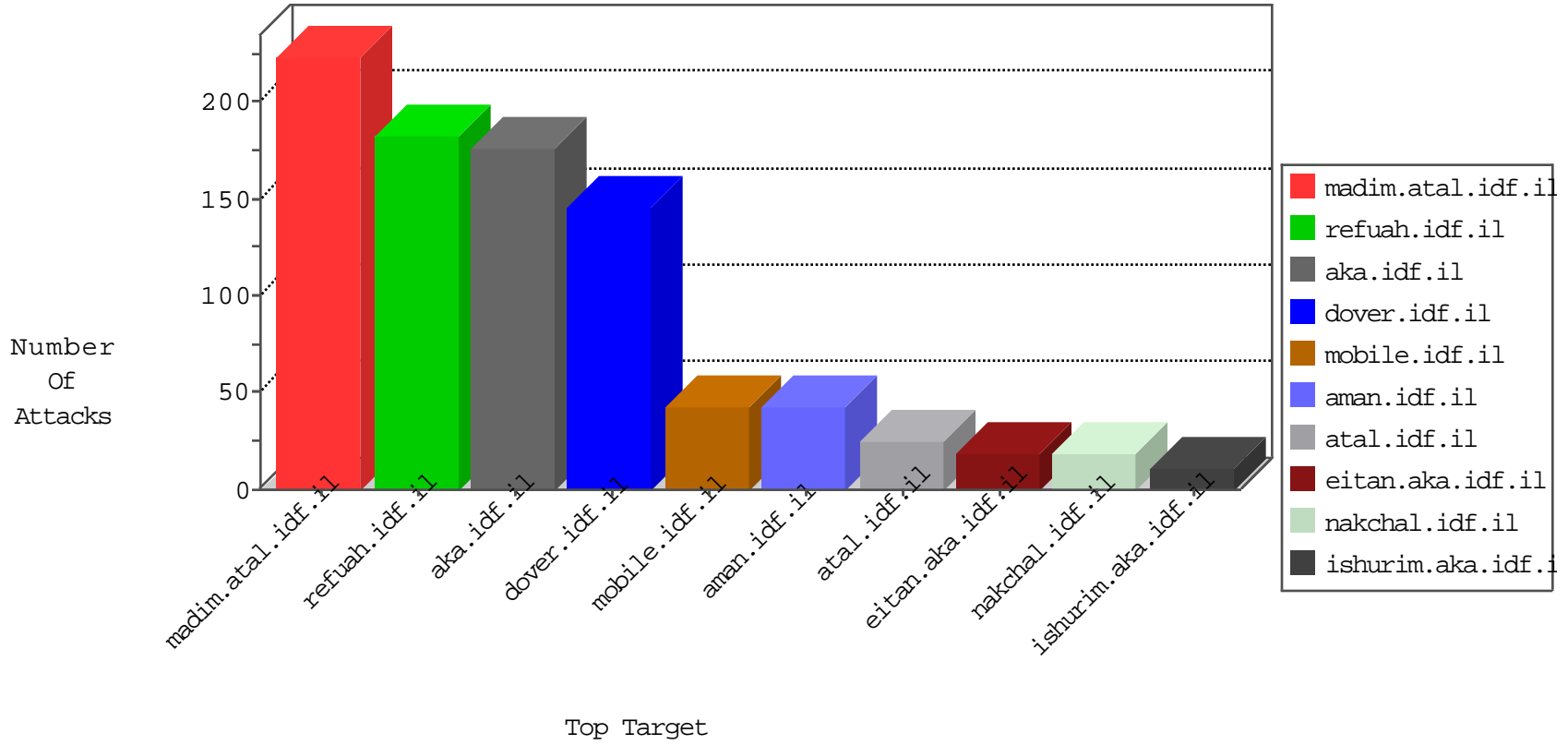


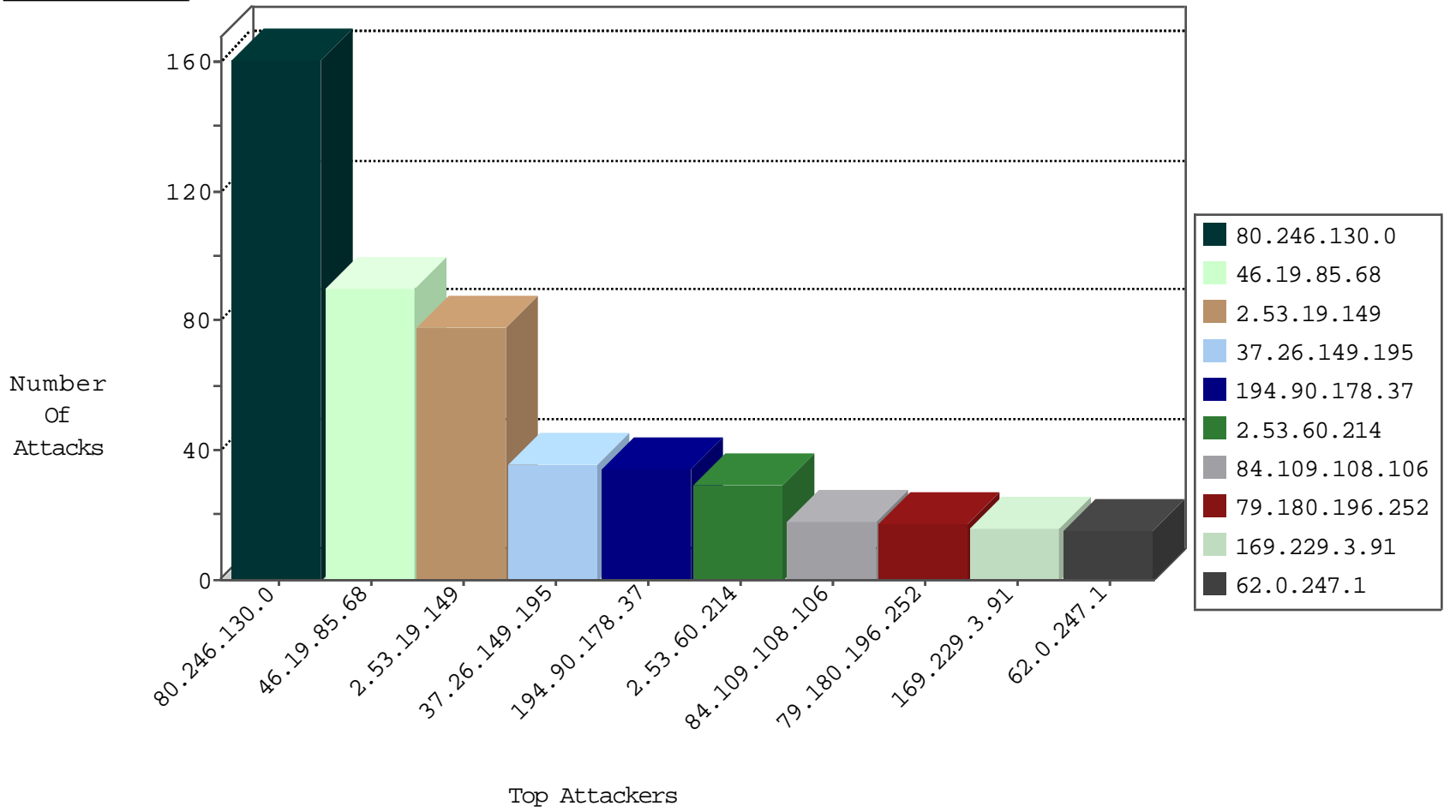
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.68.19.248	Israel	147.237.72.156	aman.idf.il	L4 Source or Dest Port Zero	drop	3
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.65.4.192	Israel	147.237.0.33	idf.il	Black List	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.197	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.167	ishurim.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
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
2.53.58.145	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-15-2016-14:04:01 to 09-15-2016-15:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.158.203.149	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.208.64	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
84.94.88.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
80.246.138.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
79.173.226.205	147.237.77.216	Jordan	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
62.90.184.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.65.35.2	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
46.116.75.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.105.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.169.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.149	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
84.110.233.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
80.250.149.60	147.237.77.216	Israel	dover.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
79.178.41.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.124	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.120.34.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.86.3.66	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.37.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.0	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	159
194.90.178.37	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	34
2.53.60.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	29
84.109.108.106	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.180.196.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
62.0.247.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
14.139.210.68	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.8.204.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.67.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
147.235.185.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.61	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.32.179.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.61	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.180	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.184	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.233.157	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.151.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.156	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.18.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.74.105.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
212.187.151.62	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.86.50	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.32.179.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.192	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.8	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.0.24.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.46.38.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
217.132.50.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.117.20.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.53.157.165	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
109.253.200.205	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
213.57.157.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
2.53.19.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
37.26.149.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
109.253.229.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
176.13.6.135	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 176.13.6.135	Block	7
147.236.238.41	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
77.139.242.57	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	4
147.236.238.41	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/2/	Block	3
77.138.111.240	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
109.253.209.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.204.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
147.236.238.41	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 147.236.238.41	Block	2
213.8.204.19	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.128.48.50	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	2
109.64.85.131	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	1
212.25.102.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/defout.aspx	Block	1
169.229.3.91	United States	147.237.77.216	doover.idf.il	Unknown HTTP Request Method '•ø°fê>øÈbô@b[[#7]]07Ú @Láé[[#0]]+ in URL	Block	1
79.179.13.116	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Method 2Ûj%ÁÖ[[#20]]„<i()Í&•Aq,^N6óEGCoT[[#18]][[#22]]%)[[#21]]*ð	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
2.55.177.135	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
116.15.55.172	Singapore	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdoover.aspx	Block	1
185.32.179.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.108.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.106.191	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
169.229.3.91	United States	147.237.77.216	doover.idf.il	Illegal Byte Code Character in Header Value	Block	1
159.203.66.80	United States	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
46.19.85.160	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
109.253.143.132	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
212.235.62.200	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized HTTP Method	Block	1
176.13.6.79	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.130.0	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Malformed URL	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
37.26.146.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.226.218.9	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
85.65.145.14	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
192.115.116.26	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.115.116.26	Block	1
169.229.3.91	United States	147.237.77.216	doover.idf.il	Illegal Byte Code Character in Method '•ø°fê>øÈbô@b[[#7]]07Ú @Láé[[#0]]+	Block	1
159.203.78.52	United States	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
46.19.85.192	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
80.246.130.141	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Unknown HTTP Request Method 2Ûj%ÁÖ[[#20]]„<i()Í&•Aq,^N6óEGCoT[[#18]][[#22]]%)[[#21]]*ð	Block	1
87.69.136.199	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
192.115.116.26	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/error.png	Block	1
77.138.238.195	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
169.229.3.91	United States	147.237.77.216	doover.idf.il	Malformed URL	Block	1