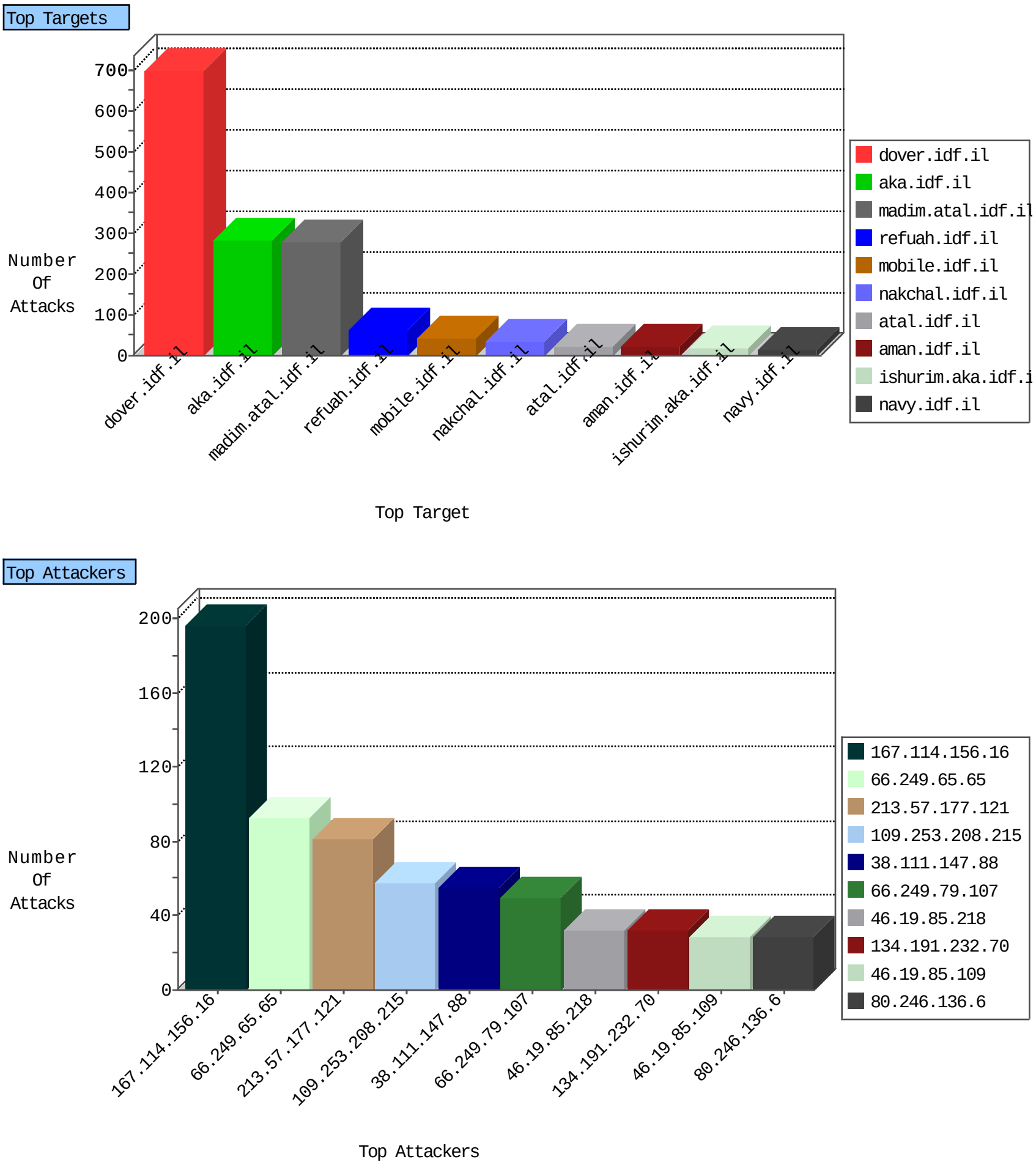
05-04-2016-10:04:00 to 05-04-2016-11:04:00

IDF Under Attack
Daily Report



05-04-2016-10:04:00 to 05-04-2016-11:04:00

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	7882
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1369
2.53.50.43	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	298
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	48
46.116.12.65	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.103.252.178	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

05-04-2016-10:04:00 to 05-04-2016-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-10:04:00 to 05-04-2016-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
104.192.0.19	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.208.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.79.232	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
62.219.182.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.191.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.1.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.231.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
149.88.102.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.167.112.76	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
77.124.1.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.161.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.118.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.57.5.123	147.237.77.216	Indonesia	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.25.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.54.168.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
134.191.232.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

05-04-2016-10:04:00 to 05-04-2016-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
105.198.242.18	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.79.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
109.253.137.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.178.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.32.200.75	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
37.26.149.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
93.109.107.131	Cyprus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.179	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.64.230.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.253.135.28	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.0.14.85	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.185.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.222.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.152.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.79.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.210.187.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.46	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.31.177	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.108.185.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.8.121.6	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.177.31.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.22.129.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.31.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.177.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
109.253.208.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
80.246.136.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
109.253.145.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
149.50.76.130	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	10
80.246.137.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
2.55.134.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.130.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.137.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
149.50.76.130	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	3
84.228.16.171	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	3
80.246.136.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.64.57.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.23.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.51.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.186.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.228.16.171	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.228.16.171	Block	2
109.253.200.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.76.114.24	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	2
109.253.201.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.1.46	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.178.189.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.183.178.118	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
46.121.71.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
109.253.128.110	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/mobile	Block	1
37.26.149.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/entebbe1.stm<p>	Block	1
195.154.199.235	France	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
93.87.220.184		147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.69.7	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-23046-he/dover.aspx	Block	1
195.154.199.235	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/wp-login.php	Block	1
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
93.87.220.184		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
5.29.210.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.50.88.46	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.73.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71576.pdf	Block	1
46.4.22.136	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/rabanut/general.aspx	Block	1
109.253.135.28	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.228.16.171	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
79.176.64.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.199.235	France	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.64.53.195	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
37.26.148.203	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1