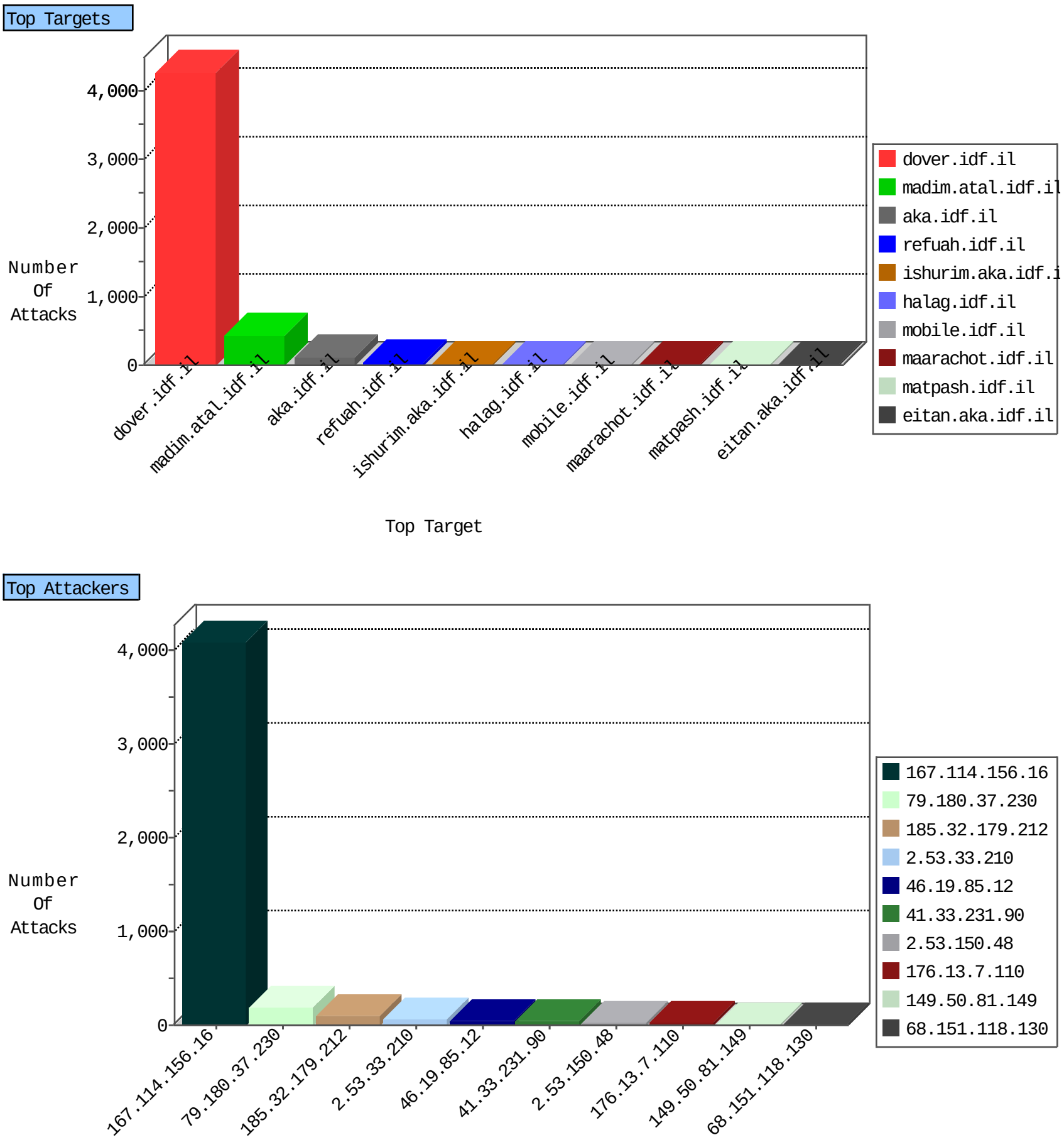
04-16-2016-18:04:08 to 04-16-2016-19:04:08

IDF Under Attack Daily Report



04-16-2016-18:04:08 to 04-16-2016-19:04:08

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	4069
79.182.16.12	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.64.163.186	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
101.201.147.32	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	2
149.88.106.86	Israel	147.237.72.166	aka.idf.il	Anomaly-TCP-SYN-FIN	dest-reset	1
106.184.3.122	Japan	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
45.32.95.13	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.194	Switzerland	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1

04-16-2016-18:04:08 to 04-16-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.14.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.178	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-16-2016-18:04:08 to 04-16-2016-19:04:08

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
185.32.179.212	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
113.59.33.61	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
101.108.114.40	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.91.29	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
113.59.33.61	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
83.235.181.57	147.237.8.50	Greece	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1

04-16-2016-18:04:08 to 04-16-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
149.50.81.149	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
68.151.118.130	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.12	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.12	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
85.64.168.239	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.102.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
87.70.77.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.210.150.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.254.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
132.68.40.14	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.215.170.135	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.135.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
100.127.158.135		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.177.102.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
199.30.24.73	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.231.187.30	Ukraine	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
81.245.49.216	Belgium	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.2.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.61.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.33	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.176.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.217.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.130.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.245.49.216	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
217.132.77.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.231.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.36.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.149.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.176	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.122.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.147.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.13.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.32.230	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.103.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.213.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.169.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

04-16-2016-18:04:08 to 04-16-2016-19:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.3.147.103	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
78.52.132.104	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.65.28.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.186.184.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

04-16-2016-18:04:08 to 04-16-2016-19:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.37.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	192
185.32.179.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
2.53.33.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
2.53.150.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
176.13.7.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
2.53.37.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
212.25.119.136	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	4
188.172.220.235	Austria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
131.253.25.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.83.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.154.168.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.20.12	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
2.53.52.248	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
93.168.189.192	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	2
79.181.7.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	Block	1
73.241.191.33	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/rights/asp/	Block	1
106.184.3.122	Japan	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
82.19.86.117	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/about/about.asp	Block	1
73.241.191.33	United States	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19484-he/idfgdover.aspx	Block	1
2.55.26.168	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
93.173.229.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.181.111.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/maingiyus	Block	1
73.241.191.33	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
157.55.39.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
106.184.3.122	Japan	147.237.77.170	maarachot.idf.il	Malformed URL	Block	1
66.249.64.75	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.109.214.195	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.182.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
149.50.81.149	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
94.54.183.45	Turkey	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
79.182.20.12	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.182.20.12	Block	1
157.55.39.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
73.241.191.33	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
106.184.3.122	Japan	147.237.77.170	maarachot.idf.il	NULL Character in Method	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
85.64.33.95	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
207.46.13.82	United States	147.237.72.166	aka.idf.il	Unknown Parameter profid in aka.idf.il/main/giyus/tafkidsearchformanilot.aspx	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
149.88.175.64	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.54.183.45	Turkey	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 94.54.183.45	Block	1
31.154.254.160	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
73.241.191.33	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
106.184.3.122	Japan	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method SSH-2.0-LYGhost_1.2.7-20100630 in URL	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3480.jpg	Block	1

04-16-2016-18:04:08 to 04-16-2016-19:04:08