 09-19-2016-13:04:08

IDF Under Attack
Daily Report



09-19-2016-12:04:08 to 09-19-2016-13:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.39	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.22.150.78	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.19.85.90	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
81.218.32.172	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.62.53.168	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1

09-19-2016-12:04:08 to 09-19-2016-13:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.119.125.159	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
74.63.228.226	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.35	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
216.119.125.159	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2

09-19-2016-12:04:08 to 09-19-2016-13:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.63.228.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	16
216.119.125.159	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	9
50.63.196.35	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
91.224.160.106	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
176.228.219.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.37.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.167.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
84.229.35.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
84.108.217.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
79.181.2.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
194.90.88.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
67.211.219.120	147.237.77.178	United States	e.matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.224.160.106	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
62.219.164.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
92.29.69.152	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.53.188.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
85.250.86.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
84.111.226.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
80.178.222.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.82.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
189.5.77.212	147.237.76.176	Brazil	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.212	147.237.76.30	Europe	himush.idf.il	ET SCAN NMAP -sA (2)	1
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1

09-19-2016-12:04:08 to 09-19-2016-13:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
77.87.228.70	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
212.235.33.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
62.0.224.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	23
141.51.86.16	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
46.19.85.247	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.247	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
82.80.158.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.237	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
62.0.247.129	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
141.51.86.16	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.220	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.13.246.130	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
54.147.183.113	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
91.106.50.237	Iraq	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
31.154.27.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.178.120.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
81.199.122.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
176.13.246.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
84.229.56.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
84.229.56.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.215	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.67.253.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.246.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
81.218.32.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.215	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
77.126.73.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.10.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.237	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.67.253.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
80.246.130.225	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.208	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
84.95.251.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.235.64.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
80.246.139.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.222.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.199	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
195.60.235.57	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

09-19-2016-12:04:08 to 09-19-2016-13:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.214.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
185.32.179.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
37.26.148.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.53.62.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
176.13.246.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
109.253.204.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.55.43.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
195.138.97.190	Moldova, Republic of	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	4
87.69.235.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.210.178.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.28.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.70.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.150.133.226	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
37.26.148.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.10.146	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/miluim/	Block	2
85.65.102.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.200.12.58	Ukraine	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	2
37.26.146.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.59.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.70.15.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.200.12.58	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
46.121.125.184	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/chinuch/general/default.asp	None	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/buttonback.png	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
91.200.12.58	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.200.12.58	Block	1
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Malformed URL	Block	1
2.53.166.136	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unknown HTTP Request Method	Block	1
80.246.130.225	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.61	Block	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
195.62.53.168	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Abnormally Long Header Line request header name	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Unknown HTTP Request Method	Block	1
77.139.58.129	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
109.253.158.159	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.102.9.30	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
212.235.64.96	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.234.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1250-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Parameter Name [[#31]]• seÜ[[#5]]Ÿ7JÛH˛8¡Ý`[in r¬z	Block	1

09-19-2016-12:04:08 to 09-19-2016-13:04:08