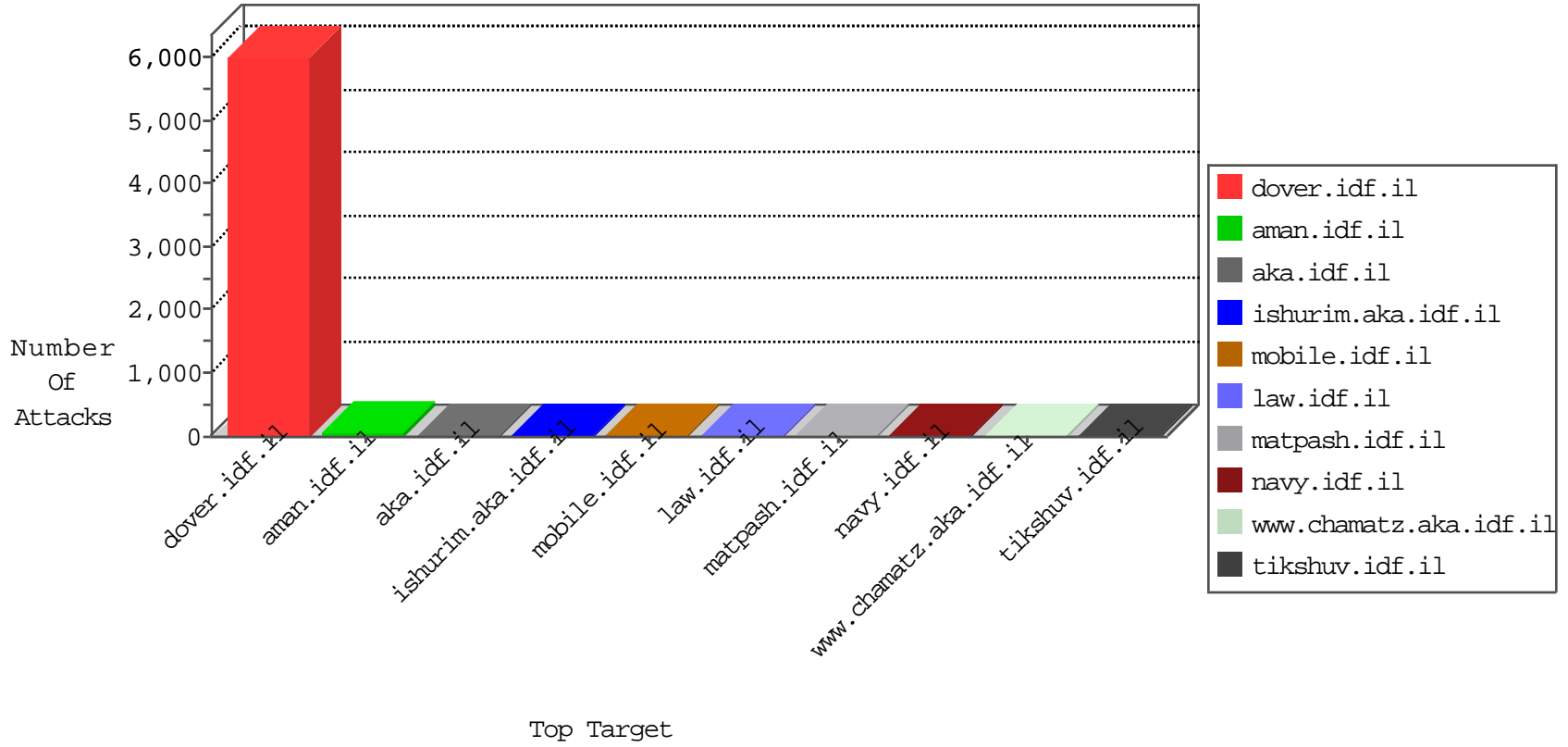
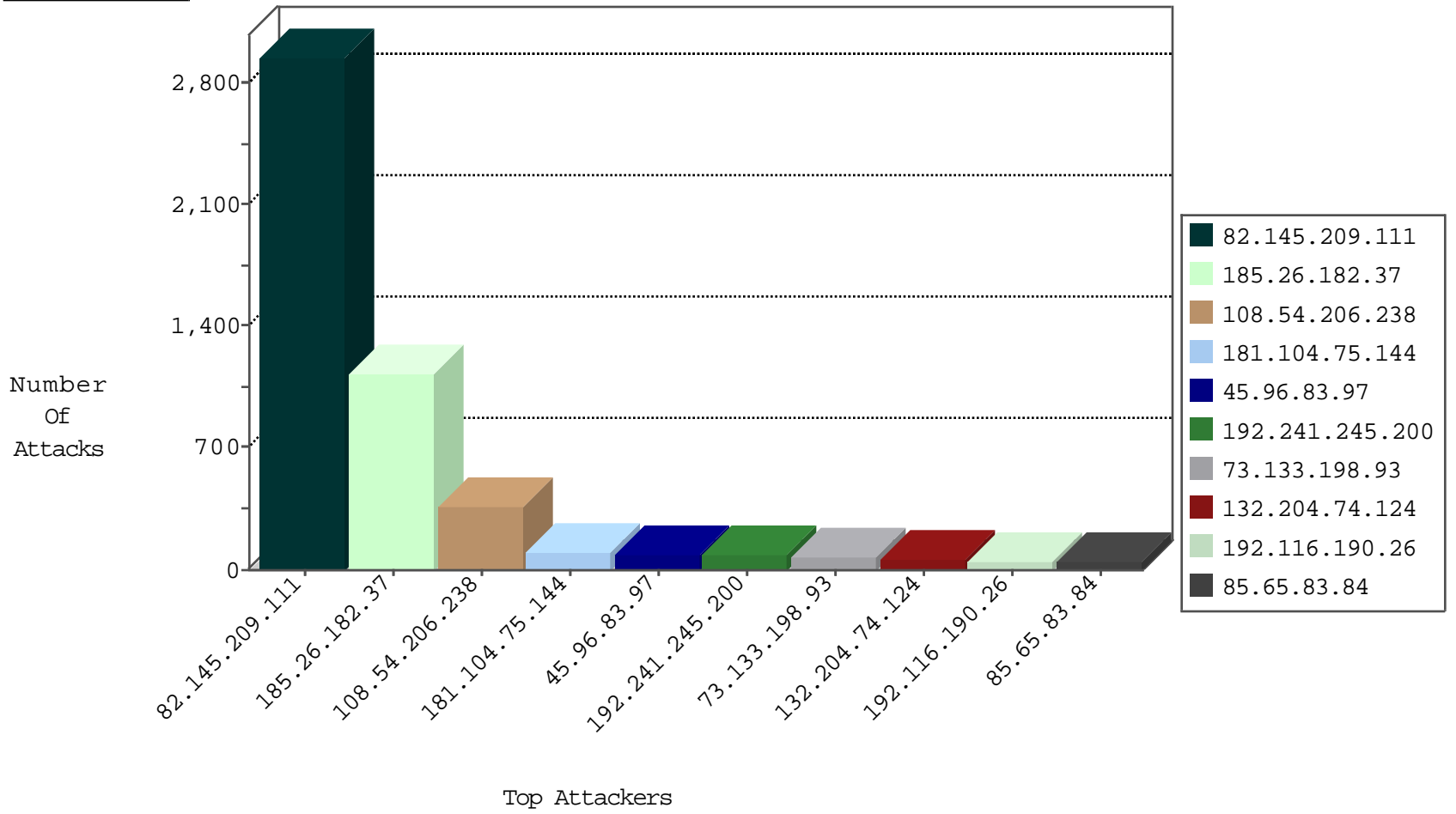




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.180.178.147	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	331
220.181.108.149	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	183
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
82.145.209.111	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23
84.108.34.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
208.201.234.242	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
5.102.254.132	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.3.207.66	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.255	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.46	e.chimuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
87.68.252.16	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.227	e.haraz.idf.il	DVRep_B-N_60_100	Block	1
188.225.154.202	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
37.142.93.224	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.248.160.215	Netherlands	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.240.162	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
194.157.118.114	Finland	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
60.18.162.244	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.4	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.215	Netherlands	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.160.215	Netherlands	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.69.94.13	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
194.157.118.114	Finland	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.4	China	147.237.76.198	e.yochanan.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.50	Netherlands	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.209.111	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2943
185.26.182.37	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1120
108.54.206.238	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	360
181.104.75.144	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	96
45.96.83.97		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	84
192.241.245.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	83
73.133.198.93	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	73
132.204.74.124	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
192.116.190.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
93.173.1.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
93.172.92.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
93.172.171.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
24.187.146.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
80.246.130.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
70.89.4.9	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
212.143.136.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
2.54.177.205	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
66.102.8.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
149.78.236.216	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
96.243.244.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
5.28.133.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
184.151.179.154	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.86.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
82.166.20.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
212.76.108.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.182.50.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
85.250.25.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
80.246.130.65	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
79.181.116.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
37.142.93.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
213.57.183.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
213.205.251.130	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.102.8.178	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
213.6.217.236	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.108.34.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
195.241.217.181	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
5.102.254.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
31.25.78.83	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	7
149.88.107.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.65.11.35	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	15
87.69.35.60	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	11
68.173.251.170	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	4
81.144.138.34	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
195.242.218.133	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.141	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/modiin/general	Block	2
85.250.43.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.125.96.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.37	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to ww.logistics.atal.idf.il/size338x0/sip_storage	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.81.85.102	Spain	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 62.81.85.102	Block	1
82.145.221.39	Europe	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/012804-1.stm	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/fund/x303E'0QaeM03aes 02A-03E'x'a,-Aš03aes02Aç03E'x'a,-Aš03aes02A¼x303E'0QaeM03aes 02A-03E'x'a,-Aš03aes02Aç03E'x'a,-Aš03aes02A¼x303E'0QaeM03aes 02A-03E'x'a,-Aš03aes02Aç03E'x'a,-Aš03aes02A¼x303E'0QaeM03aes 02A-03E'x'a,-Aš03aes02Aç03E'x'a,-Aš03aes02A¼	Block	1
66.249.67.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6363-he/patzar.aspx	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.132.204	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
79.179.12.251	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-4189-he/patzar.aspx	Block	1
62.81.85.102	Spain	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 62.81.85.102	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
207.46.13.130	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1070-he/nakhal.aspx	Block	1
54.88.168.129	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7488-he/tikshuv.aspx#.vuvjizptrhu	Block	1
148.234.86.214	Mexico	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
79.179.185.64	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6366-he/patzar.aspx	Block	1
157.55.39.199	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.64.249	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/general	Block	1
85.250.7.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
68.173.251.170	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/main/home/default.aspx	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
212.179.42.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.81.85.102	Spain	147.237.72.156	aman.idf.il	Abnormally Long Request request version	Block	1
157.55.39.101	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1071-he/nakhal.aspx	Block	1
79.180.209.147	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
180.76.5.23	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.78.29	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
213.57.183.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18645-</div></div></div><!-- google_ad_section_end --><div class=	Block	1
62.81.85.102	Spain	147.237.72.156	aman.idf.il	Illegal HTTP Version + url + ' HTTP/1.1	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/homefront/hebrew/ie-id.stm	Block	1
66.249.67.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
31.154.5.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.96.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1