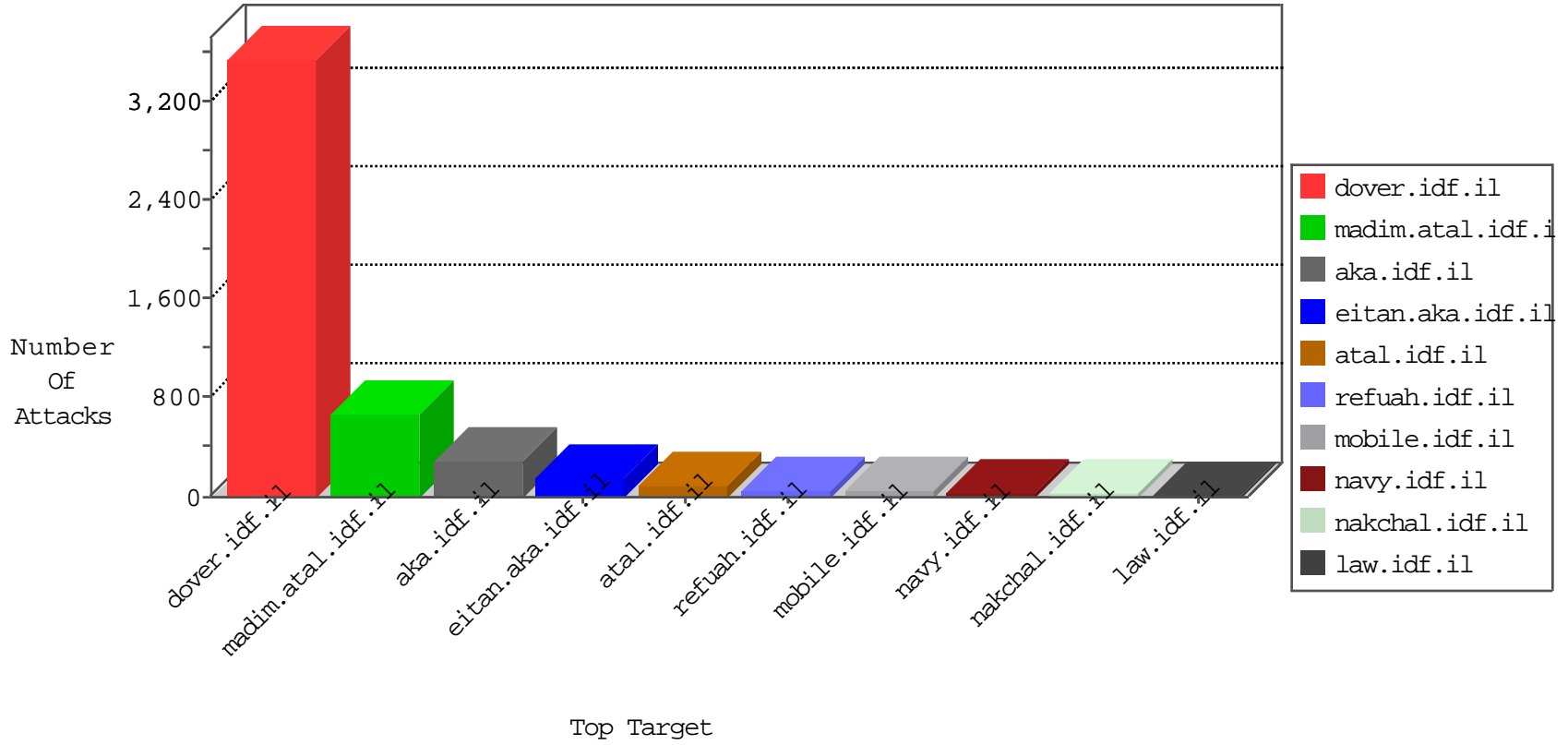


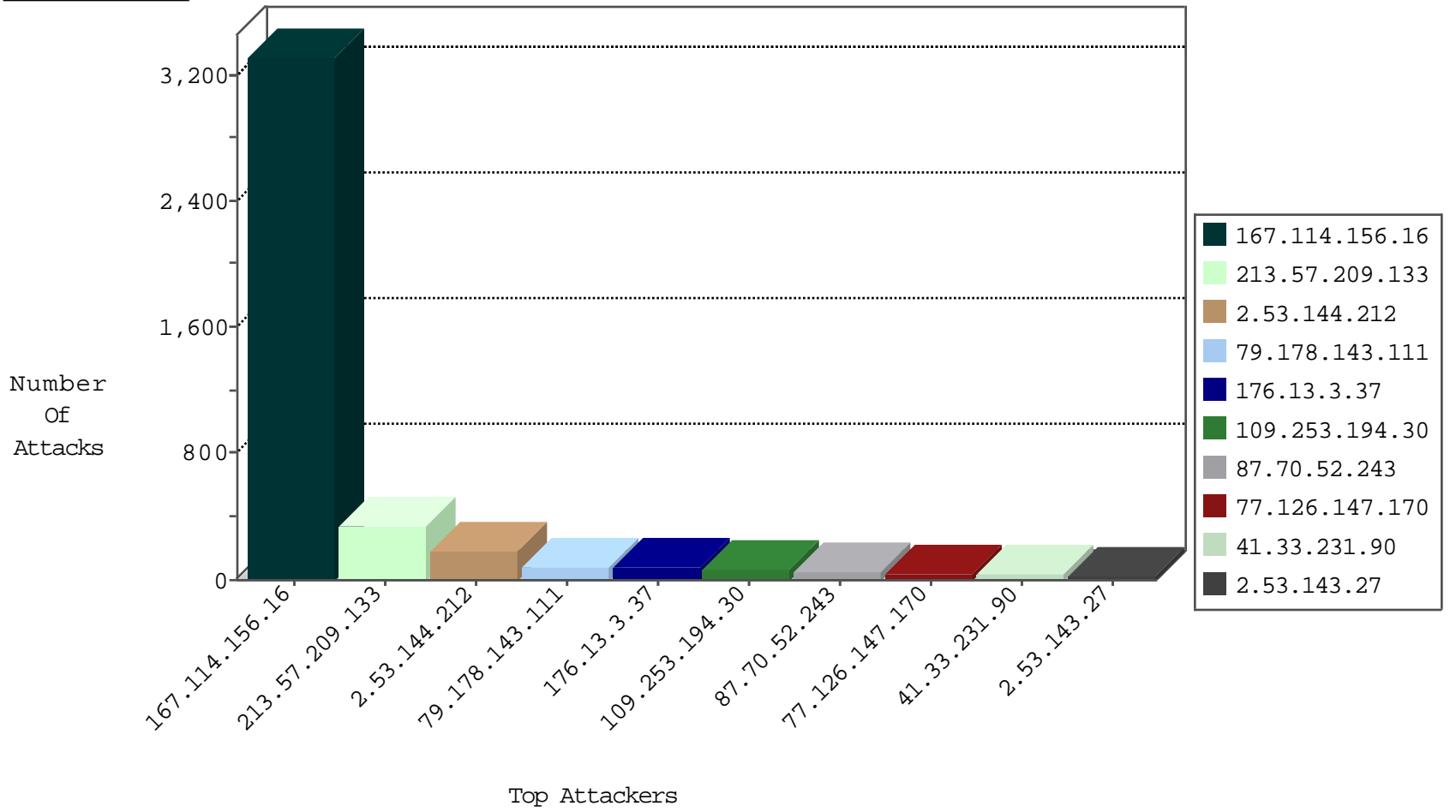
IDF Under Attack Daily Report



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	3312
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
123.59.59.52	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-trafl	forward	4
95.86.98.189	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
202.112.51.96	China	147.237.76.86	navy.idf.il	block-sp-trafl	forward	2
101.201.147.32	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-trafl	forward	2
202.112.51.96	China	147.237.77.19	law-forum.idf.il	block-sp-trafl	forward	2
202.112.51.96	China	147.237.77.205	prisha.idf.il	block-sp-trafl	forward	2
202.112.51.96	China	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	2
185.94.111.1	Russian Federation	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
134.147.203.115	Germany	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
104.153.173.100	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.90.105.112	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
176.233.137.185	Turkey	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
89.138.222.32	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.44	147.237.76.31	Europe	nakchal.idf.il	ET SCAN NMAP -sA (2)	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
89.138.174.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.56.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.153	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
5.29.223.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.134.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.66.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
85.64.36.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.153	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
77.127.88.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.214.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.234	United States	halag.idf.il	ET DROP Dshield Block Listed Source	1
185.120.126.34	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
176.13.3.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
79.178.143.111	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
79.178.143.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
77.126.147.170	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.180.101.36	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
87.69.208.124	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.57.204.87	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
70.193.196.8	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.148.217	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
31.168.181.109	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	17
46.117.76.133	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
37.26.146.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
185.3.147.221	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.3.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.55.140.29	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
85.64.148.166	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
217.132.149.72	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
82.81.37.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.12.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.139.237.160	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.78.26.214	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.13.3.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
81.218.138.243	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
81.218.138.243	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.161.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.174.171	Sweden	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.20.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.146.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.203.64.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.114.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.27.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
87.69.255.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.177.17.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.17.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.177.17.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
166.177.249.0	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
89.138.184.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.176.160.226	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
75.159.54.132	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

04-17-2016-19:04:08 to 04-17-2016-20:04:08

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.182.113	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.209.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	338
2.53.144.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
109.253.194.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
2.53.143.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.53.46.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.53.191.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.67.172.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
217.132.121.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
149.50.124.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	4
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
109.253.132.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
156.210.20.136	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.8.204.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.63.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	3
2.55.158.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.35.158.137	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.147.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.81.37.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.29.171.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.178.143.111	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.19.85.192	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/71725.pdf	Block	1
199.203.64.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/resources/common/forums/scripts/scripts.js	Block	1
46.117.123.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
202.112.51.96	China	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to bter.com/	Block	1
156.210.101.154	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.93.46	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/894-he	Block	1
181.196.89.99	Ecuador	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	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
2.53.0.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
123.59.59.52	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.ctrip.com/894-he/hamaz.aspx	Block	1
54.197.114.174	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.52	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/general/general.aspx	Block	1
157.55.39.40	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1415-he/dover.aspx	Block	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
46.19.85.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
87.69.245.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.188	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/gallery/	None	1
109.236.84.129	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-he/+navmenu.qc+	Block	1
77.126.147.170	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
192.115.99.130	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/109333.pdf	Block	1
149.78.26.214	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
93.172.229.16	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.6.64.46	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1