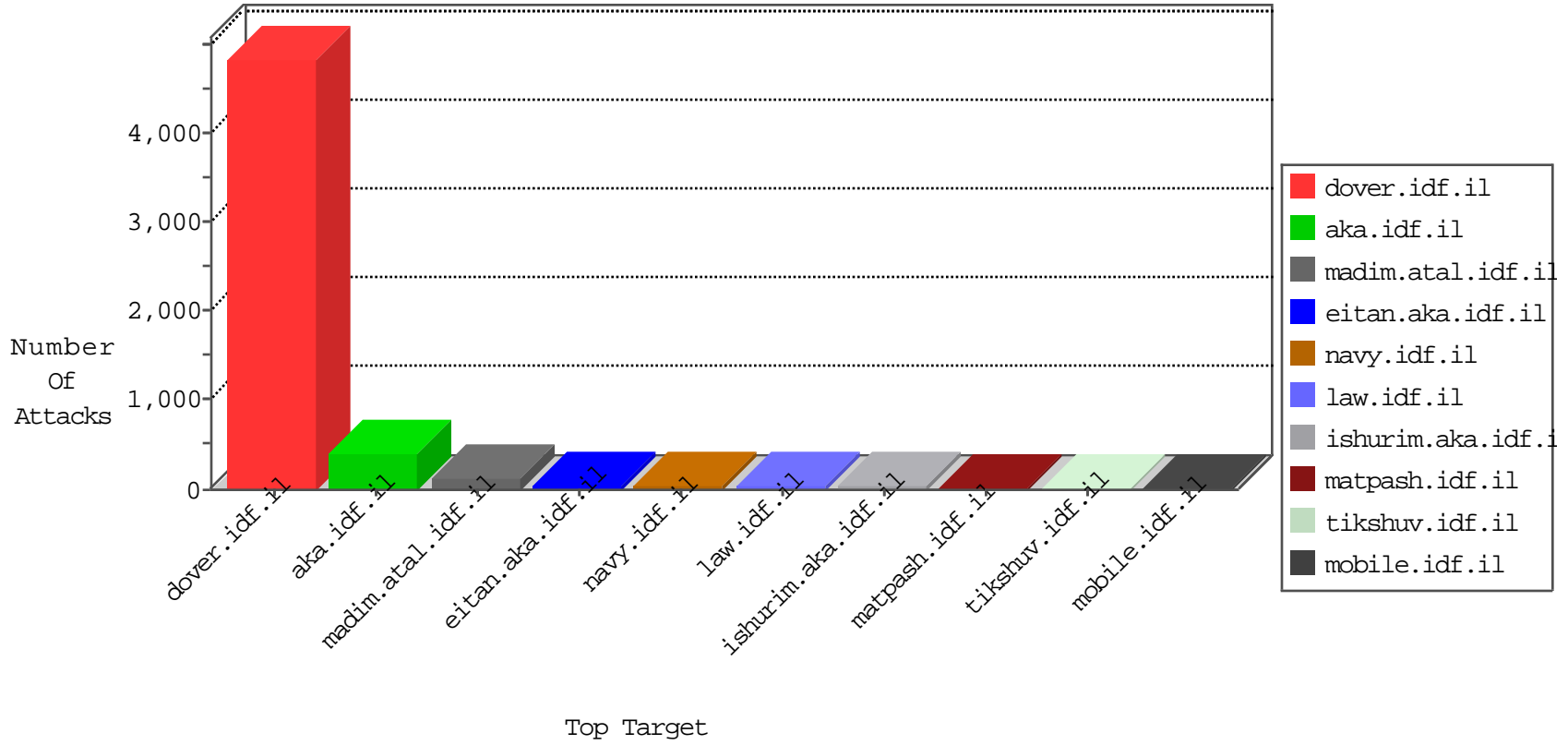


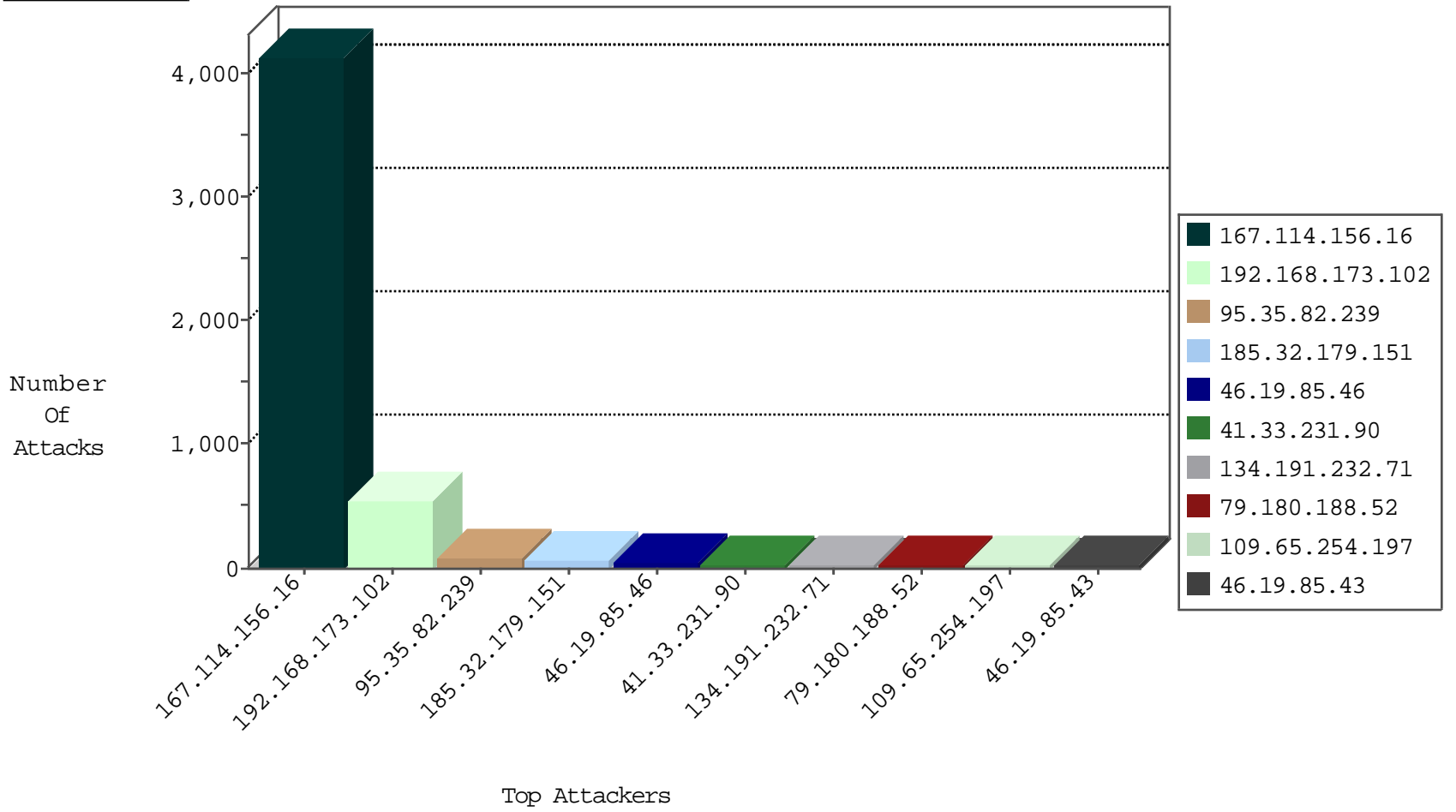
IDF Under Attack Daily Report



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	4118
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1087
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
186.202.162.108	Brazil	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	3
46.19.85.106	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.110.108.153	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
46.19.85.37	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
188.120.148.6	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
197.28.190.16	Tunisia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
110.76.40.33	China	147.237.8.28	e.mobile-ks.idf.il	Invalid TCP Flags	drop	1
2.54.164.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
177.65.133.159	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
115.28.27.173	China	147.237.77.121	e.navy.idf.il	L4 Source or Dest Port Zero	drop	1
219.232.243.28	China	147.237.77.121	e.navy.idf.il	L4 Source or Dest Port Zero	drop	1
115.159.150.148	China	147.237.76.44	e.refuah.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.22.159	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
163.172.13.244	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
163.172.13.244	United Kingdom	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
163.172.13.244	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
210.129.20.209	Japan	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
139.162.192.213	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
85.90.244.226	147.237.77.74	Germany	law.idf.il	ET SCAN Potential SSH Scan	1
77.125.117.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.143.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
107.170.174.151	147.237.0.15	United States	kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
80.178.115.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.28.116	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	343
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	194
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.180.188.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
82.80.168.133	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
134.191.232.71	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
37.26.146.155	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.178.181.184	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.85.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.125.114.222	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.254.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.84	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
141.0.15.121	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.55.29.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
79.183.62.30	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.65.254.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.22.131.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.155	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.66.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.124	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
37.26.146.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.210	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.38.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.205.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.65.254.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
134.191.232.71	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.242.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.3.144.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.140.51	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.180.18.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
87.70.98.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.31.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.54.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
134.191.232.71	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
185.120.125.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.204.47	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.28.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.85.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.31.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.146.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
177.65.133.159	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
156.203.85.136	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.249.66.59	United States	147.237.0.34	tikshuv.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
95.35.82.239	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.35.82.239	Block	63
185.32.179.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
79.182.185.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.132.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
95.35.165.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.135	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	3
2.53.31.225	Israel	147.237.72.166	aka.idf.il	Multiple Extremely Long Parameter from 2.53.31.225	Block	3
210.129.20.209	Japan	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.173.225	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authentication-service.asmx/getauthuser	Block	2
37.26.149.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.43.111.255	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
157.55.39.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.109	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.109	Block	2
109.65.220.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.35.82.239	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.not	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	1
46.19.85.160	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
197.117.240.59	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.183.173.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.173.225	Block	1
186.2.136.203	Honduras	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.0.103.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.129	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /x	Block	1
210.129.20.209	Japan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 210.129.20.209	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
177.65.133.159	Brazil	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
110.86.186.223	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
2.52.163.191	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
192.116.128.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14276-he/dover.aspx	Block	1
149.50.41.53	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
210.129.20.209	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
105.158.241.76	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.93.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
181.90.176.60	Argentina	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
2.53.31.225	Israel	147.237.72.166	aka.idf.il	Extremely Long Parameter in www.aka.idf.il x@x-x-x*x" xjx™xjxžx• x'x•x^x" xçx•xœx™x• xçxœ xžx"x™x• x^x•x"x™xš: x™x•x• x"x•x@x•xÿ, x•xœx"x	Block	1
207.46.13.58	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
94.231.235.107	Poland	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
41.102.136.72	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
107.170.174.151	United States	147.237.0.15	kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1