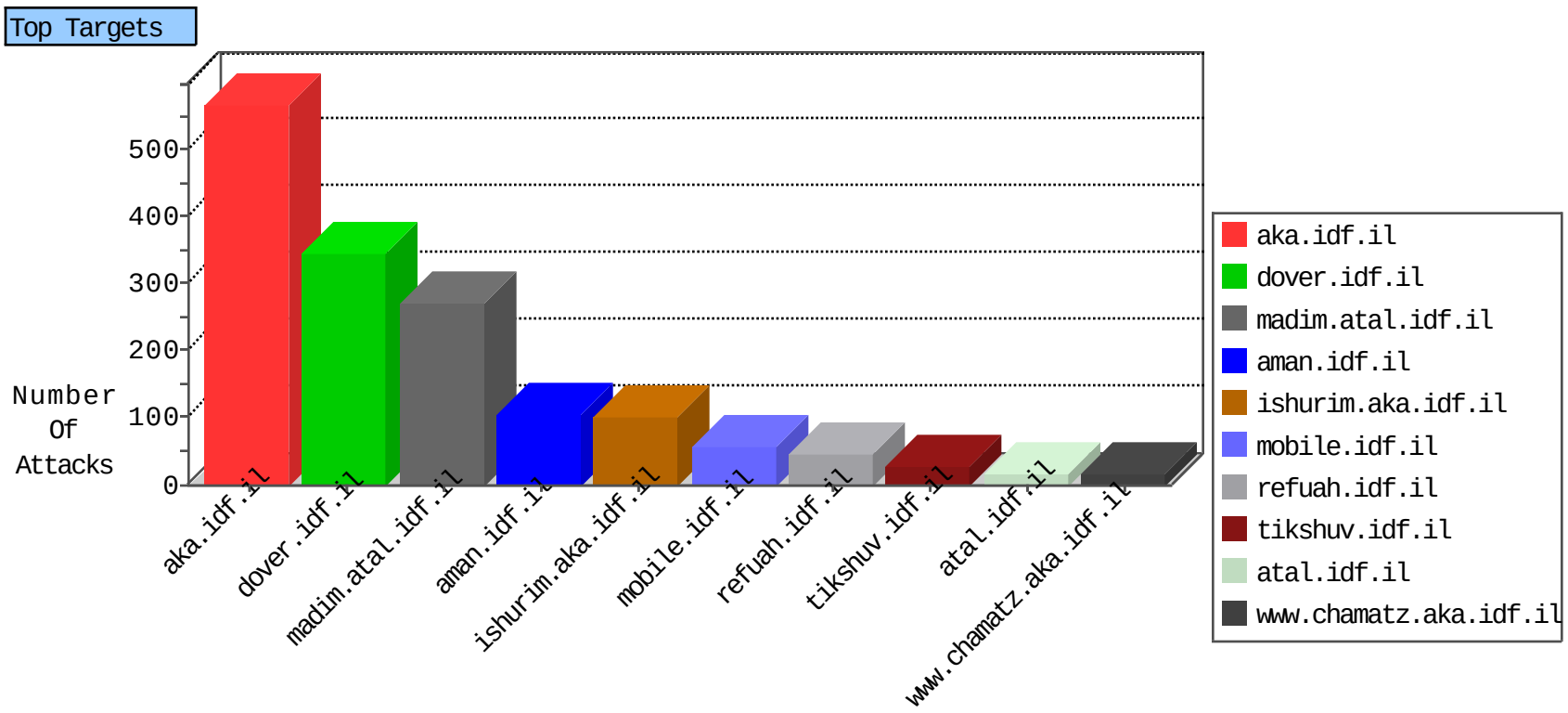
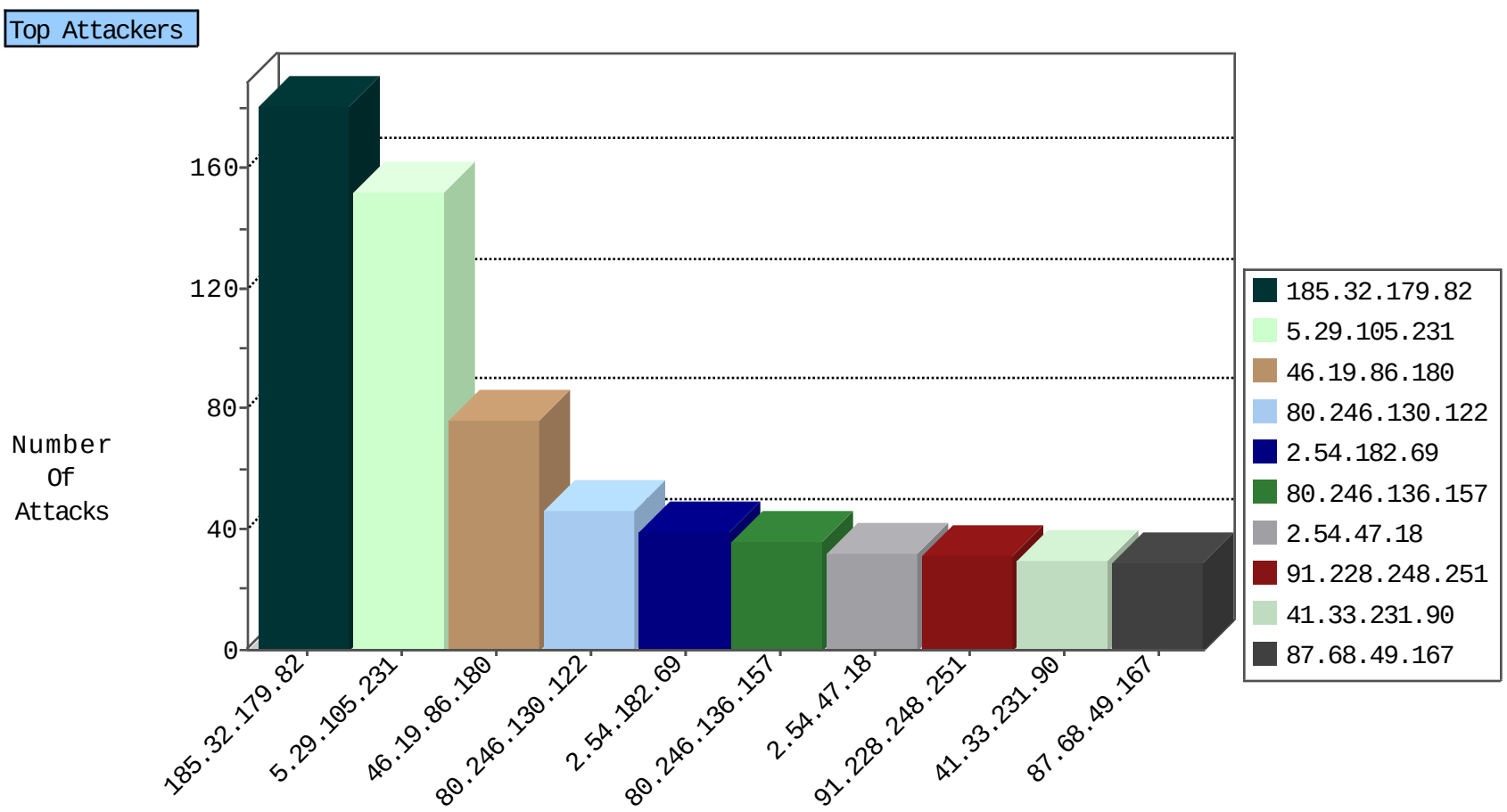
02-15-2016-09:04:01 to 02-15-2016-10:04:01

IDF Under Attack
Daily Report





02-15-2016-09:04:01 to 02-15-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.180	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
46.19.86.46	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.54.130.210	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.86.130	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.52.147.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
146.185.57.8	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
146.185.57.8	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
123.151.149.222	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
87.68.49.167	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
87.68.49.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
208.73.206.244		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-15-2016-09:04:01 to 02-15-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-15-2016-09:04:01 to 02-15-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.67.170.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
65.60.36.203	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
23.101.133.103	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.218.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.249.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.19.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.118.30.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-15-2016-09:04:01 to 02-15-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.29.105.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	109
5.29.105.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
80.246.130.122	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
46.165.234.107	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	19
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.222.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.81.209	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
82.81.129.85	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
87.68.49.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
80.246.136.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.246.136.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.47.18	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	12
80.246.136.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
87.68.49.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.12.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.47.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
2.54.47.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.85.179	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.74	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
66.249.81.206	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
80.246.130.122	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.172.50	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.135.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.210.129.196	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
199.203.130.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.172.50	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.52.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.69.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
203.133.168.41	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.29.17	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.194.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
203.133.168.41	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.193.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.179.66	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.210.129.196	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.219.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.105.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.183.101.239	Israel	147.237.72.167	ishurim.aka.idf.il	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
185.32.179.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
185.32.179.82	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.82	Block	59
2.54.182.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
91.228.248.251	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 91.228.248.251	Block	31
89.139.59.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
176.13.18.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	5
176.13.6.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.158.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.143.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.122	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.17.255	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
134.191.232.70	Israel	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
80.179.40.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
176.13.4.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.100.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.52.216.170	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-10885-he/	Block	2
109.253.219.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.179.132.204	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	2
176.13.20.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
14.18.29.60	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.118.78.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
80.246.130.122	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
73.251.84.166	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
118.159.230.98	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
81.218.57.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.39.241	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
79.179.29.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
157.55.39.218	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kapatz/	Block	1
217.194.197.76	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
109.64.159.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sacharmain/home/default.aspx	Block	1
31.168.6.66	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 31.168.6.66	Block	1
207.46.13.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
73.251.84.166	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
176.13.12.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
65.55.210.111	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.181.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.158.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.0.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
31.168.6.66	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/109591.pdf	Block	1
109.67.32.129	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
209.88.198.1	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size338x0/2255.jpg	Block	1
80.246.133.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1