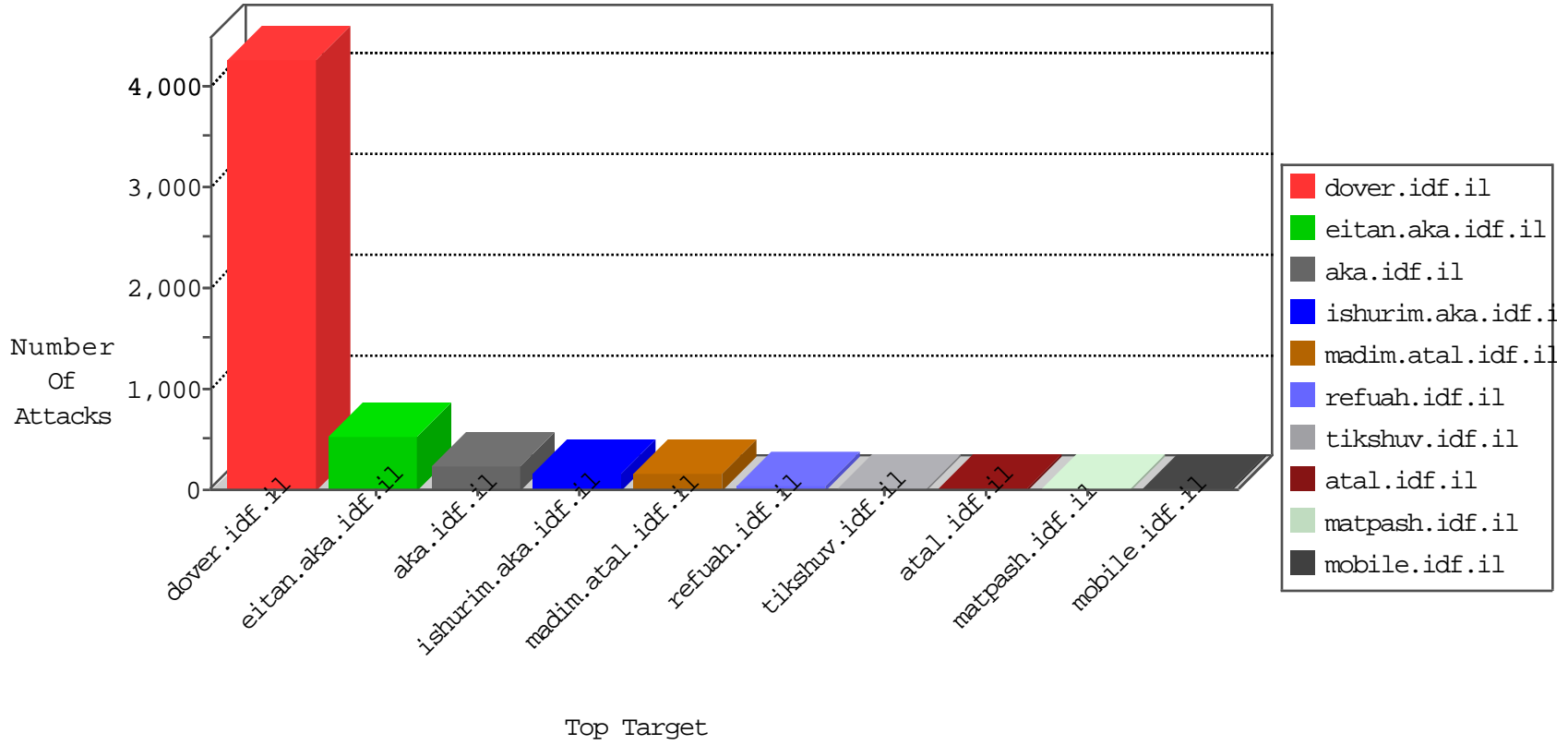


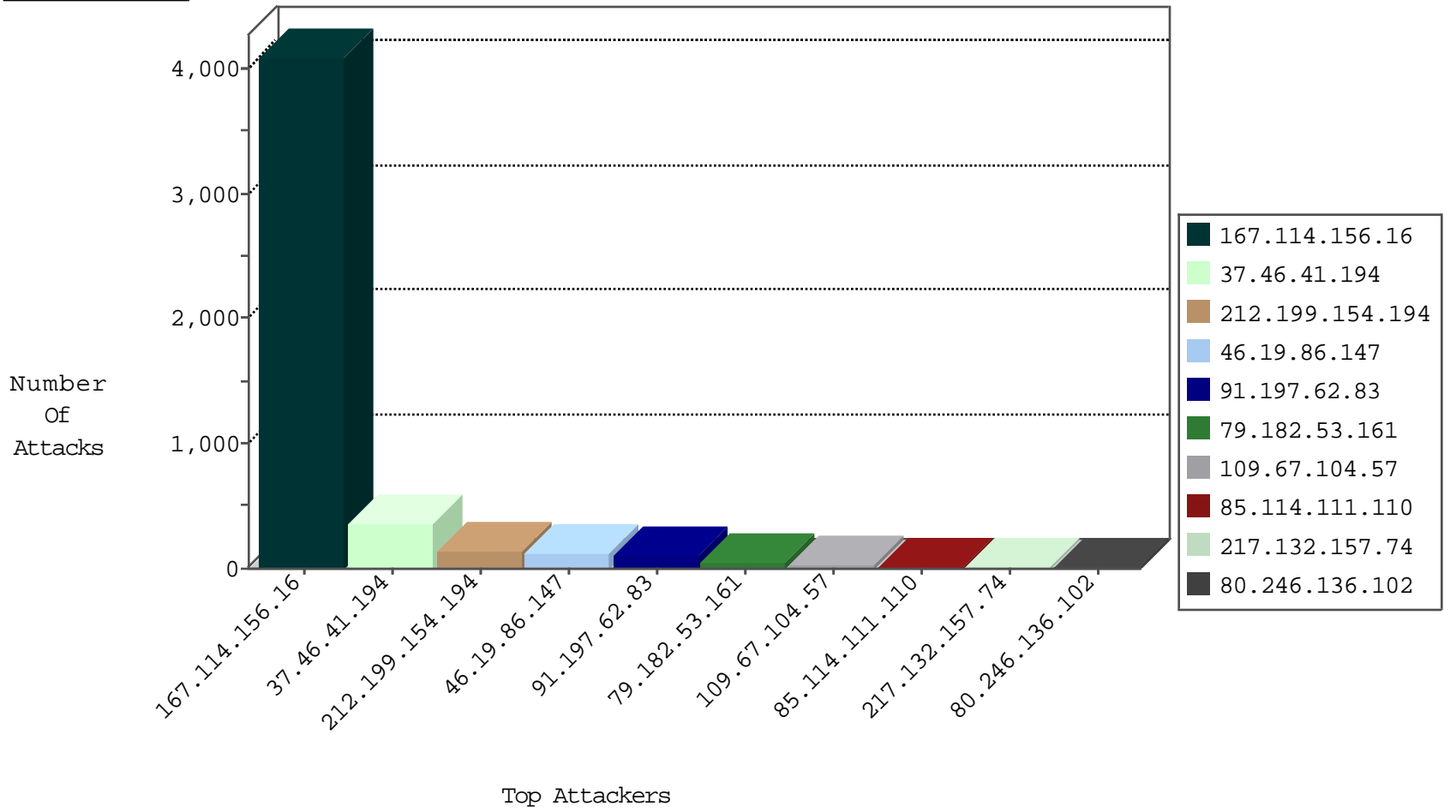
# IDF Under Attack Daily Report



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	4085
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	895
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
168.243.25.9	El Salvador	147.237.76.202	e.halag.idf.il	I4 Source or Dest Port Zero	drop	2
184.105.139.118	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.98	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.90	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.121	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
184.105.139.94	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## 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	2
196.203.149.99	147.237.76.200	Tunisia	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
149.88.240.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.214.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.223.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.203.149.99	147.237.76.200	Tunisia	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
82.80.86.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.223.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
41.232.89.224	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.214.130	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
37.46.41.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	333
91.197.62.83	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	54
79.182.53.161	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
85.114.111.110	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
217.132.157.74	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.67.104.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
109.67.104.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
80.246.136.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
2.55.59.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
153.150.118.170	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.46.41.194	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
194.114.62.160	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.46.39.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.156.7.2	Finland	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.165.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.145.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.21.241	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.4.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.84.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.21.241	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
188.120.154.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
31.168.182.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.141.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.82	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
79.180.32.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.7.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.98.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.28.190.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.99.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.33.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.93.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-19-2016-10:04:02 to 04-19-2016-11:04:02

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.116.143.232	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.183.177.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.190	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
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
176.13.13.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
62.219.21.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.21.20	Block	4
46.19.85.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
188.120.148.134	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
203.171.241.78	India	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.225.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.30.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
81.218.70.243	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	2
109.253.225.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.159.123	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	2
79.181.145.233	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.181.145.233	Block	2
109.253.217.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.0.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
66.249.66.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69051.pdf	Block	1
157.55.39.248	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
23.81.90.154	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
91.197.62.83	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
208.113.248.22	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
74.91.23.166	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.8.193	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1783-he/refuah.aspx	Block	1
213.8.204.37	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.128.144.131	Canada	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19817-he/dover.aspx	Block	1
176.13.4.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
91.197.62.83	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;rnd in www.eitan.aka.idf.il/shared/ajax/createcaptchaimage.aspx	None	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$cphSachar\$ctl167 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
176.13.21.241	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.124.7.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
216.218.206.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
104.128.144.131	Canada	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
195.156.7.2	Finland	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
81.218.146.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
176.13.5.39	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/mobile	Block	1
115.187.39.251	India	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.197.62.83	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;t in www.eitan.aka.idf.il/scriptresource.axd	None	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
185.37.148.18	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.37.148.18	Block	1
79.181.134.155	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_campaign in www.aka.idf.il/main/rabanut/general.aspx	None	1
5.9.136.219	Germany	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 5.9.136.219	Block	1
109.67.104.57	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1