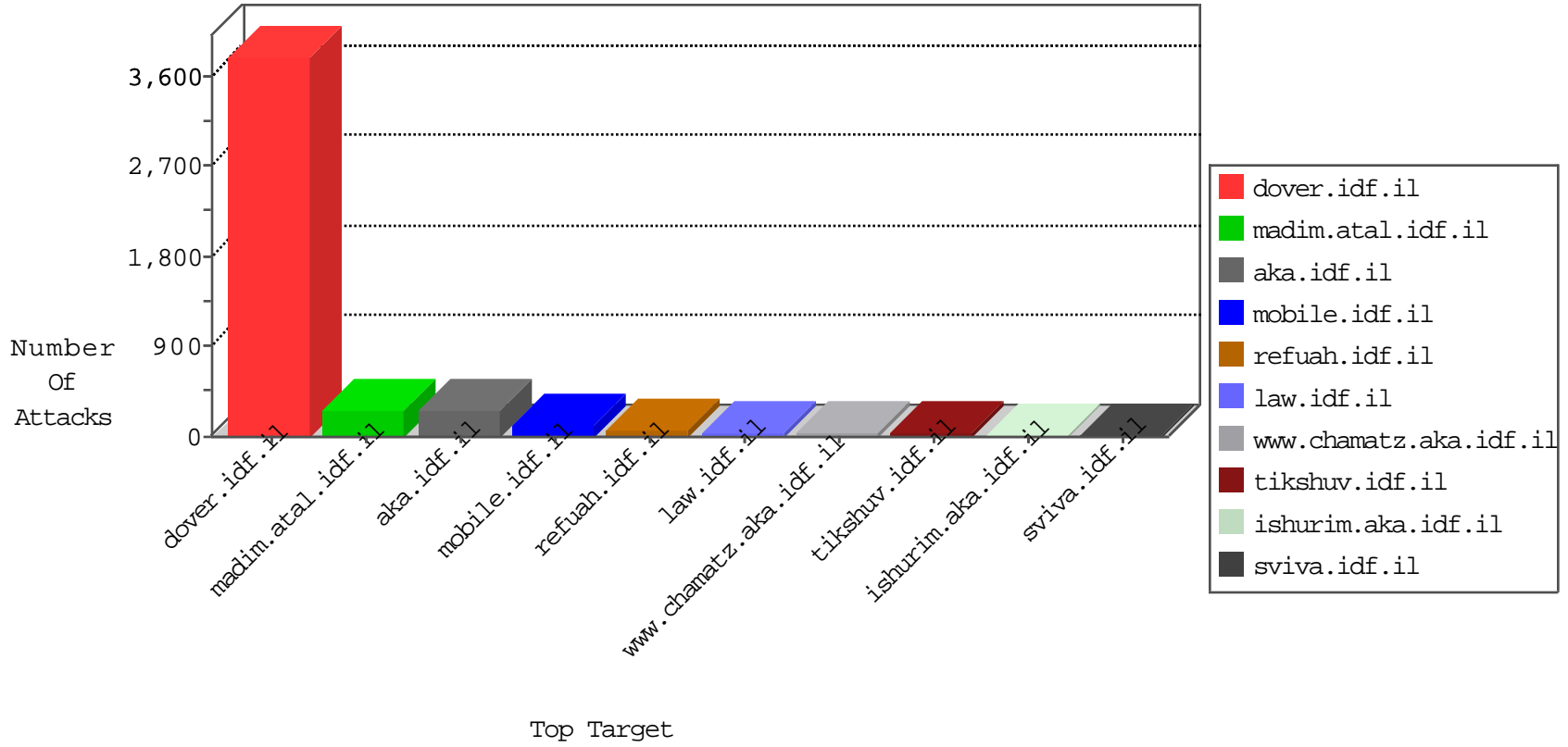


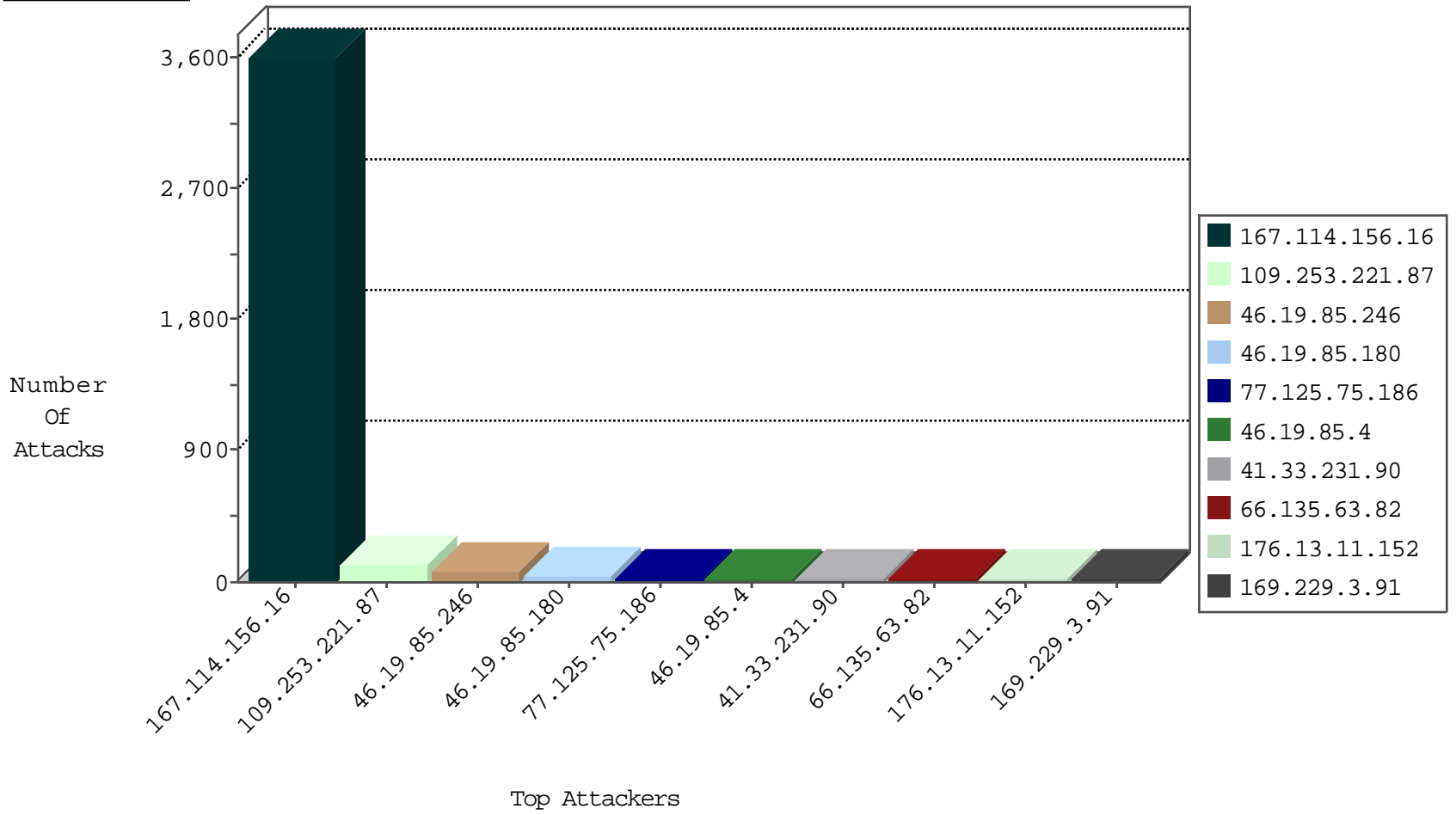
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3603
82.145.209.190	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-trafl	forward	4
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.46.102.242	Romania	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.144.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
87.106.179.116	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
209.173.241.141	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.145.99	Israel	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
41.185.31.40	South Africa	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.135.63.82	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.135.63.82	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.176.124.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.175	France	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.48.104.140	Netherlands	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	1
66.249.66.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.176	France	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.161	France	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.181	France	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.163	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.169	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.135.63.82	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	13
209.173.241.141	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	9
213.8.145.99	147.237.77.74	Israel	law.idf.il	SQL Injection - Select From	8
41.185.31.40	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	7
87.106.179.116	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	7
95.211.70.193	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
176.13.5.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.194.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.130.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.53.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.229.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
82.81.55.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.97	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.56.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.222.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.24.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
85.64.72.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.15.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.126	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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.13.11.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.130.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.100	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	12
176.13.16.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
93.172.155.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.53.191.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.139.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
95.35.16.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
193.47.165.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.102.195.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.114.23.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.31.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.16.15	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.79.123	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.94.106	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.123	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.124	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
109.65.144.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.177.104.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.177.104.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.34	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.34	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
95.86.98.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.176.124.194	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.195.133	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.41.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.217.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.130.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.144.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.178.100.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.104.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
176.13.6.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.22.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.20.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.130.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.179.215.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.221.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	12
2.53.130.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.15.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.130.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
93.172.253.145	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	4
2.55.41.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx	Block	3
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	3
37.48.104.140	Netherlands	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
212.199.176.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
2.55.29.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	3
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.21.30	Block	3
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	2
64.62.219.79	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	2
37.48.104.140	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.48.104.140	Block	2
2.53.191.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.172.253.145	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 93.172.253.145	Block	1
66.249.65.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.109.34.85	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method g*ô6~U+[[#11]]T@éI[[#27]]T[[#30]]q@QwU••[[#2]]žr+Ū'a!K[[#1]]š[[#30]]ôî-ŭç¹[[#17]]ñ>Ū[[#8]]ŪŌP<,[[#19]]-éê²-ê9 in URL	Block	1
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 77.125.75.186	Block	1
37.26.149.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/70202.pdf	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18021en/dover.aspx	Block	1
79.180.62.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx	Block	1
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version <ĂĪ.Ÿ'.•'ô}ss*/[[#12]]zRBD\£[[#3]]ă¶,€Ě[[#14]][[#23]]¢[[#15]][[#20]]©F)Hdfi..."+[[#11]]ŏ,,uĂŸ&šĂ©[[#19]]Ěă>ŸŌĚŅE{əĂ;aps[[#16]]i"[[#22]]K giŌ[[#8]]ZôExU[[#12]]pbm '³#@P\$ô%[[#5]]Ņ	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
5.150.97.127	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.idf.il/1038-en/dover.aspx	Block	1
157.55.39.199	United States	147.237.72.166	aka.idf.il	Unknown Parameter 6683f660 in www.aka.idf.il/main/home/default.aspx	None	1
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
93.172.253.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/9/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
184.14.139.16	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1