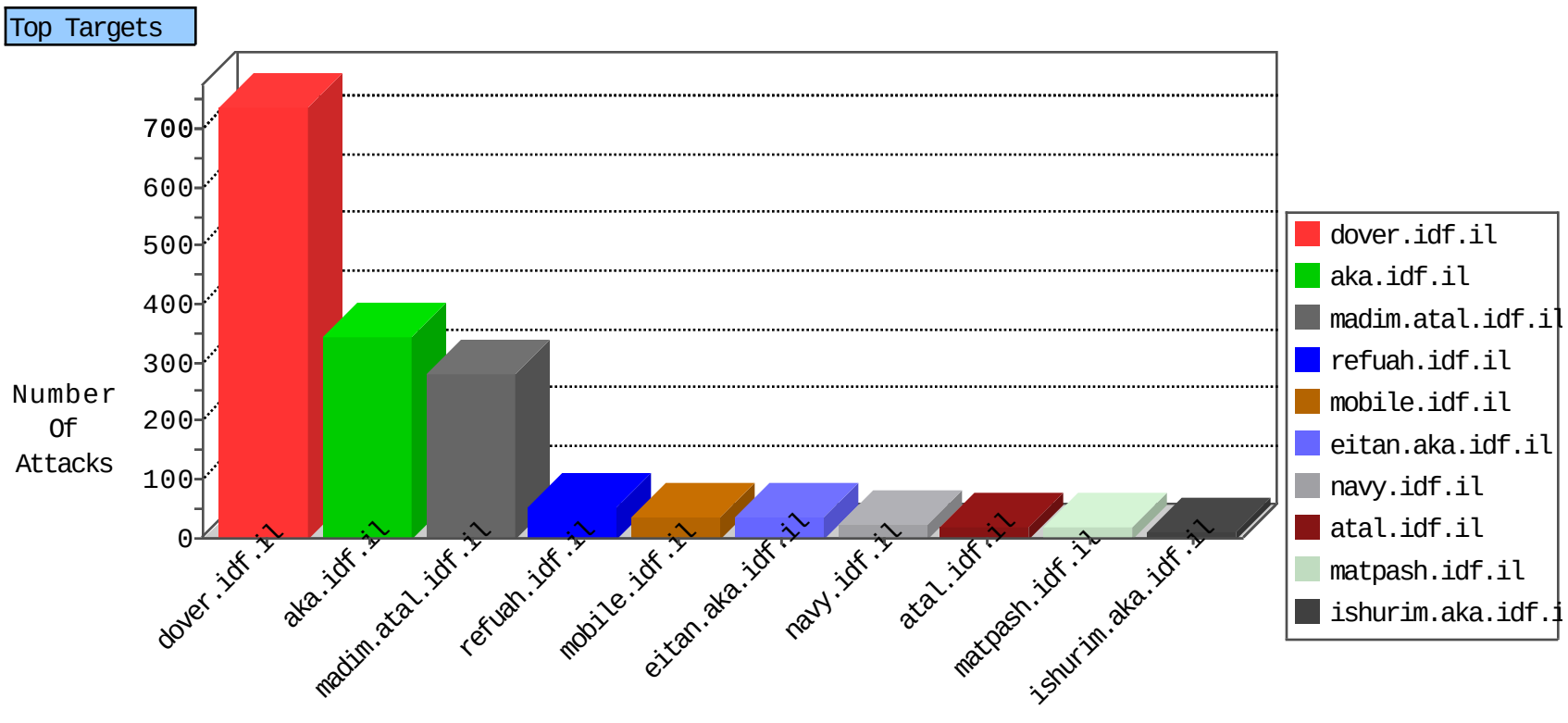
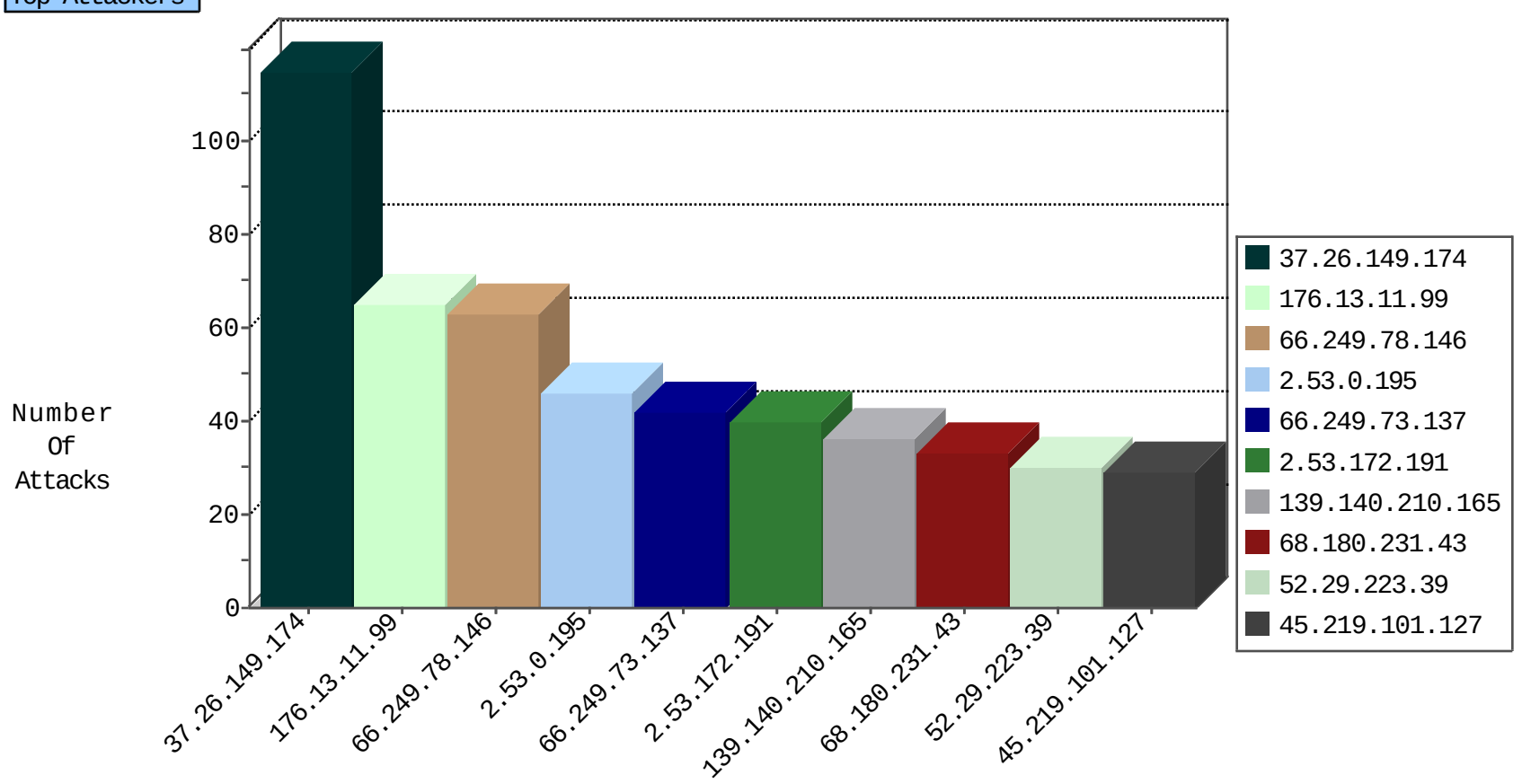
05-04-2016-18:04:01 to 05-04-2016-19:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-04-2016-18:04:01 to 05-04-2016-19:04:01

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	741
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	540
82.145.218.3	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
84.109.2.193	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
173.195.0.22	United States	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
173.195.0.21	United States	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
173.195.0.21	United States	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
173.195.0.22	United States	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1

05-04-2016-18:04:01 to 05-04-2016-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-18:04:01 to 05-04-2016-19:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.243	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.93	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
82.81.65.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.8.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
184.80.10.136	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.174	147.237.0.19	Israel	madim.atal.idf.i	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
93.173.229.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
13.92.103.193	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.46.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.165.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.76.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.178.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
80.246.130.250	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
184.80.10.136	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -f -sS	1
46.116.20.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.204.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.76.60.52	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
13.92.103.193	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
89.138.50.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.103.193	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
87.70.109.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.168.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1

05-04-2016-18:04:01 to 05-04-2016-19:04:01

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	63
139.140.210.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
204.102.229.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.186.183.238	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.55.185.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.146.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
94.230.86.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
82.145.218.40	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
45.219.101.127	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.116.177.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
172.56.29.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
45.219.101.127	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.73.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
217.132.220.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
62.90.211.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.35.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.250.184.140	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.73.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.136.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
109.65.108.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
188.120.154.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.154.173.103	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.11.99	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
91.218.192.254	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.7.210.13	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.201.141	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
2.53.0.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
176.13.11.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.53.172.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
212.150.244.228	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 212.150.244.228	Block	7
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
131.253.25.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.53.38.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
5.22.134.255	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
94.230.86.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.181.60.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/sachar	Block	3
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
109.253.215.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
197.165.248.18	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.25.132	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.158.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
197.166.77.214	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.32.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.26.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
109.67.62.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/default.aspxaka	Block	1
5.22.134.255	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.22.134.255	Block	1
198.204.249.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/shared/usercontrols/headerupper/	Block	1
184.154.48.210	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
41.205.30.108	Cameroon	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/admin/config.php	Block	1
2.53.32.37	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
92.78.130.231	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
69.89.31.60	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
46.116.20.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
164.132.161.38	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1405-he/atal.aspx	Block	1
109.67.221.93	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.130.67	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
185.32.179.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.73.146	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.85.7	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14737545 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip	Block	1
94.23.38.15	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
79.179.63.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.166.77.101	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
50.63.197.201	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
173.252.90.94	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
109.67.221.93	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.249.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1