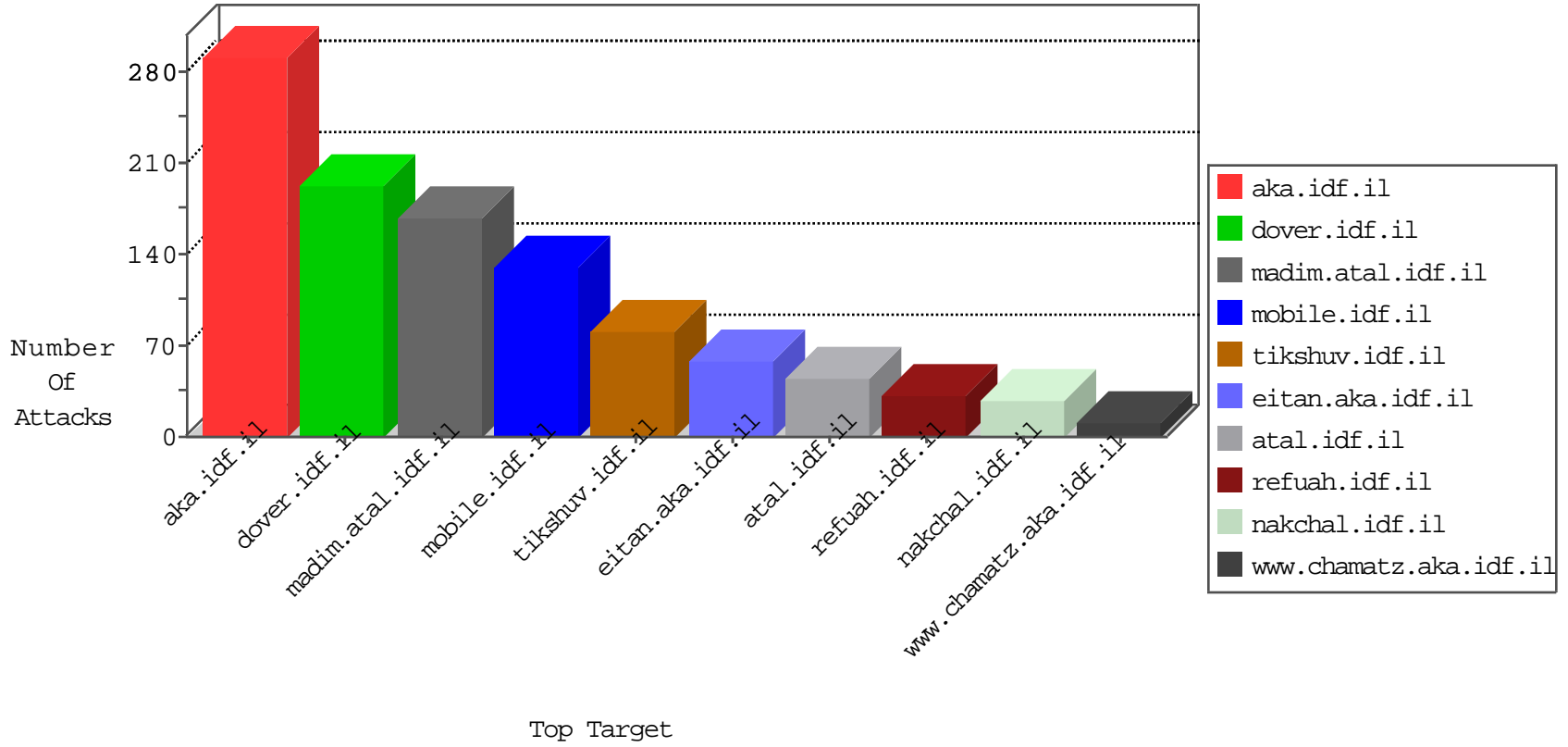


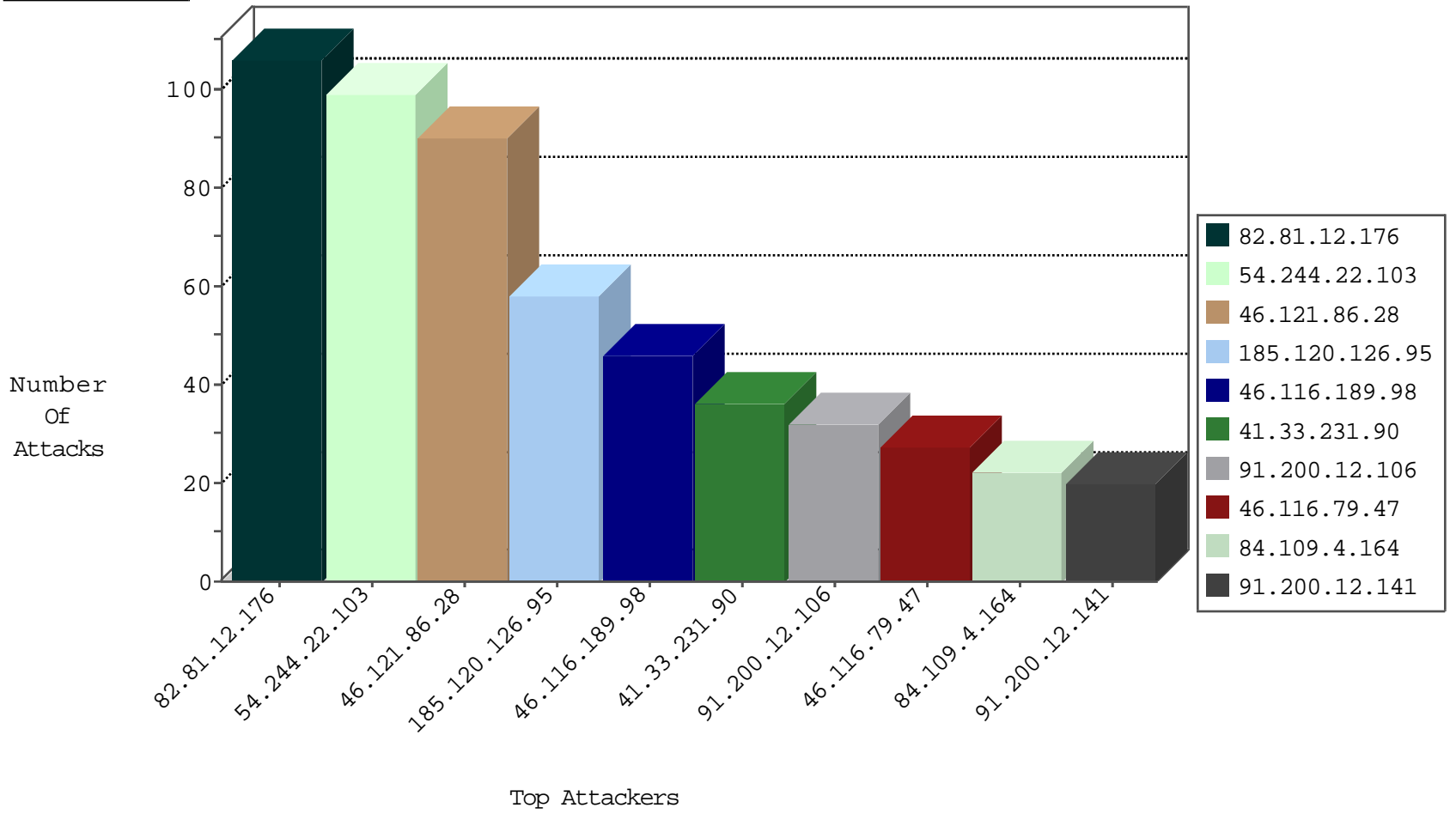
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	106
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

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
80.246.133.169	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
196.47.173.21	147.237.72.166	Cote D'Ivoire	aka.idf.il	ET SCAN NMAP -f -sS	1
191.232.39.241	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.77.227	Lithuania	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.8.46	Lithuania	e.chinuch.idf.i	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.72.166	Cote D'Ivoire	aka.idf.il	ET SCAN NMAP -sS window 2048	1
158.130.6.191	147.237.77.235	United States	sviva.idf.il	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	1
66.240.213.93	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.8.50	Lithuania	e.tikshuv.idf.i	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.0.33	Lithuania	idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.72.166	Cote D'Ivoire	aka.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	68
185.120.126.95		147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	31
46.116.79.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
79.178.147.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
89.138.42.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.109.4.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
217.132.37.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
109.253.159.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.47	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.188.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.106	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	6
37.26.149.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
91.200.12.106	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	6
61.138.61.143	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
82.81.240.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.47	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
218.60.132.40	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
175.18.112.202	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
85.65.151.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.106	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
91.200.12.141	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
85.64.234.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.5.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.141	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	4
91.200.12.106	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.141	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
94.230.86.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.163.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.40.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.192.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.159.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.191	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
221.202.205.233	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.178.96.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
149.78.32.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.135.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.86.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
46.116.189.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
81.218.106.146	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 81.218.106.146	Block	13
213.57.251.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
37.26.149.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.216	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	6
84.108.66.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
84.109.4.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
89.138.42.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.181.221.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
81.218.106.146	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390	Block	3
79.178.147.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.109.4.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
176.13.0.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.230.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	3
31.154.153.188	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
84.109.4.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.132.37.77	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/main/home/default.aspx	Block	2
77.127.163.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	2
2.52.40.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.6.129	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsunemofet.aspx	None	1
157.55.39.17	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
27.55.202.121	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Malformed URL	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchfText in www.law.idf.il/275-he/patzar.aspx	None	1
109.253.135.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.168.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.240.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.155.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.16.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.93.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.116.79.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
31.154.94.38	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/default.aspx	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.181.100.222	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method ÅÅ(Å\ in URL	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.78.89	None	1
109.253.157.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.53.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
2.54.176.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceholder\$ct138\$ct101\$ct103\$cb1Question\$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
158.69.215.68	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
69.171.231.227	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1