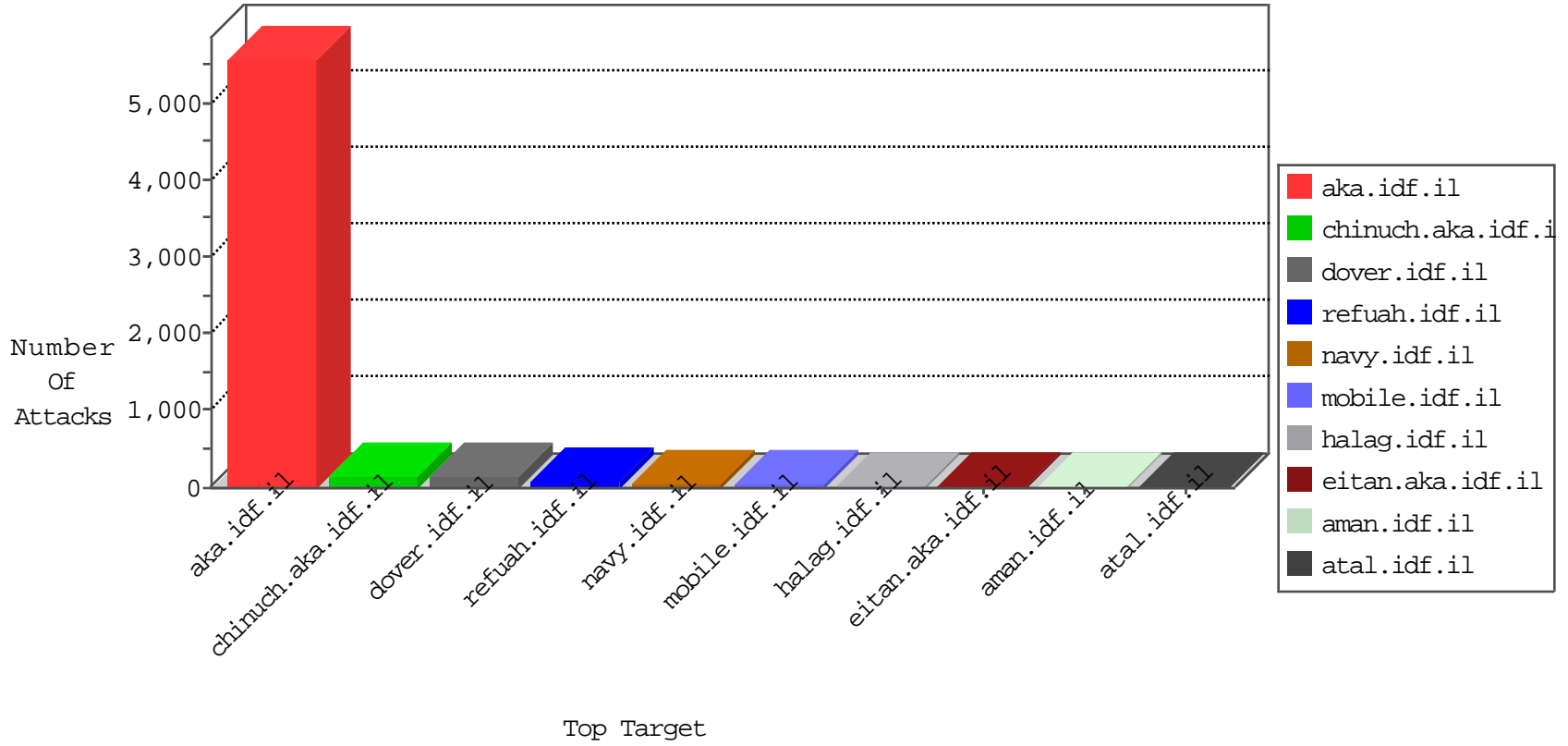


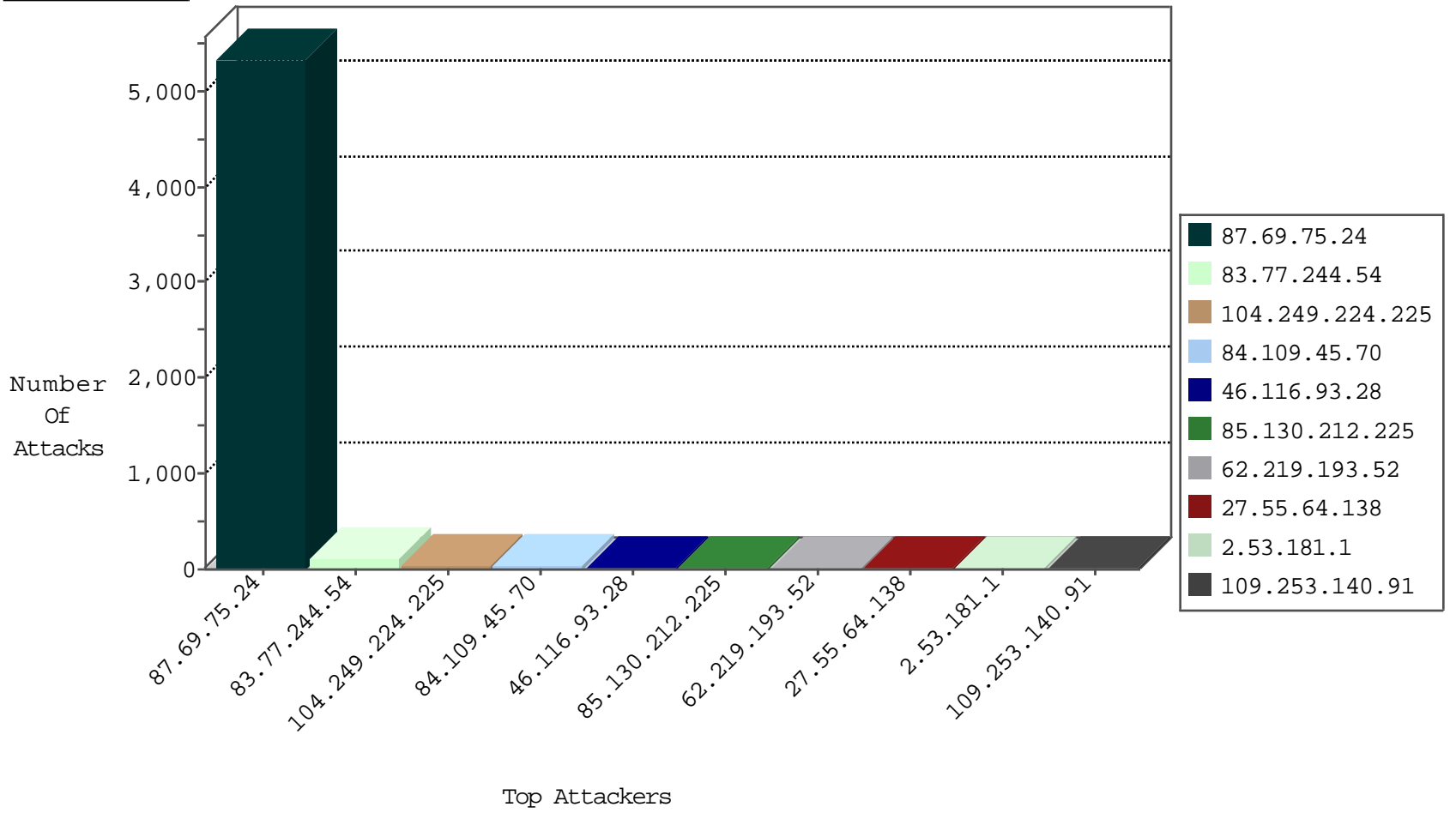
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.57.232.165	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
185.129.148.230	147.237.0.35	Latvia	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -f -sS	1
46.183.223.228	147.237.8.50	Latvia	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.76.148	Indonesia	ggcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
167.56.14.97	147.237.72.167	Uruguay	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 2048	1
46.183.223.228	147.237.76.30	Latvia	himush.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.69.75.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	936
84.109.45.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	23
62.219.193.52	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	21
27.55.64.138	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	19
212.235.68.78	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
191.99.166.201	Ecuador	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
178.122.58.131	Belarus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
104.249.224.225	Canada	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
104.249.224.225	Canada	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.120.126.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
104.249.224.225	Canada	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
100.92.5.163		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
185.120.126.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.53.181.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.177.30.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
104.249.224.225	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
123.231.111.200	Sri Lanka	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
79.177.30.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.116.93.28	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.29	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.149.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.20	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
172.58.144.209	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
5.22.134.235	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.212.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.168.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.134.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.212.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.253.140.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.116.93.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
46.19.85.20	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
85.130.212.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.150.53	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
79.178.255.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
104.249.224.225	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.136.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.181.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.134.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.137.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.55.139.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.17.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.75.24	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning V1	Block	3084
87.69.75.24	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 87.69.75.24	Block	1325
89.138.97.76	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.138.97.76	Block	6
77.138.175.180	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	3
31.210.187.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
61.0.62.122	India	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
66.249.69.14	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
5.102.229.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
66.249.69.18	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
89.138.97.76	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
66.249.75.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	2
77.127.241.20	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.32.179.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.14	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
2.55.171.221	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1411-he/atal.aspx	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8925-he/refuah.aspx	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
95.86.113.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.109.45.70	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
39.33.75.70	Pakistan	147.237.77.216	doover.idf.il	PHP Attempt	Block	1
77.138.30.92	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
213.57.156.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
61.0.62.122	India	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.231.25	France	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8750-he/refuah.aspx	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
129.113.57.28	United States	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdoover.aspx	Block	1
85.65.32.188	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
39.33.75.70	Pakistan	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
77.138.30.92	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
2.53.18.221	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	1
62.90.234.189	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$cb14847597 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.139.11.127	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
157.55.39.149	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
85.65.168.63	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
46.19.85.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
2.53.181.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.72.204	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.22	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
62.219.193.52	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
95.86.112.83	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
31.210.187.90	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.177.30.130	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.231.57	United States	147.237.77.216	doover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/doover.aspx	Block	1
167.114.234.155	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.182.146	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.129.195	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1