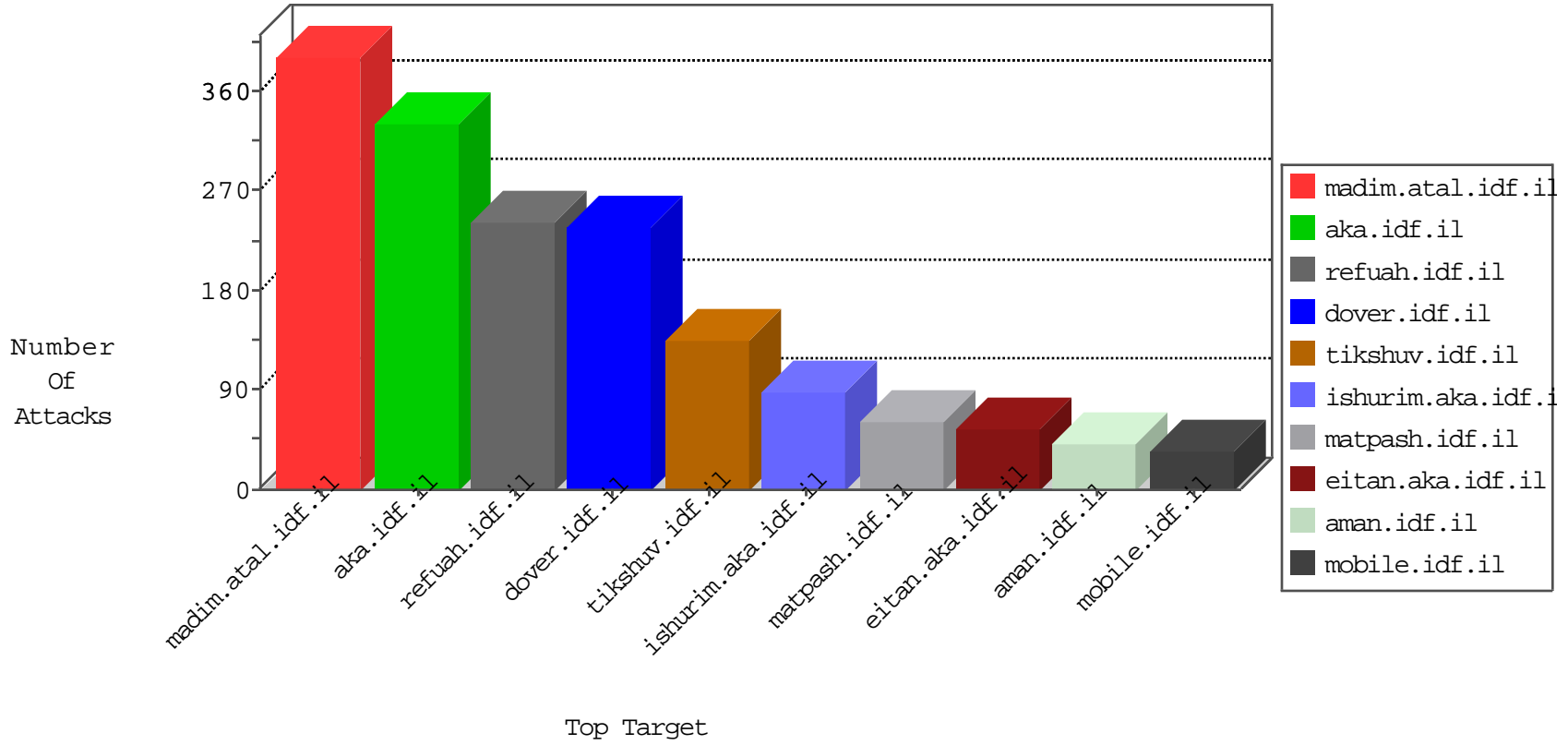


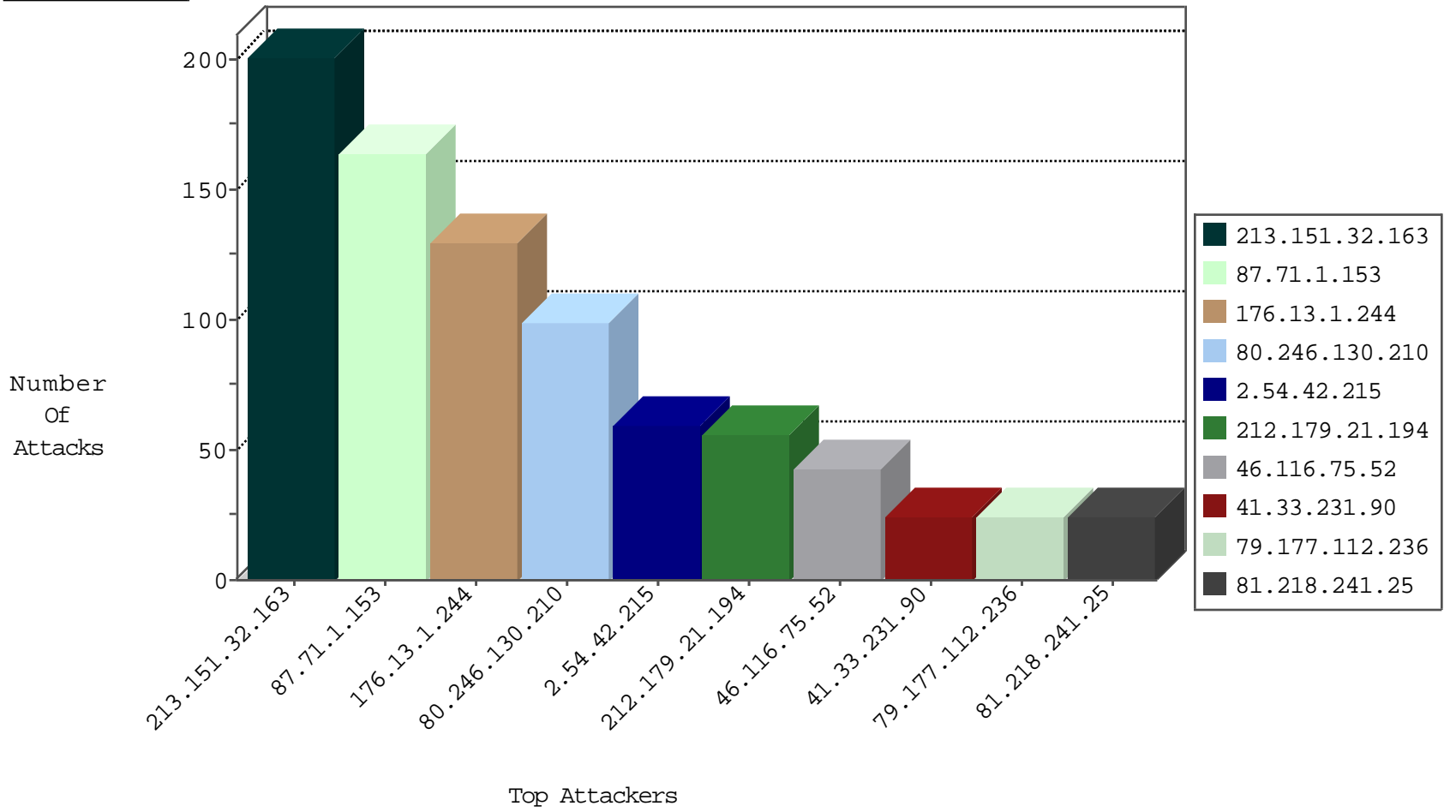
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	36
107.150.33.59	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	forward	1
207.104.161.245	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
173.208.206.202	United States	147.237.77.19	law-forum.idf.il	block-sp-trafl	drop	1
210.140.194.134	Japan	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
173.208.206.206	United States	147.237.77.234	halag.idf.il	block-sp-trafl	drop	1
185.94.111.1		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
37.46.41.95	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.253.157.78	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
79.176.14.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.158.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
80.74.117.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.76	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.11	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.43	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.74	United Kingdom	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
84.111.76.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
176.13.21.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.75.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.207.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.210.187.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.226.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.28.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.149.17	147.237.77.212	Israel	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.157.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.156.86.69	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.66.69	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
212.179.79.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
194.114.146.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
149.78.141.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.37.118.16	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.141.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.225.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.241.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.17.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.76.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.144.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
192.116.160.138	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
87.71.1.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	163
46.116.75.52	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
79.177.112.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	19
194.177.16.3	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.116.151.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.43.117.36	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
62.90.161.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.46.43.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
212.143.103.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.11.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.140.250	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.179.209.129	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.179.209.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
87.71.31.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.32.179.167	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.46.41.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.167	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.179.96.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
217.21.10.89	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
82.80.17.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
2.54.27.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.32.179.167	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
83.244.91.184	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
176.13.11.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
81.209.177.189	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.178.135.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.165.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
82.80.17.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.53.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.7.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
81.218.40.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.6.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.207.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.57.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.52.7.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.76.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	201
176.13.1.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
80.246.130.210	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
2.54.42.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
176.13.1.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Illegal Response Code	None	24
81.218.251.251	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
66.220.145.244	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
185.89.217.233		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.59	Block	4
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
5.29.163.16	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
81.209.177.189	Europe	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 81.209.177.189	Block	3
83.244.91.184	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	2
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.19.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	2
192.99.39.235	Canada	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	2
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
37.46.38.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.253.215.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
2.54.37.254	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
84.228.37.32	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.9.189	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.26.146.129	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.66.1.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
212.25.102.63	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
62.0.25.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.86.151	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
149.78.139.60	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
5.29.24.197	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.179.183.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
108.53.133.168	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
192.114.23.208	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.231.192.149	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.31	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
82.80.192.100	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.253.196.171	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
213.57.201.254	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
212.143.99.102	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
62.219.114.124	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
87.69.36.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.26.149.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.246.137.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$27 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.67.136.163	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/error.png	Block	1
79.181.118.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.64.200.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
199.255.138.45	United States	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1