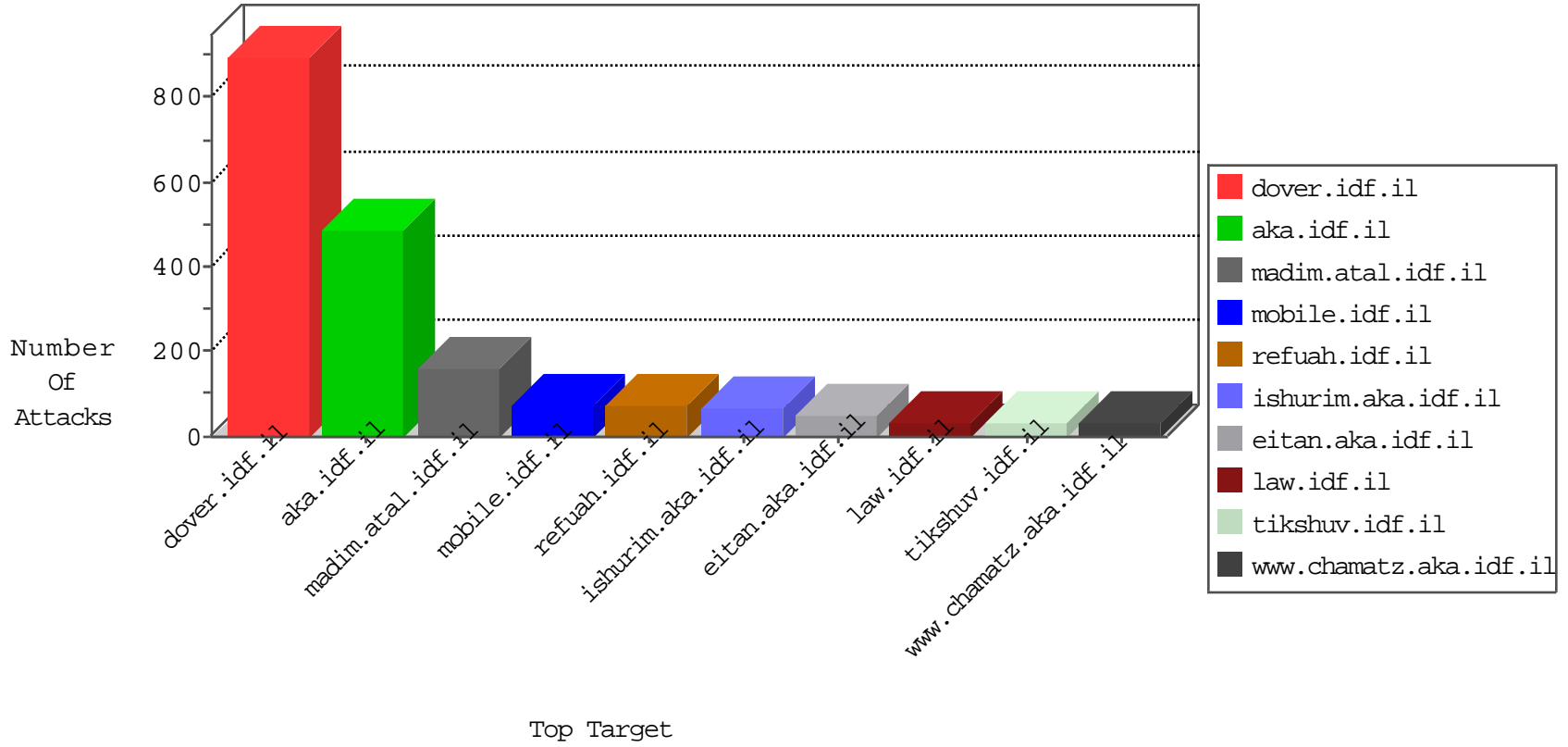


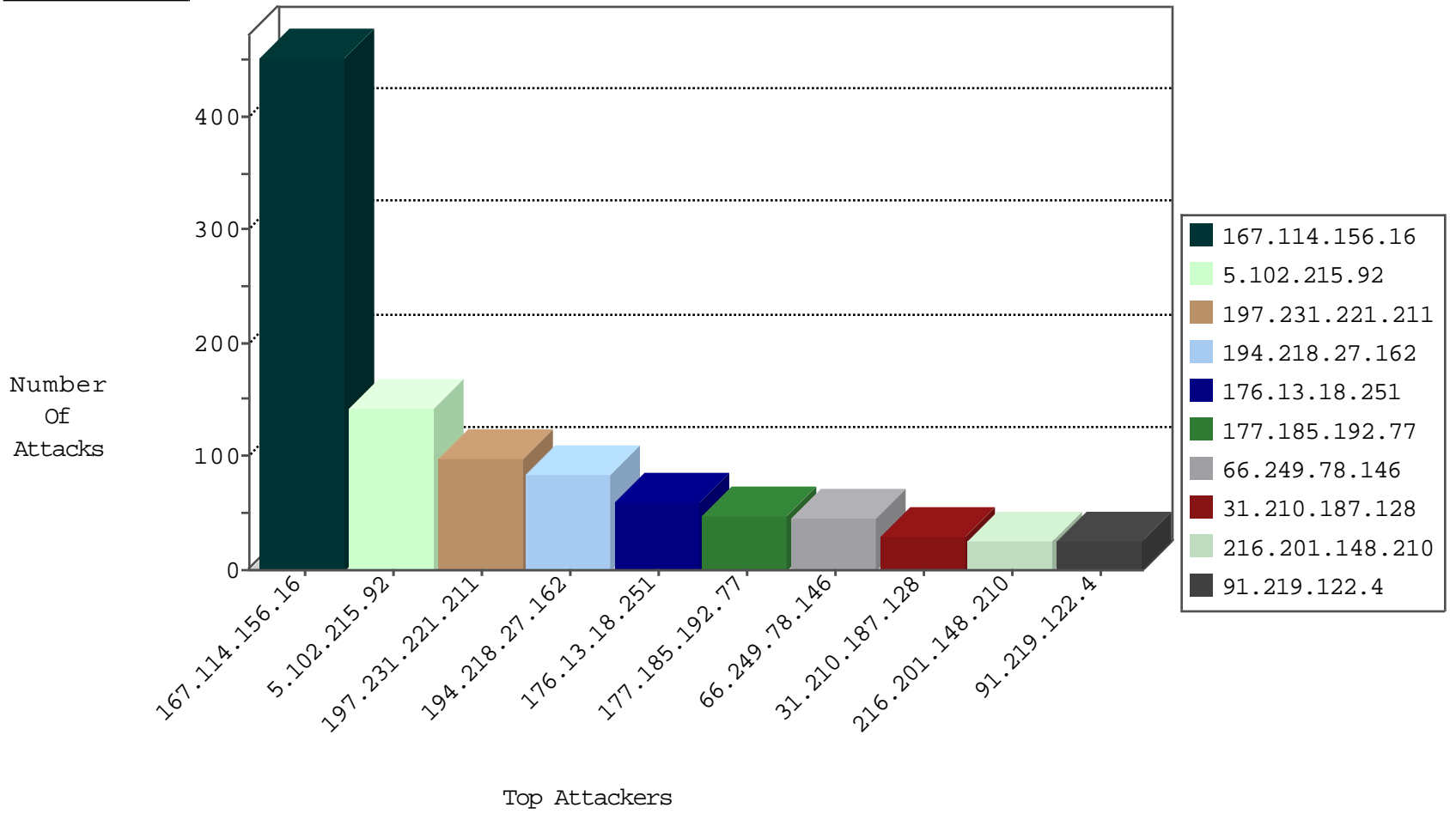
IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	16798
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4940
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4292
79.176.30.14	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	203
213.57.251.224	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	102
89.138.80.74	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
149.88.106.86	Israel	147.237.72.166	aka.idf.il	Anomaly-TCP-SYN-FIN	dest-reset	3
149.88.106.86	Israel	147.237.72.166	aka.idf.il	Anomaly-TCP-shortheadr	dest-reset	2
84.109.152.5	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
85.250.51.251	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
188.138.17.205	France	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.146.186	United States	147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.201.148.210	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
91.219.122.4	Poland	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
177.185.192.77	Brazil	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
91.219.122.4	Poland	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
37.205.0.49	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.89.19.29	Turkey	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.143.34.37	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
158.85.253.245	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
67.228.38.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.192.77	Brazil	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
177.185.192.77	Brazil	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
204.12.168.26	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.192.77	147.237.76.42	Brazil	refuah.idf.il	SQL Injection - Select From	35
216.201.148.210	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	14
91.219.122.4	147.237.77.226	Poland	www.chamatz.aka.idf.il	SQL Injection - Select From	14
63.143.34.37	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	12
67.228.38.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
37.205.0.49	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	6
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
93.89.19.29	147.237.77.216	Turkey	dover.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
82.166.247.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
213.16.45.243	147.237.76.200	Bulgaria	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
190.142.24.209	147.237.8.27	Venezuela	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
213.16.45.243	147.237.76.200	Bulgaria	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
176.13.18.251	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
31.210.187.128	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.5.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.12.127.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.152	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
87.68.4.9	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
188.139.193.98	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
188.139.193.98	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
66.249.93.43	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.64.155.142	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.177.175.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.177.18.223	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
95.86.104.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.177.175.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.188	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.137.27	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.79.84	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.139.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.22.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
88.136.210.94	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.215.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.165.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.175.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
185.120.125.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
88.136.210.94	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.215.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
46.19.85.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.53.11.232	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.11.232	Block	6
109.253.221.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.115.184.150	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	3
109.160.169.252	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.135.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.79.168.215	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.5.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.228.188.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.27.105.181	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.146.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.215.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
93.172.147.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
157.55.39.53	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18630-he/dover.aspx	Block	1
46.19.85.194	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.165.230	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
109.122.5.54	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
85.65.102.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
37.26.146.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sacgghar/home.aspx	Block	1
95.86.92.31	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
79.179.130.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsuneymofet.aspx	None	1
2.55.140.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
109.122.5.54	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
87.71.61.23	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal/izkor/print_text.asp	Block	1
199.79.170.215	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
132.74.151.43	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
104.172.208.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
2.53.11.232	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
79.183.12.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.117.182.254	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
2.55.174.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
109.122.5.54	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	1
88.136.210.94	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.57.252.78	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.113	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /x	Block	1
107.20.92.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.53.22.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.130.249	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
51.255.65.26	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
88.136.210.94	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
149.88.161.64	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
46.19.85.158	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
108.26.200.145	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1