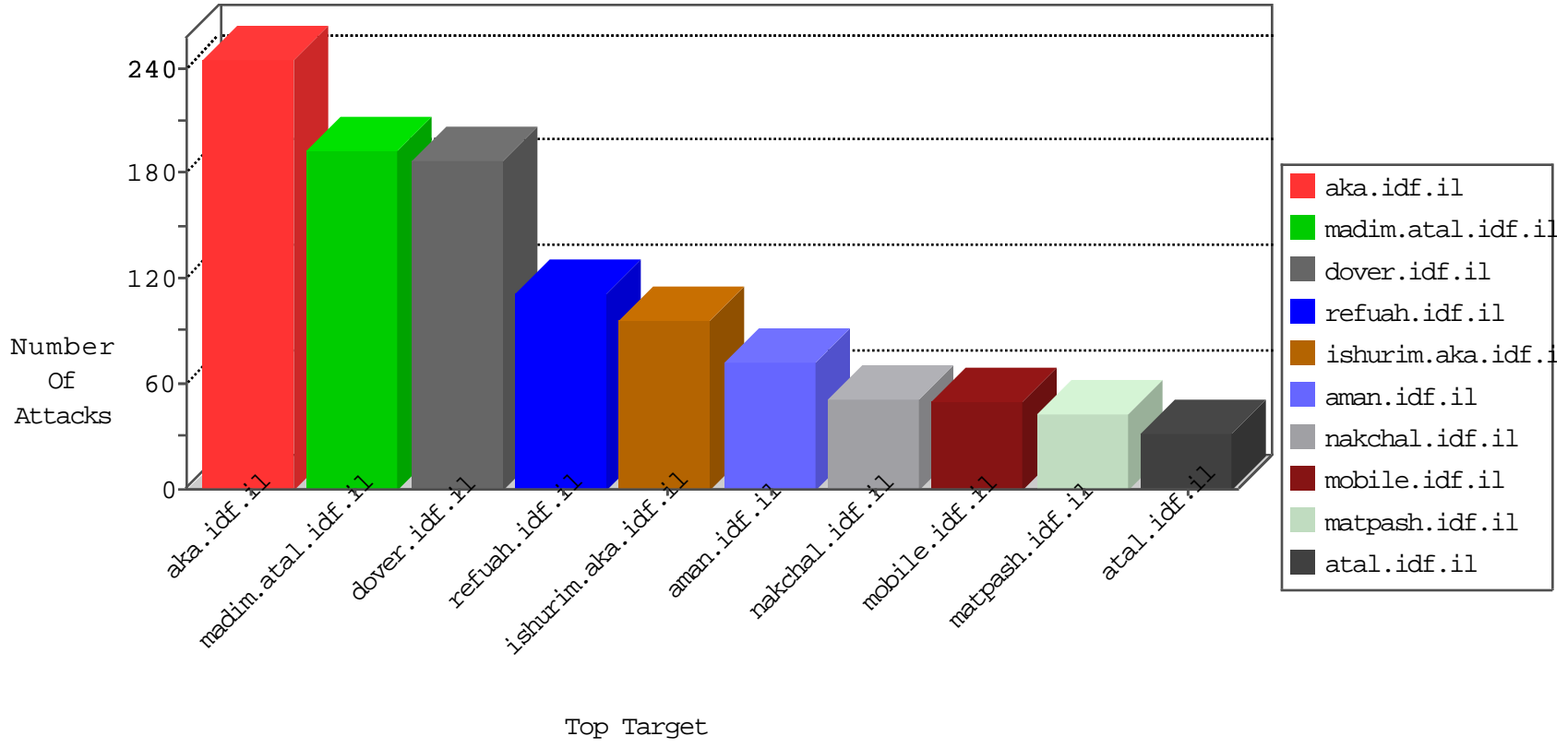


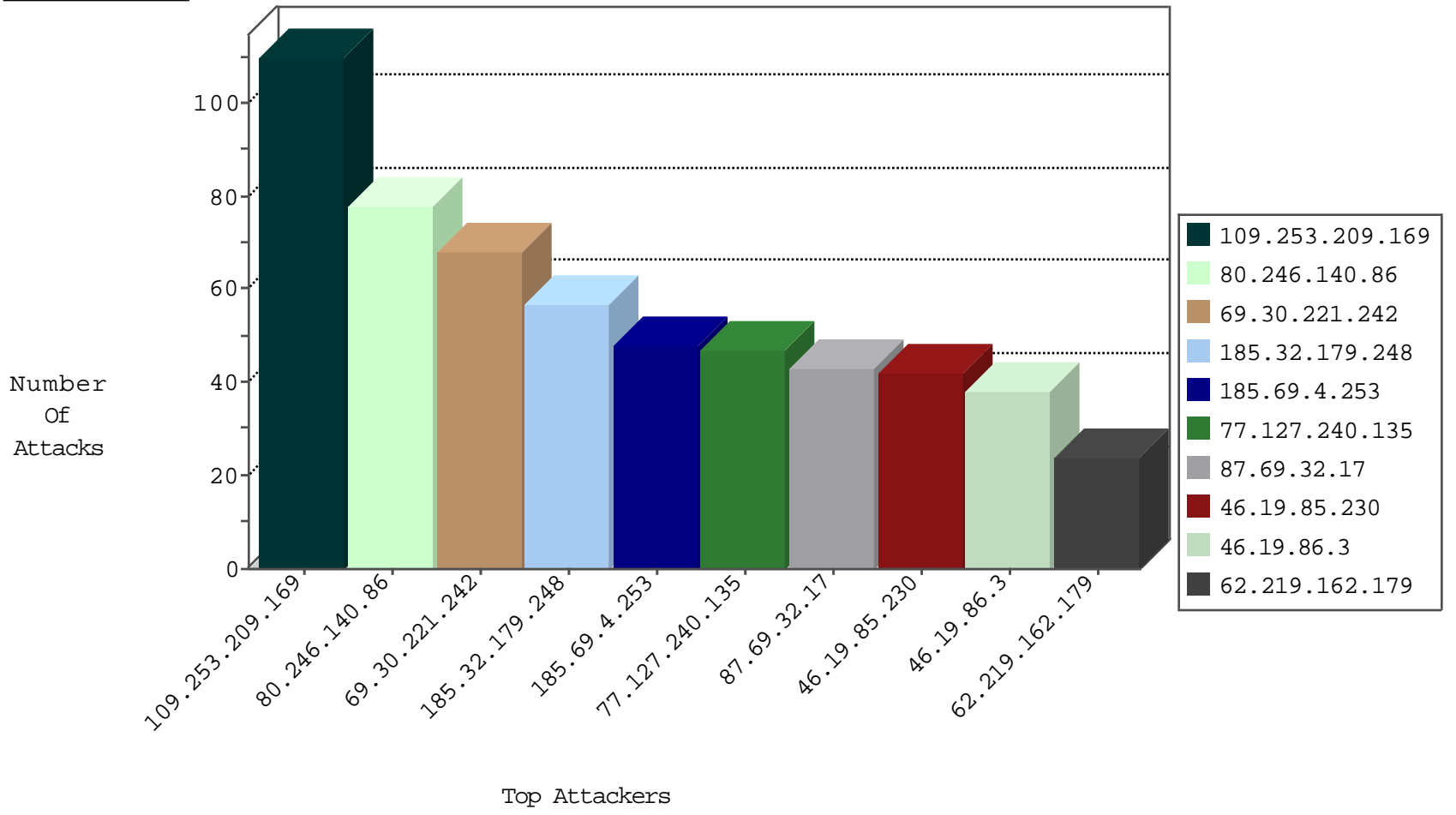
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.247.2.241	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	5
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
185.69.4.253	Iraq	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.217	e.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
222.186.56.41	China	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
193.1.13.12	Ireland	147.237.72.217	e.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
200.19.159.34	Brazil	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
195.113.161.82	Czech Republic	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
46.19.85.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.217	e.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
120.132.50.135	China	147.237.76.86	navy.idf.il	block-sp-trafl	forward	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.221.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	43
69.30.221.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	10
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	9
69.30.221.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	7
69.30.221.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	5
69.30.221.242	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	3

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.172.132.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.202.218.237	147.237.72.166	United Kingdom	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.41	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
84.109.178.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.41	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
79.179.122.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.41	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
66.102.6.115	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
200.195.135.82	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
2.53.156.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.144.56.30	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.64.162.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.240.247.43	147.237.77.226	Korea, Republic of	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
93.158.203.147	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.241.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.41	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
82.80.60.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.41	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
79.177.8.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.164.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.76.61.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.201.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.91.106	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
80.246.140.86	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
46.19.85.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
109.64.162.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
79.177.22.196	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
87.69.32.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
87.69.32.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.3	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.86.3	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
68.14.146.162	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
176.13.244.174	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
95.90.220.152	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
85.64.117.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.147.247	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.69.52.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
77.127.240.135	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.52.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.130.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
185.69.4.253	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
95.90.220.152	Germany	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.189	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
41.223.118.35	Zambia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
87.69.32.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.186	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.186	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.46.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
95.90.220.152	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
176.13.243.126	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
176.13.6.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.145.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
213.6.90.91	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.8.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.6.90.91	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
62.219.147.170	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.154.101.84	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
79.176.55.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.84.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.55.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.39.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.209.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
185.32.179.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
185.69.4.253	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 185.69.4.253	Block	35
62.219.162.179	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	12
109.67.9.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
185.120.125.114	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	10
62.219.162.179	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 62.219.162.179	Block	7
2.53.50.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.229.78.78	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
62.219.162.179	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/4/	Block	5
185.120.125.114	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	4
84.229.78.78	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	3
70.52.98.118	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	3
2.55.182.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.216.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
84.229.78.78	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.229.78.78	Block	2
2.55.44.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
218.101.86.103	New Zealand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/brothers/skira/default.asp	Block	2
37.26.146.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.77.74	law.idf.il	NULL Character in Method	Block	1
66.249.79.122	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/modiin/maslul.aspx	Block	1
37.26.148.177	Israel	147.237.76.42	refuah.idf.il	Multiple URL is Above Root Directory from 37.26.148.177	Block	1
2.53.130.63	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
77.139.194.39	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/kiosk/printablekiosk.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
104.128.144.131	Canada	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/redirect.php	Block	1
46.19.85.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/l.he/scrollpanetop.gif	Block	1
213.143.49.58	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
178.63.101.134	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/miluin/templates/inner.asp	Block	1
66.249.93.202	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.253.241.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.22.196	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.179.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/questionnaire/default.aspx	Block	1
185.120.125.114	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
104.128.144.131	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/redirect.php	Block	1
46.19.85.186	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
81.218.154.153	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
31.154.81.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
213.151.40.158	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
2.53.10.96	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
185.27.105.131	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.93.205	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
141.226.218.68	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluin/templates/inner.asp	Block	1