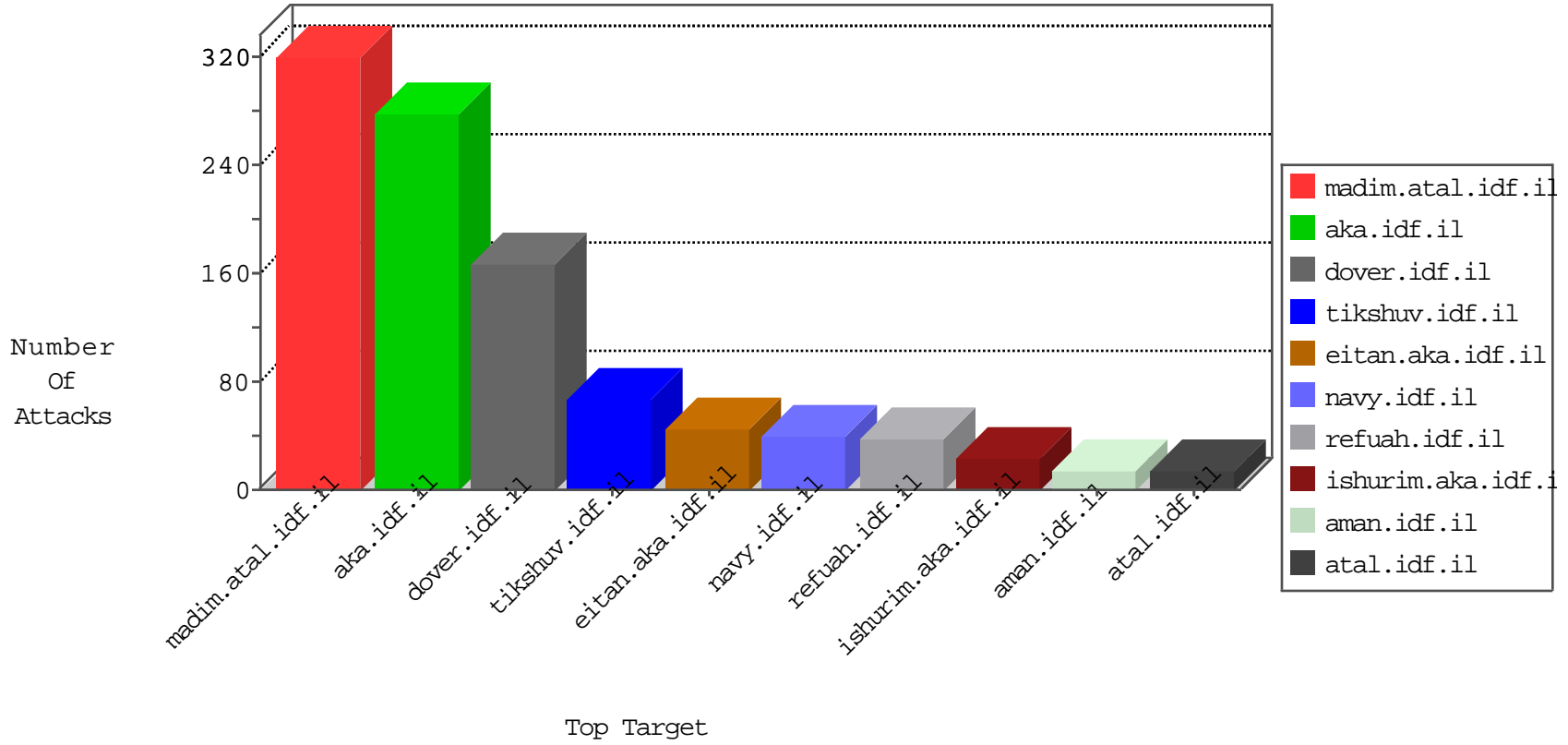


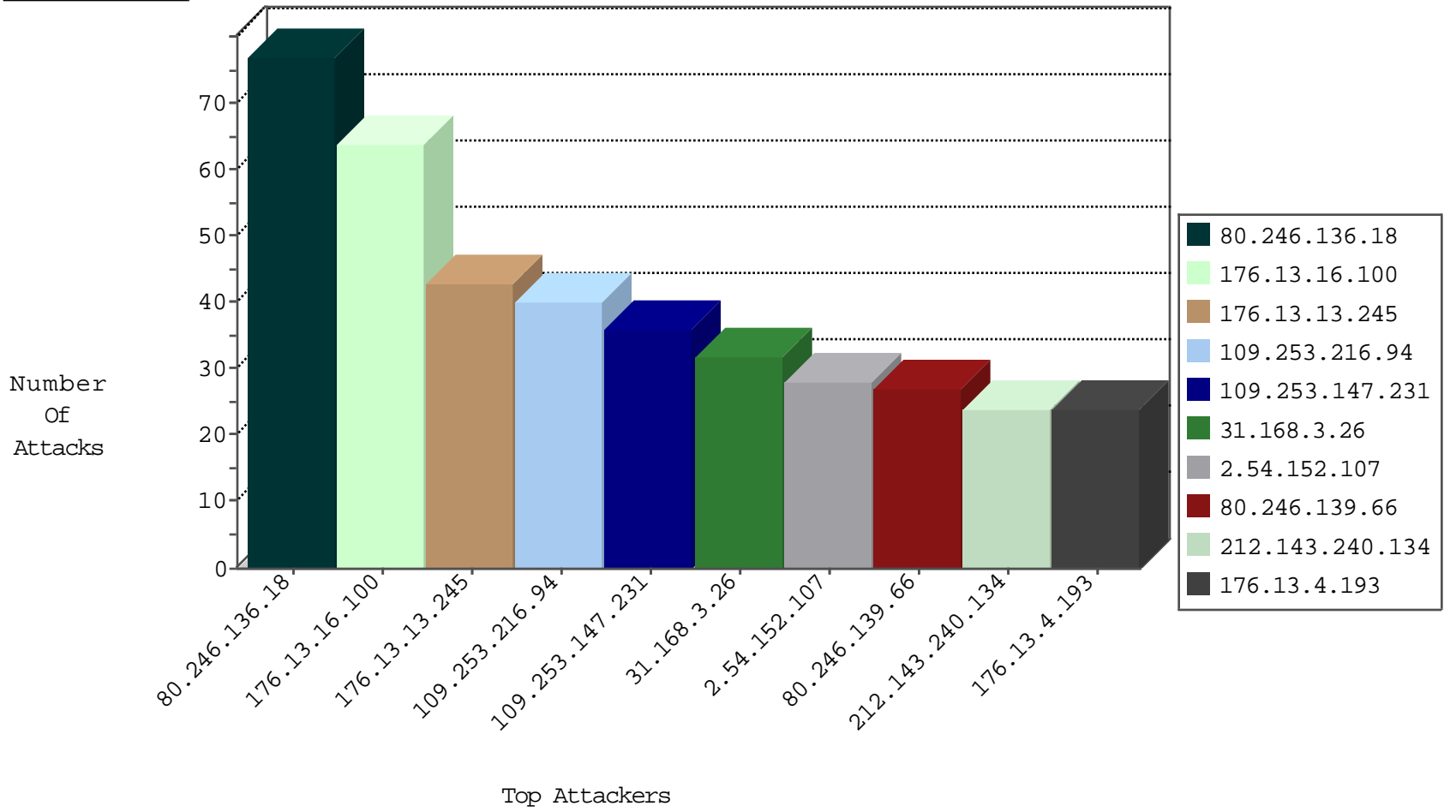
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.218.138	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
89.248.160.132	Netherlands	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
89.248.160.132	Netherlands	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
184.105.139.74	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.57	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.126	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.114	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
151.80.47.170	Italy	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
188.138.1.218	Germany	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.118	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
168.70.51.4	Hong Kong	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.118	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.6.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	24
212.143.240.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
2.54.16.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	3
2.54.14.20	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.178.196.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.151	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.146.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.143.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
132.66.54.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.135.82.79	147.237.77.216	Hungary	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.178.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.211.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.172.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.158.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.31.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.10.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.128.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.170.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.102.9.28	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
37.142.175.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.168.3.26	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
46.19.85.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.54.152.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.58	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
95.35.10.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.180.216.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.122	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.139.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
81.218.159.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.195	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
185.94.232.12		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
192.114.23.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.188.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.118.48.248	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	6
80.246.139.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
213.57.143.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.240.134	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.46	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
109.65.169.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.239.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
80.246.139.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.130.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.139.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.152.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.152.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
132.71.97.4	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.138.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.147.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
2.54.152.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.229.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.133.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.145.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.61.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.202.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.249.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.143.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.52.145.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.231.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
176.13.16.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
176.13.13.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
109.253.216.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.253.147.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.4.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.85.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
2.52.43.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.222.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.203.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.215.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.25.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.228.136.200	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
79.176.5.147	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.5.147	Block	2
199.30.24.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
188.161.65.26	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
79.176.5.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	2
31.168.17.162	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.56	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.194.199.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.168.85.158	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.176	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
216.35.195.247	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
207.46.13.100	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
89.248.160.132	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.safeskyhacks.com/forums/forum.php	Block	1
37.26.146.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.30.24.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple _vti_ from 81.218.53.114	Block	1
77.75.78.168	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/31/	Block	1
172.86.180.154		147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	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
216.218.206.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
84.108.88.60	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
37.26.148.199	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.199 (Open Mode)	None	1
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	1
131.253.25.252	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
46.165.210.17	Germany	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
207.241.229.223	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/oevent/oevent.in.aspx	Block	1
89.248.160.132	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.safeskyhacks.com/forums/forum.php	Block	1
37.26.146.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
199.30.24.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/_vti_bin/owssvr.dll	Block	1
172.86.180.154		147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1