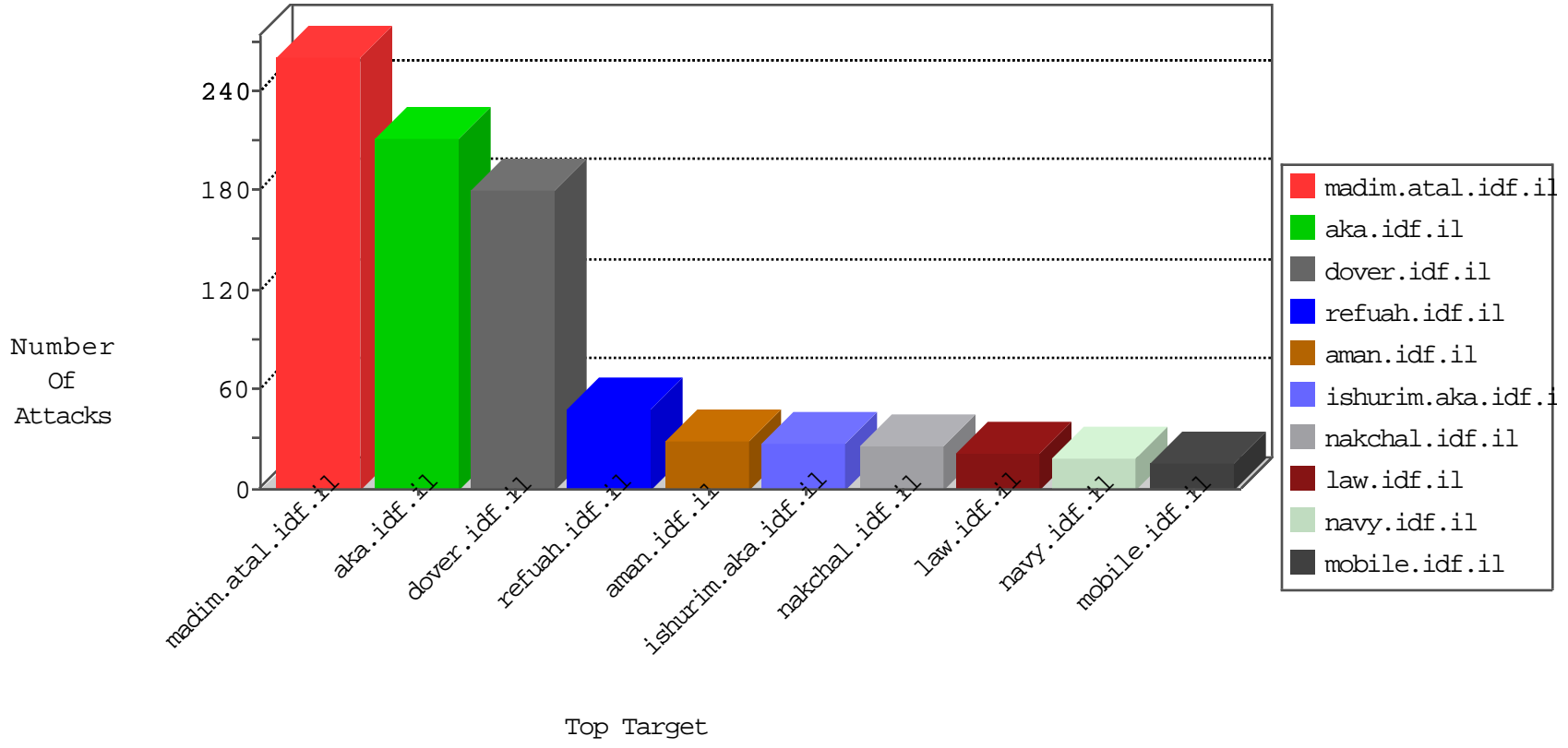


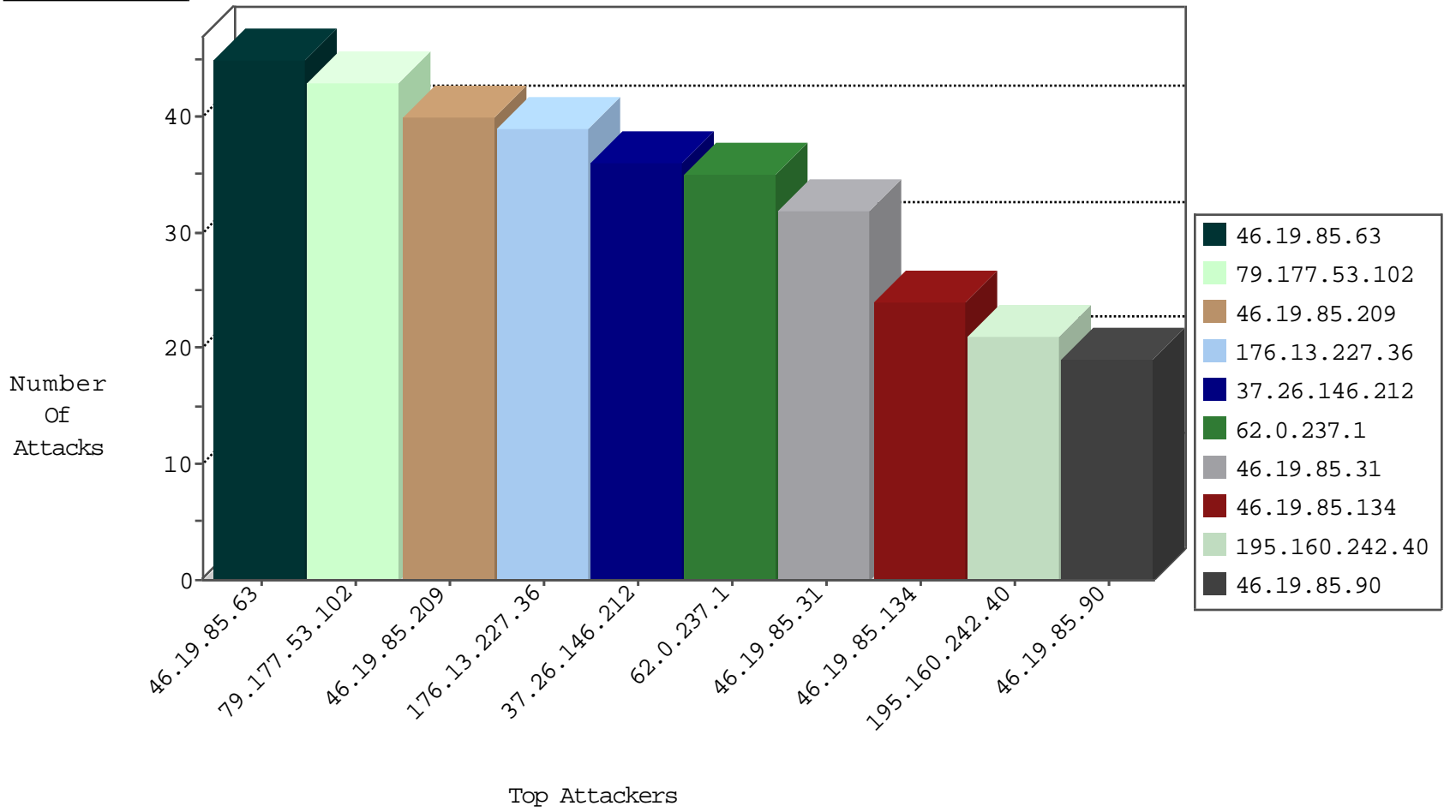
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.55.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.66.56.39	Israel	147.237.76.34	yohalan.idf.il	Black List	drop	1
193.166.167.4	Finland	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
156.56.250.226	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
81.218.208.46	Israel	147.237.77.176	matpash.idf.il	Black List	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
195.113.161.83	Czech Republic	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
81.218.208.46	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-12:04:06 to 09-13-2016-13:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	35
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
62.0.206.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.102	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
46.19.85.241	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.90	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.64	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.150.128.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.90	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
196.138.243.65	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.209	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.68.32.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
188.135.47.155	Oman	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.211.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.90.99.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.134	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.9.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.209	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.134	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.68.32.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.0.209.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
31.168.123.132	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.187	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.25.78.202	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.71.43.172	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
207.232.54.210	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
31.168.125.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.195.162.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.64	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.181.250.64	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.0.227.57	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
212.179.21.194	Israel	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.135.81	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.9.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.29.12.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.193.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.241.218.3	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.133.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.2.122	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.231.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.134.170	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	3
46.19.86.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
192.169.7.223	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
2.53.134.170	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
176.13.227.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
37.26.146.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
79.177.53.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
109.253.215.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
82.81.194.168	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	9
46.120.155.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
82.81.194.168	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 82.81.194.168	Block	6
212.150.128.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 212.150.128.10	Block	5
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	3
77.139.66.76	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	3
109.253.140.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	3
95.35.144.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.81.194.168	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/2/	Block	3
62.90.5.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	2
2.53.58.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr	Block	2
217.194.197.141	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
2.55.52.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.200.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
109.253.128.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter do in www.aka.idf.il/main/giyus/general.aspx	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
46.116.54.34	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	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
87.70.38.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.251.251	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
176.13.18.190	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.128.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ca in www.aka.idf.il/main/giyus/general.aspx	None	1
208.80.155.255	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
84.106.141.18	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
2.53.9.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
141.226.218.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
80.74.103.32	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/	Block	1
109.253.128.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/main/giyus/general.aspx	None	1
46.117.158.75	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
87.203.111.73	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
82.80.193.240	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/1.he/searchback.png	Block	1
77.139.183.254	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
120.27.35.11	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
109.253.128.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter cat in www.aka.idf.il/main/giyus/general.aspx	None	1
62.90.35.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.63	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
84.109.19.126	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1