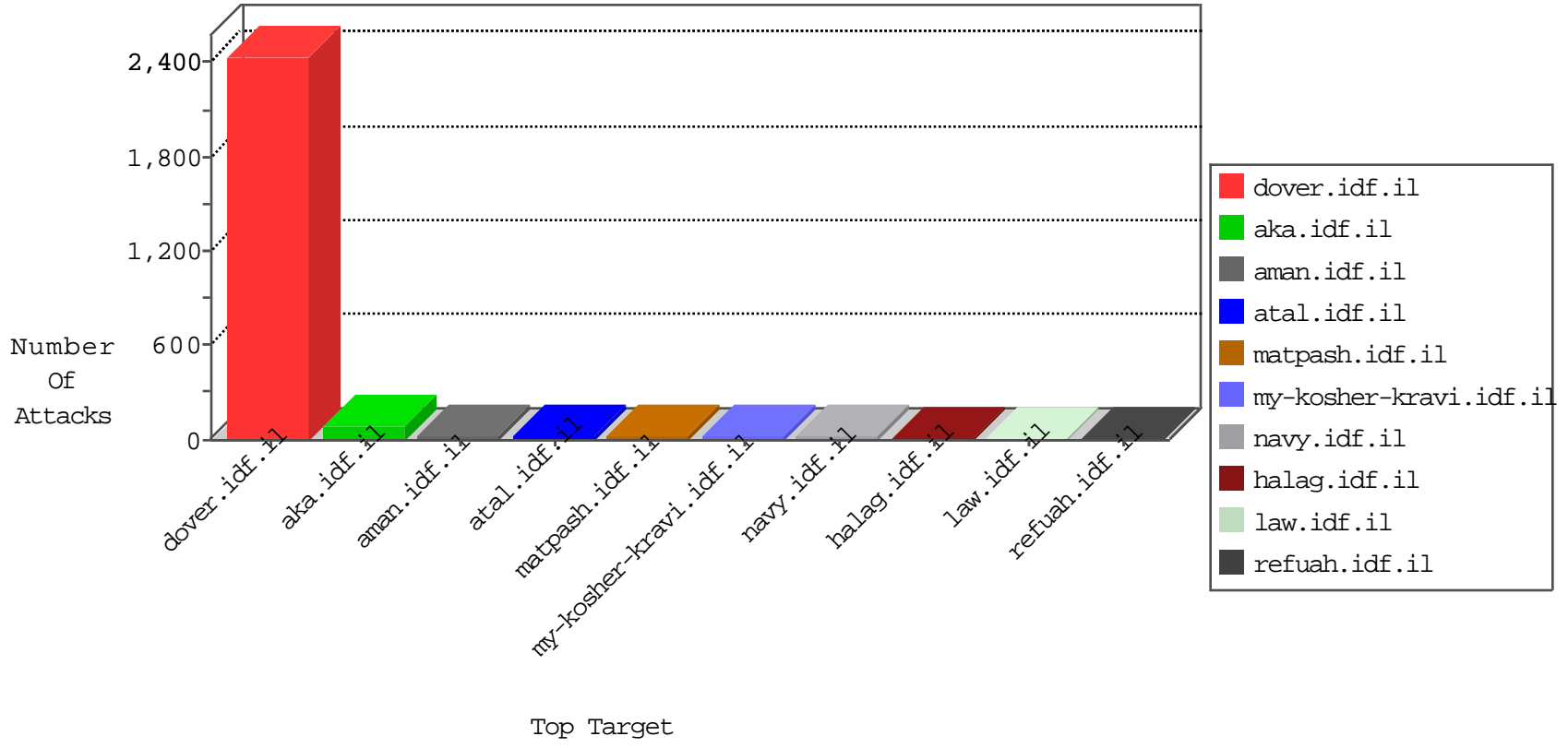


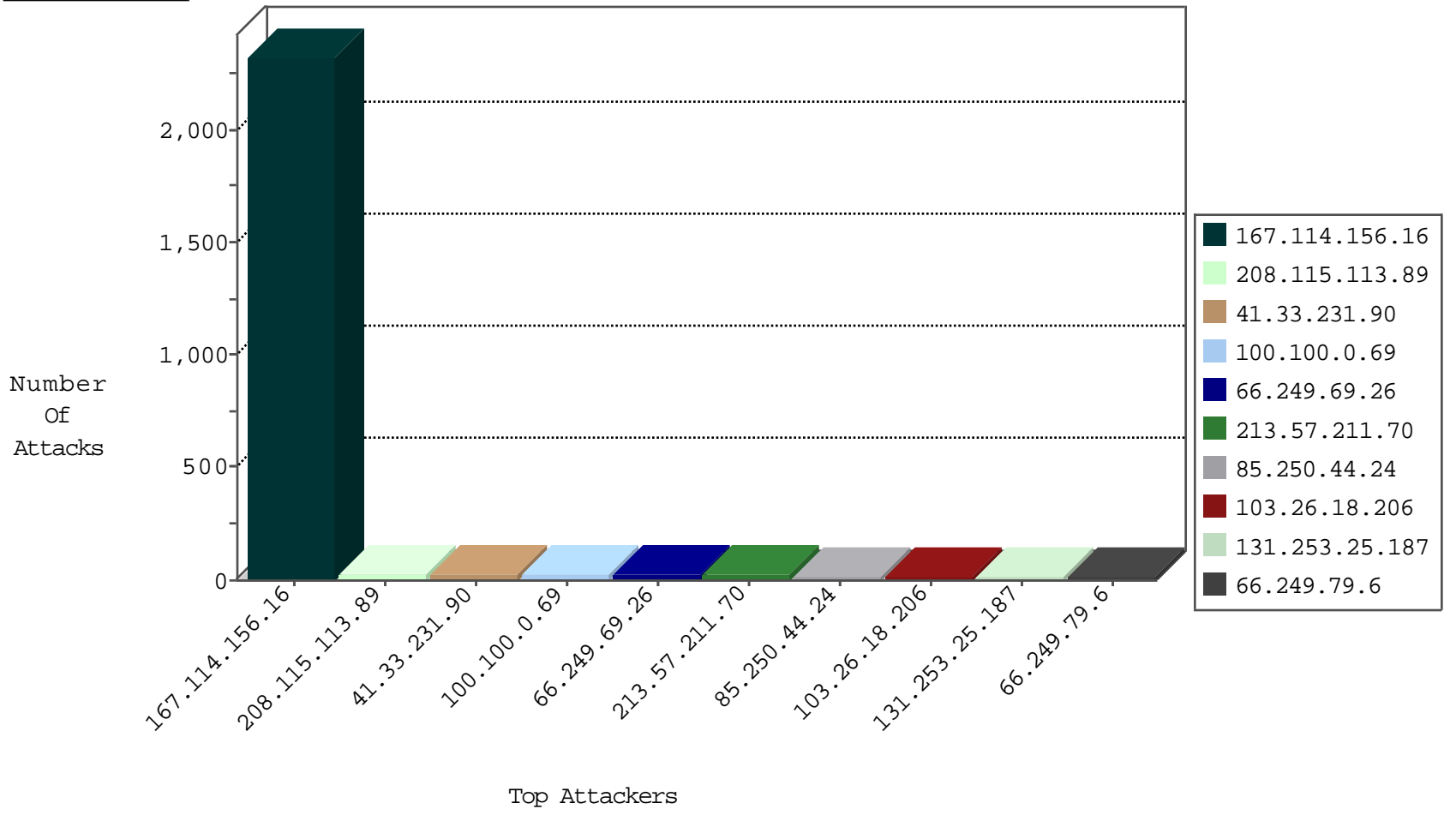
# IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3560

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.216.86	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
87.68.42.158	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.181	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.180.21	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.75.247	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.74.95	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.254	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
82.117.208.243	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.70.230	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.77.226	Poland	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.27	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.100.0.69		147.237.72.156	anan.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
213.57.211.70	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
85.250.44.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
131.253.25.187	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	9
66.249.74.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.135.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
64.19.78.242	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
103.26.18.206	New Zealand	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	4
103.26.18.206	New Zealand	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	4
103.26.18.206	New Zealand	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
182.160.163.148	Australia	147.237.76.86	navy.idf.il	drop	SAM rule	drop	4
103.26.18.206	New Zealand	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
108.35.245.215	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
77.126.166.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.61.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.142.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.233.172.163	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.3.146.89	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
64.233.172.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.121.61.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
85.65.74.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.183.49.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.3.144.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.192.0.226	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.7	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.102.254.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.65.220.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.106.94.2		147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.125.9.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.112	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.192.0.226	United States	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
79.183.49.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.88	United States	147.237.76.34	yochanan.idf.il	drop		drop	1
104.192.0.226	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.120.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.207	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.192.0.226	United States	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
82.166.74.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.106.94.2		147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	4
208.113.128.10	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.113.128.10	Block	4
60.241.215.85	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
103.9.64.178	Australia	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
103.9.64.178	Australia	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/index.php	Block	2
103.9.64.178	Australia	147.237.76.86	navy.idf.il	Distributed Admin Blocking	Block	2
60.241.215.85	Australia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
176.13.5.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
60.241.215.85	Australia	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
176.12.142.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
217.146.66.82	Estonia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
207.46.13.144	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
74.82.47.2	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
176.13.15.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
93.172.124.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 93.172.124.219	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.183.49.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.13.0.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.192.0.226	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /html/languages/es_es/main.js	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
207.46.13.158	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/pages/structure.aspx	Block	1
176.13.21.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
78.24.8.143	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
60.241.215.85	Australia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 60.241.215.85	Block	1
5.102.236.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.211.70	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	1
207.46.13.87	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
80.246.136.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.4.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.192.0.226	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /html/languages/es_es/main.js	Block	1
46.19.85.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.43.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
185.25.151.159	Poland	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
79.176.36.239	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
213.230.121.192	Uzbekistan	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
207.46.13.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/september/09.stm).	Block	1
84.94.91.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
104.192.0.226	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /html/languages/es_es/main.js	Block	1
50.17.102.193	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx	Block	1