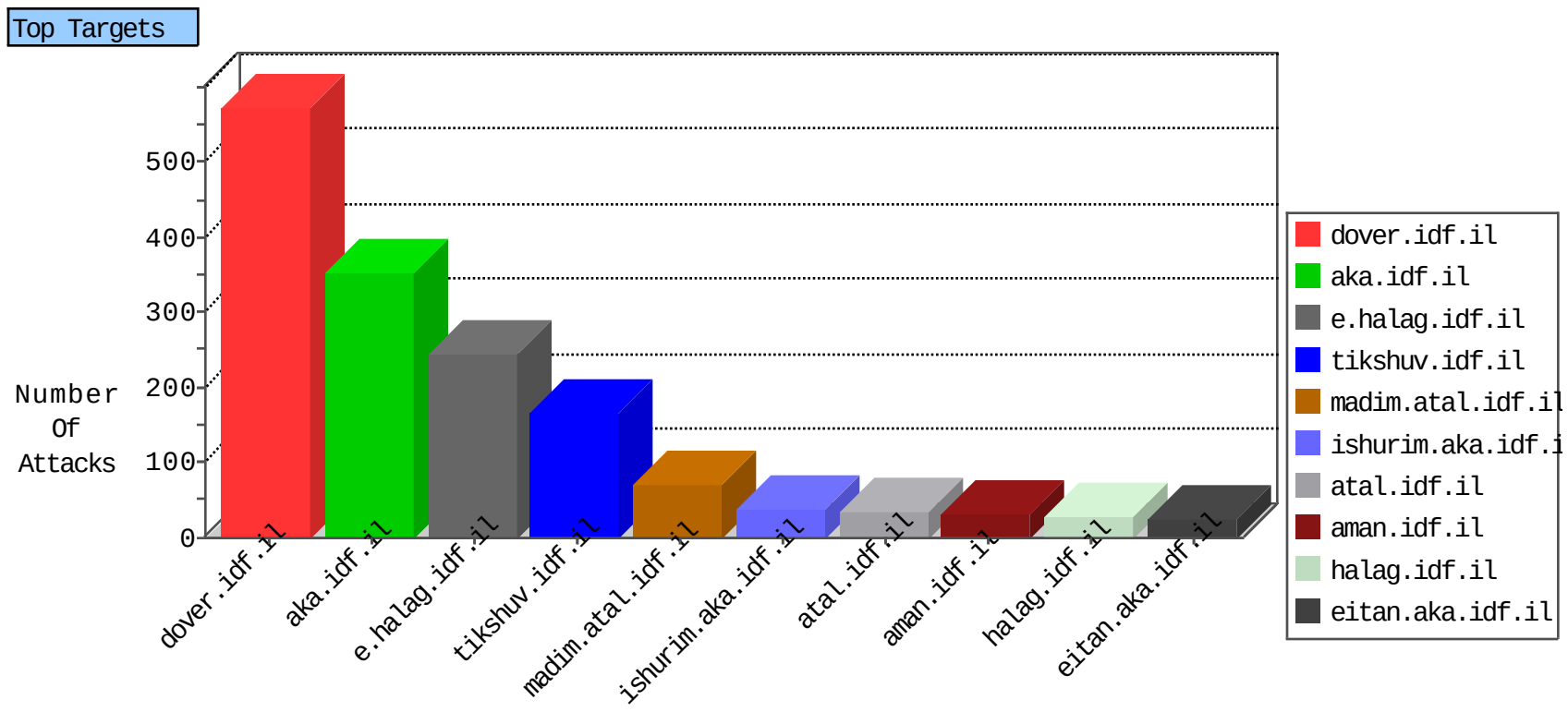
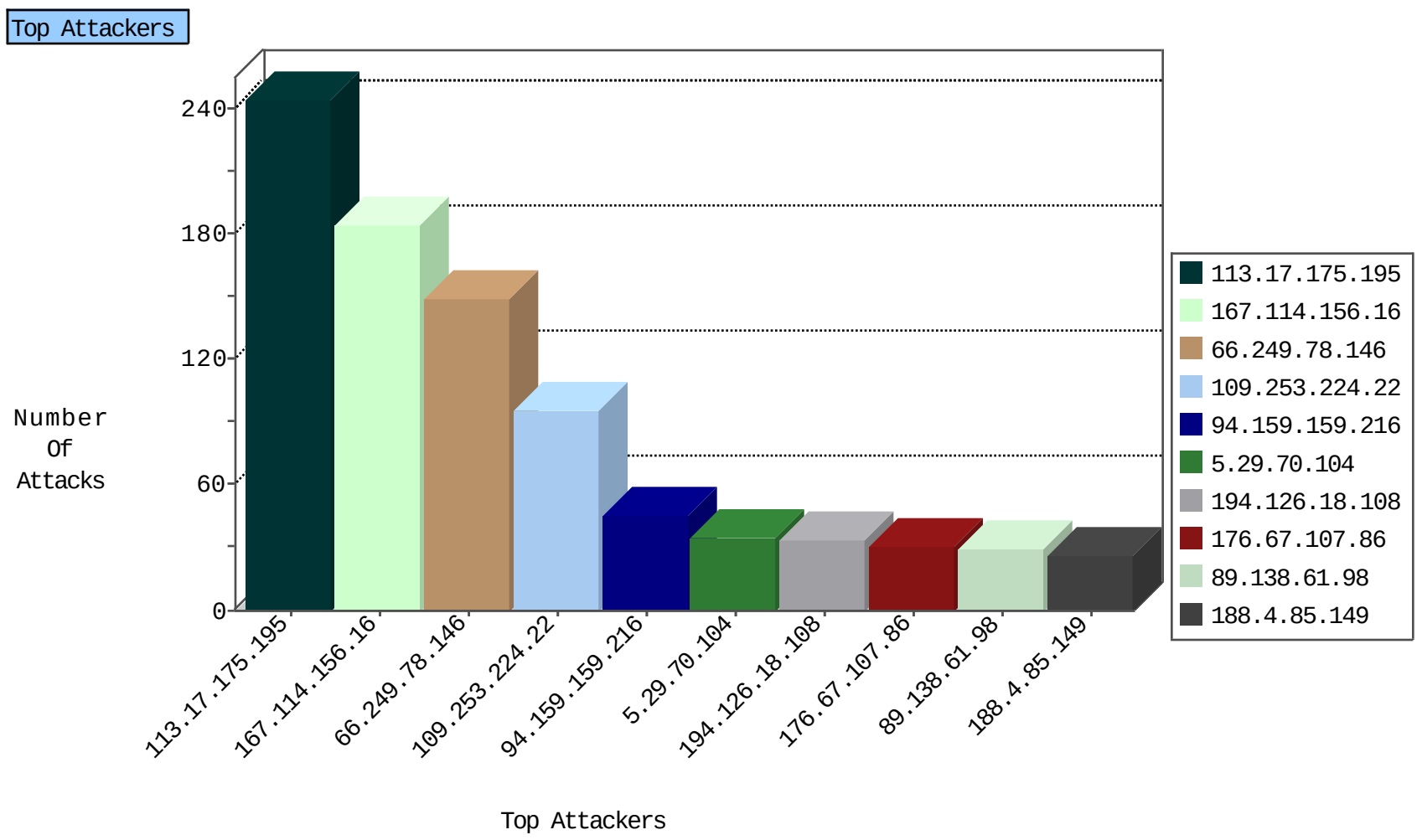
04-24-2016-19:04:07 to 04-24-2016-20:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-24-2016-19:04:07 to 04-24-2016-20:04:07

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	9099
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	804
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	245
109.65.90.27	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	206
79.180.59.194	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	202
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.64.109.103	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
74.91.20.198	United States	147.237.72.167	ishurim.aka.idf.i	block-sp-traf1	drop	1
71.6.158.166	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
79.179.131.155	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
176.67.107.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.102.52.10	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
74.91.18.43	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
69.30.198.146	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
185.27.106.14	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
107.150.46.37	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
74.91.20.195	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
71.6.146.185	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

04-24-2016-19:04:07 to 04-24-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-24-2016-19:04:07 to 04-24-2016-20:04:07

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

04-24-2016-19:04:07 to 04-24-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
109.253.224.22	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
94.159.159.216	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
194.126.18.108	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
5.29.70.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
176.67.107.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
188.4.85.149	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
84.95.59.228	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	22
70.192.25.93	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
185.27.106.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
109.64.170.196	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
109.253.206.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.187.111.11	Germany	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.87.127.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.66.65.235	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
93.173.227.43	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
82.145.211.121	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.64.222.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.46.41.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
171.96.172.133	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.251.179	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.27.106.14	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
66.249.65.20	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.18	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
38.99.252.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.173.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.50.44.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.177.210	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.151.42.39	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.53.22.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.230.86.139	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.71.63.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
2.53.185.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.108.31.210	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.195.153	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.154.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

04-24-2016-19:04:07 to 04-24-2016-20:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.61.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.223.26	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	24
46.19.86.243	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Days in mobile.idf.il/milluim	Block	12
46.120.21.182	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.120.21.182	Block	6
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.191	Block	3
109.253.224.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.0.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.163.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.224.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.224.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.175.160	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 213.57.175.160	Block	2
109.173.156.193	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il./	Block	1
78.204.103.218	France	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
173.252.90.236	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/57056.pdf&ved=0ahukewj88mpmt6fmahuc_iwkhwntar4qfggdmai&usg=afqjcnf1yolugsboijiblzxiye0gplabcg&sig2=sljt3vnb9hu32rwuqzye5w	Block	1
117.203.221.190	India	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
46.19.85.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
87.69.113.19	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
213.57.175.160	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/patzar/klali/default.asp	None	1
46.120.21.182	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
141.212.122.129	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to /x	Block	1
5.29.166.145	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/undefined	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
173.252.122.118	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/6/57056.pdf&ved=0ahukewj88mpmt6fmahuc_iwkhwntar4qfggdmai&usg=afqjcnf1yolugsboijiblzxiye0gplabcg&sig2=sljt3vnb9hu32rwuqzye5w	Block	1
117.203.221.190	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
46.19.86.12	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
46.121.93.233	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.78.8.228	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 149.78.8.228	Block	1
37.47.137.69	Poland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.181.207.188	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
66.249.66.44	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/tizmoret/news/	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
93.85.152.41	Belarus	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	Block	1
78.153.146.109	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteykatava/	Block	1
159.226.95.66	China	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
37.47.137.69	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
80.246.133.229	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
185.27.106.14	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
109.64.170.196	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
78.153.146.109	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.64.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
171.96.172.133	Thailand	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.187.157.108	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
84.108.18.212	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.108.18.212	Block	1

04-24-2016-19:04:07 to 04-24-2016-20:04:07