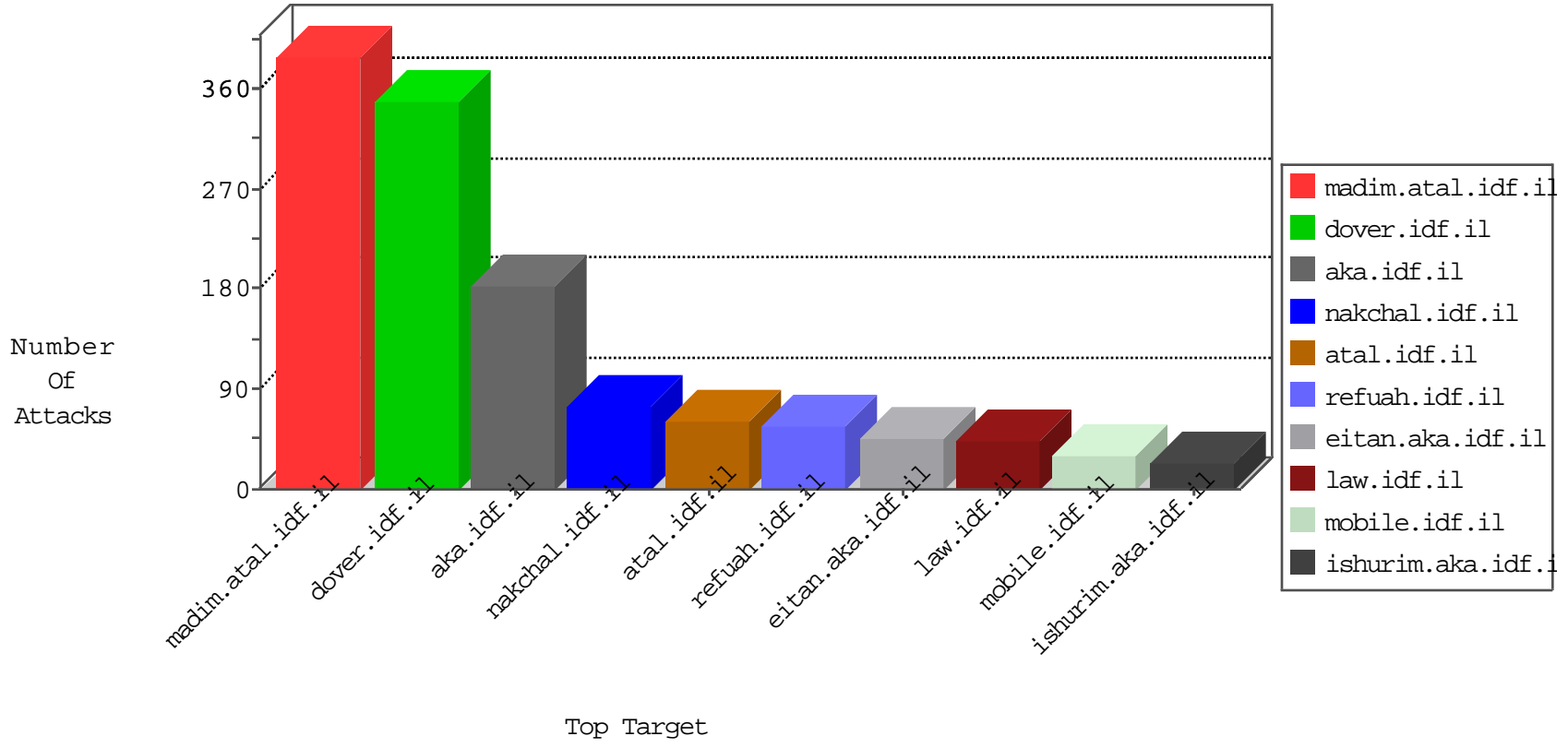


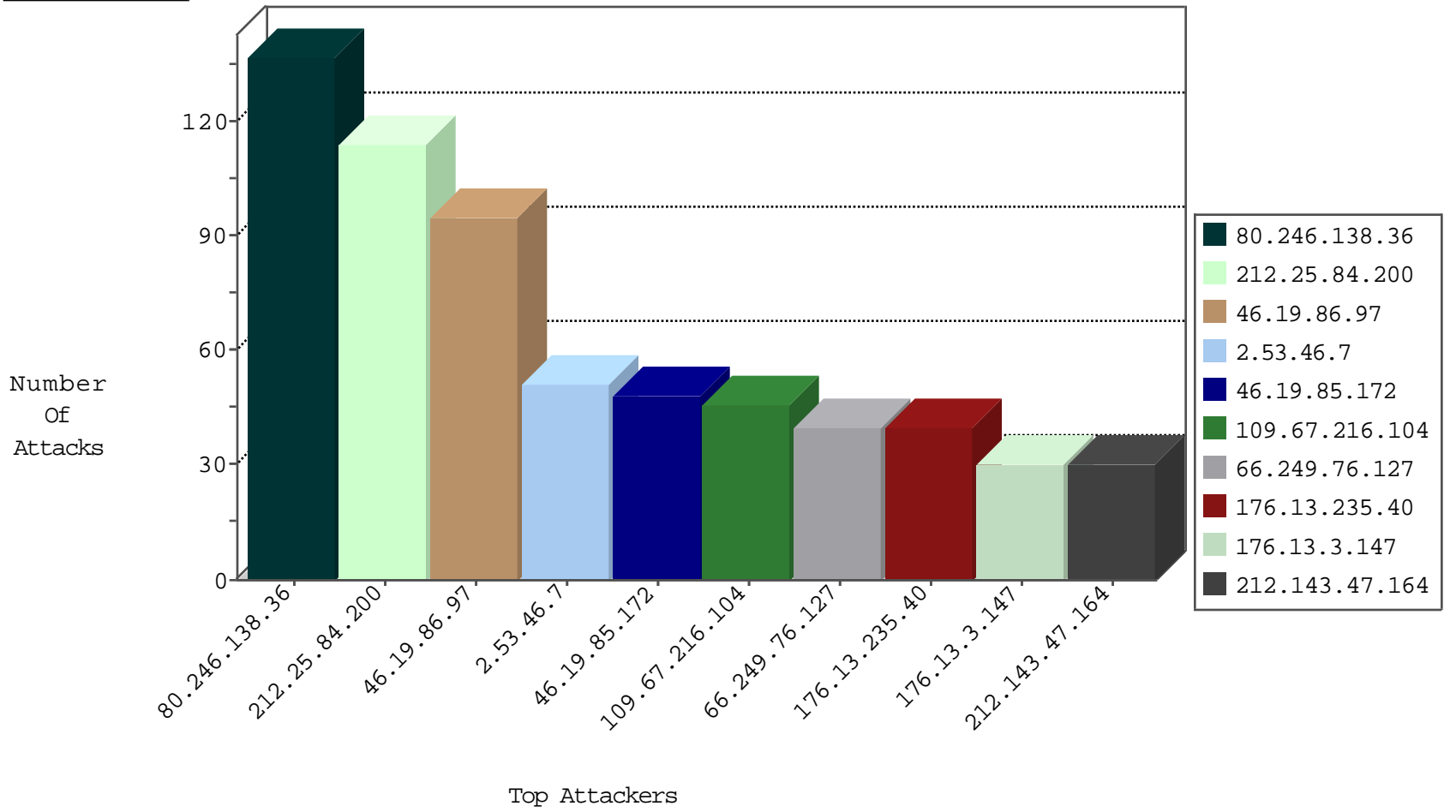
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.238.138.252	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	36
212.150.127.133	Israel	147.237.72.166	aka.idf.il	ICMP-Frag-Needed-Storm	drop	35
46.19.86.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
84.111.94.135	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
168.235.197.203	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
159.104.163.18	United States	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
118.122.119.70	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
118.122.119.70	China	147.237.72.217	e.idf.il	JLM_Purple_Con_Limit_Http	drop	1
192.33.90.67	Switzerland	147.237.72.14	dover.idf.il(old)	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
80.246.138.163	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
159.104.163.17	United States	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1

09-14-2016-12:04:00 to 09-14-2016-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.76.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	40
2.53.130.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.162.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.34.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.193.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
80.246.138.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
78.39.133.4	147.237.76.39	Iran, Islamic Republic of	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.236.189.41	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
2.53.165.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.64.102.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.37.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.33.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.102.135.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.227	China	e.hanaz.idf.il	ET SCAN Potential SSH Scan	1
81.218.207.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
80.246.130.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
78.39.133.4	147.237.72.217	Iran, Islamic Republic of	e.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
5.102.193.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.227.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.25.84.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
109.67.216.104	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
212.143.47.164	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
46.19.85.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
100.92.157.141		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.69.36.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
109.253.196.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.172	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.181.14.148	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.20	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.93	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.12.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.172	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.3.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.72	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.16.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
46.19.85.172	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
5.102.255.12	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
62.0.244.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.172	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.248.15	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.55.47.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.20	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.94.63.168	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.47.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.246.229	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
176.13.16.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.134	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.242.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
151.19.83.52	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.116.98.29	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.111.94.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.138.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
2.53.46.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
176.13.235.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
176.13.3.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.135.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
109.226.28.150	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	10
109.253.139.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
77.138.106.156	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	4
46.120.56.128	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
84.94.85.173	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	3
109.253.142.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.115.252.2	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
176.13.0.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.241.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.56.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.80.115	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.80.115	Block	3
109.226.28.150	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/2/	Block	3
2.53.60.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.103	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.241.117	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.197.61.250	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
194.78.40.94	Belgium	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	2
84.110.55.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.67.216.104	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1105-he/contactus.aspx	None	1
207.46.13.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
46.19.85.53	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.152.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.168.208	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
68.180.228.171	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
46.19.86.217	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
217.194.207.34	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.194.207.34	Block	1
85.218.46.42	Switzerland	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.218.46.42	Block	1
80.246.136.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.146.166	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
165.225.80.125	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
2.53.35.88	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
109.67.216.104	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter r in www.eitan.aka.idf.il/templates/opcontactus/govcaptchaimage.axd	None	1
66.249.64.89	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
46.19.85.112	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.25.84.200	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.94.85.173	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.94.85.173	Block	1
2.53.181.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.16.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.139.196.161	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
46.19.86.217	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
217.194.207.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/haredim/general.aspx	Block	1
85.218.46.42	Switzerland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
37.26.146.244	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTTARGET in www.aka.idf.il/main/giyus/	None	1